S Commands

same-security-traffic

To permit communication between interfaces with equal security levels, use the **same-security-traffic** command in global configuration mode. To disable the same-security interfaces, use the **no** forms 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 when traffic is IPSec protected.

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**
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Allowing communication between same security interfaces 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.

You can also redirect incoming client VPN traffic back out through the same interface unencrypted as well as encrypted. If you send VPN traffic back out through the same interface unencrypted, you must enable NAT for the interface so that publically routable addresses replace your private ip addresses (unless you already use public ip addresses in your local ip address pool). The following example commands apply an interface PAT rule to traffic sourced from the client ip pool:

```
hostname(config)# ip local pool clientpool 192.168.0.10-192.168.0.100
hostname(config)# global (outside) 1 interface
hostname config)# nat (outside) 1 192.168.0.0 255.255.255.0
```

When the security appliance sends encrypted VPN traffic back out this same interface, however, NAT is optional. To apply NAT to all outgoing traffic, implement only the commands above. To exempt the VPN-to-VPN traffic from NAT, add commands (to the example above) that implement NAT exemption for VPN-to-VPN traffic, such as:

```
hostname(config)# access-list nonat permit ip 192.168.0.0 255.255.255.0 192.168.0.0
255.255.255.0
hostname(config)# nat (outside) 0 access-list nonat
```

See the **nat** command for more information.

Examples

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

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

Related Commands

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

sdi-pre-5-slave

To specify the IP address or name of an optional SDI AAA "slave" server to use for this host connection that uses a version of SDI prior to SDI version 5, use the **sdi-pre-5-slave** command in AAA-server host configuration mode. To remove this specification, use the **no** form of this command:

sdi-pre-5-slave *host*

no sdi-pre-5-slave

Syntax Description

host	Specify the name or IP address of the slave server host.

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
AAA-server Host	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced

Usage Guidelines

This command is available for any host in an SDI AAA servergroup, but it is relevant only if the SDI version for the host is set to sdi-pre-5 in the **sdi-version** command. Prior to using this command, you must have configured the AAA server to use the SDI protocol.

The **sdi-pre-5-slave** command lets you identify an optional secondary server that is to be used if the primary server fails. The address specified by this command must be that of a server that is configured as a "slave" to the primary SDI server. In this situation, if you are using a pre-5 version, you must configure the **sdi-pre-5-slave** command so that the security appliance can access the appropriate SDI configuration record that is downloaded from the server. This is not an issue with version 5 and later versions.

Examples

The following example configures the AAA SDI server group "svrgrp1" that uses an SDI version prior to SDI version 5.

```
hostname(config)# aaa-server svrgrp1 protocol sdi
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.10.10
hostname(config-aaa-server-host)# sdi-version sdi-pre-5
hostname(config-aaa-server-host)# sdi-pre-5-slave 209.165.201.31
hostname(config-aaa-server-host)# exit
hostname(config)#
```

Related Commands

Command	Description
aaa-server host	Enter AAA server host configuration mode so you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Removes all AAA server configurations.
sdi-version	Specifies the version of SDI to use for this host connection.
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.

sdi-version

To specify the version of SDI to use for this host connection, use the **sdi-version** command in AAA-server host configuration mode. To remove this specification, use the **no** form of this command:

sdi-version *version*

no sdi-version

Syntax Description

version	Specify the version of SDI to use.Valid values are: **sdi-5** – SDI version 5.0 (default) **sdi-pre-5** – SDI versions prior to 5.0

Defaults

The default version is **sdi-5**.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced

Usage Guidelines

This command is valid only for SDI AAA servers. If you configure a secondary (failover) SDI AAA server, and if the SDI version for that server is earlier than version 5, you must also specify the **sdi-pre-5-slave** command

Examples

```
hostname(config)# aaa-server svrgrp1 protocol sdi
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 6
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# sdi-version sdi-5
hostname(config-aaa-server)# exit
hostname(config)#
```

Related Commands

Command	Description
aaa-server host	Enter AAA server host configuration mode so you can configure AAA server parameters that are host-specific.

clear configure aaa-server	Remove all AAA configurations.
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

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	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-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

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	•	—	•	—	—

Command History

Release	Modification
7.0	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	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.

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
hostname(ca-trustpoint)#
```

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-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	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
hostname(config-aaa-server-host)# exit
hostname(config)#
```

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) "|" (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.

service

To enable system services, use the **service** command in global configuration mode. To disable system services, use the **no** form of this command.

service {**resetinbound | resetoutbound**} **[interface** *intf***]**

no service {**resetinbound | resetoutbound**}**[interface** *intf***]**

Syntax Description

resetinbound	Sends a reset to a denied inbound TCP packet.
resetoutbound	Sends a reset to a denied TCP packet to the outside interface.
interface	(Optional) Specifies a specific interface.
intf	Name of 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
Preexisting	This command was preexisting.
7.0(5)	This command was modified to include the *interface* keyword.

Usage Guidelines

The **service** command works with all inbound TCP connections to static interfaces whose access lists or uauth (user authorization) do not allow inbound connections. One use is for resetting identity request (IDENT) connections. If an inbound TCP connection is attempted and denied, you can use the **service resetinbound** command to return an RST (reset flag in the TCP header) to the source. Without the keyword, the security appliance drops the packet without returning an RST.

By default a RST is always sent to the inside host when outbound TCP traffic is denied. The keyword **resetoutbound** is used to change this default. For example, if traffic is outbound through the security appliance, and the **no service resetoutbound** command is configured globally or on that interface, we do not send RST.

With the optional **interface** keyword, the TCP reset is sent only when outbound packets are denied on that interface.

The security appliance sends a TCP RST to the host connecting inbound and stops the incoming IDENT process so that outbound e-mail can be transmitted without having to wait for IDENT to time out. The security appliance sends a syslog message stating that the incoming connection was denied. Without

entering the **service resetinbound** command, the security appliance drops packets that are denied and generates a syslog message stating that the SYN was denied. However, outside hosts keep retransmitting the SYN until the IDENT times out.

When an IDENT connection times out, the connections slow down. Perform a trace to determine that IDENT is causing the delay and then enter the **service** command.

Use the **service resetinbound** command to handle an IDENT connection through the security appliance. These methods for handling IDENT connections are ranked from most secure to the least secure:

1. Use the **service resetinbound** command.
2. Use the **established** command with the **permitto tcp 113** keyword.
3. Enter the **static** and **access-list** commands to open TCP port 113.

When using the **aaa** command, if the first attempt at authorization fails and a second attempt causes a timeout, use the **service resetinbound** command to reset the client that failed the authorization so that it will not retransmit any connections. An example authorization timeout message in Telnet is as follows:

```
Unable to connect to remote host: Connection timed out
```

The following is the expected behavior of traffic on the security appliance in regards to the reset flag.

1. If **resetinbound** is configured and if denied traffic flows from a low security interface to high security interface, then a reset is sent.
2. If **resetinbound** is configured and if denied traffic flows from an interface to another interface with the same security, then a reset is sent.
3. If **resetinbound** is not configured and if denied traffic flows from high security interface to low security interface, then a reset is sent.

If you use the **resetoutside** command, the security appliance actively resets denied TCP packets that terminate at the security appliances least-secure interface. By default, these packets are silently discarded. We recommend that you use the **resetoutside** keyword with dynamic or static interface Port Address Translation (PAT). The static interface PAT is available with security appliance version 6.0 and higher. 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.

Examples

The following example shows how to enable system services:

```
hostname/context_name(config)# service resetinbound
```

This example shows how to enable system services on an interface called dmz1:

```
hostname/context_name(config)# service resetinbound interface dmz1
```

Related Commands

Command	Description
show running-config service	Displays the system services.

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	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

To activate a policy map globally on all interfaces or on a targeted interface, use the **service-policy** command in privileged EXEC mode. To disable, use the **no** form of this command. Use the **service-policy** command to enable a set of policies on an interface. In general, a **service-policy** command can be applied to any interface that can be defined by the **nameif** command.

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

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

Syntax Description

policymap_name	A unique alphanumeric policy map identifier.
global	Applies the policy map to all interfaces.
interface	Applies the policy map to a specific interface
intf	The interface name defined in the **nameif** 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
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

If an interface name is specified, the policy-map only applies to the interface. The interface name is defined in the **nameif** command, and an interface policy-map overrides a global policy-map. Only one policy-map is allowed per interface.

Only one global policy is allowed.

Examples

The following example shows the syntax of the **service-policy** command:

```
hostname(config)# service-policy outside_security_map outside
```

Related Commands

Command	Description
show service-policy	Displays the service policy.
show running-config service-policy	Displays the service policies configured in the running configuration.
clear service-policy	Clears service policy statistics.
clear configure service-policy	Clears service policy configurations.

session

To establish a Telnet session to an AIP SSM, use the **session** command in privileged EXEC mode.

session 1

Syntax Description

1	Specifies the 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	This command was introduced.

Usage Guidelines

This command is only available when the AIP 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 values within a policy-map for a traffic class, use the **set connection** command in class mode. Use this command to specify the maximum number of simultaneous connections and to specify whether to enable or disable TCP sequence number randomization. To remove these specifications, thereby allowing unlimited connections, use the **no** form of this command.

set connection {**conn-max** | **embryonic-conn-max**} *n* **random-seq# {enable | disable}**

no set connection {**conn-max** | **embryonic-conn-max**} *n* **random-seq# {enable | disable}**

Syntax Description

conn-max *n*	The maximum number of simultaneous TCP and/or UDP connections that are allowed.
disable	Turns off TCP sequence number randomization.
enable	Turns on TCP sequence number randomization.
embryonic-conn-max *n*	The maximum number of simultaneous embryonic connections allowed.
random-seq#	Enable or disable TCP sequence number randomization. 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.

Defaults

For both the **conn-max** and **embryonic-conn-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:

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You must have configured the **policy-map** command and the **class** command before issuing this command.

Note The **set connection** command parameters (**conn-max**, **embryonic-conn-max**, **random-seq#**) can co-exist with any **nat** or **static** command; that is, you can configure connection parameters either through the **nat/static** commands using **max-conn**, **emb_limit**, or **noramdomseq** parameters, or through the MPC **set connection** command using **conn-max**, **embryonic-conn-max**, or **random-seq#** parameters. A mixed configuration is not recommended, but if one exists, it behaves in the following ways:

When a traffic class is subject to a connection limit or embryonic connection limit from both the MPC **set connection** command and the **nat/static** command, then whichever limit is reached, that limit is applied.

When a TCP traffic class is configured to have sequence number randomization disabled by either the MPC **set connection** command or the **nat/static** command, then sequence number randomization is disabled.

Examples

The following is an example of the use of the set connection command in class mode to 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-seq# disable
hostname(config-pmap-c)# exit
```

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.
help policy-map	Shows syntax help for the policy-map command.

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 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:

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

Command History

Release	Modification
7.0	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
```

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 timeout

To configure the timeout period, after which an idle TCP connection is disconnected, use the **set connection timeout** command in class mode. To remove the timeout, use the **no** form of this command.

set connection timeout tcp *hh*[:*mm*[:*ss*]] [**reset**]

no set connection timeout tcp

set connection timeout embryonic *hh*[:*mm*[:*ss*]]

no set connection timeout embryonic

set connection timeout half-closed *hh*[:*mm*[:*ss*]]

no set connection timeout half-closed

Syntax Description

embryonic *hh*[:*mm*[:*ss*]]	Timeout period after which a TCP embryonic (half-opened) connection is closed.
half-closed *hh*[:*mm*[:*ss*]]	The timeout period until a TCP half-closed connection is freed.
reset	Sends a TCP RST packet to both end systems after TCP idle connections are removed.
tcp *hh*[:*mm*[:*ss*]]	The idle time after which an established connection closes.

Defaults

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

The default **half-closed** connection timeout value is 10 minutes.

The default **tcp** connection timeout value 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	•	•	—	—	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You must have configured the **policy-map** command and the **class** command before issuing this command.

A TCP connection for which a three-way handshake is not complete is an *embryonic* connection. For the **embryonic** connection timeout value, use **0:0:0** to specify that the connection never times out. Otherwise, the timeout duration must be at least 5 seconds.

When the TCP connection is in the closing state, use the half-closed parameter to configure the length of time until the connection is freed. Use **0:0:0** to specify that the connection never times out. The minimum timeout duration is 5 minutes.

The **tcp** inactive connection timeout configures the period after which an idle TCP connection in the established state is disconnected. Use **0:0:0** to specify that the connection never times out. The minimum timeout duration is 5 minutes.

The **reset** keyword is used to send a TCP RST packet to both end systems once an idle TCP connection has timed out. Some applications require a TCP RST after a timeout to perform properly.

Examples

The following is an example of a **set connection timeout** command that specifies an embryonic connection **timeout** of two minutes:

```
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)# 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 timeout embryonic 00:2:00
```

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.

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 7-1. 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 7-1 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 7-1 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.

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	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 specificed 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
Preexisting	This command was preexisting.

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/FAILED. Last transaction (success) at 11:10:08 UTC  Fri Aug 22
Number of pending requests 20
Average round trip time4ms
Number of authentication requests20
```

```
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions1
Number of accepts  16
Number of rejects  4
Number of challenges   5
Number of malformed responses0
Number of bad authenticators0
Number of pending requests0
Number of timeouts 0
Number of unrecognized responses0
hostname(config)#
```

This example shows the use of the **show aaa-server** command to show the statistics for all servers in a small, inactive system:

```
hostname(config)# show aaa-server
Server Group:      LOCAL
Server Protocol:   Local database
Server Address:    None
Server port:       None
Server status:     ACTIVE, Last transaction at unknown
Number of pending requests        0
Average round trip time           0ms
Number of authentication requests 0
Number of authorization requests  0
Number of accounting requests     0
Number of retransmissions         0
Number of accepts                 0
Number of rejects                 0
Number of challenges              0
Number of malformed responses     0
Number of bad authenticators      0
Number of timeouts                0
Number of unrecognized responses  0
hostname(config)#
```

Related Commands

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*

Syntax Description

id	Identifies the access list.

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 access-list** command:

```
hostname# show access-list ac
access-list ac; 2 elements
    access-list ac line 1 permit ip any any (hitcnt=0)
    access-list ac line 2 permit tcp any any (hitcnt=0)
```

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 commands in the configuration for features 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

Syntax Description

This command has no arguments or keywords.

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
PIX Version 7.0	Support for this command was introduced on the security appliance.

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 oldkey, it prompts for confimation. 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.

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

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

The flash activation key is the SAME as the running key.
hostname(config)#
```

Related Commands

Command	Description
activation-key	Changes the activation key.

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	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)	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	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 7-2 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 7-2 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:

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

Command History

Release	Modification
7.0	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|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|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|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|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|
```

```
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|
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|
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|
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|
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|
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|
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|
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|
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
|
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|
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|
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|
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|
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|
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|
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|
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	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	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	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.

show asp drop

To debug the accelerated security path dropped packets or connections, use the **show asp drop** command in privileged EXEC mode.

show asp drop [**flow** [*flow_drop_reason*] | **frame** [*frame_drop_reason*]]

Syntax Description

flow [*flow_drop_reason*]	(Optional) Shows the dropped flows (connections). You can specify a particular reason by using the *flow_drop_reason* argument. Valid values for the *flow_drop_reason* argument are listed in the "Usage Guidelines" section, below.
frame [*frame_drop_reason*]	(Optional) Shows the dropped packets. You can specify a particular reason by using the *frame_drop_reason* argument. Valid values for the *frame_drop_reason* argument are listed in the "Usage Guidelines" section, below.

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.
7.0(8)	Added a timestamp indicating when the counters were last cleared (see the **clear asp drop** command). It also displays the drop reason keywords next to the description, so you can easily use the **capture asp-drop** command with that keyword.

Usage Guidelines

The **show asp drop** command shows the packets or connections dropped by the accelerated security path, which might help you troubleshoot a problem. See the *Cisco Security Appliance Command Line Configuration Guide* for more information about the accelerated security path. This information is used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Table 7-3 lists valid values for the *flow_drop_reason* argument for dropped flows. Table 7-4 lists valid values for the *frame_drop_reason* argument for dropped frames.

Table 7-3 Flow Drop Reasons

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
acl-drop	Flow is denied by access rule	This counter is incremented when a packet is denied by the security appliance, and flow creation is denied. The deny rule could be a default rule created when the security appliance comes up, when various features are turned on or off, when an access list is applied to an interface, or any other feature. Apart from default rule drops, a flow could be denied because of: • An access list configured on an interface • An access list configured for AAA, and AAA denied the user • Through traffic arriving at a management-only interface • Unencrypted traffic arriving on a IPSec-enabled interface • Implicit deny at the end of an access list **Recommendation**: Observe if one of system messages related to packet drop display. Flow drop results in the corresponding packet drop that would trigger the requisite system message. **System messages**: None.
audit-failure	Audit failure	A flow was freed after matching an **ip audit** signature that had reset as the associated action. **Recommendation**: If removing the flow is not the desired outcome of matching this signature, then remove the reset action from the **ip audit** command. **System messages**: None.
closed-by-inspection	Flow closed by inspection	This reason is given for closing a flow due to an error detected during application inspection. For example, if an error is detected during inspecting an H323 message, the corresponding H323 flow is closed with this reason. **Recommendation**: None. **System messages**: None.
conn-limit-exceeded	Connection limit exceeded	This reason is given for closing a flow when the connection limit has been exceeded. The connection limit is configured using the **set connection conn-max** command. **Recommendation**: None. **System messages**: 201011

Table 7-3 Flow Drop Reasons (continued)

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
fin-timeout	FIN Timeout	This reason is given for closing a TCP flow due to expiry of half-closed timer. **Recommendation**: If these are valid sessions which take longer to close a TCP flow, increase the half-closed timeout. **System messages**: 302014
flow-reclaimed	Non-tcp/udp flow reclaimed for new request	This counter is incremented when a reclaimable flow is removed to make room for a new flow. This occurs only when the number of flows through the security appliance equals the maximum number permitted by the software imposed limit, and a new flow request is received. When this occurs, if the number of reclaimable flows exceeds the number of VPN tunnels permitted by the security appliance, then the oldest reclaimable flow is removed to make room for the new flow. All flows except the following are deemed to be reclaimable: • TCP, UDP, GRE and failover flows • ICMP flows if ICMP stateful inspection is enabled • ESP flows to the security appliance **Recommendation**: No action is required if this counter is incrementing slowly. If this counter is incrementing rapidly, it could mean that the security appliance is under attack and the security appliance is spending more time reclaiming and rebuilding flows. **System messages**: 302021
fo-primary-closed	Failover primary closed	The standby unit received a flow delete message from the active unit and terminated the flow. **Recommendation**: If the security appliance is running stateful failover, then this counter should increment for every replicated connection that is torn down on the standby appliance. **System messages**: 302014, 302016, 302018
fo-standby	Flow closed by failover standby	If a through-the-box packet arrives at the security appliance or a context that is in a standby state, then a flow is created, the packet is dropped, and the flow removed. This counter will increment each time a flow is removed in this manner. **Recommendation**: This counter should never be incrementing on the active security appliance or context. However, it is normal to see it increment on the standby security appliance or context. **System messages**: 302014, 302016, 302018

Table 7-3 Flow Drop Reasons (continued)

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
fo_rep_err	Standby flow replication error	The standby unit failed to replicate a flow. **Recommendation**: If the security appliance is processing VPN traffic, then this counter could be constantly increasing on the standby unit because the flow could be replicated before the IKE SA information. No action is required in this case. If the appliance is not processing VPN traffic, then this indicates a software detect; turn on the **debug fover fail** command on the standby unit, collect the debug output, and report the problem to Cisco TAC. **System messages**: 302014, 302016, 302018
host-removed	Host is removed	The flow was removed in response to the **clear local-host** command. **Recommendation**: This is an information counter. **System messages**: 302014, 302016, 302018, 302021, 305010, 305012, 609002
inspect-fail	Inspection failure	This counter will increment when the security appliance fails to enable protocol inspection carried out by the NP for the connection. Currently, ICMP and DNS inspections are carried out by the NP. The cause could be memory allocation failure, or for ICMP error message, the security appliance not being able to find any established connection related to the frame embedded in the ICMP error message. **Recommendation**: Check system memory usage. For the ICMP error message, if the cause is an attack, you can deny the host using the access lists. **System messages**: 313005 for ICMP error.
ips-fail-close	IPS fail-close	This reason is given for terminating a flow because the AIP SSM is down and the fail-close option was used with IPS inspection. **Recommendation**: Check and bring up the AIP SSM. **System messages**: 420001
ips-request	Flow terminated by IPS	This reason is given for terminating a flow as requested by the AIP SSM. **Recommendation**: Check system messages and alerts on the AIP SSM. **System messages**: 420002

Table 7-3 Flow Drop Reasons (continued)

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
ipsec-spoof-detect	IPsec spoof packet detected	This counter will increment when the security appliance receives a packet that should have been encrypted but was not. The packet matched the inner header security policy check of a configured and established IPSec connection on the security appliance but was received unencrypted. This is a security issue. **Recommendation**: Analyze your network traffic to determine the source of the spoofed IPSec traffic. **System messages**: 402117
loopback	Flow is a loopback	This reason is given for closing a flow due to the following conditions: • U-turn traffic is present on the flow. • **same-security-traffic permit intra-interface** is not configured. **Recommendation**: To allow U-turn traffic on an interface, configure the interface with the **same-security-traffic permit intra-interface** command. **System messages**: None.
mcast-entry-removed	Multicast entry removed	This reason is given for one of the following cases: • A packet has arrived that matches a multicast flow, but the multicast service is no longer enabled, or was re-enabled after the flow was built. **Recommendation**: Reenable multicast if it is disabled. **System messages**: None. • The multicast entry has been deleted so the flow is being cleaned up, but the packet will be reinjected into the data path. **Recommendation**: None. **System messages**: None.
mcast-intrf-removed	Multicast interface removed	This reason is given for one of the following cases: • An output interface has been removed from the multicast entry. **Recommendation**: None. **System messages**: None. • All output interfaces have been removed from the multicast entry. **Recommendation**: Verify that there are no longer any receivers for this group. **System messages**: None.

Table 7-3 Flow Drop Reasons (continued)

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
nat-failed	NAT failed	Failed to create an xlate to translate an IP or transport header. **Recommendation**: If NAT is not desired, disable **nat-control**. Otherwise, use the **static**, **nat**, or **global** command to configure NAT policy for the dropped flow. For dynamic NAT, ensure that each **nat** command is paired with at least one **global** command. Use **show running-config nat** and **debug pix process** to verify NAT rules. **System messages**: 305005, 305006, 305009, 305010, 305011, 305012
nat-rpf-failed	NAT reverse path failed	Rejected attempt to connect to a mapped host using the mapped host's real address. **Recommendation**: When not on the same interface as the host undergoing NAT, use the mapped address instead of the real address to connect to the host. Also, enable the appropriate **inspect** command if the application embeds the IP address. **System messages**: 305005
need-ike	Need to start IKE negotiation	This counter will increment when the security appliance receives a packet that requires encryption but has no established IPSec security association. This is generally a normal condition for LAN-to-LAN IPSec configurations. This indication will cause the security appliance to begin ISAKMP negotiations with the destination peer. **Recommendation**: If you have configured IPSec LAN-to-LANs on your security appliance, this indication is normal and does not indicate a problem. However, if this counter increments rapidly, it may indicate a **crypto** configuration error or network error preventing the ISAKMP negotiation from completing. Verify that you can communicate with the destination peer and verify your **crypto** configuration using the **show running-config** command. **System messages**: None.
no-ipv6-ipsec	IPsec over IPv6 unsupported	This counter will increment when the security appliance receives an IPSec ESP packet, IPSec NAT-T ESP packet, or an IPSec over UDP ESP packet encapsulated in an IPv6 header. The security appliance does not currently support any IPSec sessions encapsulated in IPv6. **Recommendation**: None. **System messages**: None.

Table 7-3 Flow Drop Reasons (continued)

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
non_tcp_syn	non-syn TCP	This reason is given for terminating a TCP flow when the first packet is not a SYN packet. **Recommendation**: None. **System messages**: None.
out-of-memory	No memory to complete flow	This counter is incremented when the security appliance is unable to create a flow because of insufficient memory. **Recommendation**: Verify that the security appliance is not under attack by checking the current connections. Also verify if the configured timeout values are too large resulting in idle flows residing in memory longer. Check the free memory available by issuing the **show memory** command. If free memory is low, issue the **show processes memory** command to determine which processes are utilizing most of the memory. **System messages**: None.
parent-closed	Parent flow is closed	When the parent flow of a subordinating flow is closed, the subordinating flow is also closed. For example, an FTP data flow (subordinating flow) will be closed with this specific reason when its control flow (parent flow) is terminated. This reason is also given when a secondary flow (pin-hole) is closed by its controlling application. For example, when the BYE messaged is received, the SIP inspection engine (controlling application) will close the corresponding SIP RTP flows (secondary flow). **Recommendation**: None. **System messages**: None.
pinhole-timeout	Pinhole timeout	This counter is incremented to report that the security appliance opened a secondary flow, but no packets passed through this flow within the timeout interval, and hence it was removed. An example of a secondary flow is the FTP data channel that is created after successful negotiation on the FTP control channel. **Recommendation**: None. **System messages**: 302014, 302016
recurse	Close recursive flow	A flow was recursively freed. This reason applies to pair flows and multicast slave flows, and serves to prevent system messages being issued for each of these subordinate flows. **Recommendation**: None. **System messages**: None.

Table 7-3 Flow Drop Reasons (continued)

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
reinject-punt	Flow terminated by punt action	This counter is incremented when a packet is punted to the exception path for processing by one of the enhanced services such as inspection or AAA. The servicing routine, having detected a violation in the traffic flowing on the flow, requests that the flow be dropped. The flow is immediately dropped. **Recommendation**: Please watch for system messages triggered by a servicing routine. Flow drop terminates the corresponding connection. **System messages**: None.
reset-by-ips	Flow reset by IPS	This reason is given for terminating a TCP flow as requested by the AIP SSM. **Recommendation**: Check system messages and alerts on the AIP SSM. **System messages**: 420003
reset-in	TCP Reset-I	This reason is given for closing an outbound flow (from a low-security interface to a same- or high-security interface) when a TCP reset is received on the flow. **Recommendation**: None. **System messages**: 302014
reset-out	TCP Reset-O	This reason is given for closing an inbound flow (from a high-security interface to low-security interface) when a TCP reset is received on the flow. **Recommendation**: None. **System messages**: 302014
shunned	Flow shunned	This counter will increment when a packet is received that has a source IP address that matches a host in the shun database. When a **shun** command is applied, it will be incremented for each existing flow that matches the **shun** command. **Recommendation**: None. **System messages**: 401004
syn-timeout	SYN Timeout	This reason is given for closing a TCP flow due to expiry of embryonic timer. **Recommendation**: If these are valid sessions that take longer to establish a connection, then increase the embryonic timeout. **System messages**: 302014
tcp-fins	TCP FINs	This reason is given for closing a TCP flow when TCP FIN packets are received. **Recommendation**: This counter will increment for each TCP connection that is terminated normally with FINs. **System messages**: 302014

Table 7-3 Flow Drop Reasons (continued)

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
tcp-intercept-no-response	TCP intercept server no respond	SYN retransmission timeout after trying three times, once every second. Server unreachable, tearing down connection. **Recommendation**: Check if the server is reachable from the security appliance. **System messages**: None.
tcp-intercept-kill	Flow terminated by TCP Intercept	TCP intercept tore down the connection for the following reasons: 1. This is the first SYN 2. A connection is created for the SYN 3. TCP intercept replied with a SYN cookie; or TCP intercept sends a SYN to the server and the server replies with a RST after seeing a valid ACK from the client. **Recommendation**: TCP intercept normally does not create a connection for the first SYN, except when there are nailed rules, the packet comes over a VPN tunnel, or the next hop gateway address to reach the client is not resolved. So for the first SYN, this indicates that a connection was created. When TCP intercept receives a RST from server, it is likely that the corresponding port is closed on the server. **System messages**: None.
tcp-intercept-unexpected	TCP intercept unexpected state	Logic error in the TCP intercept module; this should never happen. **Recommendation**: Indicates memory corruption or some other logic error in the TCP intercept module. **System messages**: None.
tcpnorm-invalid-syn	TCP invalid SYN	This reason is given for closing a TCP flow when the SYN packet is invalid. **Recommendation**: The SYN packet could be invalid for a number of reasons, such as an invalid checksum or an invalid TCP header. Please use the packet capture feature to understand why the SYN packet is invalid. If you would like to allow these connections, use the **tcp-map** configuration to bypass checks. **System messages**: 302014
tcpnorm-rexmit-bad	TCP bad retransmission	This reason is given for closing a TCP flow when the **check-retransmission** feature is enabled, and the TCP endpoint sent a retransmission with different data from the original packet. **Recommendation**: The TCP endpoint may be attacking by sending different data in TCP retransmits. Please use the packet capture feature to learn more about the origin of the packet. **System messages**: 302014

Table 7-3 Flow Drop Reasons (continued)

Flow Drop Reason Keyword	Flow Drop Reason Display	Description
tcpnorm-win-variation	TCP unexpected window size variation	This reason is given for closing a TCP flow when the window size advertised by the TCP endpoint is drastically changed without accepting that much data. **Recommendation**: In order to allow this connection, use the **window-variation** command. **System messages**: 302014
timeout	Conn-timeout	This counter is incremented when a flow is closed because of the expiration of its inactivity timer. **Recommendation**: None. **System messages**: 302014, 302016, 302018, 302021
tunnel-pending	Tunnel being brought up or torn down	This counter will increment when the security appliance receives a packet matching an entry in the security policy database (i.e. **crypto map**) but the security association is in the process of being negotiated; its not complete yet. This counter will also increment when the security appliance receives a packet matching an entry in the security policy database but the security association has been or is in the process of being deleted. The difference between this indication and the "'Tunnel has been torn down" indication is that the "Tunnel has been torn down" indication is for established flows. **Recommendation**: This is a normal condition when the IPSec tunnel is in the process of being negotiated or deleted. **System messages**: None.
tunnel-torn-down	Tunnel has been torn down	This counter will increment when the security appliance receives a packet associated with an established flow whose IPSec security association is in the process of being deleted. **Recommendation**: This is a normal condition when the IPSec tunnel is torn down for any reason. **System messages**: None
xlate-removed	Xlate Clear	The flow was removed in response to the **clear xlate** command or **clear local-host** command. **Recommendation**: This is an information counter. **System messages**: 302014, 302016, 302018, 302021, 305010, 305012, 609002

Table 7-4 lists valid values for the *frame_drop_reason* argument for dropped frames.

Table 7-4 Frame Drop Reasons

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
acl-drop	Flow is denied by access rule	This counter is incremented when a packet is denied by the security appliance. The deny rule could be a default rule created when the security appliance comes up, when various features are turned on or off, when an access list is applied to an interface, or any other feature. Apart from default rule drops, a flow could be denied because of: • An access list configured on an interface • An access list configured for AAA, and AAA denied the user • Through traffic arriving at a management-only interface • Unencrypted traffic arriving on a IPSec-enabled interface **Recommendation**: Check the access lists referenced by the following system log messages. **System messages**: 106023, 106100, 106004
bad-crypto	Bad crypto return in packet	This counter will increment when the security appliance attempts to perform a crypto operation on a packet, and the crypto operation fails. This is not a normal condition and could indicate possible software or hardware problems with the security appliance. **Recommendation**: If you are receiving many bad crypto indications, your security appliance may need servicing. You should enable system message 402123 to determine whether the crypto errors are hardware or software errors. You can also check the error counter in the global IPSec statistics with the **show ipsec stats** command. If the IPSec SA that is triggering these errors is known, the SA statistics from the **show ipsec sa detail** command will also be useful in diagnosing the problem. **System messages**: 402123
bad-ipsec-natt	Bad IPSEC NATT packet	This counter will increment when the security appliance receives a packet on an IPSec connection that has negotiated NAT-T, but the packet is not addressed to the NAT-T UDP destination port of 4500 or had an invalid payload length. **Recommendation**: Analyze your network traffic to determine the source of the NAT-T traffic. **System messages**: None.

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
bad-ipsec-prot	IPSEC not AH or ESP	This counter will increment when the security appliance receives a packet on an IPSec connection that is not an AH or ESP protocol packet. This is not a normal condition. **Recommendation**: If you are receiving many IPSec not AH or ESP indications on your security appliance, analyze your network traffic to determine the source of the traffic. **System messages**: 402115
bad-ipsec-udp	Bad IPSEC UDP packet	This counter will increment when the security appliance receives a packet on an IPSec connection that has negotiated IPSec over UDP, but the packet has an invalid payload length. **Recommendation**: Analyze your network traffic to determine the source of the NAT-T traffic. **System messages**: None.
bad-tcp-cksum	Bad TCP checksum	This counter is incremented and the packet is dropped when the security appliance receives a TCP packet whose computed TCP checksum does not match the recorded checksum in TCP header. **Recommendation**: The packet corruption may be caused by a bad cable or noise on the line. It may also be that a TCP endpoint is sending corrupted packets, and an attack is in progress. Please use the packet capture feature to learn more about the origin of the packet. To allow packets with an incorrect TCP checksum, disable the **checksum-verification** feature. **System messages**: None
bad-tcp-flags	Bad TCP flags	This counter is incremented and the packet is dropped when the security appliance receives a TCP packet with invalid TCP flags in the TCP header. For example, a packet with both SYN and FIN TCP flags set will be dropped. **Recommendation**: The packet corruption may be caused by a bad cable or noise on the line. It may also be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please use the packet capture feature to learn more about the origin of the packet. **System messages**: None.

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
conn-limit	Connection limit reached	This reason is given for dropping a packet when the connection limit or host connection limit has been exceeded. If this is a TCP packet which is dropped during TCP connection establishment phase due to connection limit, the drop reason "TCP connection limit reached" is also reported. **Recommendation**: If this is incrementing rapidly, check the system messages to determine which host's connection limit is reached. The connection limit may need to be increased if the traffic is normal, or the host may be under attack. **System messages**: 201011
ctm-error	CTM returned error	This counter will increment when the security appliance attempts to perform a crypto operation on a packet and the crypto operation fails. This is not a normal condition and could indicate possible software or hardware problems with the security appliance. **Recommendation**: If you are receiving many bad crypto indications, your security appliance may need servicing. You should enable system message 402123 to determine whether the crypto errors are hardware or software errors. You can also check the error counter in the global IPSec statistics with the **show ipsec stats** command. If the IPSec SA that is triggering these errors is known, the SA statistics from the **show ipsec sa detail** command will also be useful in diagnosing the problem. **System messages**: 402123
dns-guard-id-not-matched	DNS Guard id not matched	This counter will increment when the identification of the DNS response message does not match any DNS queries that passed across the appliance earlier on the same connection. This counter will increment by the DNS Guard function. **Recommendation**: No action required if it is an intermittent event. If the cause is an attack, you can deny the host using the access lists. **System messages**: None.
dns-guard-out-of-app-id	DNS Guard out of app id	This counter will increment when the DNS Guard function fails to allocate a data structure to store the identification of the DNS message. **Recommendation**: Check the system memory usage. This event normally happens when the system runs short of memory. **System messages**: None.

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
dst-l2_lookup-fail	Dst MAC L2 Lookup Failed	This counter will increment when the security appliance is configured for transparent mode, and the security appliance does a Layer 2 destination MAC address lookup that fails. Upon the lookup failure, the security appliance will begin the destination MAC discovery process and attempt to find the location of the host via ARP and/or ICMP messages. **Recommendation**: This is a normal condition when the security appliance is configured for transparent mode. You can also execute the **show mac-address-table** command to list the L2 MAC address locations currently discovered by the security appliance. **System messages**: None.
flow-expired	Expired flow	This counter is incremented when the security appliance tries to inject a new or cached packet belonging to a flow that has already expired. It is also incremented when the security appliance attempts to send an RST on a TCP flow that has already expired, or when a packet returns from the AIP SSM but the flow had already expired. The packet is dropped. **Recommendation**: If valid applications are getting preempted, investigate if a longer timeout is needed. **System messages**: None.
fo-standby	Dropped by standby unit	If a through-the-box packet arrives at security appliance or context in a standby state, and a flow is created, then the packet is dropped and the flow removed. This counter will increment each time a packet is dropped in this manner. **Recommendation**: This counter should never be incrementing on the active security appliance or context. However, it is normal to see it increment on the standby appliance or security appliance. **System messages**: 302014, 302016, 302018
fragment-reassembly-failed	Fragment reassembly failed	This counter is incremented when the security appliance fails to reassemble a chain of fragmented packets into a single packet. All the fragment packets in the chain are dropped. This is probably because of a failure while allocating memory for the reassembled packet. **Recommendation**: Use the **show blocks** command to monitor the current block memory. **System messages**: None.

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
host-move-pkt	FP host move packet	This counter will increment when the security appliance or context is configured for transparent mode, and the source interface of a known Layer 2 MAC address is detected on a different interface. **Recommendation**: This indicates that a host has been moved from one interface (i.e. LAN segment) to another. This condition is normal while in transparent mode if the host has in fact been moved. However, if the host move toggles back and forth between interfaces, a network loop may be present. **System messages**: 412001, 412002, 322001
ifc-classify	Virtual firewall classification failed	A packet arrived on a shared interface, but failed to classify to any specific context interface. **Recommendation**: Use the **global** or **static** command to specify the IPv4 addresses that belong to each context interface. **System messages**: None.
inspect-dns-id-not-matched	DNS Inspect id not matched	This counter will increment when the identification of the DNS response message does not match any DNS queries that passed across the security appliance earlier on the same connection. **Recommendation**: No action required if it is an intermittent event. If the cause is an attack, you can deny the host using the access lists. **System messages**: None.
inspect-dns-invalid-domain-label	DNS Inspect invalid domain label	This counter will increment when the security appliance detects an invalid DNS domain name or label. DNS domain name and label is checked per RFC 1035. **Recommendation**: None. **System messages**: None.
inspect-dns-invalid-pak	DNS Inspect invalid packet	This counter will increment when the security appliance detects an invalid DNS packet. For example, a DNS packet with no DNS header, the number of DNS resource records not matching the counter in the header, etc. **Recommendation**: None. **System messages**: None.
inspect-dns-out-of-app-id	DNS Inspect out of app id	This counter will increment when the DNS inspection engine fails to allocate a data structure to store the identification of the DNS message. **Recommendation**: Check the system memory usage. This event normally happens when the system runs short of memory. **System messages**: None.

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
inspect-dns-pak-too-long	DNS Inspect packet too long	This counter is incremented when the length of the DNS message exceeds the configured maximum allowed value. **Recommendation**: No action required. If DNS message length checking is not desired, enable DNS inspection without the **inspect dns maximum-length** option. **System messages**: 410001
inspect-icmp-error-different-embedded-conn	ICMP Error Inspect different embedded conn	This counter will increment when the frame embedded in the ICMP error message does not match the established connection that has been identified when the ICMP connection is created. **Recommendation**: No action required if it is an intermittent event. If the cause is an attack, you can deny the host using the access lists. **System messages**: 313005
inspect-icmp-error-no-existing-conn	ICMP Error Inspect no existing conn	This counter will increment when the security appliance is not able to find any established connection related to the frame embedded in the ICMP error message. **Recommendation**: No action required if it is an intermittent event. If the cause is an attack, you can deny the host using the access lists. **System messages**: 313005
inspect-icmp-out-of-app-id	ICMP Inspect out of app id	This counter will increment when the ICMP inspection engine fails to allocate an App ID data structure. The structure is used to store the sequence number of the ICMP packet. **Recommendation**: Check the system memory usage. This event normally happens when the system runs short of memory. **System messages**: None.
inspect-icmp-seq-num-not-matched	ICMP Inspect seq num not matched	This counter will increment when the sequence number in the ICMP echo reply message does not match any ICMP echo message that passed across the security appliance earlier on the same connection. **Recommendation**: No action required if it is an intermittent event. If the cause is an attack, you can deny the host using the access lists. **System messages**: 313004

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
inspect-icmpv6-error-invalid-pak	ICMPv6 Error Inspect invalid packet	This counter will increment when the security appliance detects an invalid frame embedded in the ICMPv6 packet. This check is the same as that on IPv6 packets. For example, an incomplete IPv6 header, a malformed IPv6 Next Header, etc. **Recommendation**: None. **System messages**: None.
inspect-icmpv6-error-no-existing-conn	ICMPv6 Error Inspect no existing conn	This counter will increment when the security appliance is not able to find any established connection related to the frame embedded in the ICMPv6 error message. **Recommendation**: No action required if it is an intermittent event. If the cause is an attack, you can deny the host using the access lists. **System messages**: 313005
intercept-unexpected	Intercept unexpected packet	The security appliance either received data from a client while waiting for a SYNACK from a server, or it received a packet that cannot be handled in a particular state of TCP intercept. **Recommendation**: If this drop is causing the connection to fail, please have a sniffer trace of the client- and server-side of the connection while reporting the issue. The security appliance could be under attack, and the sniffer traces or capture would help narrow down the culprit. **System messages**: None.
interface-down	Interface is down	This counter will increment for each packet received on an interface that is shutdown using the **shutdown** command. For ingress traffic, the packet is dropped after security context classification and if the interface associated with the context is shut down. For egress traffic, the packet is dropped when the egress interface is shut down. **Recommendation**: None. **System messages**: None.
invalid-app-length	Invalid app length	This counter will increment when the security appliance detects an invalid length of the Layer 7 payload in the packet. Currently, it counts the drops by the DNS Guard function only. For example, an incomplete DNS header. **Recommendation**: None. **System messages**: None.

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
invalid-encap	Invalid encapsulation	This counter is incremented when the security appliance receives a frame belonging to an unsupported link-level protocol or if the L3 type specified in the frame is not supported by the security appliance. The packet is dropped. **Recommendation**: Verify that directly-connected hosts have proper link-level protocol settings. **System messages**: None.
invalid-ethertype	Invalid ethertype	This counter is incremented when the fragmentation module on the security appliance receives or tries to send a fragmented packet that does not belong to IP version 4 or version 6. The packet is dropped. **Recommendation**: Verify the MTU of the security appliance and other devices on the connected network to determine why the security appliance is processing such fragments. **System messages**: None.
invalid-ip-header	Invalid IP header	This counter is incremented and the packet is dropped when the security appliance receives an IP packet whose computed checksum of the IP header does not match the recorded checksum in the header. **Recommendation**: The packet corruption may be caused by a bad cable or noise on the line. It may also be that a peer is sending corrupted packets and an attack is in progress. Please use the packet capture feature to learn more about the origin of the packet. **System messages**: None
invalid-ip-length	Invalid IP length	This counter is incremented when the security appliance receives an IPv4 or IPv6 packet in which the header length or total length fields in the IP header are not valid or do not conform to the received packet length. **Recommendation**: None. **System messages**: None.
invalid-ip-option	IP option configured drop	This counter is incremented when any unicast packet with IP options or a multicast packet with IP options that have not been configured to be accepted, is received by the security appliance. The packet is dropped. **Recommendation**: Investigate why a packet with IP options is being sent by the sender. **System messages**: None.

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
invalid-tcp-hdr-length	Invalid tcp length	This counter is incremented when the security appliance receives a TCP packet whose size is smaller than the minimum-allowed header length or does not conform to the received packet length. **Recommendation**: The invalid packet could be a bogus packet being sent by an attacker. Investigate the traffic from the source in the following system message. **System messages**: 500003.
invalid-udp-length	Invalid udp length	This counter is incremented when the security appliance receives a UDP packet whose size as calculated from the fields in the header is different from the measured size of the packet as received from the network. **Recommendation**: The invalid packet could be a bogus packet being sent by an attacker. **System messages**: None.
ips-fail-close	IPS card is down	This counter is incremented and the packet is dropped when the AIP SSM is down and the **fail-close** option was used in IPS inspection. **Recommendation**: Check and bring up the AIP SSM. **System messages**: 420001
ips-request	IPS Module requested drop	This counter is incremented and the packet is dropped as requested by the AIP SSM when the packet matches a signature on the IPS engine. **Recommendation**: Check system messages and alerts on the AIP SSM. **System messages**: 420002
ipsec-clearpkt-notun	IPSEC Clear Pkt w/no tunnel	This counter will increment when the security appliance receives a packet that should have been encrypted but was not. The packet matched the inner header security policy check of a configured and established IPSec connection on the security appliance but was received unencrypted. This is a security issue. **Recommendation**: Analyze your network traffic to determine the source of the spoofed IPSec traffic. **System messages**: 402117
ipsec-ipv6	IPSEC via IPV6	This counter will increment when the security appliance receives an IPSec ESP packet, IPSec NAT-T ESP packet, or an IPSec over UDP ESP packet encapsulated in an IPv6 header. The security appliance does not currently support any IPSec sessions encapsulated in IPv6. **Recommendation**: None. **System messages**: None.

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
ipsec-need-sa	IPSEC SA Not negotiated yet	This counter will increment when the security appliance receives a packet that requires encryption but has no established IPSec security association. This is generally a normal condition for LAN-to-LAN IPSec configurations. This indication will cause the security appliance to begin ISAKMP negotiations with the destination peer. **Recommendation**: If you have configured IPSec LAN-to-LAN on your security appliance, this indication is normal and does not indicate a problem. However, if this counter increments rapidly it may indicate a **crypto** configuration error or network error preventing the ISAKMP negotiation from completing. Verify that you can communicate with the destination peer and verify your **crypto** configuration using the **show running-config** command. **System messages**: None.
ipsec-spoof	IPSEC Spoof detected	This counter will increment when the security appliance receives a packet which should have been encrypted but was not. The packet matched the inner header security policy check of a configured and established IPSec connection on the security appliance but was received unencrypted. This is a security issue. **Recommendation**: Analyze your network traffic to determine the source of the spoofed IPSec traffic. **System messages**: 402117
ipsec-tun-down	IPSEC tunnel is down	This counter will increment when the security appliance receives a packet associated with an IPSec connection which is in the process of being deleted. **Recommendation**: This is a normal condition when the IPSec tunnel is torn down for any reason. **System messages**: None.

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
ipsecudp-keepalive	IPSEC/UDP keepalive message	This counter will increment when the security appliance receives an IPSec over UDP keepalive message. IPSec over UDP keepalive messages are sent from the IPSec peer to the security appliance to keep NAT/PAT flow information current in network devices between the IPSec over UDP peer and the security appliance. **Note** These are not industry-standard NAT-T keepalive messages that are also carried over UDP and addressed to UDP port 4500. **Recommendation**: If you have configured IPSec over UDP on your security appliance, this indication is normal and does not indicate a problem. If IPSec over UDP is not configured on your security appliance, analyze your network traffic to determine the source of the IPSec over UDP traffic. **System messages**: None.
ipv6_sp-security-failed	IPv6 slowpath security checks failed	This counter is incremented and the packet is dropped for one of the following reasons: • An IPv6 through-the-box packet has the identical source and destination address. • An IPv6 through-the-box packet has a linklocal source or destination address. • An IPv6 through-the-box packet has a multicast destination address. **Recommendation**: These packets could indicate malicious activity, or could be the result of a misconfigured IPv6 host. Use the packet capture feature to capture type asp packets, and use the source MAC address to identify the source. **System messages**: For identical source and destination address, system message 106016.

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
l2_acl	FP L2 rule drop	This counter increments when the security appliance denies a packet due to an EtherType access list. The transparent mode security appliance permits the following traffic by default: • IPv4 traffic is allowed through the transparent firewall automatically from a higher security interface to a lower security interface, without an access list. **Note** For Layer 3 traffic travelling from a low to a high security interface, an extended access list is required on the low security interface. • ARPs are allowed through the transparent firewall in both directions without an access list. ARP traffic can be controlled by ARP inspection. In routed mode, some types of traffic cannot pass through the security appliance even if you allow it in an access list. The transparent firewall, however, can allow almost any traffic through using either an extended access list (for IP traffic) or an EtherType access list (for non-IP traffic). **Note** The transparent mode security appliance does not pass CDP packets or IPv6 packets, or any packets that do not have a valid EtherType greater than or equal to 0x600. For example, you cannot pass IS-IS packets. An exception is made for BPDUs, which are supported. Packets permitted by EtherType access lists might still be dropped by an extended access list. The EtherType access list only supports EtherTypes and not Layer 2 destination MAC addresses. The following destination MAC addresses are allowed through the transparent firewall. Any MAC address not on this list is dropped. • TRUE broadcast destination MAC address equal to FFFF.FFFF.FFFF • IPv4 multicast MAC addresses from 0100.5E00.0000 to 0100.5EFE.FFFF • BPDU multicast address equal to 0100.0CCC.CCCD • Appletalk multicast MAC addresses from 0900.0700.0000 to 0900.07FF.FFFF **Recommendation**: If your non-IP packets are dropped by the security appliance, you can configure an EtherType access list to permit the Layer 2 traffic. **System log messages**: 106026, 106027

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
l2_same-lan-port	L2 Src/Dst same LAN port	This counter will increment when the security appliance or context is configured for transparent mode, and the security appliance determines that the destination interface's L2 MAC address is the same as its ingress interface. **Recommendation**: This is a normal condition when the security appliance or context is configured for transparent mode. Since the security appliance interface is operating in promiscuous mode, the security appliance or context receives all packets on the local LAN segment. **System messages**: None.
loopback-buffer-full	Loopback buffer full	This counter is incremented and the packet is dropped when packets are sent from one context of the security appliance to another context through a shared interface, and there is no buffer space in the loopback queue. **Recommendation**: Check the system CPU to make sure it is not overloaded. **System messages**: None.
lu-invalid-pkt	Invalid LU packet	The standby unit received a corrupted Logical Update packet. **Recommendation**: The packet corruption could be caused by a bad cable, interface card, line noise, or software defect. If the interface appears to be functioning properly, then report the problem to Cisco TAC. **System messages**: None.
natt-keepalive	NAT-T keepalive message	This counter will increment when the security appliance receives an IPSec NAT-T keepalive message. NAT-T keepalive messages are sent from the IPSec peer to the security appliance to keep NAT/PAT flow information current in network devices between the NAT-T IPSec peer and the security appliance. **Recommendation**: If you have configured IPSec NAT-T on your security appliance, this indication is normal and does not indicate a problem. If NAT-T is not configured on your security appliance, analyze your network traffic to determine the source of the NAT-T traffic. **System messages**: None
no-adjacency	No valid adjacency	This counter is incremented when the security appliance has tried to obtain an adjacency and could not obtain the MAC address for the next hop. The packet is dropped. **Recommendation**: Configure a capture for this drop reason and check if a host with the specified destination address exists on the connected network or is routable from the security appliance. **System messages**: None.

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
no-mcast-entry	FP no mcast entry	This counter increments because of one of the following reasons: • A packet has arrived that matches a multicast flow, but the multicast service is no longer enabled, or was re-enabled after the flow was built. **Recommendation**: Reenable multicast if it is disabled. **System messages**: None. • A multicast entry change has been detected after a packet was punted to the CP, and the NP can no longer forward the packet since no entry is present. **Recommendation**: None. **System messages**: None.
no-mcast-intrf	FP no mcast output intrf	This counter increments because of one of the following reasons: • All output interfaces have been removed from the multicast entry. **Recommendation**: Verify that there are no longer any receivers for this group. **System messages**: None. • The multicast packet could not be forwarded. **Recommendation**: Verify that a flow exists for this packet. **System messages**: None.
no-route	No route to host	This counter is incremented when the security appliance tries to send a packet out of an interface and does not find a route for it in the routing table. **Recommendation**: Verify that a route exists for the destination address obtained from the generated system message. **System messages**: 110001
non-ip-pkt-in-routed-mode	Non-IP packet received in routed mode	This counter will increment when the security appliance receives a packet that is not an IPv4, IPv6, or ARP packet, and the security appliance or context is configured for routed mode. In normal operation such packets should be dropped. **Recommendation**: This indicates that a software error should be reported to the Cisco TAC. **System messages**: 106026, 106027

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
np-sp-invalid-spi	Invalid SPI	This counter increments when the security appliance receives an IPSec ESP packet addressed to the security appliance that specifies an SPI (security parameter index) not currently known by the security appliance. **Recommendation**: Occasional invalid SPI indications are common, especially during rekey processing. Many invalid SPI indications may suggest a problem or DoS attack. If you are experiencing a high rate of invalid SPI indications, analyze your network traffic to determine the source of the ESP traffic. **System messages**: 402114
punt-rate-limit	Punt rate limit exceeded	This counter will increment when the security appliance attempts to forward a Layer 2 packet to a rate-limited control point service routine, and the rate limit (per/second) is now being exceeded. Currently, the only Layer 2 packets destined for a control point service routine that are rate limited are ARP packets. The ARP packet rate limit is 500 ARPs per second per interface. **Recommendation**: Analyze your network traffic to determine the reason behind the high rate of ARP packets. **System messages**: 322002, 322003
queue-removed	Queued packet dropped	When the QoS configuration is changed or removed, the existing packets in the output queues awaiting transmission are dropped and this counter is incremented. **Recommendation**: Under normal conditions, this may be seen when the QoS configuration has been changed by the user. If this occurs when no changes to the QoS configuration were performed, please contact Cisco TAC. **System messages**: None.
rate-exceeded	QoS rate exceeded	This counter is incremented when rate-limiting (policing) is configured on an egress interface, and the egress traffic rate exceeds the burst rate configured. The counter is incremented fo each packet dropped. **Recommendation**: Investigate and determine why the rate of traffic leaving the interface is higher than the configured rate. This may be normal, or could be an indication of virus or attempted attack. **System messages**: None.

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
rpf-violated	Reverse-path verify failed	This counter is incremented when **ip verify reverse-path** is configured on an interface and the security appliance receives a packet for which the route lookup of the source IP did not yield the same interface as the one on which the packet was received. **Recommendation**: Trace the source of traffic based on the source IP printed in the system message below, and investigate why it is sending spoofed traffic. **System messages**: 106021
security-failed	Early security checks failed	This counter is incremented and the packet is dropped when the security appliance: • Receives an IPv4 multicast packet when the packet multicast MAC address does not match the packet multicast destination IP address • Receives an IPv6 or IPv4 teardrop fragment containing either small offset or fragment overlapping • Receives an IPv4 packet that matches an IP audit signature **Recommendation**: Contact the remote peer administrator or escalate this issue according to your security policy. For detailed description and system messages for IP audit attack checks please refer the **ip audit signature** command. **System messages**: 106020, 400xx in case of IP audit checks
send-ctm-error	Send to CTM returned error	This counter is obsolete in the security appliance and should never increment. **Recommendation**: None. **System messages**: None.

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
sp-security-failed	Slowpath security checks failed	This counter is incremented and the packet is dropped when the security appliance: • Is in routed mode and receives a through-the-box: – L2 broadcast packet – IPv4 packet with destination IP address equal to 0.0.0.0 – IPv4 packet with source IP address equal to 0.0.0.0 **Recommendation**: Determine if an external user is trying to compromise the protected network. Check for misconfigured clients. **System messages**: 106016 • Is in routed or transparent mode and receives a through-the-box IPv4 packet with: – The first octet of the source IP address is equal to zero – The source IP address is equal to the loopback IP address – Network part of the source IP address is equal to all 0s – The network part of the source IP address is equal to all 1s – The source IP address host part is equal to all 0s or all 1s **Recommendation**: Determine if an external user is trying to compromise the protected network. Check for misconfigured clients. **System messages**: 106016 • In routed or transparent mode and receives an IPv4 or IPv6 packet with the same source and destination IP addresses **Recommendation**: If this message counter is incrementing rapidly, an attack may be in progress. Use the packet capture feature to capture type asp packets, and check the source MAC address in the packet to see where they are coming from. **System messages**: 106017

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
tcp-3whs-failed	TCP failed 3 way handshake	This counter is incremented and the packet is dropped when security appliance receives an invalid TCP packet during the three-way handshake. For example, the SYN-ACK from a client will be dropped for this reason. **Recommendation**: None. **System messages**: None.
tcp-ack-syn-diff	TCP ACK in SYNACK invalid	This counter is incremented and the packet is dropped when the security appliance receives a SYN-ACK packet during the three-way handshake with an incorrect TCP acknowledgement number. **Recommendation**: None. **System messages**: None.
tcp-acked	TCP DUP and has been ACKed	This counter is incremented and the packet is dropped when the security appliance receives a retransmitted data packet and the data has been acknowledged by the peer TCP endpoint. **Recommendation**: None. **System messages**: None.
tcp-bad-option-len	Bad option length in TCP	This counter is incremented and the packet is dropped when the security appliance receives a TCP packet with a TCP option set, but the option length does not match the length defined for that option in the TCP RFC. **Recommendation**: The packet corruption may be caused by a bad cable or noise on the line. It may also be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please use the packet capture feature to learn more about the origin of the packet. **System messages**: None.
tcp-bad-option-list	TCP option list invalid	This counter is incremented and the packet is dropped when the security appliance receives a TCP packet with a non-standard TCP header option. **Recommendation**: To allow such TCP packets or clear non-standard TCP header options and then allow the packet, use the **tcp-options** command. **System messages**: None.

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
tcp-bad-sack-allow	Bad TCP SACK ALLOW option	This counter is incremented and the packet is dropped when the appliance receives a TCP packet with the selective acknowledgement option, but the SYN flag is not set. **Recommendation**: The packet corruption may be caused by a bad cable or noise on the line. It may also be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please use the packet capture feature to learn more about the origin of the packet. **System messages**: None.
tcp-bad-winscale	Bad TCP window scale value	This counter is incremented and the packet is dropped when the security appliance receives a TCP packet with the window-scale option greater than 14. **Recommendation**: The packet corruption may be caused by a bad cable or noise on the line. It may also be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please use the packet capture feature to learn more about the origin of the packet. **System messages**: None.
tcp-buffer-full	TCP packet buffer full	This counter is incremented and the packet is dropped when the security appliance receives an out-of-order TCP packet on a connection, and there is no buffer space to store this packet. Typically TCP packets are put into order on connections that are inspected by the security appliance or when packets are sent to an SSM for inspection. There is a default queue size, and when packets in excess of this default queue size are received they will be dropped. **Recommendation**: On ASA platforms the queue size could be increased using the **queue-size** command. **System messages**: None.
tcp-conn-limit	TCP Connection limit reached	This reason is given for dropping a TCP packet during the TCP connection establishment phase when the connection limit has been exceeded. The connection limit is configured using the **set connection conn-max** command. **Recommendation**: If this is incrementing rapidly, check the system messages to determine which host's connection limit is reached. The connection limit may need to be increased if the traffic is normal, or the host may be under attack. **System messages**: 201011
tcp-data-past-fin	TCP data send after FIN	This counter is incremented and the packet is dropped when the security appliance receives new a TCP data packet from an endpoint which had sent a FIN to close the connection. **Recommendation**: None. **System messages**: None.

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
tcp-discarded-ooo	TCP ACK in 3 way handshake invalid	This counter is incremented and the packet is dropped when the security appliance receives a TCP ACK packet from a client during the three-way-handshake and the sequence number is not the next expected sequence number. **Recommendation**: None. **System messages**: None.
tcp-dual-open	TCP Dual open denied	This counter is incremented and the packet is dropped when the security appliance receives a TCP SYN packet from the server and an embryonic TCP connection is already open. **Recommendation**: None. **System messages**: None.
tcp-fo-drop	TCP replicated flow pak drop	This counter is incremented and the packet is dropped when the security appliance receives a TCP packet with a control flag like SYN, FIN, or RST on an established connection just after the security appliance has taken over as active unit. **Recommendation**: None. **System messages**: None.
tcp-invalid-ack	TCP invalid ACK	This counter is incremented and the packet is dropped when the security appliance receives a TCP packet with an acknowledgement number greater than the data sent by the peer TCP endpoint. **Recommendation**: None. **System messages**: None.
tcp-mss-exceeded	TCP data exceeded MSS	This counter is incremented and the packet is dropped when the security appliance receives a TCP packet with a data length greater than the MSS advertized by the peer TCP endpoint. **Recommendation**: To allow such TCP packets, use the **exceed-mss** command. **System messages**: 4419001
tcp-not-syn	First TCP packet not SYN	The security appliance received a non-SYN packet as the first packet of a non-intercepted and non-nailed connection. **Recommendation**: Under normal conditions, this may be seen when the security appliance has already closed a connection, and the client or server still believe the connection is open, and continue to transmit data. Some examples where this may occur is just after a **clear local-host** or **clear xlate** command is issued. Also, if connections have not been recently removed, and the counter is incrementing rapidly, the security appliance may be under attack. Capture a sniffer trace to help isolate the cause. **System messages**: 6106015

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
tcp-paws-fail	TCP packet failed PAWS test	This counter is incremented and the packet is dropped when a TCP packet with a timestamp header option fails the PAWS (Protect Against Wrapped Sequences) test. **Recommendation**: To allow such connections to proceed, use the **tcp-options** command to clear the timestamp option. **System messages**: None.
tcp-reserved-set	TCP reserved flags set	This counter is incremented and the packet is dropped when the security appliance receives a TCP packet with reserved flags set in TCP header. **Recommendation**: The packet corruption may be caused by a bad cable or noise on the line. It may also be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please use the packet capture feature to learn more about the origin of the packet. To allow such TCP packets or clear reserved flags and then pass the packet, use the **reserved-bits** command. **System messages**: None
tcp-rst-syn-in-win	TCP RST/SYN in window	This counter is incremented and the packet is dropped when the security appliance receives a TCP SYN or TCP RST packet on an established connection with a sequence number within the window, but not as the next expected sequence number. **Recommendation**: None. **System messages**: None.
tcp-rstfin-ooo	TCP RST/FIN out of order	This counter is incremented and the packet is dropped when the security appliance receives a RST or a FIN packet with the incorrect TCP sequence number. **Recommendation**: None. **System messages**: None.
tcp-seq-past-win	TCP packet SEQ past window	This counter is incremented and the packet is dropped when the security appliance receives a TCP data packet with a sequence number beyond the window allowed by the peer TCP endpoint. **Recommendation**: None. **System messages**: None.
tcp-seq-syn-diff	TCP SEQ in SYN/SYNACK invalid	This counter is incremented and the packet is dropped when the security appliance receives a SYN or SYN-ACK packet during the three-way handshake with an incorrect TCP sequence number. **Recommendation**: None. **System messages**: None.

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
tcp-syn-data	TCP SYN with data	This counter is incremented and the packet is dropped when the security appliance receives a TCP SYN packet with data. **Recommendation**: To allow such TCP packets use the **syn-data** command. **System messages**: None.
tcp-syn-ooo	TCP SYN on established conn	This counter is incremented and the packet is dropped when the security appliance receives a TCP SYN packet on an established TCP connection. **Recommendation**: None. **System messages**: None.
tcp-synack-data	TCP SYNACK with data	This counter is incremented and the packet is dropped when the security appliance receives a TCP SYN-ACK packet with data. **Recommendation**: The packet corruption may be caused by a bad cable or noise on the line. It may also be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please use the packet capture feature to learn more about the origin of the packet. **System messages**: None.
tcp-synack-ooo	TCP SYNACK on established conn	This counter is incremented and the packet is dropped when the security appliance receives a TCP SYN-ACK packet on an established TCP connection. **Recommendation**: None. **System messages**: None.
tcp-winscale-no-syn	TCP Window scale on non-SYN	This counter is incremented and the packet is dropped when the security appliance receives a TCP packet with the window-scale TCP option without SYN flag set. **Recommendation**: The packet corruption may be caused by a bad cable or noise on the line. It may also be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please use the packet capture feature to learn more about the origin of the packet. **System messages**: None.
tcp_xmit_partial	TCP retransmission partial	This counter is incremented and the packet is dropped when the **check-retransmission** feature is enabled, and a partial TCP retransmission was received. **Recommendation**: None. **System messages**: None.

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
tcpnorm-rexmit-bad	TCP bad retransmission	This counter is incremented and the packet is dropped when the **check-retransmission** feature is enabled, and a TCP retransmission with different data from the original packet was received. **Recommendation**: None. **System messages**: None.
tcpnorm-win-variation	TCP unexpected window size variation	This counter is incremented and the packet is dropped when the window size advertised by the TCP endpoint is drastically changed without accepting that much data. **Recommendation**: To allow such packet, use the **window-variation** command. **System messages**: None.
tfw-no-mgmt-ip-config	No management IP address configured for TFW	This counter is incremented when the security appliance receives an IP packet in transparent mode and has no management IP address defined. The packet is dropped. **Recommendation**: Configure the security appliance with a management IP address and mask values. **System messages**: 322004
unable-to-add-flow	Flow hash full	This counter is incremented when a newly created flow is inserted into the flow hash table, and the insertion failed because the hash table was full. The flow and the packet are dropped. This is different from the counter that increments when the maximum connection limit is reached. **Recommendation**: This message signifies a lack of resources on the security appliance to support an operation that should have been successful. Please check if the connections in the **show conn** output have exceeded their configured idle timeout values. If so, contact Cisco TAC. **System messages**: None.

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
unable-to-create-flow	Flow denied due to resource limitation	This counter is incremented and the packet is dropped when flow creation fails due to a system resource limitation. The resource limit may be either: • System memory • Packet block extension memory • System connection limit The first two causes occur simultaneously with flow drop reason "No memory to complete flow." **Recommendation**: • Observe if free system memory is low. • Observe if flow drop reason "No memory to complete flow" occurs. • Observe if the connection count reaches the system connection limit using the **show resource usage** command. **System messages**: None.
unexpected-packet	Unexpected packet	This counter is incremented when the security appliance in transparent mode receives a non-IP packet destined to its MAC address, but there is no corresponding service running on the security appliance to process the packet. Recommendation: Verify if the security appliance is under attack. If there are no suspicious packets, or the security appliance is not in transparent mode, this counter is most likely being incremented due to a software error. Attempt to capture the traffic that is causing the counter to increment and contact the Cisco TAC. **System messages**: None.

Table 7-4 Frame Drop Reasons (continued)

Frame Drop Reason Keyword	Frame Drop Reason Display	Description
unsupport-ipv6-hdr	Unsupported IPV6 header	This counter is incremented and the packet is dropped if an IPv6 packet is received with an unsupported IPv6 extension header. The supported IPv6 extension headers are: TCP, UDP, ICMPv6, ESP, AH, Hop Options, Destination Options, and Fragment. The IPv6 routing extension header is not supported, and any extension header not listed above is not supported. IPv6 ESP and AH headers are supported only if the packet is through-the-box. To-the-box IPv6 ESP and AH packets are not supported and will be dropped. **Recommendation**: This error may be due to a misconfigured host. If this error occurs repeatedly or in large numbers, it could also indicate spurious or malicious activity such as an attempted DoS attack. **System messages**: None.
unsupported-ip-version	Unsupported IP version	This counter is incremented when the security appliance receives an IP packet that has an unsupported version in the version field of the IP header. Specifically, if the packet does not belong to version 4 or version 6, the packet is dropped. **Recommendation**: Verify that other devices on the connected network are configured to send IP packets belonging to versions 4 or 6 only. **System messages**: None.

Examples

The following is sample output from the **show asp drop** command, with the timestamp indicating when the last time the counters were cleared:

```
hostname# show asp drop

Frame drop:
  Flow is denied by configured rule (acl-drop)                    3
  Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                4110
  L2 Src/Dst same LAN port (l2_same-lan-port)                   760
  Expired flow (flow-expired)                                     1

Last clearing: Never

Flow drop:
  Flow is denied by access rule (acl-drop)                       24
  NAT failed (nat-failed)                                     28739
  NAT reverse path failed (nat-rpf-failed)                    22266
  Inspection failure (inspect-fail)                           19433

Last clearing: 17:02:12 UTC Jan 17 2008 by enable_15
```

Related Commands

Command	Description
clear asp drop	Clears drop statistics for the accelerated security path.
show conn	Shows information about connections.

show asp table arp

To debug the accelerated security path ARP tables, use the **show asp table arp** command in privileged EXEC mode.

show asp table arp [**interface** *interface_name*] [**address** *ip_address* [**netmask** *mask*]]

Syntax Description

address *ip_address*	(Optional) Identifies an IP address for which you want to view ARP table entries.
interface *interface_name*	(Optional) Identifies a specific interface for which you want to view the ARP table.
netmask *mask*	(Optional) Sets the subnet mask for the IP address.

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	This command was introduced.

Usage Guidelines

The **show arp** command shows the contents of the control plane, while the **show asp table arp** command shows the contents of the accelerated security path, which might help you troubleshoot a problem. See the *Cisco Security Appliance Command Line Configuration Guide* for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

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

```
hostname# show asp table arp

Context: single_vf, Interface: inside
  10.86.194.50                            Active   000f.66ce.5d46 hits 0
  10.86.194.1                             Active   00b0.64ea.91a2 hits 638
  10.86.194.172                           Active   0001.03cf.9e79 hits 0
  10.86.194.204                           Active   000f.66ce.5d3c hits 0
  10.86.194.188                           Active   000f.904b.80d7 hits 0

Context: single_vf, Interface: identity
```

```
::                                      Active   0000.0000.0000 hits 0
0.0.0.0                                 Active   0000.0000.0000 hits 50208
```

Related Commands

Command	Description
show arp	Shows the ARP table.
show arp statistics	Shows ARP statistics.

show asp table classify

To debug the accelerated security path classifier tables, use the **show asp table classify** command in privileged EXEC mode. The classifier examines properties of incoming packets, such as protocol, and source and destination address, to match each packet to an appropriate classification rule. Each rule is labeled with a classification domain that determines what types of actions are performed, such as dropping a packet or allowing it through.

show asp table classify [**hit** | **crypto** | **domain** *domain_name* | **interface** *interface_name*]

Syntax Description

crypto	(Optional) Shows the encrypt, decrypt, and ipsec tunnel flow domains only.
domain *domain_name*	(Optional) Shows entries for a specific classifier domain. See "Usage Guidelines" for a list of domains.
hits	(Optional) Shows classifier entries which have non-zero hits values
interface *interface_name*	(Optional) Identifies a specific interface for which you want to view the classifier table.

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	This command was introduced.
7.2(4)	Added the **hits** option, and the timestamp indicating when the last time the asp table counters were cleared.

Usage Guidelines

The **show asp table classifier** command shows the classifier contents of the accelerated security path, which might help you troubleshoot a problem. See the *Cisco Security Appliance Command Line Configuration Guide* for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Classifier domains include the following:

```
aaa-acct
aaa-auth
aaa-user
accounting
arp
```

```
capture
capture
conn-nailed
conn-set
ctcp
decrypt
encrypt
established
filter-activex
filter-ftp
filter-https
filter-java
filter-url
host
ids
inspect
inspect-ctiqbe
inspect-dns
inspect-dns-ids
inspect-ftp
inspect-ftp-data
inspect-gtp
inspect-h323
inspect-http
inspect-icmp
inspect-icmp-error
inspect-ils
inspect-mgcp
inspect-netbios
inspect-pptp
inspect-rsh
inspect-rtsp
inspect-sip
inspect-skinny
inspect-smtp
inspect-snmp
inspect-sqlnet
inspect-sqlnet-plus
inspect-sunrpc
inspect-tftp
inspect-xdmcp
ipsec-natt
ipsec-tunnel-flow
ipsec-user
limits
lu
mac-permit
mgmt-lockdown
mgmt-tcp-intercept
multicast
nat
nat-exempt
nat-exempt-reverse
nat-reverse
null
permit
permit-ip-option
permit-log
pim
ppp
priority-q
punt
punt-l2
punt-root
```

```
qos
qos-per-class
qos-per-dest
qos-per-flow
qos-per-source
shun
tcp-intercept
```

Examples

The following is sample output from the **show asp table classify** command:

```
hostname# show asp table classify

Interface test:
in  id=0x36f3800, priority=10, domain=punt, deny=false
        hits=0, user_data=0x0, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=10.86.194.60, mask=255.255.255.255, port=0
in  id=0x33d3508, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
in  id=0x33d3978, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=53
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
...
```

The following is sample output from the **show asp table classify hits** command with a record of the last clearing hits counters:

```
Interface mgmt:
in id=0x494cd88, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
       dscp=0x0
in id=0x494d1b8, priority=112, domain=permit, deny=false
       hits=1, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0

Interface inside:
in id=0x48f1580, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
       dscp=0x0
in id=0x48f09e0, priority=1, domain=permit, deny=false
       hits=101, user_data=0x0, cs_id=0x0, l3_type=0x608 src mac=0000.0000.0000,
       mask=0000.0000.0000 dst mac=0000.0000.0000, mask=0000.0000.0000
Interface outside:
in id=0x48c0970, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
       dscp=0x0
```

Related Commands

Command	Description
show asp drop	Shows the accelerated security path counters for dropped packets.

show asp table interfaces

To debug the accelerated security path interface tables, use the **show asp table interfaces** command in privileged EXEC mode.

show asp table interfaces

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	This command was introduced.

Usage Guidelines

The **show asp table interfaces** command shows the interface table contents of the accelerated security path, which might help you troubleshoot a problem. See the *Cisco Security Appliance Command Line Configuration Guide* for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table interfaces** command:

```
hostname# show asp table interfaces

** Flags: 0x0001-DHCP, 0x0002-VMAC, 0x0010-Ident Ifc, 0x0020-HDB Initd,
   0x0040-RPF Enabled
Soft-np interface 'dmz' is up
    context single_vf, nicnum 0, mtu 1500
        vlan 300, Not shared, seclvl 50
        0 packets input, 1 packets output
        flags 0x20

Soft-np interface 'foo' is down
    context single_vf, nicnum 2, mtu 1500
        vlan <None>, Not shared, seclvl 0
        0 packets input, 0 packets output
        flags 0x20
```

```
Soft-np interface 'outside' is down
    context single_vf, nicnum 1, mtu 1500
        vlan <None>, Not shared, seclvl 50
        0 packets input, 0 packets output
        flags 0x20

Soft-np interface 'inside' is up
    context single_vf, nicnum 0, mtu 1500
        vlan <None>, Not shared, seclvl 100
        680277 packets input, 92501 packets output
        flags 0x20
...
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.

show asp table routing

To debug the accelerated security path routing tables, use the **show asp table routing** command in privileged EXEC mode. This command supports IPv4 and IPv6 addresses.

show asp table routing [**input** | **output**] [**address** *ip_address* [**netmask** *mask*] | **interface** *interface_name*]

Syntax Description

address *ip_address*	Sets the IP address for which you want to view routing entries. For IPv6 addresses, you can include the subnet mask as a slash (/) followed by the prefix (0 to 128). For example, enter the following: `fe80::2e0:b6ff:fe01:3b7a/128`
input	Shows the entries from the input route table.
interface *interface_name*	(Optional) Identifies a specific interface for which you want to view the routing table.
netmask *mask*	For IPv4 addresses, specifies the subnet mask.
output	Shows the entries from the output route table.

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	This command was introduced.

Usage Guidelines

The **show asp table routing** command shows the routing table contents of the accelerated security path, which might help you troubleshoot a problem. See the *Cisco Security Appliance Command Line Configuration Guide* for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table routing** command:

```
hostname# show asp table routing

in   255.255.255.255 255.255.255.255 identity
```

```
in   224.0.0.9       255.255.255.255 identity
in   10.86.194.60    255.255.255.255 identity
in   10.86.195.255   255.255.255.255 identity
in   10.86.194.0     255.255.255.255 identity
in   209.165.202.159 255.255.255.255 identity
in   209.165.202.255 255.255.255.255 identity
in   209.165.201.30  255.255.255.255 identity
in   209.165.201.0   255.255.255.255 identity
in   10.86.194.0     255.255.254.0   inside
in   224.0.0.0       240.0.0.0       identity
in   0.0.0.0         0.0.0.0         inside
out  255.255.255.255 255.255.255.255 foo
out  224.0.0.0       240.0.0.0       foo
out  255.255.255.255 255.255.255.255 test
out  224.0.0.0       240.0.0.0       test
out  255.255.255.255 255.255.255.255 inside
out  10.86.194.0     255.255.254.0   inside
out  224.0.0.0       240.0.0.0       inside
out  0.0.0.0         0.0.0.0         via 10.86.194.1, inside
out  0.0.0.0         0.0.0.0         via 0.0.0.0, identity
out  ::              ::              via 0.0.0.0, identity
```

Related Commands

Command	Description
show route	Shows the routing table in the control plane.

show asp table vpn-context

To debug the accelerated security path VPN context tables, use the **show asp table vpn-context** command in privileged EXEC mode.

show asp table vpn-context [**detail**]

Syntax Description

detail	(Optional) Shows additional detail for the VPN context tables.

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	This command was introduced.

Usage Guidelines

The **show asp table vpn-context** command shows the VPN context contents of the accelerated security path, which might help you troubleshoot a problem. See the *Cisco Security Appliance Command Line Configuration Guide* for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table vpn-context** command:

```
hostname# show asp table vpn-context

VPN ID=0058070576, DECR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058193920, ENCR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058168568, DECR+ESP, UP, pk=0000299627, rk=0000000061, gc=2
VPN ID=0058161168, ENCR+ESP, UP, pk=0000305043, rk=0000000061, gc=1
VPN ID=0058153728, DECR+ESP, UP, pk=0000271432, rk=0000000061, gc=2
VPN ID=0058150440, ENCR+ESP, UP, pk=0000285328, rk=0000000061, gc=1
VPN ID=0058102088, DECR+ESP, UP, pk=0000268550, rk=0000000061, gc=2
VPN ID=0058134088, ENCR+ESP, UP, pk=0000274673, rk=0000000061, gc=1
VPN ID=0058103216, DECR+ESP, UP, pk=0000252854, rk=0000000061, gc=2
...
```

The following is sample output from the **show asp table vpn-context detail** command:

```
hostname# show asp table vpn-context detail
```

```
VPN Ctx  = 0058070576 [0x03761630]
State    = UP
Flags    = DECR+ESP
SA       = 0x037928F0
SPI      = 0xEA0F21F0
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN Ctx  = 0058193920 [0x0377F800]
State    = UP
Flags    = ENCR+ESP
SA       = 0x037B4B70
SPI      = 0x900FDC32
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
...
```

Related Commands

Command	Description
show asp drop	Shows the accelerated security path counters for dropped packets.

show blocks

To show the packet buffer utilization, use the **show blocks** command in privileged EXEC mode.

show blocks [{**address** *hex* | **all** | **assigned** | **free** | **old** | **pool** *size* [**summary**]} [**diagnostics** | **dump** | **header** | **packet**] | **queue history** [**detail**]]

Syntax Description

address *hex*	(Optional) Shows a block corresponding to this address, in hexadecimal.
all	(Optional) Shows all blocks.
assigned	(Optional) Shows blocks that are assigned and in use by an application.
detail	(Optional) Shows a portion (128 bytes) of the first block for each unique queue type.
dump	(Optional) Shows the entire block contents, including the header and packet information. The difference between dump and packet is that dump includes additional information between the header and the packet.
diagnostics	(Optional) Shows block diagnostics.
free	(Optional) Shows blocks that are available for use.
header	(Optional) Shows the header of the block.
old	(Optional) Shows blocks that were assigned more than a minute ago.
packet	(Optional) Shows the header of the block as well as the packet contents.
pool *size*	(Optional) Shows blocks of a specific size.
queue history	(Optional) Shows where blocks are assigned when the security appliance runs out of blocks. Sometimes, a block is allocated from the pool but never assigned to a queue. In that case, the location is the code address that allocated the block.
summary	(Optional) Shows detailed information about block usage sorted by the program addresses of applications that allocated blocks in this class, program addresses of applications that released blocks in this class, and the queues to which valid blocks in this class belong.

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	The **pool summary** option was added.

Usage Guidelines

The **show blocks** command helps you determine if the security appliance is overloaded. This command lists preallocated system buffer utilization. A full memory condition is not a problem as long as traffic is moving through the security appliance. You can use the **show conn** command to see if traffic is moving. If traffic is not moving and the memory is full, there may be a problem.

You can also view this information using SNMP.

The information shown in a security context includes the system-wide information as well as context-specific information about the blocks in use and the high water mark for block usage.

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show blocks** command in single mode:

```
hostname# show blocks
SIZE     MAX    LOW    CNT
     4    1600   1598   1599
    80     400    398    399
   256    3600   3540   3542
  1550    4716   3177   3184
 16384      10     10     10
  2048    1000   1000   1000
```

Table 7-5 shows each field description.

Table 7-5 show blocks Fields

Field	Description
SIZE	Size, in bytes, of the block pool. Each size represents a particular type. Examples are shown below.
4	Duplicates existing blocks in applications such as DNS, ISAKMP, URL filtering, uauth, TFTP, and TCP modules.
80	Used in TCP intercept to generate acknowledgment packets and for failover hello messages.
256	Used for Stateful Failover updates, syslogging, and other TCP functions. These blocks are mainly used for Stateful Failover messages. The active security appliance generates and sends packets to the standby security appliance to update the translation and connection table. In bursty traffic, where high rates of connections are created or torn down, the number of available blocks might drop to 0. This situation indicates that one or more connections were not updated to the standby security appliance. The Stateful Failover protocol catches the missing translation or connection the next time. If the CNT column for 256-byte blocks stays at or near 0 for extended periods of time, then the security appliance is having trouble keeping the translation and connection tables synchronized because of the number of connections per second that the security appliance is processing. Syslog messages sent out from the security appliance also use the 256-byte blocks, but they are generally not released in such quantity to cause a depletion of the 256-byte block pool. If the CNT column shows that the number of 256-byte blocks is near 0, ensure that you are not logging at Debugging (level 7) to the syslog server. This is indicated by the logging trap line in the security appliance configuration. We recommend that you set logging at Notification (level 5) or lower, unless you require additional information for debugging purposes.

Table 7-5 show blocks Fields (continued)

Field	Description
1550	Used to store Ethernet packets for processing through the security appliance. When a packet enters a security appliance interface, it is placed on the input interface queue, passed up to the operating system, and placed in a block. The security appliance determines whether the packet should be permitted or denied based on the security policy and processes the packet through to the output queue on the outbound interface. If the security appliance is having trouble keeping up with the traffic load, the number of available blocks will hover close to 0 (as shown in the CNT column of the command output). When the CNT column is zero, the security appliance attempts to allocate more blocks, up to a maximum of 8192. If no more blocks are available, the security appliance drops the packet.
16384	Only used for the 64-bit, 66-MHz Gigabit Ethernet cards (i82543). See the description for 1550 for more information about Ethernet packets.
2048	Control or guided frames used for control updates.
MAX	Maximum number of blocks available for the specified byte block pool. The maximum number of blocks are carved out of memory at bootup. Typically, the maximum number of blocks does not change. The exception is for the 256- and 1550-byte blocks, where the security appliance can dynamically create more when needed, up to a maximum of 8192.
LOW	Low-water mark. This number indicates the lowest number of this size blocks available since the security appliance was powered up, or since the last clearing of the blocks (with the **clear blocks** command). A zero in the LOW column indicates a previous event where memory was full.
CNT	Current number of blocks available for that specific size block pool. A zero in the CNT column means memory is full now.

The following is sample output from the **show blocks all** command:

```
hostname# show blocks all
Class 0, size 4
     Block   allocd_by    freed_by  data size    alloccnt     dup_cnt  oper location
0x01799940  0x00000000  0x00101603          0           0           0 alloc not_specified
0x01798e80  0x00000000  0x00101603          0           0           0 alloc not_specified
0x017983c0  0x00000000  0x00101603          0           0           0 alloc not_specified

...

    Found 1000 of 1000 blocks
    Displaying 1000 of 1000 blocks
```

Table 7-6 shows each field description.

Table 7-6 show blocks all Fields

Field	Description
Block	The block address.
allocd_by	The program address of the application that last used the block (0 if not used).
freed_by	The program address of the application that last released the block.
data size	The size of the application buffer/packet data that is inside the block.

Table 7-6 show blocks all Fields

Field	Description
alloccnt	The number of times this block has been used since the block came into existence.
dup_cnt	The current number of references to this block if used: 0 means 1 reference, 1 means 2 references.
oper	One of the four operations that was last performed on the block: alloc, get, put, or free.
location	The application that uses the block, or the program address of the application that last allocated the block (same as the allocd_by field).

The following is sample output from the **show blocks** command in a context:

```
hostname/contexta# show blocks
  SIZE    MAX    LOW    CNT  INUSE   HIGH
     4   1600   1599   1599      0      0
    80    400    400    400      0      0
   256   3600   3538   3540      0      1
  1550   4616   3077   3085      0      0
```

The following is sample output from the **show blocks queue history** command:

```
hostname# show blocks queue history
Each Summary for User and Queue_type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    200     1 alloc   ip_rx             tcp       contexta
    108     1 get     ip_rx             udp       contexta
     85     1 free    fixup             h323_ras  contextb
     42     1 put     fixup             skinny    contextb

Block Size: 1550
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1000
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
...
```

The following is sample output from the **show blocks queue history detail** command:

```
hostname# show blocks queue history detail
History buffer memory usage: 2136 bytes (default)
Each Summary for User and Queue type is followed its top 5 individual queues
Block Size: 4
```

```
Summary for User "http", Queue_Type "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...

Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...
...

total_count: total buffers in this class
```

The following is sample output from the **show blocks pool summary** command:

```
hostname# show blocks pool 1550 summary
Class 3, size 1550

================================================
         total_count=1531    miss_count=0
Alloc_pc        valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000012
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

================================================
         total_count=9716    miss_count=0
Freed_pc        valid_cnt       invalid_cnt
0x9a81f3        00000104        00000007
         0x05006140 0x05000380 0x04fffa20 0x04ffde00 00000000 0x00000000
0x9a0326        00000053        00000033
         0x05006aa0 0x050057e0 0x05004e80 0x05003260 00000000 0x00000000
0x4605a2        00000005        00000000
         0x04ff5ac0 0x01e8e2e0 0x01e2eac0 0x01e17d20 00000000 0x00000000
...
================================================
```

```
         total_count=1531    miss_count=0
Queue   valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000  Invalid Bad qtype
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000000  Invalid Bad qtype
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

================================================
free_cnt=8185  fails=0  actual_free=8185  hash_miss=0
   03a8d3e0  03a8b7c0  03a7fc40  03a6ff20  03a6f5c0  03a6ec60 kao-f1#
```

Table 7-7 shows each field description.

Table 7-7 show blocks pool summary Fields

Field	Description
total_count	The number of blocks for a given class.
miss_count	The number of blocks not reported in the specified category due to technical reasons.
Freed_pc	The program addresses of applications that released blocks in this class.
Alloc_pc	The program addresses of applications that allocated blocks in this class.
Queue	The queues to which valid blocks in this class belong.
valid_cnt	The number of blocks that are currently allocated.
invalid_cnt	The number of blocks that are not currently allocated.
Invalid Bad qtype	Either this queue has been freed and the contents are invalid or this queue was never initialized.
Valid tcp_usr_conn_inp	The queue is valid.

Related Commands

Command	Description
blocks	Increases the memory assigned to block diagnostics
clear blocks	Clears the system buffer statistics.
show conn	Shows active connections.

show bootvar

To show the boot file and configuration properties, use the **show boot** command in privileged configuration mode.

show bootvar

Syntax Description

show bootvar	The system boot properties.

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 Mode	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The BOOT variable specifies a list of bootable images on various devices. The CONFIG_FILE variable specifies the configuration file used during system initialization. Set these variables with the **boot system** command, and **boot config** command, respectively.

Examples

The following example, the BOOT variable contains disk0:/f1_image, which is the image booted when the system reloads. The current value of BOOT is disk0:/f1_image; disk0:/f1_backupimage. This meansboot variable has been modified with the boot system command, but the running configuration has notbeen saved with the **write memory** command. When the running config is saved, the BOOT variable and current BOOT variable will both be disk0:/f1_image; disk0:/f1_backupimage. Assuming the running configuration is saved the boot loader will attempt to load the contents of the BOOT variable, starting with disk0:/f1image, but if that is not present or invalid, it will attempt to boot disk0:1/f1_backupimage.

The CONFIG_FILE variable points to the system startup configuration. In this example it is not set, so the startup configuration file is the default specified with the **boot config** command. The current CONFIG_FILE variable may be modified with the **boot config** command and saved with the **write memory** command.

```
hostname# show bootvar
BOOT variable = disk0:/f1_image
Current BOOT variable = disk0:/f1_image; disk0:/f1_backupimage
CONFIG_FILE variable =
Current CONFIG_FILE variable =
hostname#
```

Related Commands

Command	Description
boot	Specifies the configuration file or image file used at startup.

show capture

To display the capture configuration when no options are specified, use the **show capture** command.

show capture [*capture_name*] [**access-list** *access_list_name*] [**count** *number*] [**decode**] [**detail**] [**dump**] [**packet-number** *number*]

Syntax Description

capture_name	(Optional) Name of the packet capture.
access-list *access_list_name*	(Optional) Displays information for packets that are based on IP or higher fields for the specific access list identification.
count *number*	(Optional) Displays the number of packets specified data.
decode	This option is useful when a capture of type isakmp is applied to an interface. All isakmp data flowing through that interface will be captured after decryption and shown with more information after decoding the fields.
detail	(Optional) Displays additional protocol information for each packet.
dump	(Optional) Displays a hexadecimal dump of the packets that are transported over the data link transport.
packet-number *number*	Starts the display at the specified packet number.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
PIX Version 7.0	Support for this command was introduced on the security appliance.

Usage Guidelines

If you specify the *capture_name*, then the capture buffer contents for that capture are displayed.

The **dump** keyword does not display MAC information in the hexadecimal dump.

The decoded output of the packets depend on the protocol of the packet. In Table 7-8, the bracketed output is displayed when you specify the **detail** keyword.

Table 7-8 Packet Capture Output Formats

Packet Type	Capture Output Format
802.1Q	*HH:MM:SS.ms* [ether-hdr] *VLAN-info encap-ether-packet*
ARP	*HH:MM:SS.ms* [ether-hdr] *arp-type arp-info*

Table 7-8 Packet Capture Output Formats (continued)

Packet Type	Capture Output Format
IP/ICMP	*HH:MM:SS.ms* [ether-hdr] *ip-source* > *ip-destination:* icmp: *icmp-type icmp-code* [checksum-failure]
IP/UDP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port dest-addr.dst-port*: [checksum-info] udp *payload-len*
IP/TCP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port* d*est-addr.dst-port*: *tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*
IP/Other	*HH:MM:SS.ms* [ether-hdr] *src-addr dest-addr*: *ip-protocol ip-length*
Other	*HH:MM:SS.ms ether-hdr*: *hex-dump*

Examples

This example shows how to display the capture configuration:

```
hostname(config)# show capture
capture arp ethernet-type arp interface outside
capture http access-list http packet-length 74 interface inside
```

This example shows how to display the packets that are captured by an ARP capture:

```
hostname(config)# show capture arp
2 packets captured
19:12:23.478429 arp who-has 171.69.38.89 tell 171.69.38.10
19:12:26.784294 arp who-has 171.69.38.89 tell 171.69.38.10
2 packets shown
```

Related Commands

Command	Description
capture	Enables packet capture capabilities for packet sniffing and network fault isolation.
clear capture	Clears the capture buffer.
copy capture	Copies a capture file to a server.

show chardrop

To display the count of characters dropped from the serial console, use the **show chardrop** command in privileged EXEC mode.

show chardrop

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	This command was introduced.

Examples

The following is sample output from the **show chardrop** command:

```
hostname# show chardrop
Chars dropped pre-TxTimeouts: 0, post-TxTimeouts: 0
```

Related Commands

Command	Description
show running-config	Shows the current operating configuration.

show checkheaps

To show the checkheaps statistics, use the **show checkheaps** command in privileged EXEC mode. Checkheaps is a periodic process that verifies the sanity of the heap memory buffers (dynamic memory is allocated from the system heap memory region) and the integrity of the code region.

show checkheaps

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	This command was introduced.

Examples

The following is sample output from the **show checkheaps** command:

```
hostname# show checkheaps

Checkheaps stats from buffer validation runs
--------------------------------------------
Time elapsed since last run     : 42 secs
Duration of last run            : 0 millisecs
Number of buffers created       : 8082
Number of buffers allocated     : 7808
Number of buffers free          : 274
Total memory in use             : 43570344 bytes
Total memory in free buffers    : 87000 bytes
Total number of runs            : 310
```

Related Commands

Command	Description
checkheaps	Sets the checkheap verification intervals.

show checksum

To display the configuration checksum, use the **show checksum** command in privileged EXEC mode.

show checksum

Syntax Description

This command has no arguments or keywords.

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	Support for this command was introduced on the security appliance.

Usage Guidelines

The **show checksum** command allows you to display four groups of hexadecimal numbers that act as a digital summary of the configuration contents. This checksum is calculated only when you store the configuration in Flash memory.

If a dot (“.”) appears before the checksum in the **show config** or **show checksum** command output, the output indicates a normal configuration load or write mode indicator (when loading from or writing to the security appliance Flash partition). The “.” shows that the security appliance is preoccupied with the operation but is not “hung up.” This message is similar to a “system processing, please wait” message.

Examples

This example shows how to display the configuration or the checksum:

```
hostname(config)# show checksum
Cryptochecksum: 1a2833c0 129ac70b 1a88df85 650dbb81
```

show chunkstat

To display the chunk statistics, use the **show chunkstat** command in privileged EXEC mode.

show chunkstat

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

This example shows how to display the chunk statistics:

```
hostname# show chunkstat
Global chunk statistics: created 181, destroyed 34, siblings created 94, siblings
destroyed 34

Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01edb4cc, name "Managed Chunk Queue Elements", data start @ 01edbd24, end
@ 01eddc54
next: 01eddc8c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 499, elt size: 16, index first free 498
# chunks in use: 1, HWM of total used: 1, alignment: 0
Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01eddc8c, name "Registry Function List", data start @ 01eddea4, end @
01ede348
next: 01ede37c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 99, elt size: 12, index first free 42
# chunks in use: 57, HWM of total used: 57, alignment: 0
```

Related Commands

Command	Description
show counters	Displays the protocol stack counters.
show cpu	Displays the CPU utilization information.

show clock

To view the time on the security appliance, use the **show clock** command in user EXEC mode.

show clock [**detail**]

Syntax Description

detail	(Optional) Indicates the clock source (NTP or user configuration) and the current summer-time setting (if any).

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
User EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following is sample output from the **show clock** command:

```
hostname> show clock
12:35:45.205 EDT Tue Jul 27 2004
```

The following is sample output from the **show clock detail** command:

```
hostname> show clock detail
12:35:45.205 EDT Tue Jul 27 2004
Time source is user configuration
Summer time starts 02:00:00 EST Sun Apr 4 2004
Summer time ends 02:00:00 EDT Sun Oct 31 2004
```

Related Commands

Command	Description
clock set	Manually sets the clock on the security appliance.
clock summer-time	Sets the date range to show daylight saving time.
clock timezone	Sets the time zone.
ntp server	Identifies an NTP server.
show ntp status	Shows the status of the NTP association.

show conn

To display the connection state for the designated connection type, use the **show conn** command in privileged EXEC mode. This command supports IPv4 and IPv6 addresses.

show conn [**count** | [**all**] [**detail**] [**long**] [**state** *state_type*] [**protocol** {**tcp** | **udp**}]
[**address** *src_ip*[**-***src_ip*] [**netmask** *mask*]] [**port** *src_port*[**-***src_port*]]
[**address** *dest_ip*[**-***dest_ip*] [**netmask** *mask*]] [**port** *dest_port*[**-***dest_port*]]]

Syntax Description

address	(Optional) Displays connections with the specified source or destination IP address.
all	(Optional) Displays connections that are to the device or from the device, in addition to through-traffic connections.
count	(Optional) Displays the number of active connections.
dest_ip	(Optional) Specifies the destination IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-), For example: `10.1.1.1-10.1.1.5`
dest_port	(Optional) Specifies the destination port number. To specify a range, separate the port numbers with a dash (-), For example: `1000-2000`
detail	(Optional) Displays connections in detail, including translation type and interface information.
long	(Optional) Displays connections in long format.
netmask *mask*	(Optional) Specifies a subnet mask for use with the given IP address.
port	(Optional) Displays connections with the specified source or destination port.
protocol {tcp | udp}	(Optional) Specifies the connection protocol, **tcp** or **udp**.
src_ip	(Optional) Specifies the source IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-), For example: `10.1.1.1-10.1.1.5`
src_port	(Optional) Specifies the source port number. To specify a range, separate the port numbers with a dash (-), For example: `1000-2000`
state *state_type*	(Optional) Specifies the connection state type. See Table 7-9 for a list of the keywords available for connection state types.

Defaults

All through connections are shown by default.

Command Modes

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

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

Command History

Release	Modification
7.0(8)	The syntax was simplified to use source and destination concepts instead of "local" and "foreign." In the new syntax, the source address is the first address entered and the destination is the second address. The old syntax used keywords like **foreign** and **fport** to determine the destination address and port.

Usage Guidelines

The **show conn** command displays the number of active TCP and UDP connections, and provides information about connections of various types. Use the **show conn all** command to see the entire table of connections.

Note When the security appliance creates a pinhole to allow secondary connections, this is shown as an incomplete conn by the **show conn** command. To clear this incomplete conn use the **clear conn** command.

The connection types that you can specify using the **show conn state** command are defined in Table 7-9. When specifying multiple connection types, use commas without spaces to separate the keywords.

Table 7-9 Connection State Types

Keyword	Connection Type Displayed
up	Connections in the up state.
conn_inbound	Inbound connections.
ctiqbe	CTIQBE connections
data_in	Inbound data connections.
data_out	Outbound data connections.
finin	FIN inbound connections.
finout	FIN outbound connections.
h225	H.225 connections
h323	H.323 connections
http_get	HTTP get connections.
mgcp	MGCP connections.
nojava	Connections that deny access to Java applets.
rpc	RPC connections.

Table 7-9 Connection State Types (continued)

Keyword	Connection Type Displayed
sip	SIP connections.
skinny	SCCP connections.
smtp_data	SMTP mail data connections.
sqlnet_fixup_data	SQL*Net data inspection engine connections.

When you use the **detail** option, the system displays information about the translation type and interface information using the connection flags defined in Table 7-10.

Table 7-10 Connection Flags

Flag	Description
a	awaiting outside ACK to SYN
A	awaiting inside ACK to SYN
B	initial SYN from outside
C	Computer Telephony Interface Quick Buffer Encoding (CTIQBE) media connection
d	dump
D	DNS
E	outside back connection
f	inside FIN
F	outside FIN
g	Media Gateway Control Protocol (MGCP) connection
G	connection is part of a group[1]
h	H.225
H	H.323
i	incomplete TCP or UDP connection
I	inbound data
k	Skinny Client Control Protocol (SCCP) media connection
m	SIP media connection
M	SMTP data
O	outbound data
p	replicated (unused)
P	inside back connection
q	SQL*Net data
r	inside acknowledged FIN
R	outside acknowledged FIN for TCP connection
R	UDP RPC[2]
s	awaiting outside SYN
S	awaiting inside SYN

Table 7-10 Connection Flags (continued)

Flag	Description
t	SIP transient connection[3]
T	SIP connection[4]
U	up

1. The G flag indicates the connection is part of a group. It is set by the GRE and FTP Strict fixups to designate the control connection and all its associated secondary connections. If the control connection terminates, then all associated secondary connections are also terminated.
2. Because each row of **show conn** command output represents one connection (TCP or UDP), there will be only one R flag per row.
3. For UDP connections, the value t indicates that it will timeout after one minute.
4. For UDP connections, the value T indicates that the connection will timeout according to the value specified using the **timeout sip** command.

Note For connections using a DNS server, the source port of the connection may be replaced by the *IP address of DNS server* in the **show conn** command output.

A single connection is created for multiple DNS sessions, as long as they are between the same two hosts, and the sessions have the same 5-tuple (source/destination IP address, source/destination port, and protocol). DNS identification is tracked by *app_id*, and the idle timer for each app_id runs independently.

Because the app_id expires independently, a legitimate DNS response can only pass through the security appliance within a limited period of time and there is no resource build-up. However, when you enter the **show conn** command, you will see the idle timer of a DNS connection being reset by a new DNS session. This is due to the nature of the shared DNS connection and is by design.

Note When there is no TCP traffic for the period of inactivity defined by the **timeout conn** command (by default, 1:00:00), the connection is closed and the corresponding conn flag entries are no longer displayed.

Examples

When specifying multiple connection types, use commas without spaces to separate the keywords. The following example displays information about RPC, H.323, and SIP connections in the Up state:

```
hostname# show conn state up,rpc,h323,sip
```

The following is sample output from the **show conn count** command:

```
ciscoasa(config)# show conn count
22 in use, 27775 most used
```

The following is sample output from the **show conn** command. This example shows a TCP session connection from inside host 10.1.1.15 to the outside Telnet server at 10.2.49.10. Because there is no B flag, the connection is initiated from the inside. The “U”, “I”, and “O” flags denote that the connection is active and has received inbound and outbound data.

```
hostname# show conn
22 in use, 27775 most used
TCP out 10.2.49.10:23 in 10.1.1.15:1026 idle 0:00:22 bytes 1774 flags UIO
```

```
UDP out 10.2.49.10:31649 in 10.1.1.15:1028 idle 0:00:14 bytes 0 flags D-
TCP out 10.30.2.2:1500 in 10.1.1.7:1000 idle 0:00:00 bytes 0 flags saA
TCP out 10.30.2.2:1500 in 10.1.1.14:1000 idle 0:00:00 bytes 0 flags saA
TCP out 10.30.2.2:1500 in 10.1.1.1:1000 idle 0:00:00 bytes 0 flags saA
TCP out 10.30.2.2:1500 in 10.1.1.3:1000 idle 0:00:00 bytes 0 flags saA
TCP out 10.30.2.2:80 in 10.30.1.1:45804 idle 0:01:26 bytes 7918 flags UFRIO
TCP out 10.30.2.2:80 in 10.30.1.1:45003 idle 0:02:17 bytes 7918 flags UFRIO
```

The following is sample output from the **show conn detail** command. This example shows many connections, including a UDP connection from outside host 192.168.49.10 to inside host 10.1.1.15. The D flag denotes that this is a DNS connection. The number 1028 is the DNS ID over the connection.

```
hostname# show conn detail
22 in use, 27775 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
       E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, O - outbound data,
       P - inside back connection, q - SQL*Net data, R - outside acknowledged FI
N,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up
TCP outside:10.30.2.2/1500 inside:10.1.1.7/1000 flags saA
TCP outside:10.30.2.2/1500 inside:10.1.1.14/1000 flags saA
TCP outside:10.30.2.2/1500 inside:10.1.1.1/1000 flags saA
TCP outside:10.30.2.2/1500 inside:10.1.1.3/1000 flags saA
TCP outside:10.30.2.2/80 inside:10.30.1.1/45804 flags UFRIO
TCP outside:10.30.2.2/80 inside:10.30.1.1/45003 flags UFRIO
TCP outside:192.168.49.10/23 inside:10.1.1.15/1026 flags UIO
UDP outside:192.168.49.10/31649 inside:10.1.1.15/1028 flags dD
```

Related Commands

Commands	Description
clear conn	Clears connections.
inspect ctiqbe	Enables CTIQBE application inspection.
inspect h323	Enables H.323 application inspection.
inspect mgcp	Enables MGCP application inspection.
inspect sip	Removes java applets from HTTP traffic.
inspect skinny	Enables SCCP application inspection.

show console-output

To display the currently captured console output, use the **show console-output** command in privileged EXEC mode.

show console-output

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 example shows the message that displays when there is no console output:

```
hostname# show console-output
Sorry, there are no messages to display
```

Related Commands

Command	Description
show console-output	Displays the captured console output.

show context

To show context information including allocated interfaces and the configuration file URL, the number of contexts configured, or from the system execution space, a list of all contexts, use the **show context** command in privileged EXEC mode.

show context [*name* | **detail** | **count**]

Syntax Description

count	(Optional) Shows the number of contexts configured.
detail	(Optional) Shows additional detail about the context(s) including the running state and information for internal use.
name	(Optional) Sets the context name. If you do not specify a name, the security appliance displays all contexts. Within a context, you can only enter the current context name.

Defaults

In the system execution space, the security appliance displays all contexts if you do not specify a name.

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	This command was introduced.

Usage Guidelines

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show context** command. The following sample display shows three contexts:

```
hostname# show context

Context Name      Interfaces                  URL
*admin            GigabitEthernet0/1.100      flash:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200      flash:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300      flash:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

Table 7-11 shows each field description.

Table 7-11 show context Fields

Field	Description
Context Name	Lists all context names. The context name with the asterisk (*) is the admin context.
Interfaces	The interfaces assigned to the context.
URL	The URL from which the security appliance loads the context configuration.

The following is sample output from the **show context detail** command:

```
hostname# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: flash:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Control0/0, GigabitEthernet0/0,
     GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
     GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
     GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257

Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Flags: 0x00000009, ID: 258
```

Table 7-12 shows each field description.

Table 7-12 Context States

Field	Description
Context	The context name. The null context information is for internal use only. The system context represents the system execution space.
State Message:	The context state. See the possible messages below.

Table 7-12 Context States

Field	Description
Has been created, but initial ACL rules not complete	The security appliance parsed the configuration but has not yet downloaded the default ACLs to establish the default security policy. The default security policy applies to all contexts initially, and includes disallowing traffic from lower security levels to higher security levels, enabling application inspection, and other parameters. This security policy ensures that no traffic can pass through the security appliance after the configuration is parsed but before the configuration ACLs are compiled. You are unlikely to see this state because the configuration ACLs are compiled very quickly.
Has been created, but not initialized	You entered the **context** *name* command, but have not yet entered the **config-url** command.
Has been created, but the config hasn't been parsed	The default ACLs were downloaded, but the security appliance has not parsed the configuration. This state might exist because the configuration download might have failed because of network connectivity issues, or you have not yet entered the **config-url** command. To reload the configuration, from within the context, enter **copy startup-config running-config**. From the system, reenter the **config-url** command. Alternatively, you can start configuring the blank running configuration.
Is a system resource	This state applies only to the system execution space and to the null context. The null context is used by the system, and the information is for internal use only.
Is a zombie	You deleted the context using the **no context** or **clear context** command, but the context information persists in memory until the security appliance reuses the context ID for a new context, or you restart.
Is active	This context is currently running and can pass traffic according to the context configuration security policy.
Is ADMIN and active	This context is the admin context and is currently running.
Was a former ADMIN, but is now a zombie	You deleted the admin context using the **clear configure context** command, but the context information persists in memory until the security appliance reuses the context ID for a new context, or you restart.
Real Interfaces	The interfaces assigned to the context. If you mapped the interface IDs in the **allocate-interface** command, this display shows the real name of the interface. The system execution space includes all interfaces.
Mapped Interfaces	If you mapped the interface IDs in the **allocate-interface** command, this display shows the mapped names. If you did not map the interfaces, the display lists the real names again.
Flag	For internal use only.
ID	An internal ID for this context.

The following is sample output from the **show context count** command:

```
hostname# show context count
Total active contexts: 2
```

Related Commands

Command	Description
admin-context	Sets the admin context.
allocate-interface	Assigns interfaces to a context.
changeto	Changes between contexts or the system execution space.
config-url	Specifies the location of the context configuration.
context	Creates a security context in the system configuration and enters context configuration mode.

show counters

To display the protocol stack counters, use the **show counters** command in privileged EXEC mode.

show counters [all | context *context-name* **| summary | top** *N* **] [detail] [protocol** *protocol_name* **[:***counter_name***]] [threshold** *N***]**

Syntax Description

all	Displays the filter details.
context *context-name*	Specifies the context name.
:*counter_name*	Specifies a counter by name.
detail	Displays additional counters information.
protocol *protocol_name*	Displays the counters for the specified protocol.
summary	Displays a counter summary.
threshold *N*	Displays only those counters at or above the specified threshold. The range is 1 through 4294967295.
top *N*	Displays the counters at or above the specified threshold. The range is 1 through 4294967295.

Defaults

show counters summary detail threshold 1

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to display all counters:

```
hostname# show counters all
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               2   single_vf
IOS_IPC      OUT_PKTS              2   single_vf

hostname# show counters
Protocol     Counter           Value   Context
NPCP         IN_PKTS            7195   Summary
NPCP         OUT_PKTS           7603   Summary
IOS_IPC      IN_PKTS             869   Summary
IOS_IPC      OUT_PKTS            865   Summary
IP           IN_PKTS             380   Summary
```

```
IP            OUT_PKTS             411   Summary
IP            TO_ARP               105   Summary
IP            TO_UDP                 9   Summary
UDP           IN_PKTS                9   Summary
UDP           DROP_NO_APP            9   Summary
FIXUP         IN_PKTS              202   Summary
```

The following example shows how to display a summary of counters:

```
hostname# show counters summary
Protocol      Counter            Value   Context
IOS_IPC       IN_PKTS                2   Summary
IOS_IPC       OUT_PKTS               2   Summary
```

The following example shows how to display counters for a context:

```
hostname# show counters context single_vf
Protocol      Counter            Value   Context
IOS_IPC       IN_PKTS                4   single_vf
IOS_IPC       OUT_PKTS               4   single_vf
```

Related Commands

Command	Description
clear counters	Clears the protocol stack counters.

show cpu

To display the CPU utilization information, use the **show cpu usage** command in privileged EXEC mode.

show cpu [**usage**]

From the system configuration in multiple context mode:

show cpu [**usage**] [**context** {**all** | *context_name*}]

Syntax Description

all	Specifies that the display show all contexts.
context	Specifies that the display show a context.
context_name	Specifies the name of the context to display.
usage	(Optional) Displays the CPU usage.

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.

Usage Guidelines

The cpu usage is computed using an approximation of the load every five seconds, and by further feeding this approximation into two, following moving averages.

You can use the **show cpu** command to find process related loads (that is, activity on behalf of items listed by the output of the **show process** command in both single mode and from the system configuration in multiple context mode).

Further, you can request, when in multiple context mode, a breakdown of the process related load to CPU consumed by any configured contexts by changing to each context and entering the **show cpu** command or by entering the **show cpu context** variant of this command.

While process related load is rounded to the nearest whole number, context related loads include one additional decimal digit of precision. For example, entering **show cpu** from the system context produces a different number than from entering the **show cpu context system** command. The former is an approximate summary of everything in **show cpu context all**, and the latter is only a portion of that summary.

Examples

The following example shows how to display the CPU utilization:

```
hostname# show cpu usage
CPU utilization for 5 seconds = 18%; 1 minute: 18%; 5 minutes: 18%
```

This example shows how to display the CPU utilization for the system context in multiple mode:

```
hostname# show cpu context system
CPU utilization for 5 seconds = 9.1%; 1 minute: 9.2%; 5 minutes: 9.1%
```

The following shows how to display the CPU utilization for all contexts:

```
hostname# show cpu usage context all
5 sec  1 min  5 min  Context Name
9.1%   9.2%   9.1%  system
0.0%   0.0%   0.0%  admin
5.0%   5.0%   5.0%  one
4.2%   4.3%   4.2%  two
```

This example shows how to display the CPU utilization for a context named “one”:

```
hostname/one# show cpu usage
CPU utilization for 5 seconds = 5.0%; 1 minute: 5.0%; 5 minutes: 5.0%
```

Related Commands

Command	Description
show counters	Displays the protocol stack counters.

show crashinfo

To display the contents of the crash file stored in Flash memory, enter the **show crashinfo** command in privileged EXEC mode.

show crashinfo [**save**]

Syntax Description

save	(Optional) Displays if the security appliance is configured to save crash information to Flash memory or not.

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.

Usage Guidelines

If the crash file is from a test crash (generated from the **crashinfo test** command), the first string of the crash file is "**: Saved_Test_Crash**" and the last string is "**: End_Test_Crash**". If the crash file is from a real crash, the first string of the crash file is "**: Saved_Crash**" and the last string is "**: End_Crash**". (This includes crashes from use of the **crashinfo force page-fault** or **crashinfo force watchdog** commands).

If there is no crash data saved in flash, or if the crash data has been cleared by entering the **clear crashinfo** command, the **show crashinfo** command displays an error message.

Examples

The following example shows how to display the current crash information configuration:

```
hostname# show crashinfo save
crashinfo save enable
```

The following example shows the output for a crash file test. (However, this test does not actually crash the security appliance. It provides a simulated example file.)

```
hostname(config)# crashinfo test
hostname(config)# exit
hostname# show crashinfo
: Saved_Test_Crash

Thread Name: ci/console (Old pc 0x001a6ff5 ebp 0x00e88920)
```

```
Traceback:
0: 00323143
1: 0032321b
2: 0010885c
3: 0010763c
4: 001078db
5: 00103585
6: 00000000
    vector 0x000000ff (user defined)
       edi 0x004f20c4
       esi 0x00000000
       ebp 0x00e88c20
       esp 0x00e88bd8
       ebx 0x00000001
       edx 0x00000074
       ecx 0x00322f8b
       eax 0x00322f8b
error code n/a
       eip 0x0010318c
        cs 0x00000008
    eflags 0x00000000
       CR2 0x00000000
Stack dump: base:0x00e8511c size:16384, active:1476
0x00e89118: 0x004f1bb4
0x00e89114: 0x001078b4
0x00e89110-0x00e8910c: 0x00000000
0x00e89108-0x00e890ec: 0x12345678
0x00e890e8: 0x004f1bb4
0x00e890e4: 0x00103585
0x00e890e0: 0x00e8910c
0x00e890dc-0x00e890cc: 0x12345678
0x00e890c8: 0x00000000
0x00e890c4-0x00e890bc: 0x12345678
0x00e890b8: 0x004f1bb4
0x00e890b4: 0x001078db
0x00e890b0: 0x00e890e0
0x00e890ac-0x00e890a8: 0x12345678
0x00e890a4: 0x001179b3
0x00e890a0: 0x00e890b0
0x00e8909c-0x00e89064: 0x12345678
0x00e89060: 0x12345600
0x00e8905c: 0x20232970
0x00e89058: 0x616d2d65
0x00e89054: 0x74002023
0x00e89050: 0x29676966
0x00e8904c: 0x6e6f6328
0x00e89048: 0x31636573
0x00e89044: 0x7069636f
0x00e89040: 0x64786970
0x00e8903c-0x00e88e50: 0x00000000
0x00e88e4c: 0x000a7473
0x00e88e48: 0x6574206f
0x00e88e44: 0x666e6968
0x00e88e40: 0x73617263
0x00e88e3c-0x00e88e38: 0x00000000
0x00e88e34: 0x12345600
0x00e88e30-0x00e88dfc: 0x00000000
0x00e88df8: 0x00316761
0x00e88df4: 0x74706100
0x00e88df0: 0x12345600
0x00e88dec-0x00e88ddc: 0x00000000
0x00e88dd8: 0x00000070
0x00e88dd4: 0x616d2d65
```

```
0x00e88dd0: 0x74756f00
0x00e88dcc: 0x00000000
0x00e88dc8: 0x00e88e40
0x00e88dc4: 0x004f20c4
0x00e88dc0: 0x12345600
0x00e88dbc: 0x00000000
0x00e88db8: 0x00000035
0x00e88db4: 0x315f656c
0x00e88db0: 0x62616e65
0x00e88dac: 0x0030fcf0
0x00e88da8: 0x3011111f
0x00e88da4: 0x004df43c
0x00e88da0: 0x0053fef0
0x00e88d9c: 0x004f1bb4
0x00e88d98: 0x12345600
0x00e88d94: 0x00000000
0x00e88d90: 0x00000035
0x00e88d8c: 0x315f656c
0x00e88d88: 0x62616e65
0x00e88d84: 0x00000000
0x00e88d80: 0x004f20c4
0x00e88d7c: 0x00000001
0x00e88d78: 0x01345678
0x00e88d74: 0x00f53854
0x00e88d70: 0x00f7f754
0x00e88d6c: 0x00e88db0
0x00e88d68: 0x00e88d7b
0x00e88d64: 0x00f53874
0x00e88d60: 0x00e89040
0x00e88d5c-0x00e88d54: 0x12345678
0x00e88d50-0x00e88d4c: 0x00000000
0x00e88d48: 0x004f1bb4
0x00e88d44: 0x00e88d7c
0x00e88d40: 0x00e88e40
0x00e88d3c: 0x00f53874
0x00e88d38: 0x004f1bb4
0x00e88d34: 0x0010763c
0x00e88d30: 0x00e890b0
0x00e88d2c: 0x00e88db0
0x00e88d28: 0x00e88d88
0x00e88d24: 0x0010761a
0x00e88d20: 0x00e890b0
0x00e88d1c: 0x00e88e40
0x00e88d18: 0x00f53874
0x00e88d14: 0x0010166d
0x00e88d10: 0x0000000e
0x00e88d0c: 0x00f53874
0x00e88d08: 0x00f53854
0x00e88d04: 0x0048b301
0x00e88d00: 0x00e88d30
0x00e88cfc: 0x0000000e
0x00e88cf8: 0x00f53854
0x00e88cf4: 0x0048a401
0x00e88cf0: 0x00f53854
0x00e88cec: 0x00f53874
0x00e88ce8: 0x0000000e
0x00e88ce4: 0x0048a64b
0x00e88ce0: 0x0000000e
0x00e88cdc: 0x00f53874
0x00e88cd8: 0x00f7f96c
0x00e88cd4: 0x0048b4f8
0x00e88cd0: 0x00e88d00
0x00e88ccc: 0x0000000f
0x00e88cc8: 0x00f7f96c
```

```
0x00e88cc4-0x00e88cc0: 0x0000000e
0x00e88cbc: 0x00e89040
0x00e88cb8: 0x00000000
0x00e88cb4: 0x00f5387e
0x00e88cb0: 0x00f53874
0x00e88cac: 0x00000002
0x00e88ca8: 0x00000001
0x00e88ca4: 0x00000009
0x00e88ca0-0x00e88c9c: 0x00000001
0x00e88c98: 0x00e88cb0
0x00e88c94: 0x004f20c4
0x00e88c90: 0x0000003a
0x00e88c8c: 0x00000000
0x00e88c88: 0x0000000a
0x00e88c84: 0x00489f3a
0x00e88c80: 0x00e88d88
0x00e88c7c: 0x00e88e40
0x00e88c78: 0x00e88d7c
0x00e88c74: 0x001087ed
0x00e88c70: 0x00000001
0x00e88c6c: 0x00e88cb0
0x00e88c68: 0x00000002
0x00e88c64: 0x0010885c
0x00e88c60: 0x00e88d30
0x00e88c5c: 0x00727334
0x00e88c58: 0xa0ffffff
0x00e88c54: 0x00e88cb0
0x00e88c50: 0x00000001
0x00e88c4c: 0x00e88cb0
0x00e88c48: 0x00000002
0x00e88c44: 0x0032321b
0x00e88c40: 0x00e88c60
0x00e88c3c: 0x00e88c7f
0x00e88c38: 0x00e88c5c
0x00e88c34: 0x004b1ad5
0x00e88c30: 0x00e88c60
0x00e88c2c: 0x00e88e40
0x00e88c28: 0xa0ffffff
0x00e88c24: 0x00323143
0x00e88c20: 0x00e88c40
0x00e88c1c: 0x00000000
0x00e88c18: 0x00000008
0x00e88c14: 0x0010318c
0x00e88c10-0x00e88c0c: 0x00322f8b
0x00e88c08: 0x00000074
0x00e88c04: 0x00000001
0x00e88c00: 0x00e88bd8
0x00e88bfc: 0x00e88c20
0x00e88bf8: 0x00000000
0x00e88bf4: 0x004f20c4
0x00e88bf0: 0x000000ff
0x00e88bec: 0x00322f87
0x00e88be8: 0x00f5387e
0x00e88be4: 0x00323021
0x00e88be0: 0x00e88c10
0x00e88bdc: 0x004f20c4
0x00e88bd8: 0x00000000 *
0x00e88bd4: 0x004eabb0
0x00e88bd0: 0x00000001
0x00e88bcc: 0x00f5387e
0x00e88bc8-0x00e88bc4: 0x00000000
0x00e88bc0: 0x00000008
0x00e88bbc: 0x0010318c
0x00e88bb8-0x00e88bb4: 0x00322f8b
```

```
0x00e88bb0: 0x00000074
0x00e88bac: 0x00000001
0x00e88ba8: 0x00e88bd8
0x00e88ba4: 0x00e88c20
0x00e88ba0: 0x00000000
0x00e88b9c: 0x004f20c4
0x00e88b98: 0x000000ff
0x00e88b94: 0x001031f2
0x00e88b90: 0x00e88c20
0x00e88b8c: 0xffffffff
0x00e88b88: 0x00e88cb0
0x00e88b84: 0x00320032
0x00e88b80: 0x37303133
0x00e88b7c: 0x312f6574
0x00e88b78: 0x6972772f
0x00e88b74: 0x342f7665
0x00e88b70: 0x64736666
0x00e88b6c: 0x00020000
0x00e88b68: 0x00000010
0x00e88b64: 0x00000001
0x00e88b60: 0x123456cd
0x00e88b5c: 0x00000000
0x00e88b58: 0x00000008

Cisco XXX Firewall Version X.X
Cisco XXX Device Manager Version X.X

Compiled on Fri 15-Nov-04 14:35 by root

hostname up 10 days 0 hours

Hardware:   XXX-XXX, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB

0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited

This XXX has a Restricted (R) license.

Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 13:49:42.148 UTC Wed Nov 20 2004

------------------ show clock ------------------

15:34:28.129 UTC Sun Nov 24 2004

------------------ show memory ------------------

Free memory:        50444824 bytes
Used memory:        16664040 bytes
```

```
-------------     ----------------
Total memory:       67108864 bytes

------------------ show conn count ------------------

0 in use, 0 most used

------------------ show xlate count ------------------

0 in use, 0 most used

------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550   1188    795    927

------------------ show interface ------------------

interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0003.e300.73fd
  IP address 172.23.59.232, subnet mask 255.255.0.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        6139 packets input, 830375 bytes, 0 no buffer
        Received 5990 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        90 packets output, 6160 bytes, 0 underruns
        0 output errors, 13 collisions, 0 interface resets
        0 babbles, 0 late collisions, 47 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (5/128) software (0/2)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
  Hardware is i82559 ethernet, address is 0003.e300.73fe
  IP address 10.1.1.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1 packets output, 60 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        1 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet2 "intf2" is administratively down, line protocol is down
  Hardware is i82559 ethernet, address is 00d0.b7c8.139e
  IP address 127.0.0.1, subnet mask 255.255.255.255
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)

------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%
```

```
------------------ show process ------------------

     PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 001e3329 00763e7c 0053e5c8           0 00762ef4 3784/4096 arp_timer
Lsi 001e80e9 00807074 0053e5c8           0 008060fc 3792/4096 FragDBGC
Lwe 00117e3a 009dc2e4 00541d18           0 009db46c 3704/4096 dbgtrace
Lwe 003cee95 009de464 00537718           0 009dc51c 8008/8192 Logger
Hwe 003d2d18 009e155c 005379c8           0 009df5e4 8008/8192 tcp_fast
Hwe 003d2c91 009e360c 005379c8           0 009e1694 8008/8192 tcp_slow
Lsi 002ec97d 00b1a464 0053e5c8           0 00b194dc 3928/4096 xlate clean
Lsi 002ec88b 00b1b504 0053e5c8           0 00b1a58c 3888/4096 uxlate clean
Mrd 002e3a17 00c8f8d4 0053e600           0 00c8d93c 7908/8192 tcp_intercept_times
Lsi 00423dd5 00d3a22c 0053e5c8           0 00d392a4 3900/4096 route_process
Hsi 002d59fc 00d3b2bc 0053e5c8           0 00d3a354 3780/4096 PIX Garbage Collecr
Hwe 0020e301 00d5957c 0053e5c8           0 00d55614 16048/16384 isakmp_time_keepr
Lsi 002d377c 00d7292c 0053e5c8           0 00d719a4 3928/4096 perfmon
Hwe 0020bd07 00d9c12c 0050bb90           0 00d9b1c4 3944/4096 IPSec
Mwe 00205e25 00d9e1ec 0053e5c8           0 00d9c274 7860/8192 IPsec timer handler
Hwe 003864e3 00db26bc 00557920           0 00db0764 6904/8192 qos_metric_daemon
Mwe 00255a65 00dc9244 0053e5c8           0 00dc8adc 1436/2048 IP Background
Lwe 002e450e 00e7bb94 00552c30           0 00e7ad1c 3704/4096 pix/trace
Lwe 002e471e 00e7cc44 00553368           0 00e7bdcc 3704/4096 pix/tconsole
Hwe 001e5368 00e7ed44 00730674           0 00e7ce9c 7228/8192 pix/intf0
Hwe 001e5368 00e80e14 007305d4           0 00e7ef6c 7228/8192 pix/intf1
Hwe 001e5368 00e82ee4 00730534        2470 00e8103c 4892/8192 pix/intf2
H*  001a6ff5 0009ff2c 0053e5b0        4820 00e8511c 12860/16384 ci/console
Csi 002dd8ab 00e8a124 0053e5c8           0 00e891cc 3396/4096 update_cpu_usage
Hwe 002cb4d1 00f2bfbc 0051e360           0 00f2a134 7692/8192 uauth_in
Hwe 003d17d1 00f2e0bc 00828cf0           0 00f2c1e4 7896/8192 uauth_thread
Hwe 003e71d4 00f2f20c 00537d20           0 00f2e294 3960/4096 udp_timer
Hsi 001db3ca 00f30fc4 0053e5c8           0 00f3004c 3784/4096 557mcfix
Crd 001db37f 00f32084 0053ea40   508286220 00f310fc 3688/4096 557poll
Lsi 001db435 00f33124 0053e5c8           0 00f321ac 3700/4096 557timer
Hwe 001e5398 00f441dc 008121e0           0 00f43294 3912/4096 fover_ip0
Cwe 001dcdad 00f4523c 00872b48         120 00f44344 3528/4096 ip/0:0
Hwe 001e5398 00f4633c 008121bc          10 00f453f4 3532/4096 icmp0
Hwe 001e5398 00f47404 00812198           0 00f464cc 3896/4096 udp_thread/0
Hwe 001e5398 00f4849c 00812174           0 00f475a4 3456/4096 tcp_thread/0
Hwe 001e5398 00f495bc 00812150           0 00f48674 3912/4096 fover_ip1
Cwe 001dcdad 00f4a61c 008ea850           0 00f49724 3832/4096 ip/1:1
Hwe 001e5398 00f4b71c 0081212c           0 00f4a7d4 3912/4096 icmp1
Hwe 001e5398 00f4c7e4 00812108           0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4           0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0           0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534           0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c           0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078           0 00f50c8c 3896/4096 udp_thread/2
Hwe 001e5398 00f52c5c 00812054           0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8           0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8           0 00f786c4 7640/8192 Crypto CA

------------------ show failover ------------------

No license for Failover

------------------ show traffic ------------------

outside:
        received (in 865565.090 secs):
                6139 packets    830375 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
```

```
                90 packets      6160 bytes
                0 pkts/sec      0 bytes/sec
inside:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                1 packets       60 bytes
                0 pkts/sec      0 bytes/sec
intf2:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec

------------------ show perfmon ------------------


PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
TCPIntercept         0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
: End_Test_Crash
```

Related Commands

Command	Description
clear crashinfo	Deletes the contents of the crash file.
crashinfo force	Forces a crash of the security appliance.
crashinfo save disable	Disables crash information from writing to Flash memory.
crashinfo test	Tests the ability of the security appliance to save crash information to a file in Flash memory.

show crashinfo console

To display the configuration setting of the **crashinfo console** command, enter the **show crashinfo console** command in privileged EXEC mode.

show crashinfo console

Syntax Description

This command has no arguments or keywords.

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(4)	This command was introduced.

Usage Guidelines

Compliance with FIPS 140-2 prohibits the distribution of Critical Secu rity Parameters (keys, passwords, etc.) outside of the crypto boundary (chassis). When the device crashes, due to an assert or checkheaps failure, it is possible that the stack or memory regions dumped to the console contain sensitive data. This output must be suppressed in FIPS-mode.

Examples

```
sw8-5520(config)# show crashinfo console
crashinfo console enable
```

Related Commands

Command	Description
clear configure fips	Clears the system or module FIPS configuration information stored in NVRAM.
crashinfo console disable	Disables the reading, writing and configuration of crash write info to flash.
fips enable	Enables or disablea policy-checking to enforce FIPS compliance on the system or module.

Command	Description
fips self-test poweron	Executes power-on self-tests.
show running-config fips	Displays the FIPS configuration that is running on the security appliance.

show crypto accelerator statistics

To display the global and accelerator-specific statistics from the hardware crypto accelerator MIB, use the **show crypto accelerator statistics** command in global configuration or privileged EXEC mode.

show crypto accelerator statistics

Syntax Description

This command has no keywords or variables.

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	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example entered in global configuration mode, displays global crypto accelerator statistics:

```
hostname # show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capacity]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
   Max accelerators: 1
   Max crypto throughput: 100 Mbps
   Max crypto connections: 750
[Global Statistics]
   Number of active accelerators: 1
   Number of non-operational accelerators: 0
   Input packets: 700
   Input bytes: 753488
   Output packets: 700
   Output error packets: 0
   Output bytes: 767496
[Accelerator 0]
   Status: Active
   Software crypto engine
   Slot: 0
   Active time: 167 seconds
   Total crypto transforms: 7
```

```
   Total dropped packets: 0
   [Input statistics]
      Input packets: 0
      Input bytes: 0
      Input hashed packets: 0
      Input hashed bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [Output statistics]
      Output packets: 0
      Output bad packets: 0
      Output bytes: 0
      Output hashed packets: 0
      Output hashed bytes: 0
      Encrypted packets: 0
      Encrypted bytes: 0
   [Diffie-Hellman statistics]
      Keys generated: 0
      Secret keys derived: 0
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 98
      Random number request failures: 0
[Accelerator 1]
   Status: Active
   Encryption hardware device : Cisco ASA-55x0 on-board accelerator
(revision 0x0)
                            Boot microcode   : CNlite-MC-Boot-Cisco-1.2
                            SSL/IKE microcode: CNlite-MC-IPSEC-Admin-3.03
                            IPSec microcode  : CNlite-MC-IPSECm-MAIN-2.03
   Slot: 1
   Active time: 170 seconds
   Total crypto transforms: 1534
   Total dropped packets: 0
   [Input statistics]
      Input packets: 700
      Input bytes: 753544
      Input hashed packets: 700
      Input hashed bytes: 736400
      Decrypted packets: 700
      Decrypted bytes: 719944
   [Output statistics]
      Output packets: 700
      Output bad packets: 0
      Output bytes: 767552
      Output hashed packets: 700
      Output hashed bytes: 744800
      Encrypted packets: 700
      Encrypted bytes: 728352
   [Diffie-Hellman statistics]
```

```
      Keys generated: 97
      Secret keys derived: 1
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 1
      Random number request failures: 0
hostname #
```

Related Commands

Command	Description
clear crypto accelerator statistics	Clears the global and accelerator-specific statistics in the crypto accelerator MIB.
clear crypto protocol statistics	Clears the protocol-specific statistics in the crypto accelerator MIB.
show crypto protocol statistics	Displays the protocol-specific statistics from the crypto accelerator MIB.

show crypto ca certificates

To display the certificates associated with a specific trustpoint or to display all the certificates installed on the system, use the **show crypto ca certificates** command in global configuration or privileged EXEC mode.

show crypto ca certificates [*trustpointname*]

Syntax Description

trustpointname	(Optional) The name of a trustpoint. If you do not specify a name, this command displays all certificates installed on the system.

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	•	•	•	•	—
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example entered in global configuration mode, displays a CA certificate for a trustpoint named tp1:

```
hostname(config)# show crypto ca certificates tp1
CA Certificate
    Status: Available
    Certificate Serial Number 2957A3FF296EF854FD0D6732FE25B45
    Certificate Usage: Signature
    Issuer:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST - massachusetts
        C = US
        EA = a@b.con
    Subject:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST = massachusetts
        C = US
        EA = a@b.com
```

```
    CRL Distribution Point
        ldap://w2kadvancedsrv/CertEnroll/ms-root-sha-06-2004.crl
    Validity Date:
        start date: 14:11:40 UTC Jun 26 2004
        end date: 14:01:30 UTC Jun 4 2022
    Associated Trustpoints: tp2 tp1
hostname(config)#
```

Related Commands

Command	Description
crypto ca authenticate	Obtains a CA certificate for a specified trustpoint.
crypto ca crl request	Requests a CRL based on the configuration parameters of a specified trustpoint.
crypto ca enroll	Initiates the enrollment process with a CA.
crypto ca import	Imports a certificate to a specified trustpoint.
crypto ca trustpoint	Enters trustpoint mode for a specified trustpoint.

show crypto ca crls

To display all cached CRLs or to display all CRLs cached for a specified trustpoint, use the **show crypto ca crls** command in global configuration or privileged EXEC mode.

show crypto ca crls [*trustpointname*]

Syntax Description

trustpointname	(Optional) The name of a trustpoint. If you do not specify a name, this command displays all CRLs cached on the system.

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	•	•	•	•	
Privileged EXEC	•	•	•	•	

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example entered in global configuration mode, displays a CRL for a trustpoint named tp1:

```
hostname(config)# show crypto ca crls tp1
CRL Issuer Name:
    cn=ms-sub1-ca-5-2004,ou=Franklin DevTest,o=Cisco
Systems,l=Franklin,st=MA,c=US,ea=user@cisco.com
    LastUpdate: 19:45:53 UTC Dec 24 2004
    NextUpdate: 08:05:53 UTC Jan 1 2005
    Retrieved from CRL Distribution Point:
      http://win2k-ad2.frk-ms-pki.cisco.com/CertEnroll/ms-sub1-ca-5-2004.crl
    Associated Trustpoints: tp1
hostname(config)#
```

Related Commands

Command	Description
crypto ca authenticate	Obtains a CA certificate for a specified trustpoint.
crypto ca crl request	Requests a CRL based on the configuration parameters of a specified trustpoint.
crypto ca enroll	Initiates the enrollment process with a CA.
crypto ca import	Imports a certificate to a specified trustpoint.
crypto ca trustpoint	Enters trustpoint mode for a specified trustpoint.

show crypto ipsec df-bit

To display the IPSec DF-bit policy for IPSec packets for a specified interface, use the **show crypto ipsec df-bit** command in global configuration mode and privileged EXEC mode.

show crypto ipsec df-bit *interface*

Syntax Description

interface	Specifies an interface name.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example displays the IPSec DF-bit policy for interface named inside:

```
hostname(config)# show crypto ipsec df-bit inside
df-bit inside copy
hostname(config)#
```

Related Commands

Command	Description
crypto ipsec df-bit	Configures the IPSec DF-bit policy for IPSec packets.
crypto ipsec fragmentation	Configures the fragmentation policy for IPSec packets.
show crypto ipsec fragmentation	Displays the fragmentation policy for IPSec packets.

show crypto ipsec fragmentation

To display the fragmentation policy for IPSec packets, use the **show crypto ipsec fragmentation** command in global configuration or privileged EXEC modes.

show crypto ipsec fragmentation *interface*

Syntax Description

interface	Specifies an interface name.

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	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example, entered in global configuration mode, displays the IPSec fragmentation policy for an interface named inside:

```
hostname(config)# show crypto ipsec fragmentation inside
fragmentation inside before-encryption
hostname(config)#
```

Related Commands

Command	Description
crypto ipsec fragmentation	Configures the fragmentation policy for IPSec packets.
crypto ipsec df-bit	Configures the DF-bit policy for IPSec packets.
show crypto ipsec df-bit	Displays the DF-bit policy for a specified interface.

show crypto key mypubkey

To display key pairs of the indicated type, use the **show crypto key mypubkey** command in global configuration or privileged EXEC mode.

show crypto key mypubkey {**rsa** | **dsa**}

Syntax Description

dsa	Displays DSA key pairs.
rsa	Displays RSA key pairs.

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	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example entered in global configuration mode, displays RSA key pairs:

```
hostname(config)# show crypto key mypubkey rsa
[Display]
hostname(config)#
```

Related Commands

Command	Description
crypto key generate dsa	Generates DSA key pairs.
crypto key generate rsa	Generates RSA key pairs.
crypto key zeroize	Removes all key pairs of the indicated type.

show crypto protocol statistics

To display the protocol-specific statistics in the crypto accelerator MIB, use the **show crypto protocol statistics** command in global configuration or privileged EXEC mode.

show crypto protocol statistics *protocol*

Syntax Description

protocol	Specifies the name of the protocol for which to display statistics. Protocol choices are as follows: **ikev1**—Internet Key Exchange version 1. **ipsec**—IP Security Phase-2 protocols. **ssl**—Secure Socket Layer. **other**—Reserved for new protocols. **all**—All protocols currently supported.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following examples entered in global configuration mode, display crypto accelerator statistics for specified protocols:

```
hostname # show crypto protocol statistics ikev1
[IKEv1 statistics]
   Encrypt packet requests: 39
   Encapsulate packet requests: 39
   Decrypt packet requests: 35
   Decapsulate packet requests: 35
   HMAC calculation requests: 84
   SA creation requests: 1
   SA rekey requests: 3
    SA deletion requests: 2
   Next phase key allocation requests: 2
   Random number generation requests: 0
    Failed requests: 0
```

```
hostname # show crypto protocol statistics ipsec
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
   Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0

hostname # show crypto protocol statistics ssl
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0

hostname # show crypto protocol statistics other
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0

hostname # show crypto protocol statistics all
[IKEv1 statistics]
   Encrypt packet requests: 46
   Encapsulate packet requests: 46
   Decrypt packet requests: 40
   Decapsulate packet requests: 40
   HMAC calculation requests: 91
    SA creation requests: 1
   SA rekey requests: 3
   SA deletion requests: 3
   Next phase key allocation requests: 2
   Random number generation requests: 0
   Failed requests: 0
[IKEv2 statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
    Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
```

```
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
    Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSH statistics are not supported]
[SRTP statistics are not supported]
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
    HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0
hostname #
```

Related Commands

Command	Description
clear crypto accelerator statistics	Clears the global and accelerator-specific statistics in the crypto accelerator MIB.
clear crypto protocol statistics	Clears the protocol-specific statistics in the crypto accelerator MIB.
show crypto accelerator statistics	Displays the global and accelerator-specific statistics from the crypto accelerator MIB.

show ctiqbe

To display information about CTIQBE sessions established across the security appliance, use the **show ctiqbe** command in privileged EXEC mode.

show ctiqbe

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.

Usage Guidelines

The **show ctiqbe** command displays information of CTIQBE sessions established across the security appliance. Along with **debug ctiqbe** and **show local-host**, this command is used for troubleshooting CTIQBE inspection engine issues.

Note We recommend that you have the **pager** command configured before using the **show ctiqbe** command. If there are a lot of CTIQBE sessions and the **pager** command is not configured, it can take a while for the **show ctiqbe** command output to reach the end.

Examples

The following is sample output from the **show ctiqbe** command under the following conditions. There is only one active CTIQBE session setup across the security appliance. It is established between an internal CTI device (for example, a Cisco IP SoftPhone) at local address 10.0.0.99 and an external Cisco Call Manager at 172.29.1.77, where TCP port 2748 is the Cisco CallManager. The heartbeat interval for the session is 120 seconds.

```
hostname# show ctiqbe

Total: 1
  LOCAL  FOREIGN  STATE  HEARTBEAT
-----------------------------------------------------------------
1  10.0.0.99/1117   172.29.1.77/2748  1  120
  RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028  1029)
```

```
|MEDIA: Device ID 27|Call ID 0
|Foreign 172.29.1.99|(1028|1029)
|Local|172.29.1.88|(26822|26823)
|-------------------------------------------
```

The CTI device has already registered with the CallManager. The device internal address and RTP listening port is PATed to 172.29.1.99 UDP port 1028. Its RTCP listening port is PATed to UDP 1029.

The line beginning with `RTP/RTCP: PAT xlates:` appears only if an internal CTI device has registered with an external CallManager and the CTI device address and ports are PATed to that external interface. This line does not appear if the CallManager is located on an internal interface, or if the internal CTI device address and ports are NATed to the same external interface that is used by the CallManager.

The output indicates a call has been established between this CTI device and another phone at 172.29.1.88. The RTP and RTCP listening ports of the other phone are UDP 26822 and 26823. The other phone locates on the same interface as the CallManager because the security appliance does not maintain a CTIQBE session record associated with the second phone and CallManager. The active call leg on the CTI device side can be identified with Device ID 27 and Call ID 0.

The following is the xlate information for these CTIBQE connections:

```
hostname# show xlate debug
3 in use, 3 most used
Flags: D|DNS, d|dump, I|identity, i|inside, n|no random,
|o|outside, r|portmap, s|static
TCP PAT from inside:10.0.0.99/1117 to outside:172.29.1.99/1025 flags ri idle 0:00:22
timeout 0:00:30
UDP PAT from inside:10.0.0.99/16908 to outside:172.29.1.99/1028 flags ri idle 0:00:00
timeout 0:04:10
UDP PAT from inside:10.0.0.99/16909 to outside:172.29.1.99/1029 flags ri idle 0:00:23
timeout 0:04:10
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
inspect ctiqbe	Enables CTIQBE application inspection.
service-policy	Applies a policy map to one or more interfaces.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

show curpriv

To display the current user privileges, use the **show curpriv** command:

show curpriv

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
Global configuration	•	•	—	—	•
Privileged EXEC	•	•	—	—	•
Unprivileged	•	•	—	—	•

Command History

Release	Modification
7.0	Modified to conform to CLI guidelines.

Usage Guidelines

The show curpriv command displays the current privilege level. Lower privilege level numbers indicate lower privilege levels.

Examples

These examples show output from the **show curpriv** command when a user named enable_15 is at different privilege levels. The username indicates the name that the user entered when the user logged in, P_PRIV indicates that the user has entered the **enable** command, and P_CONF indicates that the user has entered the **config terminal** command.

```
hostname(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
hostname(config)# exit

hostname(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
hostname(config)# exit

hostname(config)# show curpriv
Username : enable_1
```

```
Current privilege level : 1
Current Mode/s : P_UNPR
hostname(config)#
```

Related Commands

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

show debug

To show the current debugging configuration, use the **show debug** command.

show debug [*command* [*keywords*]]

Syntax Description

command	(Optional) Specifies the debug command whose current configuration you want to view. For each *command*, the syntax following *command* is identical to the syntax supported by the associated **debug** command. For example, valid *keywords* following **show debug aaa** are the same as the valid keywords for the **debug aaa** command. Thus, **show debug aaa** supports an **accounting** keyword, which allows you to specify that you want to see the debugging configuration for that portion of AAA debugging.

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
Preexisting	This command was preexisting.

Usage Guidelines

The valid *command* values follow. For information about valid syntax after *command*, see the entry for **debug** *command*, as applicable.

Note The availability of each *command* value depends upon the command modes that support the applicable **debug** command.

- **aaa**
- **appfw**
- **arp**
- **asdm**
- **context**
- **crypto**
- **ctiqbe**

- **ctm**
- **dhcpc**
- **dhcpd**
- **dhcprelay**
- **disk**
- **dns**
- **email**
- **entity**
- **fixup**
- **fover**
- **fsm**
- **ftp**
- **generic**
- **gtp**
- **h323**
- **http**
- **http-map**
- **icmp**
- **igmp**
- **ils**
- **imagemgr**
- **ipsec-over-tcp**
- **ipv6**
- **iua-proxy**
- **kerberos**
- **ldap**
- **mfib**
- **mgcp**
- **mrib**
- **ntdomain**
- **ntp**
- **ospf**
- **parser**
- **pim**
- **pix**
- **pptp**
- **radius**
- **rip**

- **rtsp**
- **sdi**
- **sequence**
- **sip**
- **skinny**
- **smtp**
- **sqlnet**
- **ssh**
- **ssl**
- **sunrpc**
- **tacacs**
- **timestamps**
- **vpn-sessiondb**
- **webvpn**
- **xdmcp**

Examples

The following commands enable debugging for authentication, accounting, and Flash memory. The **show debug** command is used in three ways to demonstrate how you can use it to view all debugging configuration, debugging configuration for a specific feature, and even debugging configuration for a subset of a feature.

```
hostname# debug aaa authentication
debug aaa authentication enabled at level 1
hostname# debug aaa accounting
debug aaa accounting enabled at level 1
hostname# debug disk filesystem
debug disk filesystem enabled at level 1
hostname# show debug
debug aaa authentication enabled at level 1
debug aaa accounting enabled at level 1
debug disk filesystem enabled at level 1
hostname# show debug aaa
debug aaa authentication enabled at level 1
debug aaa authorization is disabled.
debug aaa accounting enabled at level 1
debug aaa internal is disabled.
debug aaa vpn is disabled.
hostname# show debug aaa accounting
debug aaa accounting enabled at level 1
hostname#
```

Related Commands

Command	Description
debug	See all **debug** commands.

show dhcpd

To view DHCP binding, state, and statistical information, use the **show dhcpd** command in privileged EXEC or global configuration mode.

show dhcpd {**binding** [*IP_address*] | **state** | **statistics**}

Syntax Description

binding	Displays binding information for a given server IP address and its associated client hardware address and lease length.
IP_address	Shows the binding information for the specified IP address.
state	Displays the state of the DHCP server, such as whether it is enabled in the current context and whether it is enabled on each of the interfaces.
statistics	Displays statistical information, such as the number of address pools, bindings, expired bindings, malformed messages, sent messages, and received messages.

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.

Usage Guidelines

If you include the optional IP address in the **show dhcpd binding** command, only the binding for that IP address is shown.

The **show dhcpd binding | state | statistics** commands are also available in global configuration mode.

Examples

The following is sample output from the **show dhcpd binding** command:

```
hostname# show dhcpd binding
IP Address Hardware Address Lease Expiration Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds automatic
```

The following is sample output from the **show dhcpd state** command:

```
hostname# show dhcpd state
Context Not Configured for DHCP
Interface outside, Not Configured for DHCP
```

```
Interface inside, Not Configured for DHCP
```

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

```
hostname# show dhcpd statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Address pools        1
Automatic bindings   1
Expired bindings     1
Malformed messages   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         1
DHCPREQUEST          2
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            1
DHCPACK              1
DHCPNAK              1
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
clear dhcpd	Clears the DHCP server bindings and statistic counters.
dhcpd lease	Defines the lease length for DHCP information granted to clients.
show running-config dhcpd	Displays the current DHCP server configuration.

show dhcprelay state

To view the state of the DHCP relay agent, use the **show dhcprelay state** command in privileged EXEC or global configuration mode.

show dhcprelay state

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.

Usage Guidelines

This command displays the DHCP relay agent state information for the current context and each interface.

Examples

The following is sample output from the **show dhcprelay state** command:

```
hostname# show dhcprelay state

Context  Configured as DHCP Relay
Interface outside, Not Configured for DHCP
Interface infrastructure, Configured for DHCP RELAY SERVER
Interface inside, Configured for DHCP RELAY
```

Related Commands

Command	Description
show dhcpd	Displays DHCP server statistics and state information.
show dhcprelay statistics	Displays the DHCP relay statistics.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

show dhcprelay statistics

To display the DHCP relay statistics, use the **show dhcprelay statistics** command in privileged EXEC mode.

show dhcprelay 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.

Usage Guidelines

The output of the **show dhcprelay statistics** command increments until you enter the **clear dhcprelay statistics** command.

Examples

The following shows sample output for the **show dhcprelay statistics** command:

```
hostname# show dhcprelay statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Packets Relayed
BOOTREQUEST          0
DHCPDISCOVER         7
DHCPREQUEST          3
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

BOOTREPLY            0
DHCPOFFER            7
DHCPACK              3
DHCPNAK              0
FeralPix(config)#
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
clear dhcprelay statistics	Clears the DHCP relay agent statistic counters.
debug dhcprelay	Displays debug information for the DHCP relay agent.
show dhcprelay state	Displays the state of the DHCP relay agent.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

show disk

To display the contents of the Flash memory, use the **show disk** command in privileged EXEC mode. To view the Flash memory for a PIX security appliance, see the **show flash** command.

show disk[**0** | **1**] [**filesys** | **all**]

Syntax Description

**0	1**	Specifies the internal Flash memory (0, the default) or the external Flash memory (1).
filesys	Shows information about the compact Flash card.
all	Shows the contents of Flash memory plus the file system information,

Defaults

Shows the internal Flash memory by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following is sample output from the **show disk** command:

```
hostname# show disk
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 test1.cfg
 13 2551       Jan 06 2005 10:07:36 test2.cfg
 14 609223     Jan 21 2005 07:14:18 test3.cfg
 15 1619       Jul 16 2004 16:06:48 test4.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 test5.cfg
 20 1792       Jan 21 2005 07:29:24 test6.cfg
 21 7765184    Mar 07 2005 19:38:30 test7.cfg
 22 1674       Nov 11 2004 02:47:52 test8.cfg
 23 1863       Jan 21 2005 07:29:18 test9.cfg
 24 1197       Jan 19 2005 08:17:48 test10.cfg
 25 608554     Jan 13 2005 06:20:54 backupconfig.cfg
 26 5124096    Feb 20 2005 08:49:28 cdisk1
 27 5124096    Mar 01 2005 17:59:56 cdisk2
 28 2074       Jan 13 2005 08:13:26 test11.cfg
 29 5124096    Mar 07 2005 19:56:58 cdisk3
 30 1276       Jan 28 2005 08:31:58 lead
 31 7756788    Feb 24 2005 12:59:46 asdmfile.dbg
```

```
 32 7579792    Mar 08 2005 11:06:56 asdmfile1.dbg
 33 7764344    Mar 04 2005 12:17:46 asdmfile2.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk4
 35 15322      Mar 04 2005 12:30:24 hs_err.log

10170368 bytes available (52711424 bytes used)
```

The following is sample output from the **show disk filesys** command:

```
hostname# show disk filesys
******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184

COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
```

Related Commands

Command	Description
dir	Displays the directory contents.
show flash	Displays the contents of the internal Flash memory.

show dns-hosts

To show the DNS cache, use the **show dns-hosts** command in privileged EXEC mode.The DNS cache includes dynamically learned entries from a DNS server as well as manually entered name and IP addresses using the **name** command.

show dns-hosts

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	This command was introduced.

Usage Guidelines

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show dns-hosts** command:

```
hostname# show dns-hosts
Host                      Flags      Age Type   Address(es)
ns2.example.com           (temp, OK) 0    IP    10.102.255.44
ns1.example.com           (temp, OK) 0    IP    192.168.241.185
snowmass.example.com      (temp, OK) 0    IP    10.94.146.101
server.example.com        (temp, OK) 0    IP    10.94.146.80
```

Table 7-11 shows each field description.

Table 7-13 show dns-hosts Fields

Field	Description
Host	Shows the hostname.
Flags	Shows the entry status, as a combination of the following: • temp—This entry is temporary because it comes from a DNS server. The security appliance removes this entry after 72 hours of inactivity. • perm—This entry is permanent because it was added with the **name** command. • OK—This entry is valid. • ??—This entry is suspect and needs to be revalidated. • EX—This entry is expired.
Age	Shows the number of hours since this entry was last referenced.
Type	Shows the type of DNS record; this value is always IP.
Address(es)	The IP addresses.

Related Commands

Command	Description
clear dns-hosts cache	Clears the DNS cache.
dns domain-lookup	Enables the security appliance to perform a name lookup.
dns name-server	Configures a DNS server address.
dns retries	Specifies the number of times to retry the list of DNS servers when the security appliance does not receive a response.
dns timeout	Specifies the amount of time to wait before trying the next DNS server.

show failover

To display information about the failover status of the unit, use the **show failover** command in privileged EXEC mode.

show failover [**group** *num* | **history** | **interface** | **state** | **statistics**]

Syntax Description

group	Displays the running state of the specified failover group.
history	Displays failover history. The failover history displays past failover state changes and the reason for the state change.
interface	Displays failover command and stateful link information.
num	Failover group number.
state	Displays the failover state of both failover units. The information displayed includes the primary or secondary status of the unit, the Active/Standby status of the unit, and, if a unit is in the failed state, the reason for the failure.
statistics	Displays transmit and receive packet count of failover command 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**
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0	This command was modified. The output includes additional information.

Usage Guidelines

The **show failover** command displays the dynamic failover information, interface status, and Stateful Failover statistics. The Stateful Failover Logical Update Statistics output appears only when Stateful Failover is enabled. The “xerr” and “rerr” values do not indicate errors in failover, but rather the number of packet transmit or receive errors.

In the **show failover** command output, the fields have the following values:

- Stateful Obj has these values:
  - xmit—Indicates the number of packets transmitted.
  - xerr—Indicates the number of transmit errors.
  - rcv—Indicates the number of packets received.
  - rerr—Indicates the number of receive errors.

- Each row is for a particular object static count as follows:
  - General—Indicates the sum of all stateful objects.
  - sys cmd—Refers to the logical update system commands, such as **login** or **stay alive**.
  - up time—Indicates the value for the security appliance up time, which the active security appliance passes on to the standby security appliance.
  - RPC services—Remote Procedure Call connection information.
  - TCP conn—Dynamic TCP connection information.
  - UDP conn—Dynamic UDP connection information.
  - ARP tbl—Dynamic ARP table information.
  - Xlate_Timeout—Indicates connection translation timeout information.
  - VPN IKE upd—IKE connection information.
  - VPN IPSEC upd—IPSec connection information.
  - VPN CTCP upd—cTCP tunnel connection information.
  - VPN SDI upd—SDI AAA connection information.
  - VPN DHCP upd—Tunneled DHCP connection information.

If you do not enter a failover IP address, the **show failover** command displays 0.0.0.0 for the IP address, and monitoring of the interfaces remain in a "waiting" state. You must set a failover IP address for failover to work.

Table 7-14 describes the interface states for failover.

Table 7-14 Failover Interface States

State	Description
Normal	The interface is up and receiving hello packets from the corresponding interface on the peer unit.
Normal (Waiting)	The interface is up but has not yet received a hello packet from the corresponding interface on the peer unit. Verify that a standby IP address has been configured for the interface and that there is connectivity between the two interfaces.
Normal (Not-Monitored)	The interface is up but is not monitored by the failover process. The failure of an interface that is not monitored does not trigger failover.
No Link	The physical link is down.
No Link (Waiting)	The physical link is down and the interface has not yet received a hello packet from the corresponding interface on the peer unit. After restoring the link, verify that a standby IP address has been configured for the interface and that there is connectivity between the two interfaces.
No Link (Not-Monitored)	The physical link is down but is not monitored by the failover process. The failure of an interface that is not monitored does not trigger failover.
Link Down	The physical link is up, but the interface is administratively down.

Table 7-14 Failover Interface States (continued)

State	Description
Link Down (Waiting)	The physical link is up, but the interface is administratively down and the interface has not yet received a hello packet from the corresponding interface on the peer unit. After bringing the interface up (using the **no shutdown** command in interface configuration mode), verify that a standby IP address has been configured for the interface and that there is connectivity between the two interfaces.
Link Down (Not-Monitored)	The physical link is up, but the interface is administratively down but is not monitored by the failover process. The failure of an interface that is not monitored does not trigger failover.
Testing	The interface is in testing mode due to missed hello packets from the corresponding interface on the peer unit.
Failed	Interface testing has failed and the interface is marked as failed. If the interface failure causes the failover criteria to be met, then the interface failure causes a failover to the secondary unit or failover group.

In multiple configuration mode, only the **show failover** command is available in a security context; you cannot enter the optional keywords.

Examples

The following is sample output from the **show failover** command for Active/Standby Failover.

```
hostname# show failover

Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: fover Ethernet2 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
failover replication http
Last Failover at: 22:44:03 UTC Dec 8 2004
        This host: Primary - Active
                Active time: 13434 (sec)
                Interface inside (10.130.9.3): Normal
                Interface outside (10.132.9.3): Normal
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                Interface inside (10.130.9.4): Normal
                Interface outside (10.132.9.4): Normal

Stateful Failover Logical Update Statistics
        Link : fover Ethernet2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         1733       0          1733       0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        6          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         106        0          0          0
        Xlate_Timeout   0          0          0          0
        VPN IKE upd     15         0          0          0
```

```
        VPN IPSEC upd   90          0           0           0
        VPN CTCP upd    0           0           0           0
        VPN SDI upd     0           0           0           0
        VPN DHCP upd    0           0           0           0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       2       1733
        Xmit Q:         0       2       15225
```

The following is sample output from the **show failover** command for Active/Active Failover.

```
hostname# show failover

Failover On
Failover unit Primary
Failover LAN Interface: third GigabitEthernet0/2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 4 seconds
Interface Policy 1
Monitored Interfaces 8 of 250 maximum
failover replication http
Group 1 last failover at: 13:40:18 UTC Dec 9 2004
Group 2 last failover at: 13:40:06 UTC Dec 9 2004

  This host:    Primary
  Group 1       State:          Active
                Active time:    2896 (sec)
  Group 2       State:          Standby Ready
                Active time:    0 (sec)

                slot 0: ASA-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.11)S91(0.11)) status (Up)
                admin Interface outside (10.132.8.5): Normal
                admin Interface third (10.132.9.5): Normal
                admin Interface inside (10.130.8.5): Normal
                admin Interface fourth (10.130.9.5): Normal
                ctx1 Interface outside (10.1.1.1): Normal
                ctx1 Interface inside (10.2.2.1): Normal
                ctx2 Interface outside (10.3.3.2): Normal
                ctx2 Interface inside (10.4.4.2): Normal

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    190 (sec)
  Group 2       State:          Active
                Active time:    3322 (sec)

                slot 0: ASA-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.1)S91(0.1)) status (Up)
                admin Interface outside (10.132.8.6): Normal
                admin Interface third (10.132.9.6): Normal
                admin Interface inside (10.130.8.6): Normal
                admin Interface fourth (10.130.9.6): Normal
                ctx1 Interface outside (10.1.1.2): Normal
                ctx1 Interface inside (10.2.2.2): Normal
                ctx2 Interface outside (10.3.3.1): Normal
                ctx2 Interface inside (10.4.4.1): Normal

Stateful Failover Logical Update Statistics
        Link : third GigabitEthernet0/2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         380        0          380        0
```

```
up time         0          0          0          0
RPC services    0          0          0          0
TCP conn        1435       0          1450       0
UDP conn        0          0          0          0
ARP tbl         124        0          65         0
Xlate_Timeout   0          0          0          0
VPN IKE upd     15         0          0          0
VPN IPSEC upd   90         0          0          0
VPN CTCP upd    0          0          0          0
VPN SDI upd     0          0          0          0
VPN DHCP upd    0          0          0          0

Logical Update Queue Information
                Cur     Max     Total
Recv Q:         0       1       1895
Xmit Q:         0       0       1940
```

The following is sample output from the **show failover state** command for an active-active setup:

```
hostname(config)# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Secondary
    Group 1    Failed         Backplane Failure        03:42:29 UTC Apr 17 2009
    Group 2    Failed         Backplane Failure        03:42:29 UTC Apr 17 2009
Other host -   Primary
    Group 1    Active         Comm Failure             03:41:12 UTC Apr 17 2009
    Group 2    Active         Comm Failure             03:41:12 UTC Apr 17 2009

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

The following is sample output from the **show failover state** command for an active-standby setup:

```
hostname(config)# show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Negotiation    Backplane Failure        15:44:56 UTC Jun 20 2009
Other host -   Secondary
               Not Detected   Comm Failure             15:36:30 UTC Jun 20 2009

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

Table 7-15 describes the output of the **show failover state** command.

Table 7-15 show failover state Output Description

Field	Description
Configuration State	Displays the state of configuration synchronization. The following are possible configuration states for the standby unit: • **Config Syncing - STANDBY**—Set while the synchronized configuration is being executed. • **Interface Config Syncing - STANDBY** • **Sync Done - STANDBY**—Set when the standby unit has completed a configuration synchronization from the active unit. The following are possible configuration states for the active unit: • **Config Syncing**—Set on the active unit when it is performing a configuration synchronization to the standby unit. • **Interface Config Syncing** • **Sync Done**—Set when the active unit has completed a successful configuration synchronization to the standby unit. • **Ready for Config Sync**—Set on the active unit when the standby unit signals that it is ready to receive a configuration synchronization.
Communication State	Displays the status of the MAC address synchronization. • **Mac set**—The MAC addresses have been synchronized from the peer unit to this unit. • **Updated Mac**—Used when a MAC address is updated and needs to be synchronized to the other unit. Also used during the transition period where the unit is updating the local MAC addresses synchronized from the peer unit.
Date/Time	Displays a date and timestamp for the failure.
Last Failure Reason	Displays the reason for the last reported failure. This information is not cleared, even if the failure condition is cleared. This information changes only when a failover occurs. The following are possible fail reasons: • **Ifc Failure**—The number of interfaces that failed met the failover criteria and caused failover. • **Comm Failure**—The failover link failed or peer is down. • **Backplane Failure**
State	Displays the Primary/Secondary and Active/Standby status for the unit.
This host/Other host	This host indicates information for the device upon which the command was executed. Other host indicates information for the other device in the failover pair.

Related Commands

Command	Description
show running-config failover	Displays the **failover** commands in the current configuration.

show file

To display information about the file system, use the **show file** command in privileged EXEC mode.

show file descriptors | system | information *filename*

Syntax Description

descriptors	Displays all open file descriptors.
information	Displays information about a specific file.
filename	Specifies the filename.
system	Displays the size, bytes available, type of media, flags, and prefix information about the disk file system.

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	This command was introduced.

Examples

The following example shows how to display the file system information:

```
hostname# show file descriptors
No open file descriptors
hostname# show file system
File Systems:
   Size(b)     Free(b)    Type  Flags  Prefixes
* 60985344    60973056    disk    rw     disk:
```

Related Commands

Command	Description
dir	Displays the directory contents.
pwd	Displays the current working directory.

show firewall

To show the current firewall mode (routed or transparent), use the **show firewall** command in privileged EXEC mode.

show firewall

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	This command was introduced.

Examples

The following is sample output from the **show firewall** command:

```
hostname# show firewall
Firewall mode: Router
```

Related Commands

Command	Description
firewall transparent	Sets the firewall mode.
show mode	Shows the current context mode, either single or multiple.

show flash

To display the contents of the internal Flash memory, use the **show flash:** command in privileged EXEC mode.

show flash:

Note In the ASA 5500 series, the **flash** keyword is aliased to **disk0**.

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 example shows how to display the contents of the internal Flash memory:

```
hostname# show flash:
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 pepsi.cfg
 13 2551       Jan 06 2005 10:07:36 Leo.cfg
 14 609223     Jan 21 2005 07:14:18 rr.cfg
 15 1619       Jul 16 2004 16:06:48 hackers.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 admin.cfg
 20 1792       Jan 21 2005 07:29:24 Marketing.cfg
 21 7765184    Mar 07 2005 19:38:30 asdmfile-RLK
 22 1674       Nov 11 2004 02:47:52 potts.cfg
 23 1863       Jan 21 2005 07:29:18 r.cfg
 24 1197       Jan 19 2005 08:17:48 tst.cfg
 25 608554     Jan 13 2005 06:20:54 500kconfig
 26 5124096    Feb 20 2005 08:49:28 cdisk70102
 27 5124096    Mar 01 2005 17:59:56 cdisk70104
 28 2074       Jan 13 2005 08:13:26 negateACL
 29 5124096    Mar 07 2005 19:56:58 cdisk70105
 30 1276       Jan 28 2005 08:31:58 steel
 31 7756788    Feb 24 2005 12:59:46 asdmfile.50074.dbg
```

```
 32 7579792    Mar 08 2005 11:06:56 asdmfile.gusingh
 33 7764344    Mar 04 2005 12:17:46 asdmfile.50075.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk70103
 35 15322      Mar 04 2005 12:30:24 hs_err_pid2240.log

10170368 bytes available (52711424 bytes used)
```

Related Commands

Command	Description
dir	Displays the directory contents.
show disk0	Displays the contents of the internal Flash memory.
show disk1	Displays the contents of the external Flash memory card.

show fragment

To display the operational data of the IP fragment reassembly module, enter the **show fragment** command in privileged EXEC mode.

show fragment [*interface*]

Syntax Description

interface	(Optional) Specifies the security appliance interface.

Defaults

If an *interface* is not specified, the command applies to 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
Privileged EXEC mode	•	•	•	•	

Command History

Release	Modification
7.0	The command was separated into two commands, **show fragment** and **show running-config fragment**, to separate the configuration data from the operational data.

Examples

This example shows how to display the operational data of the IP fragment reassembly module:

```
hostname# show fragment
Interface: inside
    Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: outside1
    Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test1
    Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test2
    Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
```

Related Commands

Command	Description
clear configure fragment	Clears the IP fragment reassembly configuration and resets the defaults.
clear fragment	Clears the operational data of the IP fragment reassembly module.

Command	Description
fragment	Provides additional management of packet fragmentation and improves compatibility with NFS.
show running-config fragment	Displays the IP fragment reassembly configuration.

show gc

To display the garbage collection process statistics, use the **show gc** command in privileged EXEC mode.

show gc

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
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following is sample output from the **show gc** command:

```
hostname# show gc

Garbage collection process stats:
Total tcp conn delete response             :            0
Total udp conn delete response             :            0
Total number of zombie cleaned             :            0
Total number of embryonic conn cleaned     :            0
Total error response                       :            0
Total queries generated                    :            0
Total queries with conn present response   :            0
Total number of sweeps                     :          946
Total number of invalid vcid               :            0
Total number of zombie vcid                :            0
```

Related Commands

Command	Description
clear gc	Removes the garbage collection process statistics.

show h225

To display information for H.225 sessions established across the security appliance, use the **show h225** command in privileged EXEC mode.

show h225

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.

Usage Guidelines

The **show h225** command displays information for H.225 sessions established across the security appliance. Along with the **debug h323 h225 event**, **debug h323 h245 event**, and **show local-host** commands, this command is used for troubleshooting H.323 inspection engine issues.

Before using the **show h225**, **show h245**, or **show h323-ras** commands, we recommend that you configure the **pager** command. If there are a lot of session records and the **pager** command is not configured, it may take a while for the **show** output to reach its end. If there is an abnormally large number of connections, check that the sessions are timing out based on the default timeout values or the values set by you. If they are not, then there is a problem that needs to be investigated.

Examples

The following is sample output from the **show h225** command:

```
hostname# show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
| Local: | 10.130.56.3/1040 | Foreign: 172.30.254.203/1720
| 1. CRV 9861
| Local: | 10.130.56.3/1040 | Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
| Local: | 10.130.56.4/1050 | Foreign: 172.30.254.205/1720
```

This output indicates that there is currently 1 active H.323 call going through the security appliance between the local endpoint 10.130.56.3 and foreign host 172.30.254.203, and for these particular endpoints, there is 1 concurrent call between them, with a CRV (Call Reference Value) for that call of 9861.

For the local endpoint 10.130.56.4 and foreign host 172.30.254.205, there are 0 concurrent Calls. This means that there is no active call between the endpoints even though the H.225 session still exists. This could happen if, at the time of the **show h225** command, the call has already ended but the H.225 session has not yet been deleted. Alternately, it could mean that the two endpoints still have a TCP connection opened between them because they set "maintainConnection" to TRUE, so the session is kept open until they set it to FALSE again, or until the session times out based on the H.225 timeout value in your configuration.

Related Commands

Commands	Description
debug h323	Enables the display of debug information for H.323.
inspect h323	Enables H.323 application inspection.
show h245	Displays information for H.245 sessions established across the security appliance by endpoints using slow start.
show h323-ras	Displays information for H.323 RAS sessions established across the security appliance.
timeout h225 | h323	Configures idle time after which an H.225 signalling connection or an H.323 control connection will be closed.

show h245

To display information for H.245 sessions established across the security appliance by endpoints using slow start, use the **show h245** command in privileged EXEC mode.

show h245

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.

Usage Guidelines

The **show h245** command displays information for H.245 sessions established across the security appliance by endpoints using slow start. (Slow start is when the two endpoints of a call open another TCP control channel for H.245. Fast start is where the H.245 messages are exchanged as part of the H.225 messages on the H.225 control channel.) Along with the **debug h323 h245 event**, **debug h323 h225 event**, and **show local-host** commands, this command is used for troubleshooting H.323 inspection engine issues.

Examples

The following is sample output from the **show h245** command:

```
hostname# show h245
Total: 1
  | LOCAL | TPKT | FOREIGN | TPKT
1 | 10.130.56.3/1041 | 0 | 172.30.254.203/1245 | 0
  | MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
  | Local | 10.130.56.3 RTP 49608 RTCP 49609
  | MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
  | Local | 10.130.56.3 RTP 49606 RTCP 49607
```

There is currently one H.245 control session active across the security appliance. The local endpoint is 10.130.56.3, and we are expecting the next packet from this endpoint to have a TPKT header because the TPKT value is 0. (The TKTP header is a 4-byte header preceding each H.225/H.245 message. It gives

the length of the message, including the 4-byte header.) The foreign host endpoint is 172.30.254.203, and we are expecting the next packet from this endpoint to have a TPKT header because the TPKT value is 0.

The media negotiated between these endpoints have a LCN (logical channel number) of 258 with the foreign RTP IP address/port pair of 172.30.254.203/49608 and a RTCP IP address/port of 172.30.254.203/49609 with a local RTP IP address/port pair of 10.130.56.3/49608 and a RTCP port of 49609.

The second LCN of 259 has a foreign RTP IP address/port pair of 172.30.254.203/49606 and a RTCP IP address/port pair of 172.30.254.203/49607 with a local RTP IP address/port pair of 10.130.56.3/49606 and RTCP port of 49607.

Related Commands

Commands	Description
debug h323	Enables the display of debug information for H.323.
inspect h323	Enables H.323 application inspection.
show h245	Displays information for H.245 sessions established across the security appliance by endpoints using slow start.
show h323-ras	Displays information for H.323 RAS sessions established across the security appliance.
timeout h225 | h323	Configures idle time after which an H.225 signalling connection or an H.323 control connection will be closed.

show h323-ras

To display information for H.323 RAS sessions established across the security appliance between a gatekeeper and its H.323 endpoint, use the **show h323-ras** command in privileged EXEC mode.

show h323-ras

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.

Usage Guidelines

The **show h323-ras** command displays information for H.323 RAS sessions established across the security appliance between a gatekeeper and its H.323 endpoint. Along with the **debug h323 ras event** and **show local-host** commands, this command is used for troubleshooting H.323 RAS inspection engine issues.

The **show h323-ras** command displays connection information for troubleshooting H.323 inspection engine issues, and is described in the **inspect protocol h323 {h225 | ras}** command page.

Examples

The following is sample output from the **show h323-ras** command:

```
hostname# show h323-ras
Total: 1
| GK | Caller
| 172.30.254.214 10.130.56.14
```

This output shows that there is one active registration between the gatekeeper 172.30.254.214 and its client 10.130.56.14.

Related Commands

Commands	Description
debug h323	Enables the display of debug information for H.323.
inspect h323	Enables H.323 application inspection.
show h245	Displays information for H.245 sessions established across the security appliance by endpoints using slow start.
show h323-ras	Displays information for H.323 RAS sessions established across the security appliance.
timeout h225 | h323	Configures idle time after which an H.225 signalling connection or an H.323 control connection will be closed.

show history

To display the previously entered commands, use the **show history** command in user EXEC mode.

show history

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
User EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show history** command lets you display previously entered commands. You can examine commands individually with the up and down arrows, enter **^p** to display previously entered lines, or enter **^n** to display the next line.

Examples

The following example shows how to display previously entered commands when you are in user EXEC mode:

```
hostname> show history
    show history
    help
    show history
```

The following example shows how to display previously entered commands in privileged EXEC mode:

```
hostname# show history
    show history
    help
    show history
    enable
    show history
```

This example shows how to display previously entered commands in global configuration mode:

```
hostname(config)# show history
    show history
    help
```

```
show history
enable
show history
config t
show history
```

Related Commands

Command	Description
help	Displays help information for the command specified.

show icmp

To display the ICMP configuration, use the **show icmp** command in privileged EXEC mode.

show icmp

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 previously existing.

Usage Guidelines

The **show icmp** command displays the ICMP configuration.

Examples

The following example shows the ICMP configuration:

```
hostname# show icmp
```

Related Commands

clear configure icmp	Clears the ICMP configuration.
debug icmp	Enables the display of debug information for ICMP.
icmp	Configures access rules for ICMP traffic that terminates at a security appliance interface.
inspect icmp	Enables or disables the ICMP inspection engine.
timeout icmp	Configures the idle timeout for ICMP.

show idb

To display information about the status of interface descriptor blocks, use the **show idb** command in privileged EXEC mode.

show idb

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:

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

IDBs are the internal data structure representing interface resources. See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show idb** command:

```
hostname# show idb
Maximum number of Software IDBs 280.  In use 23.

                    HWIDBs     SWIDBs
             Active 6          21
           Inactive 1          2
         Total IDBs 7          23
 Size each (bytes) 116        212
        Total bytes 812        4876

HWIDB#   1 0xbb68ebc  Control0/0
HWIDB#   2 0xcd47d84  GigabitEthernet0/0
HWIDB#   3 0xcd4c1dc  GigabitEthernet0/1
HWIDB#   4 0xcd5063c  GigabitEthernet0/2
HWIDB#   5 0xcd54a9c  GigabitEthernet0/3
HWIDB#   6 0xcd58f04  Management0/0

SWIDB#   1 0x0bb68f54 0x01010001 Control0/0
SWIDB#   2 0x0cd47e1c 0xffffffff GigabitEthernet0/0
SWIDB#   3 0x0cd772b4 0xffffffff GigabitEthernet0/0.1
```

```
  PEER IDB#  1 0x0d44109c 0xffffffff     3  GigabitEthernet0/0.1
  PEER IDB#  2 0x0d2c0674 0x00020002     2  GigabitEthernet0/0.1
  PEER IDB#  3 0x0d05a084 0x00010001     1  GigabitEthernet0/0.1
SWIDB#  4 0x0bb7501c 0xffffffff GigabitEthernet0/0.2
SWIDB#  5 0x0cd4c274 0xffffffff GigabitEthernet0/1
SWIDB#  6 0x0bb75704 0xffffffff GigabitEthernet0/1.1
  PEER IDB#  1 0x0cf8686c 0x00020003     2  GigabitEthernet0/1.1
SWIDB#  7 0x0bb75dec 0xffffffff GigabitEthernet0/1.2
  PEER IDB#  1 0x0d2c08ac 0xffffffff     2  GigabitEthernet0/1.2
SWIDB#  8 0x0bb764d4 0xffffffff GigabitEthernet0/1.3
  PEER IDB#  1 0x0d441294 0x00030001     3  GigabitEthernet0/1.3
SWIDB#  9 0x0cd506d4 0x01010002 GigabitEthernet0/2
SWIDB# 10 0x0cd54b34 0xffffffff GigabitEthernet0/3
  PEER IDB#  1 0x0d3291ec 0x00030002     3  GigabitEthernet0/3
  PEER IDB#  2 0x0d2c0aa4 0x00020001     2  GigabitEthernet0/3
  PEER IDB#  3 0x0d05a474 0x00010002     1  GigabitEthernet0/3
SWIDB# 11 0x0cd58f9c 0xffffffff Management0/0
  PEER IDB#  1 0x0d05a65c 0x00010003     1  Management0/0
```

Table 7-11 shows each field description.

Table 7-16 show idb stats Fields

Field	Description
HWIDBs	Shows the statistics for all HWIDBs. HWIDBs are created for each hardware port in the system.
SWIDBs	Shows the statistics for all SWIDBs. SWIDBs are created for each main and subinterface in the system, and for each interface that is allocated to a context. Some other internal software modules also create IDBs.
HWIDB#	Specifies a hardware interface entry. The IDB sequence number, address, and interface name is displayed in each line.
SWIDB#	Specifies a software interface entry. The IDB sequence number, address, corresponding vPif id, and interface name are displayed in each line.
PEER IDB#	Specifies an interface allocated to a context. The IDB sequence number, address, corresponding vPif id, context id and interface name are displayed in each line.

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.

show igmp groups

To display the multicast groups with receivers that are directly connected to the security appliance and that were learned through IGMP, use the **show igmp groups** command in privileged EXEC mode.

show igmp groups [[**reserved** | *group*] [*if_name*] [**detail**]] | **summary**]

Syntax Description

detail	(Optional) Provides a detailed description of the sources.
group	(Optional) The address of an IGMP group. Including this optional argument limits the display to the specified group.
if_name	(Optional) Displays group information for the specified interface.
reserved	(Optional) Displays information about reserved groups.
summary	(Optional) Displays group joins summary information.

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	This command was introduced.

Usage Guidelines

If you omit all optional arguments and keywords, the **show igmp groups** command displays all directly connected multicast groups by group address, interface type, and interface number.

Examples

The following is sample output from the **show igmp groups** command:

```
hostname#show igmp groups

IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
224.1.1.1        inside               00:00:53  00:03:26  192.168.1.6
```

Related Commands

Command	Description
show igmp interface	Displays multicast information for an interface.

show igmp interface

To display multicast information for an interface, use the **show igmp interface** command in privileged EXEC mode.

show igmp interface [*if_name*]

Syntax Description

if_name	(Optional) Displays IGMP group information for the selected 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
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was modified. The **detail** keyword was removed.

Usage Guidelines

If you omit the optional *if_name* argument, the **show igmp interface** command displays information about all interfaces.

Examples

The following is sample output from the **show igmp interface** command:

```
hostname# show igmp interface inside

inside is up, line protocol is up
 Internet address is 192.168.37.6, subnet mask is 255.255.255.0
 IGMP is enabled on interface
 IGMP query interval is 60 seconds
 Inbound IGMP access group is not set
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 192.168.37.33
 No multicast groups joined
```

Related Commands

Command	Description
show igmp groups	Displays the multicast groups with receivers that are directly connected to the security appliance and that were learned through IGMP.

show igmp traffic

To display IGMP traffic statistics, use the **show igmp traffic** command in privileged EXEC mode.

show igmp traffic

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	This command was introduced.

Examples

The following is sample output from the **show igmp traffic** command:

```
hostname# show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 00:02:30
                             Received     Sent
Valid IGMP Packets              3           6
Queries                         2           6
Reports                         1           0
Leaves                          0           0
Mtrace packets                  0           0
DVMRP packets                   0           0
PIM packets                     0           0

Errors:
Malformed Packets               0
Martian source                  0
Bad Checksums                   0
```

Related Commands

Command	Description
clear igmp counters	Clears all IGMP statistic counters.
clear igmp traffic	Clear the IGMP traffic counters.

show interface

To view interface statistics, use the **show interface** command in user EXEC mode.

show interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*] [**stats** | **detail**]

Syntax Description

detail	(Optional) Shows detailed interface information, including the order in which the interface was added, the configured state, the actual state, and asymmetrical routing statistics, if enabled by the **asr-group** command. If you show all interfaces, then information about the internal interfaces for SSMs displays, if installed on the ASA 5500 series adaptive security appliance. The internal interface is not user-configurable, and the information is for debugging purposes only.
interface_name	(Optional) Identifies the interface name set with the **nameif** command.
mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
stats	(Default) Shows interface information and statistics. This keyword is the default, so this keyword is optional.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

If you do not identify any options, this command shows basic statistics 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**
User EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was modified to include the new interface numbering scheme, and to add the **stats** keyword for clarity, and the **detail** keyword.
7.0(4)	This command added support for the 4GE SSM interfaces.

Usage Guidelines

If an interface is shared among contexts, and you enter this command within a context, the security appliance shows only statistics for the current context. When you enter this command in the system execution space for a physical interface, the security appliance shows the combined statistics for all contexts.

The number of statistics shown for subinterfaces is a subset of the number of statistics shown for a physical interface.

You cannot use the interface name in the system execution space, because the **nameif** command is only available within a context. Similarly, if you mapped the interface ID to a mapped name using the **allocate-interface** command, you can only use the mapped name in a context. If you set the **visible** keyword in the **allocate-interface** command, the security appliance shows the interface ID in the output of the **show interface** command.

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show interface** command:

```
hostname> show interface
Interface GigabitEthernet0/0 "", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        Available but not configured via nameif
        MAC address 000f.f775.540e, MTU not set
        IP address unassigned
        752 packets input, 173435 bytes, 0 no buffer
        Received 752 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        752 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/6) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
Interface Management0/0 "intm00", is up, line protocol is up
  Hardware is i82557, BW 100 Mbps
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 000f.f775.5412, MTU 1500
        IP address unassigned
        751 packets input, 170487 bytes, 0 no buffer
        Received 753 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/1)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
        Received 738 VLAN untagged packets, 156831 bytes
        Transmitted 0 VLAN untagged packets, 0 bytes
        Dropped 413 VLAN untagged packets
        Management-only interface. Blocked 0 through-the-device packets
                0 IPv4 packets originated from management network
                0 IPv4 packets destined to management network
                0 IPv6 packets originated from management network
                0 IPv6 packets destined to management network
Interface GigabitEthernet1/0 "intg10", is down, line protocol is down
  Hardware is VCS7380 rev01, BW 1000 Mbps
        Auto-Duplex, Auto-Speed
        Media-type configured as RJ45 connector
        MAC address 000b.fcff.b548, MTU 1500
        IP address 17.1.9.115, subnet mask 255.0.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 rate limit drops
        input queue (curr/max blocks): hardware (0/0) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
        Received 0 VLAN untagged packets, 0 bytes
        Transmitted 0 VLAN untagged packets, 0 bytes
        Dropped 0 VLAN untagged packets
...
```

Table 7-11 shows each field description.

Table 7-17 show interface Fields

Field	Description
Interface *ID*	The interface ID. Within a context, the security appliance shows the mapped name (if configured), unless you set the **allocate-interface** command **visible** keyword.
"*interface_name*"	The interface name set with the **nameif** command. In the system execution space, this field is blank because you cannot set the name in the system. If you do not configure a name, the following message appears after the Hardware line: `Available but not configured via nameif`
is *state*	The administrative state, as follows: • up—The interface is not shut down. • administratively down—The interface is shut down with the **shutdown** command.
Line protocol is *state*	The line status, as follows: • up—A working cable is plugged into the network interface. • down—Either the cable is incorrect or not plugged into the interface connector.
VLAN identifier	For subinetrfaces, the VLAN ID.
Hardware	The interface type, maximum bandwidth, duplex, and speed. When the link is down, the duplex and speed show the configured values. When the link is up, these fields show the configured values with the actual settings in parentheses. The following list describes the common hardware types: • i82542 - Intel PCI Fiber Gigabit card used on PIX platforms • i82543 - Intel PCI-X Fiber Gigabit card used on PIX platforms • i82546GB - Intel PCI-X Copper Gigabit used on ASA platforms • i82547GI - Intel CSA Copper Gigabit used as backplane on ASA platforms • i82557 - Intel PCI Copper Fast Ethernet used on ASA platforms • i82559 - Intel PCI Copper Fast Ethernet used on PIX platforms • VCS7380 - Vitesse Four Port Gigabit Switch used in SSM-4GE
Media-type	(For 4GE SSM interfaces only) Shows if the interface is set as RJ-45 or SFP.

Table 7-17 show interface Fields (continued)

Field	Description

message area	A message might be displayed in some circumstances. See the following examples:
	• In the system execution space, you might see the following message:
	`Available for allocation to a context`
	• If you do not configure a name, you see the following message:
	`Available but not configured via nameif`

MAC address	The interface MAC address.
MTU	The maximum size, in bytes, of packets allowed on this interface. If you do not set the interface name, this field shows "MTU not set."
IP address	The interface IP address set using the **ip address** command or received from a DHCP server. In the system execution space, this field shows "IP address unassigned" because you cannot set the IP address in the system.
Subnet mask	The subnet mask for the IP address.
Packets input	The number of packets received on this interface.
Bytes	The number of bytes received on this interface.
No buffer	The number of received packets discarded because there was no buffer space in the main system. Compare this with the ignored count. Broadcast storms on Ethernet networks are often responsible for no input buffer events.
Received:	
Broadcasts	The number of broadcasts received.
Input errors	The number of total input errors, including the types listed below. Other input-related errors can also cause the input error count to increase, and some datagrams might have more than one error; therefore, this sum might exceed the number of errors listed for the types below.
Runts	The number of packets that are discarded because they are smaller than the minimum packet size, which is 64 bytes. Runts are usually caused by collisions. They might also be caused by poor wiring and electrical interference.
Giants	The number of packets that are discarded because they exceed the maximum packet size. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
CRC	The number of Cyclical Redundancy Check errors. When a station sends a frame, it appends a CRC to the end of the frame. This CRC is generated from an algorithm based on the data in the frame. If the frame is altered between the source and destination, the security appliance notes that the CRC does not match. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
Frame	The number of frame errors. Bad frames include packets with an incorrect length or bad frame checksums. This error is usually the result of collisions or a malfunctioning Ethernet device.
Overrun	The number of times that the security appliance was incapable of handing received data to a hardware buffer because the input rate exceeded the security appliance capability to handle the data.

Table 7-17 show interface Fields (continued)

Field	Description
Ignored	This field is not used. The value is always 0.
Abort	This field is not used. The value is always 0.
L2 decode drops	The number of packets dropped because the name is not configured (**nameif** command) or a frame with an invalid VLAN id is received.
Packets output	The number of packets sent on this interface.
Bytes	The number of bytes sent on this interface.
Underruns	The number of times that the transmitter ran faster than the security appliance could handle.
Output Errors	The number of frames not transmitted because the configured maximum number of collisions was exceeded. This counter should only increment during heavy network traffic.
Collisions	The number of messages retransmitted due to an Ethernet collision (single and multiple collisions). This usually occurs on an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once by the output packets.
Interface resets	The number of times an interface has been reset. If an interface is unable to transmit for three seconds, the security appliance resets the interface to restart transmission. During this interval, connection state is maintained. An interface reset can also happen when an interface is looped back or shut down.
Babbles	Unused. ("babble" means that the transmitter has been on the interface longer than the time taken to transmit the largest frame.)
Late collisions	The number of frames that were not transmitted because a collision occurred outside the normal collision window. A late collision is a collision that is detected late in the transmission of the packet. Normally, these should never happen. When two Ethernet hosts try to talk at once, they should collide early in the packet and both back off, or the second host should see that the first one is talking and wait. If you get a late collision, a device is jumping in and trying to send the packet on the Ethernet while the security appliance is partly finished sending the packet. The security appliance does not resend the packet, because it may have freed the buffers that held the first part of the packet. This is not a real problem because networking protocols are designed to cope with collisions by resending packets. However, late collisions indicate a problem exists in your network. Common problems are large repeated networks and Ethernet networks running beyond the specification.
Deferred	The number of frames that were deferred before transmission due to activity on the link.
Rate limit drops	(For 4GE SSM interfaces only) The number of packets dropped if you configured the interface at non-Gigabit speeds and attempted to transmit more than 10 Mbps or 100 Mbps, depending on configuration..
Lost carrier	The number of times the carrier signal was lost during transmission.
No carrier	Unused.

Table 7-17 show interface Fields (continued)

Field	Description
Input queue (curr/max blocks):	The number of packets in the input queue, the current and the maximum.
Hardware	The number of packets in the hardware queue.
Software	The number of packets in the software queue.
Output queue (curr/max blocks):	The number of packets in the output queue, the current and the maximum.
Hardware	The number of packets in the hardware queue.
Software	The number of packets in the software queue.
Received [VLAN untagged] packets	For a physical interface, the number of untagged VLAN packets received, and the number of bytes. For a subinterface, the number of packets received that are tagged with the correct VLAN.
Transmitted [VLAN untagged] packets	For a physical interface, the number of untagged VLAN packets transmitted, and the number of bytes. For a subinterface, the number of packets transmitted that are tagged with the correct VLAN.
Dropped [VLAN untagged] packets	For a physical interface, the number of untagged VLAN packets dropped. For a subinterface, the number of packets dropped that are tagged with the correct VLAN.

The following is sample output from the **show interface detail** command. The following example shows detailed interface statistics for all interfaces, including the internal interfaces (if present for your platform) and asymmetrical routing statistics, if enabled by the **asr-group** command:

```
hostname> show interface detail
Interface GigabitEthernet0/0 "", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        Available but not configured via nameif
        MAC address 000f.f775.540e, MTU not set
        IP address unassigned
        752 packets input, 173435 bytes, 0 no buffer
        Received 752 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        752 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/6) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
        Control Point Interface States:
                Interface number is unassigned
Interface Internal-Data0/0 "", is up, line protocol is up
  Hardware is i82547GI rev00, BW 1000 Mbps
        (Full-duplex), (1000 Mbps)
        MAC address 0000.0001.0002, MTU not set
        IP address unassigned
        6 packets input, 1094 bytes, 0 no buffer
        Received 6 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
        0 L2 decode drops, 0 demux drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/2) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
        Control Point Interface States:
                Interface number is unassigned
Interface Management0/0 "intm00", is up, line protocol is up
  Hardware is i82557, BW 100 Mbps
        Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
        MAC address 000f.f775.5412, MTU 1500
        IP address unassigned
        751 packets input, 170487 bytes, 0 no buffer
        Received 753 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/1)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
        Received 738 VLAN untagged packets, 156831 bytes
        Transmitted 0 VLAN untagged packets, 0 bytes
        Dropped 413 VLAN untagged packets
        Management-only interface. Blocked 0 through-the-device packets
                0 IPv4 packets originated from management network
                0 IPv4 packets destined to management network
                0 IPv6 packets originated from management network
                0 IPv6 packets destined to management network
        Control Point Interface States:
                Interface number is 1
                Interface config status is active
                Interface state is active
Interface GigabitEthernet1/0 "intg10", is down, line protocol is down
  Hardware is VCS7380 rev01, BW 1000 Mbps
        Auto-Duplex, Auto-Speed
        Media-type configured as RJ45 connector
        MAC address 000b.fcff.b548, MTU 1500
        IP address 17.1.9.115, subnet mask 255.0.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 rate limit drops
        input queue (curr/max blocks): hardware (0/0) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
        Received 0 VLAN untagged packets, 0 bytes
        Transmitted 0 VLAN untagged packets, 0 bytes
        Dropped 0 VLAN untagged packets
        Control Point Interface States:
                Interface number is 2
                Interface config status is active
                Interface state is not active
...
```

Table 7-16 shows each field description for the **show interface detail** command. See Table 7-11 for fields that are also shown for the **show interface** command.

Table 7-18 show interface detail Fields

Field	Description
Demux drops	(On Internal-Data interface only) The number of packets dropped because the security appliance was unable to demultiplex packets from SSM interfaces. SSM interfaces communicate with the native interfaces across the backplane, and packets from all SSM interfaces are multiplexed on the backplane.
Control Point Interface States:	
Interface number	A number used for debugging that indicates in what order this interface was created, starting with 0.
Interface config status	The administrative state, as follows: • active—The interface is not shut down. • not active—The interface is shut down with the **shutdown** command.
Interface state	The actual state of the interface. In most cases, this state matches the config status above. If you configure high availability, it is possible there can be a mismatch because the security appliance brings the interfaces up or down as needed.
Asymmetrical Routing Statistics:	
Received X1 packets	Number of ASR packets received on this interface.
Transmitted X2 packets	Number of ASR packets sent on this interfaces.
Dropped X3 packets	Number of ASR packets dropped on this interface. The packets might be dropped if the interface is down when trying to forward the packet.

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
clear interface	Clears counters for the **show interface** command.
interface	Configures an interface and enters interface configuration mode.
nameif	Sets the interface name.
show interface ip brief	Shows the interface IP address and status.

show interface ip brief

To view interface IP addresses and status, use the **show interface ip brief** command in privileged EXEC mode.

show interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*] **ip brief**

Syntax Description

interface_name	(Optional) Identifies the interface name set with the **nameif** command.
mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

If you do not specify an interface, the security appliance shows 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
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

In multiple context mode, if you mapped the interface ID in the **allocate-interface** command, you can only specify the mapped name or the interface name in a context.

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show ip brief** command:

```
hostname# show interface ip brief
    Interface                  IP-Address      OK? Method  Status                Protocol
    Control0/0                 127.0.1.1       YES CONFIG  up                    up
    GigabitEthernet0/0         209.165.200.226 YES CONFIG  up                    up
    GigabitEthernet0/1         unassigned      YES unset   administratively down down
    GigabitEthernet0/2         10.1.1.50       YES manual  administratively down down
    GigabitEthernet0/3         192.168.2.6     YES DHCP    administratively down down
    Management0/0              209.165.201.3   YES CONFIG  up
```

Table 7-16 shows each field description.

Table 7-19 show interface ip brief Fields

Field	Description
Interface	The interface ID or, in multiple context mode, the mapped name if you configured it using the **allocate-interface** command. If you show all interfaces, then information about the internal interface for the AIP SSM displays, if installed on the ASA adaptive security appliance. The internal interface is not user-configurable, and the information is for debugging purposes only.
IP-Address	The interface IP address.
OK?	This column is not currently used, and always shows "Yes."
Method	The method by which the interface received the IP address. Values include the following: • unset—No IP address configured. • manual—Configured the running configuration. • CONFIG—Loaded from the startup configuration. • DHCP—Received from a DHCP server.
Status	The administrative state, as follows: • up—The interface is not shut down. • administratively down—The interface is shut down with the **shutdown** command.
Protocol	The line status, as follows: • up—A working cable is plugged into the network interface. • down—Either the cable is incorrect or not plugged into the interface connector.

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
interface	Configures an interface and enters interface configuration mode.
ip address	Sets the IP address for the interface or sets the management IP address for a transparent firewall.
nameif	Sets the interface name.
show interface	Displays the runtime status and statistics of interfaces.

show inventory

To display information about all of the Cisco products installed in the networking device that are assigned a product identifier (PID), version identifier (VID), and serial number (SN), use the **show inventory** command in user EXEC or privileged EXEC mode. If a Cisco entity is not assigned a PID, that entity is not retrieved or displayed.

show inventory [**slot**]

Syntax Description

slot	(Optional) Specifies the SSM slot number (the system is slot 0)

Defaults

If you do not specify a slot to show inventory for:

- Show inventory information of all SSMs (including for power supply)

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	Minor semantic changes.

Usage Guidelines

The **show inventory** command retrieves and displays inventory information about each Cisco product in the form of a UDI. The UDI is a combination of three separate data elements: a product identifier (PID), a version identifier (VID), and the serial number (SN).

The PID is the name by which the product can be ordered; it has been historically called the "Product Name" or "Part Number." This is the identifier that one would use to order an exact replacement part.

The VID is the version of the product. Whenever a product has been revised, the VID will be incremented. The VID is incremented according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product will carry a unique serial number assigned at the factory, which cannot be changed in the field. This is the means by which to identify an individual, specific instance of a product.

The UDI refers to each product as an entity. Some entities, such as a chassis, will have subentities like slots. Each entity will display on a separate line in a logically ordered presentation that is arranged hierarchically by Cisco entities.

Use the **show inventory** command without options to display a list of Cisco entities installed in the networking device that are assigned a PID.

Examples

The following is sample output from the **show inventory** command without any keywords or arguments. This sample output displays a list of Cisco entities installed in a router that are assigned a PID.

```
ciscoasa# show inventory
Name:"Chassis", DESCR:"ASA 5540 Adaptive Security Appliance"
PID:ASA5540           , VID:V01 , SN:P3000000998

Name:"slot 1", DESCR:"ASA 5500 Series Security Services Module-20"
PID:ASA-SSM-20        , VID:V01 , SN:P0000000999

Name:"power supply", DESCR:"ASA 5500 Series 180W AC Power Supply"
PID:ASA-180W-PWR-AC   , VID:V01 , SN:123456789AB

ciscoasa# show inventory 0
Name:"Chassis", DESCR:"ASA 5540 Adaptive Security Appliance"
PID:ASA5540           , VID:V01 , SN:P3000000998

ciscoasa# show inventory 1
Name:"slot 1", DESCR:"ASA 5500 Series Security Services Module-20"
PID:ASA-SSM-20        , VID:V01 , SN:P0000000999
```

Table 7-18describes the fields shown in the display.

Table 7-20 show inventory Field Descriptions

Field	Description
Name	Physical name (text string) assigned to the Cisco entity. For example, console or a simple component number (port or module number), such as “1,” depending on the physical component naming syntax of the device. Equivalent to the entPhysicalName MIB variable in RFC 2737.
DESCR	Physical description of the Cisco entity that characterizes the object. Equivalent to the entPhysicalDesc MIB variable in RFC 2737.
PID	Entity product identifier. Equivalent to the entPhysicalModelName MIB variable in RFC 2737.
VID	Entity version identifier. Equivalent to the entPhysicalHardwareRev MIB variable in RFC 2737.
SN	Entity serial number. Equivalent to the entPhysicalSerialNum MIB variable in RFC 2737.

Related Commands

Command	Description
show diag	Displays diagnostic information about the controller, interface processor, and port adapters for a networking device.
show tech-support	Displays general information about the router when it reports a problem.

show ip address

To view interface IP addresses or, for transparent mode, the management IP address, use the **show ip address** command in privileged EXEC mode.

show ip address [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

Syntax Description

interface_name	(Optional) Identifies the interface name set with the **nameif** command.
mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

If you do not specify an interface, the security appliance shows all interface IP addresses.

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.

Usage Guidelines

This command shows the primary IP addresses (called "System" in the display) for when you configure high availability as well as the current IP addresses. If the unit is active, then the system and current IP addresses match. If the unit is standby, then the current IP addresses show the standby addresses.

Examples

The following is sample output from the **show ip address** command:

```
hostname# show ip address
System IP Addresses:
Interface               Name         IP address      Subnet mask       Method
GigabitEthernet0/0      mgmt         10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1      inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40   outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3      dmz          209.165.200.225 255.255.255.224   manual
Current IP Addresses:
Interface               Name         IP address      Subnet mask       Method
GigabitEthernet0/0      mgmt         10.7.12.100     255.255.255.0     CONFIG
```

```
GigabitEthernet0/1       inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40    outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3       dmz          209.165.200.225 255.255.255.224   manual
```

Table 7-16 shows each field description.

Table 7-21 show ip address Fields

Field	Description
Interface	The interface ID or, in multiple context mode, the mapped name if you configured it using the **allocate-interface** command.
Name	The interface name set with the **nameif** command.
IP address	The interface IP address.
Subnet mask	The IP address subnet mask.
Method	The method by which the interface received the IP address. Values include the following: • unset—No IP address configured. • manual—Configured the running configuration. • CONFIG—Loaded from the startup configuration. • DHCP—Received from a DHCP server.

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
interface	Configures an interface and enters interface configuration mode.
nameif	Sets the interface name.
show interface	Displays the runtime status and statistics of interfaces.
show interface ip brief	Shows the interface IP address and status.

show ip address dhcp

To view detailed information about the DHCP lease or server for an interface, use the **show ip address dhcp** command in privileged EXEC mode.

show ip address {*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*} **dhcp** {**lease** | **server**}

Syntax Description

interface_name	Identifies the interface name set with the **nameif** command.
lease	Shows information about the DHCP lease.
mapped_name	In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
server	Shows information about the DHCP server.
subinterface	Identifies an integer between 1 and 4294967293 designating a logical subinterface.

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	This command was changed to include the **lease** and **server** keywords to accommodate the new server functionality.

Usage Guidelines

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show ip address dhcp lease** command:

```
hostname# show ip address outside dhcp lease
Temp IP Addr:209.165.201.57 for peer on interface:outside
Temp sub net mask:255.255.255.224
   DHCP Lease server:209.165.200.225, state:3 Bound
   DHCP Transaction id:0x4123
   Lease:259200 secs, Renewal:129600 secs, Rebind:226800 secs
   Temp default-gateway addr:209.165.201.1
```

```
Temp ip static route0: dest 10.9.0.0 router 10.7.12.255
Next timer fires after:111797 secs
Retry count:0, Client-ID:cisco-0000.0000.0000-outside
Proxy: TRUE  Proxy Network: 10.1.1.1
Hostname: device1
```

Table 7-16 shows each field description.

Table 7-22 show ip address dhcp lease Fields

Field	Description
Temp IP Addr	The IP address assigned to the interface.
Temp sub net mask	The subnet mask assigned to the interface.
DHCP Lease server	The DHCP server address.
state	The state of the DHCP lease, as follows: • Initial—The initialization state, where the security appliance begins the process of acquiring a lease. This state is also shown when a lease ends or when a lease negotiation fails. • Selecting—The security appliance is waiting to receive DHCPOFFER messages from one or more DHCP servers, so it can choose one. • Requesting—The security appliance is waiting to hear back from the server to which it sent its request. • Purging—The security appliance is removing the lease because of the client has released the IP address or there was some other error. • Bound—The security appliance has a valid lease and is operating normally. • Renewing—The security appliance is trying to renew the lease. It regularly sends DHCPREQUEST messages to the current DHCP server, and waits for a reply. • Rebinding—The security appliance failed to renew the lease with the original server, and now sends DHCPREQUEST messages until it gets a reply from any server or the lease ends. • Holddown—The security appliance started the process to remove the lease. • Releasing—The security appliance sends release messages to the server indicating that the IP address is no longer needed.
DHCP transaction id	A random number chosen by the client, used by the client and server to associate the request messages.
Lease	The length of time, specified by the DHCP server, that the interface can use this IP address.
Renewal	The length of time until the interface automatically attempts to renew this lease.

Table 7-22 show ip address dhcp lease Fields (continued)

Field	Description
Rebind	The length of time until the security appliance attempts to rebind to a DHCP server. Rebinding occurs if the security appliance cannot communicate with the original DHCP server, and 87.5 percent of the lease time has expired. The security appliance then attempts to contact any available DHCP server by broadcasting DHCP requests.
Temp default-gateway addr	The default gateway address supplied by the DHCP server.
Temp ip static route0	The default static route.
Next timer fires after	The number of seconds until the internal timer triggers.
Retry count	If the security appliance is attempting to establish a lease, this field shows the number of times the security appliance tried sending a DHCP message. For example, if the security appliance is in the Selecting state, this value shows the number of times the security appliance sent discover messages. If the security appliance is in the Requesting state, this value shows the number of times the security appliance sent request messages.
Client-ID	The client ID used in all communication with the server.
Proxy	Specifies if this interface is a proxy DHCP client for VPN clients, True or False.
Proxy Network	The requested network.
Hostname	The client hostname.

The following is sample output from the **show ip address dhcp server** command:

```
hostname# show ip address outside dhcp server

   DHCP server: ANY (255.255.255.255)
    Leases:   0
    Offers:   0      Requests: 0     Acks: 0     Naks: 0
    Declines: 0      Releases: 0     Bad:  0

   DHCP server: 40.7.12.6
    Leases:   1
    Offers:   1      Requests: 17     Acks: 17     Naks: 0
    Declines: 0      Releases: 0     Bad:  0
    DNS0:   171.69.161.23,   DNS1:  171.69.161.24
    WINS0:  172.69.161.23,   WINS1: 172.69.161.23
    Subnet: 255.255.0.0   DNS Domain: cisco.com
```

Table 7-21 shows each field description.

Table 7-23 show ip address dhcp server Fields

Field	Description
DHCP server	The DHCP server address from which this interface obtained a lease. The top entry (“ANY”) is the default server and is always present.
Leases	The number of leases obtained from the server. For an interface, the number of leases is typically 1. If the server is providing address for an interface that is running proxy for VPN, there will be several leases.

Table 7-23 show ip address dhcp server Fields (continued)

Field	Description
Offers	The number of offers from the server.
Requests	The number of requests sent to the server.
Acks	The number of acknowledgements received from the server.
Naks	The number of negative acknowledgements received from the server.
Declines	The number of declines received from the server.
Releases	The number of releases sent to the server.
Bad	The number of bad packets received from the server.
DNS0	The primary DNS server address obtained from the DHCP server.
DNS1	The secondary DNS server address obtained from the DHCP server.
WINS0	The primary WINS server address obtained from the DHCP server.
WINS1	The secondary WINS server address obtained from the DHCP server.
Subnet	The subnet address obtained from the DHCP server.
DNS Domain	The domain obtained from the DHCP server.

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
ip address dhcp	Sets the interface to obtain an IP address from a DHCP server.
nameif	Sets the interface name.
show interface ip brief	Shows the interface IP address and status.
show ip address	Displays the IP addresses of interfaces.

show ip audit count

To show the number of signature matches when you apply an audit policy to an interface, use the **show ip audit count** command in privileged EXEC mode.

show ip audit count [**global** | **interface** *interface_name*]

Syntax Description

global	(Default) Shows the number of matches for all interfaces.
interface *interface_name*	(Optional) Shows the number of matches for the specified interface.

Defaults

If you do not specify a keyword, this command shows the matches for all interfaces (**global**).

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To create an audit policy, use the **ip audit name** command, and to apply the policy, use the **ip audit interface** command.

Examples

The following is sample output from the **show ip audit count** command:

```
hostname# show ip audit count
IP AUDIT GLOBAL COUNTERS

1000 I Bad IP Options List        0
1001 I Record Packet Route        0
1002 I Timestamp                  0
1003 I Provide s,c,h,tcc          0
1004 I Loose Source Route         0
1005 I SATNET ID                  0
1006 I Strict Source Route        0
1100 A IP Fragment Attack         0
1102 A Impossible IP Packet       0
1103 A IP Teardrop                0
2000 I ICMP Echo Reply            0
2001 I ICMP Unreachable           0
2002 I ICMP Source Quench         0
2003 I ICMP Redirect              0
```

```
2004 I ICMP Echo Request          10
2005 I ICMP Time Exceed           0
2006 I ICMP Parameter Problem     0
2007 I ICMP Time Request          0
2008 I ICMP Time Reply            0
2009 I ICMP Info Request          0
2010 I ICMP Info Reply            0
2011 I ICMP Address Mask Request  0
2012 I ICMP Address Mask Reply    0
2150 A Fragmented ICMP            0
2151 A Large ICMP                 0
2154 A Ping of Death              0
3040 A TCP No Flags               0
3041 A TCP SYN & FIN Flags Only   0
3042 A TCP FIN Flag Only          0
3153 A FTP Improper Address       0
3154 A FTP Improper Port          0
4050 A Bomb                       0
4051 A Snork                      0
4052 A Chargen                    0
6050 A DNS Host Info              0
6051 A DNS Zone Xfer              0
6052 A DNS Zone Xfer High Port    0
6053 A DNS All Records            0
6100 I RPC Port Registration      0
6101 I RPC Port Unregistration    0
6102 I RPC Dump                   0
6103 A Proxied RPC                0
6150 I ypserv Portmap Request     0
6151 I ypbind Portmap Request     0
6152 I yppasswdd Portmap Request  0
6153 I ypupdated Portmap Request  0
6154 I ypxfrd Portmap Request     0
6155 I mountd Portmap Request     0
6175 I rexd Portmap Request       0
6180 I rexd Attempt               0
6190 A statd Buffer Overflow      0

IP AUDIT INTERFACE COUNTERS: inside
...
```

Related Commands

Command	Description
clear ip audit count	Clears the count of signature matches for an audit policy.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
show running-config ip audit attack	Shows the configuration for the **ip audit attack** command.

show ip verify statistics

To show the number of packets dropped because of the Unicast RPF feature, use the **show ip verify statistics** command in privileged EXEC mode. Use the **ip verify reverse-path** command to enable Unicast RPF.

show ip verify statistics [interface *interface_name*]

Syntax Description

interface *interface_name*	(Optional) Shows statistics for the specified interface.

Defaults

This command shows statistics 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
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

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

```
hostname# show ip verify statistics
interface outside: 2 unicast rpf drops
interface inside: 1 unicast rpf drops
interface intf2: 3 unicast rpf drops
```

Related Commands

Command	Description
clear configure ip verify reverse-path	Clears the **ip verify reverse-path** configuration.
clear ip verify statistics	Clears the Unicast RPF statistics.
ip verify reverse-path	Enables the Unicast Reverse Path Forwarding feature to prevent IP spoofing.
show running-config ip verify reverse-path	Shows the **ip verify reverse-path** configuration.

show ipsec sa

To display a list of IPSec SAs, use the **show ipsec sa** command in global configuration mode or privileged EXEC mode. You can also use the alternate form of this command: **show crypto ipsec sa**.

show ipsec sa [**entry | identity | map** *map-name* **| peer** *peer-addr*] [**detail**]

Syntax Description

detail	(Optional) Displays detailed error information on what is displayed.
entry	(Optional) Displays IPSec SAs sorted by peer address
identity	(Optional) Displays IPSec SAs for sorted by identity, not including ESPs. This is a condensed form.
map *map-name*	(Optional) Displays IPSec SAs for the specified crypto map.
peer *peer-addr*	(Optional) Displays IPSec SAs for specified peer IP addresses.

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	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following example, entered in global configuration mode, displays IPSec SAs.

```
hostname(config)# show ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21
```

```
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
hostname(config)#
```

The following example, entered in global configuration mode, displays IPSec SAs for a crypto map named def.

```
hostname(config)# show ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
```

```
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

The following example, entered in global configuration mode, shows IPSec SAs for the keyword **entry**.

```
hostname(config)# show ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
```

```
            sa timing: remaining key lifetime (sec): 429
            IV size: 8 bytes
            replay detection support: Y
        outbound esp sas:
          spi: 0xDC15BF68 (3692412776)
            transform: esp-3des esp-md5-hmac
            in use settings ={RA, Tunnel, }
            slot: 0, conn_id: 3, crypto-map: def
            sa timing: remaining key lifetime (sec): 429
            IV size: 8 bytes
            replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

The following example, entered in global configuration mode, shows IPSec SAs with the keywords **entry detail**.

```
hostname(config)# show ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
```

```
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
```

```
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

The following example shows IPSec SAs with the keyword **identity**.

```
hostname(config)# show ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

The following example shows IPSec SAs with the keywords **identity** and **detail**.

```
hostname(config)# show ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
```

```
    #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
    #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
    #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
    #pkts invalid prot (rcv): 0, #pkts verify failed: 0
    #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
    #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
    #pkts replay failed (rcv): 0
    #pkts internal err (send): 0, #pkts internal err (rcv): 0

    local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

    path mtu 1500, ipsec overhead 60, media mtu 1500
    current outbound spi: DC15BF68

  Crypto map tag: def, local addr: 172.20.0.17

    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
    current_peer: 10.135.1.8
    dynamic allocated peer ip: 0.0.0.0

    #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
    #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
    #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
    #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
    #pkts invalid prot (rcv): 0, #pkts verify failed: 0
    #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
    #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
    #pkts replay failed (rcv): 0
    #pkts internal err (send): 0, #pkts internal err (rcv): 0

    local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

    path mtu 1500, ipsec overhead 60, media mtu 1500
    current outbound spi: 3B6F6A35
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show running-config isakmp	Displays all the active ISAKMP configuration.

show ipsec sa summary

To display a summary of IPSec SAs, use the **show ipsec sa summary** command in global configuration mode or privileged EXEC mode.

show ipsec sa summary

Syntax Description

This command has no arguments or variables.

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	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example, entered in global configuration mode, displays a summary of IPSec SAs by the following connection types:

- IPSec
- IPSec over UDP
- IPSec over NAT-T
- IPSec over TCP
- IPSec VPN load balancing

```
hostname(config)# show ipsec sa summary

Current IPSec SA's:           Peak IPSec SA's:
IPSec            :     2        Peak Concurrent SA  :    14
IPSec over UDP   :     2        Peak Concurrent L2L :     0
IPSec over NAT-T :     4        Peak Concurrent RA  :    14
IPSec over TCP   :     6
IPSec VPN LB     :     0
Total            :    14
hostname(config)#
```

Related Commands

Command	Description
clear ipsec sa	Removes IPSec SAs entirely or based on specific parameters.
show ipsec sa	Displays a list of IPSec SAs.
show ipsec stats	Displays a list of IPSec statistics.

show ipsec stats

To display a list of IPSec statistics, use the **show ipsec stats** command in global configuration mode or privileged EXEC mode.

show ipsec stats

Syntax Description

This command has no keywords or variables.

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	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example, entered in global configuration mode, displays IPSec statistics:

```
hostname(config)# show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
```

```
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
hostname(config)#
```

Related Commands

Command	Description
clear ipsec sa	Clears IPSec SAs or counters based on specified parameters.
crypto ipsec transform-set	Defines a transform set.
show ipsec sa	Displays IPSec SAs based on specified parameters.
show ipsec sa summary	Displays a summary of IPSec SAs.

show ipv6 access-list

To display the IPv6 access list, use the **show ipv6 access-list** command in privileged EXEC mode. The IPv6 access list determines what IPv6 traffic can pass through the security appliance.

show ipv6 access-list [*id* [*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*]]

Syntax Description

any	(Optional) An abbreviation for the IPv6 prefix ::/0.
host *source-ipv6-address*	(Optional) IPv6 address of a specific host. When provided, only the access rules for the specified host are displayed.
id	(Optional) The access list name. When provided, only the specified access list is displayed.
source-ipv6-prefix /prefix-length	(Optional) IPv6 network address and prefix. When provided, only the access rules for the specified IPv6 network are displayed.

Defaults

Displays all IPv6 access lists.

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	This command was introduced.

Usage Guidelines

The **show ipv6 access-list** command provides output similar to the **show ip access-list** command, except that it is IPv6-specific.

Examples

The following is sample output from the **show ipv6 access-list** command. It shows IPv6 access lists named inbound, tcptraffic, and outbound.

```
hostname# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
        left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
        (time left 296) sequence 2
```

```
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

Related Commands

Command	Description
ipv6 access-list	Creates an IPv6 access list.

show ipv6 interface

To display the status of interfaces configured for IPv6, use the **show ipv6 interface** command in privileged EXEC mode.

show ipv6 interface [**brief**] [*if_name* [**prefix**]]

Syntax Description

brief	Displays a brief summary of IPv6 status and configuration for each interface.
if_name	(Optional) The internal or external interface name, as designated by the **nameif** command. The status and configuration for only the designated interface is shown.
prefix	(Optional) Prefix generated from a local IPv6 prefix pool.

Defaults

Displays all IPv6 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
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **show ipv6 interface** command provides output similar to the **show interface** command, except that it is IPv6-specific. If the interface hardware is usable, the interface is marked *up*. If the interface can provide two-way communication, the line protocol is marked *up*.

When an interface name is not specified, information on all IPv6 interfaces is displayed. Specifying an interface name displays information about the specified interface.

Examples

The following is sample output from the **show ipv6 interface** command:

```
hostname# show ipv6 interface outside
interface ethernet0 "outside" is up, line protocol is up
  IPv6 is enabled, link-local address is 2001:0DB8::/29 [TENTATIVE]
  Global unicast address(es):
    2000::2, subnet is 2000::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF11:6770
  MTU is 1500 bytes
```

```
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
```

The following is sample output from the **show ipv6 interface** command when entered with the **brief** keyword:

```
hostname# show ipv6 interface brief
outside [up/up]
    unassigned
inside [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::a:0:0:a0a:a70
vlan101 [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::65:0:0:a0a:6570
dmz-ca [up/up]
    unassigned
```

The following is sample output from the **show ipv6 interface** command. It shows the characteristics of an interface which has generated a prefix from an address.

```
hostname# show ipv6 interface inside prefix
IPv6 Prefix Advertisements inside
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default       N - Not advertised, C - Calendar

AD      fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 neighbor

To display the IPv6 neighbor discovery cache information, use the **show ipv6 neighbor** command in privileged EXEC mode.

show ipv6 neighbor [*if_name* | *address*]

Syntax Description

address	(Optional) Displays neighbor discovery cache information for the supplied IPv6 address only.
if_name	(Optional) Displays cache information for the supplied interface name, as configure by the **nameif** command, only.

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	This command was introduced.

Usage Guidelines

The following information is provided by the **show ipv6 neighbor** command:

- **IPv6 Address**—the IPv6 address of the neighbor or interface.
- **Age**—the time (in minutes) since the address was confirmed to be reachable. A hyphen (-) indicates a static entry.
- **Link-layer Addr**—MAC address. If the address is unknown, a hyphen (-) is displayed.
- **State**—The state of the neighbor cache entry.

Note Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the **INCMP** (Incomplete) and **REACH** (Reachable) states are different for dynamic and static cache entries.

The following are possible states for dynamic entries in the IPv6 neighbor discovery cache:

- **INCMP**—(Incomplete) Address resolution is being performed on the entry. A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received.

  - **REACH**—(Reachable) Positive confirmation was received within the last ReachableTime milliseconds that the forward path to the neighbor was functioning properly. While in **REACH** state, the device takes no special action as packets are sent.
  - **STALE**—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in **STALE** state, the device takes no action until a packet is sent.
  - **DELAY**—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the **DELAY** state, send a neighbor solicitation message and change the state to **PROBE**.
  - **PROBE**—A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received.
  - **????**—Unknown state.

  The following are possible states for static entries in the IPv6 neighbor discovery cache:

  - **INCMP**—(Incomplete) The interface for this entry is down.
  - **REACH**—(Reachable) The interface for this entry is up.

- **Interface**
  Interface from which the address was reachable.

Examples

The following is sample output from the **show ipv6 neighbor** command when entered with an interface:

```
hostname# show ipv6 neighbor inside
IPv6 Address                             Age Link-layer Addr State Interface
2000:0:0:4::2                              0 0003.a0d6.141e  REACH inside
FE80::203:A0FF:FED6:141E                   0 0003.a0d6.141e  REACH inside
3001:1::45a                                - 0002.7d1a.9472  REACH inside
```

The following is sample output from the **show ipv6 neighbor** command when entered with an IPv6 address:

```
hostname# show ipv6 neighbor 2000:0:0:4::2
IPv6 Address                             Age Link-layer Addr State Interface
2000:0:0:4::2                              0 0003.a0d6.141e  REACH inside
```

Related Commands

Command	Description
clear ipv6 neighbors	Deletes all entries in the IPv6 neighbor discovery cache, except static entries.
ipv6 neighbor	Configures a static entry in the IPv6 neighbor discovery cache.

show ipv6 route

To display the contents of the IPv6 routing table, use the **show ipv6 route** command in privileged EXEC mode.

show ipv6 route

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	This command was introduced.

Usage Guidelines

The **show ipv6 route** command provides output similar to the **show route** command, except that the information is IPv6-specific.

The following information appears in the IPv6 routing table:

- **Codes**—Indicates the protocol that derived the route. Values are as follows:
  - **C**—Connected
  - **L**—Local
  - **S**—Static
  - **R**—RIP derived
  - **B**—BGP derived
  - **I1**—ISIS L1—Integrated IS-IS Level 1 derived
  - **I2**—ISIS L2—Integrated IS-IS Level 2 derived
  - **IA**—ISIS interarea—Integrated IS-IS interarea derived
- **fe80::/10**—Indicates the IPv6 prefix of the remote network.
- **[0/0]**—The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
- **via ::**—Specifies the address of the next router to the remote network.

- **inside**—Specifies the interface through which the next router to the specified network can be reached.

Examples

The following is sample output from the **show ipv6 route** command:

```
hostname# show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
L   fe80::/10 [0/0]
     via ::, inside
     via ::, vlan101
L   fec0::a:0:0:a0a:a70/128 [0/0]
     via ::, inside
C   fec0:0:0:a::/64 [0/0]
     via ::, inside
L   fec0::65:0:0:a0a:6570/128 [0/0]
     via ::, vlan101
C   fec0:0:0:65::/64 [0/0]
     via ::, vlan101
L   ff00::/8 [0/0]
     via ::, inside
     via ::, vlan101
S   ::/0 [0/0]
     via fec0::65:0:0:a0a:6575, vlan101
```

Related Commands

Command	Description
debug ipv6 route	Displays debug messages for IPv6 routing table updates and route cache updates.
ipv6 route	Adds a static entry to the IPv6 routing table.

show ipv6 routers

To display IPv6 router advertisement information received from on-link routers, use the **show ipv6 routers** command in privileged EXEC mode.

show ipv6 routers [*if_name*]

Syntax Description

if_name	(Optional) The internal or external interface name, as designated by the **nameif** command, that you want to display information about.

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	This command was introduced.

Usage Guidelines

When an interface name is not specified, information on all IPv6 interfaces is displayed. Specifying an interface name displays information about the specified interface.

Examples

The following is sample output from the **show ipv6 routers** command when entered without an interface name:

```
hostname# show ipv6 routers
Router FE80::83B3:60A4 on outside, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
Router FE80::290:27FF:FE8C:B709 on inside, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

Related Commands

Command	Description
ipv6 route	Adds a static entry to the IPv6 routing table.

show ipv6 traffic

To display statistics about IPv6 traffic, use the **show ipv6 traffic** command in privileged EXEC mode.

show ipv6 traffic

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	This command was introduced.

Usage Guidelines

Use the **clear ipv6 traffic** command to clear the traffic counters.

Examples

The following is sample output from the **show ipv6 traffic** command:

```
hostname# show ipv6 traffic
IPv6 statistics:
  Rcvd:  545 total, 545 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         218 fragments, 109 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  228 generated, 0 forwarded
         1 fragmented into 2 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 168 received, 70 sent

ICMP statistics:
  Rcvd: 116 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
```

```
        0 router solicit, 60 router advert, 0 redirects
        31 neighbor solicit, 25 neighbor advert
  Sent: 85 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 18 router advert, 0 redirects
        33 neighbor solicit, 34 neighbor advert

UDP statistics:
  Rcvd: 109 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 37 output

TCP statistics:
  Rcvd: 85 input, 0 checksum errors
  Sent: 103 output, 0 retransmitted
```

Related Commands

Command	Description
clear ipv6 traffic	Clears ipv6 traffic counters.

show isakmp sa

To display the IKE runtime SA database, use the **show isakmp sa** command in global configuration mode or privileged EXEC mode.

show isakmp sa [**detail**]

Syntax Description

detail	Displays detailed output about the SA database.

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	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The output from this command includes the following fields:

Detail not specified.

Table 7-24

IKE Peer	Type	Dir	Rky	State
209.165.200.225	L2L	Init	No	MM_Active

Detail specified.

Table 7-25

IKE Peer	Type	Dir	Rky	State	Encrypt	Hash	Auth	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

Examples

The following example, entered in global configuration mode, displays detailed information about the SA database:

```
hostname(config)# show isakmp sa detail
hostname(config)# sho isakmp sa detail
```

```
IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

hostname(config)#
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show running-config isakmp	Displays all the active ISAKMP configuration.

show isakmp stats

To display runtime statistics, use the **show isakmp stats** command in global configuration mode or privileged EXEC mode.

show isakmp stats

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	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The output from this command includes the following fields:

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets
- Out Drop Packets
- Out Notifys
- Out P2 Exchanges

- Out P2 Exchange Invalids
- Out P2 Exchange Rejects
- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

Examples

The following example, issued in global configuration mode, displays ISAKMP statistics:

```
hostname(config)# show isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
hostname(config)#
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.

Command	Description
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show running-config isakmp	Displays all the active ISAKMP configuration.

show local-host

To display the network states of local hosts, use the **show local-host** command in privileged EXEC mode.

show local-host [*ip_address*] [**detail**] [**all**][**brief**] **[connection {tcp <start>[-<end>] | udp <start>[-<end>] | embryonic <start>[-<end>]}]**

Syntax Description

all	(Optional) Specifies to include the list of local hosts state-made connections, including to the security appliance and from the security appliance.
brief	(Optional) Displays brief informationon local hosts.
connection	(Optional) Displays three typs of filters based on the number and type of connetcions: tcp, udp and embryonic. These filters can be used individually or jointly.
detail	(Optional) Displays the detailed network states of local host information.
ip_address	(Optional) Specifies the local host IP address.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.
7.0(8)	Added the **connection** and **brief** options.

Usage Guidelines

The **show local-host** command lets you display the network states of local hosts. A local-host is created for any host that forwards traffic to, or through, the security appliance.

This command lets you show the translation and connection slots for the local hosts or stop all traffic on these hosts. This command provides information for hosts that are configured with the **nat 0 access-list** command when normal translation and connection states may not apply.

The **show local-host detail** command displays more information about active xlates and network connections.

Use the *ip_address* argument to limit the display to a single host.

Use the **all** keyword to list local hosts-made connections, including to the security appliance and from the security appliance. If you do not use the **all** keyword, local hosts connections to the security appliance and from the appliance do not display.

This command displays the connection limit values. If a connection limit is not set, the value displays as 0 and the limit is not applied.

In the event of a syn attack (with TCP intercept configured), the **show local-host** command output includes the number of intercepted connections in the usage count. This field typically displays only full open connections.

In the **show local-host** command output, the `TCP embryonic count to host counter` is used when a maximum embryonic limit (TCP intercept watermark) is configured for a host using a static connection. This counter shows the total embryonic connections to the host from other hosts. If this total exceeds the maximum configured limit, TCP intercept is applied to new connections to the host.

Examples

The following examples show how to display the network states of local hosts:

```
hostname# show local-host all
Interface outside: 1 active, 2 maximum active, 0 denied
local host: <11.0.0.4>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
Interface inside: 1 active, 2 maximum active, 0 denied
local host: <17.3.8.2>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
Interface NP Identity Ifc: 2 active, 4 maximum active, 0 denied
local host: <11.0.0.3>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
local host: <17.3.8.1>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464

hostname# show local-host 10.1.1.91
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
```

```
PAT Global 192.150.49.1(1024) Local 10.1.1.91(4984)

Conn:
TCP out 192.150.49.10:21 in 10.1.1.91:4984 idle 0:00:07 bytes 75 flags UI Interface
outside: 1 active, 1 maximum active, 0 denied

hostname# show local-host 10.1.1.91 detail
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
TCP PAT from inside:10.1.1.91/4984 to outside:192.150.49.1/1024 flags ri

Conn:
TCP outside:192.150.49.10/21 inside:10.1.1.91/4984 flags UI Interface outside: 1 active, 1
maximum active, 0 denied
```

The following example shows all hosts who have at least four udp connections and have between one to 10 tcp connections at the same time:

```
hostname# show local-host connection udp 4 tcp 1-10
Interface mng: 0 active, 3 maximum active, 0 denied
Interface INSIDE: 4 active, 5 maximum active, 0 denied
local host: <10.1.1.11>,
       TCP flow count/limit = 1/unlimited TCP embryonic count to host = 0 TCP intercept
       watermark = unlimited UDP flow count/limit = 4/unlimited
Xlate:
       Global 192.168.1.24 Local 10.1.1.11 Conn: UDP out 192.168.1.10:80 in
       10.1.1.11:1730 idle 0:00:21 bytes 0 flags - UDP out 192.168.1.10:80 in
       10.1.1.11:1729 idle 0:00:22 bytes 0 flags - UDP out 192.168.1.10:80 in
       10.1.1.11:1728 idle 0:00:23 bytes 0 flags - UDP out 192.168.1.10:80 in
       10.1.1.11:1727 idle 0:00:24 bytes 0 flags - TCP out 192.168.1.10:22 in
       10.1.1.11:27337 idle 0:01:55 bytes 2641 flags UIO Interface OUTSIDE: 3 active, 5
       maximum active, 0 denied
```

The following example shows local-host addresses and connection counters using the **brief** option:

```
hostname# show local-host connection udp 2
Interface mng: 0 active, 3 maximum active, 0 denied
Interface INSIDE: 4 active, 5 maximum active, 0 denied
local host: <10.1.1.11>,
       TCP flow count/limit = 1/unlimited
       TCP embryonic count to host = 0
       TCP intercept watermark = unlimited UDP flow count/limit = 4/unlimited
Interface OUTSIDE: 3 active, 5 maximum active, 0 denied
```

The following examples shows the output when using the *brief* and *connection* syntax:

```
hostname#show local-host brief
Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 1 active, 1 maximum active, 0 denied
Interface mgmt: 5 active, 6 maximum active, 0 denied

hostname# show local-host connection
Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 1 active, 1 maximum active, 0 denied
Interface mgmt: 5 active, 6 maximum active, 0 denied
```

Related Commands

Command	Description
clear local-host	Releases network connections from local hosts displayed by the **show local-host** command.
nat	Associates a network with a pool of global IP addresses.

show logging

To show the logs in the buffer or to show other logging settings, use the **show logging** command.

show logging [**message** [*syslog_id* | **all**] | **asdm** | **queue** | **setting**]

Syntax Description

message	(Optional) Displays messages that are at a non-default level. See the **logging message** command to set the message level.
syslog_id	(Optional) Specifies a message number to display.
all	(Optional) Displays all syslog message IDs, along with whether they are enabled or disabled.
setting	(Optional) Displays the logging setting, without displaying the logging buffer.
asdm	(Optional) Displays ASDM logging buffer content.
queue	(Optional) Displays the syslog message queue.

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
Preexisting	This command was preexisting.

Usage Guidelines

If the **logging buffered** command is in use, the **show logging** command without any keywords shows the current message buffer and the current settings.

The **show logging queue** command allows you to display the following:

- Number of messages that are in the queue
- Highest number of messages recorded that are in the queue
- Number of messages that are discarded because block memory was not available to process them

Examples

The following is sample output from the **show logging** command:

```
hostname(config)# show logging
Syslog logging: enabled
    Timestamp logging: disabled
    Console logging: disabled
```

```
    Monitor logging: disabled
    Buffer logging: level debugging, 37 messages logged
    Trap logging: disabled
305001: Portmapped translation built for gaddr 209.165.201.5/0 laddr 192.168.1.2/256
...
```

The following is sample output from the **show logging message all** command:

```
hostname(config)# show logging message all

syslog 111111: default-level alerts (enabled)
syslog 101001: default-level alerts (enabled)
syslog 101002: default-level alerts (enabled)
syslog 101003: default-level alerts (enabled)
syslog 101004: default-level alerts (enabled)
syslog 101005: default-level alerts (enabled)
syslog 102001: default-level alerts (enabled)
syslog 103001: default-level alerts (enabled)
syslog 103002: default-level alerts (enabled)
syslog 103003: default-level alerts (enabled)
syslog 103004: default-level alerts (enabled)
syslog 103005: default-level alerts (enabled)
syslog 103011: default-level alerts (enabled)
syslog 103012: default-level informational (enabled)
```

Related Commands

Command	Description
logging asdm	Enables logging to ASDM
logging buffered	Enables logging to the buffer.
logging message	Sets the message level, or disables messages.
logging queue	Configures the logging queue.

show logging rate-limit

To display the disallowed messages to the original set, use the **show logging rate-limit** command.

show logging rate-limit

Syntax Description

This command has no arguments or keywords.

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	Support for this command was introduced on the security appliance.

Usage Guidelines

After the information is cleared, nothing more displays until the hosts reestablish their connections.

Examples

This example shows how to display the disallowed messages:

```
hostname(config)# show logging rate-limit
```

Related Commands

Command	Description
show logging	Displays the enabled logging options.

show mac-address-table

To show the MAC address table, use the **show mac-address-table** command in privileged EXEC mode.

show mac-address-table [*interface_name* **| count | static]**

Syntax Description

count	(Optional) Lists the total number of dynamic and static entries.
interface_name	(Optional) Identifies the interface name for which you want to view MAC address table entries.
static	(Optional) Lists only static entries.

Defaults

If you do not specify an interface, all interface MAC address entries are shown.

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	This command was introduced.

Examples

The following is sample output from the **show mac-address-table** command:

```
hostname# show mac-address-table
interface          mac address       type      Time Left
------------------------------------------------------------------------
outside            0009.7cbe.2100    static      -
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

The following is sample output from the **show mac-address-table** command for the inside interface:

```
hostname# show mac-address-table inside
interface          mac address       type      Time Left
------------------------------------------------------------------------
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

The following is sample output from the **show mac-address-table count** command:

```
hostname# show mac-address-table count
Static     mac-address bridges (curr/max): 0/65535
Dynamic    mac-address bridges (curr/max): 103/65535
```

Related Commands

Command	Description
firewall transparent	Sets the firewall mode to transparent.
mac-address-table aging-time	Sets the timeout for dynamic MAC address entries.
mac-address-table static	Adds a static MAC address entry to the MAC address table.
mac-learn	Disables MAC address learning.

show management-access

To display the name of the internal interface configured for management access, use the show management-access command in privileged EXEC mode.

show management-access

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.

Usage Guidelines

The **management-access** command lets you define an internal management interface using the IP address of the firewall interface specified in *mgmt_if*. (The interface names are defined by the **nameif** command and displayed in quotes, " ", in the output of the **show interface** command.)

Examples

The following example shows how to configure a firewall interface named "inside" as the management access interface and display the result:

```
hostname(config)# management-access inside
hostname(config)# show management-access
management-access inside
```

Related Commands

Command	Description
clear configure management-access	Removes the configuration of an internal interface for management access of the security appliance.
management-access	Configures an internal interface for management access.

show memory

To display a summary of the maximum physical memory and current free memory available to the operating system, use the **show memory** command in privileged EXEC mode.

show memory [**detail**]

Syntax Description

detail	(Optional) Displays a detailed view of free and allocated system memory.

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.

Usage Guidelines

The **show memory** command lets you display a summary of the maximum physical memory and current free memory available to the operating system. Memory is allocated as needed.

You can use the **show memory detail** output with **show memory binsize** command to debug memory leaks.

You can also display the information from the **show memory** command using SNMP.

Examples

This example shows how to display a summary of the maximum physical memory and current free memory available:

```
hostname# show memory
Free memory:       845044716 bytes (79%)
Used memory:       228697108 bytes (21%)
-------------     ----------------
Total memory:     1073741824 bytes (100%)
```

This example shows detailed memory output:

```
hostname# show memory detail
Free memory: 15958088 bytes (24%)
Used memory:
Allocated memory in use: 29680332 bytes (44%)
Reserved memory: 21470444 bytes (32%)
---------------------------- ----------------
```

```
Total memory: 67108864 bytes (100%)

Least free memory: 4551716 bytes ( 7%)
Most used memory: 62557148 bytes (93%)

----- fragmented memory statistics -----

fragment size count total
(bytes) (bytes)
---------------- ---------- --------------
16 8 128
24 4 96
32 2 64
40 5 200
64 3 192
88 1 88
168 1 168
224 1 224
256 1 256
296 2 592
392 1 392
400 1 400
1816 1 1816*
4435968 1 4435968**
11517504 1 11517504

* - top most releasable chunk.
** - contiguous memory on top of heap.


----- allocated memory statistics -----

fragment size count total
(bytes) (bytes)
---------------- ---------- --------------
40 50 2000
48 144 6912
56 24957 1397592
64 101 6464
72 99 7128
80 1032 82560
88 18 1584
96 64 6144
104 57 5928
112 6 672
120 112 13440
128 15 1920
136 87 11832
144 22 3168
152 31 4712
160 90 14400
168 65 10920
176 74 13024
184 11 2024
192 8 1536
200 1 200
<output omitted>
```

Related Commands

Command	Description
show memory profile	Displays information about the memory usage (profiling) of the security appliance.
show memory binsize	Displays summary information about the chunks allocated for a specific bin size.

show memory binsize

To display summary information about the chunks allocated for a specific bin size, use the **show memory binsize** command in privileged EXEC mode.

show memory binsize *size*

Syntax Description

size	Displays chunks (memory blocks) of a specific bin size. The bin size is from the "fragment size" column of the **show memory detail** command output.

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	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

The following example displays summary information about a chunk allocated to a bin size of 500:

```
hostname# show memory binsize 500
pc = 0x00b33657, size = 460      , count = 1
```

Related Commands

Command	Description
show memory-caller address	Displays the address ranges configured on the security appliance.
show memory profile	Displays information about the memory usage (profiling) of the security appliance.
show memory	Displays a summary of the maximum physical memory and current free memory available to the operating system.

show memory delayed-free-poisoner

To display a summary of the **memory delayed-free-poisoner** queue usage, use the **show memory delayed-free-poisoner** command in privileged EXEC mode.

show memory delayed-free-poisoner

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

Use the **clear memory delayed-free-poisoner** command to clear the queue and statistics.

Examples

This following is sample output from the **show memory delayed-free-poisoner** command:

```
hostname# show memory delayed-free-poisoner
delayed-free-poisoner statistics:
        3335600:  memory held in queue
           6095:  current queue count
              0:  elements dequeued
              3:  frees ignored by size
           1530:  frees ignored by locking
             27:  successful validate runs
              0:  aborted validate runs
       01:09:36:  local time of last validate
```

Table 7-26 describes the significant fields in the **show memory delayed-free-poisoner** command output.

Table 7-26 **show memory delayed-free-poisoner** Command Output Descriptions

Field	Description
memory held in queue	The memory that is held in the delayed free-memory poisoner tool queue. Such memory is normally in the "Free" quantity in the **show memory** output if the delayed free-memory poisoner tool is not enabled.
current queue count	The number of elements in the queue.
elements dequeued	The number of elements that have been removed from the queue. This number begins to increase when most or all of the otherwise free memory in the system ends up in being held in the queue.
frees ignored by size	The number of free requests not placed into the queue because the request was too small to hold required tracking information.
frees ignored by locking	The number of free requests intercepted by the tool not placed into the queue because the memory is in use by more than one application. The last application to free the memory back to the system ends up placing such memory regions into the queue.
successful validate runs	The number of times since monitoring was enabled or cleared using the **clear memory delayed-free-poisoner** command that the queue contents were validated (either automatically or by the **memory delayed-free-poisoner validate** command).
aborted validate runs	The number of times since monitoring was enabled or cleared using the **clear memory delayed-free-poisoner** command that requests to check the queue contents have been aborted because more than one task (either the periodic run or a validate request from the CLI) attempted to use the queue at a time.
local time of last validate	The local system time when the last validate run completed.

Related Commands

Command	Description
clear memory delayed-free-poisoner	Clears the delayed free-memory poisoner tool queue and statistics.
memory delayed-free-poisoner enable	Enables the delayed free-memory poisoner tool.
memory delayed-free-poisoner validate	Forces validation of the elements in the delayed free-memory poisoner tool queue.

show memory profile

To display information about the memory usage (profiling) of the security appliance, use the **show memory profile** command in privileged EXEC mode.

show memory profile [peak] [detail | collated | status]

Syntax Description

collated	(Optional) Collates the memory information displayed.
detail	(Optional) Displays detailed memory information.
peak	(Optional) Displays the peak capture buffer rather than the “in use” buffer.
status	(Optional) Displays the current state of memory profiling and the peak capture buffer.

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	This command was introduced.

Usage Guidelines

Use the **show memory profile** command to troubleshoot memory usage level and memory leaks. You can still see the profile buffer contents even if profiling has been stopped. Starting profiling clears the buffer automatically.

Note The security appliance might experience a temporary reduction in performance when memory profiling is enabled.

Examples

The following example shows...

```
hostname# show memory profile
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 0
```

The output of the **show memory profile detail** command (below) is divided into six data columns and one header column, at the far left. The address of the memory bucket corresponding to the first data column is given at the header column (the hexidecimal number). The data itself is the number of bytes

that is held by the text/code that falls in the bucket address. A period (.) in the data column means no memory is held by the text at this bucket. Other columns in the row correspond to the bucket address that is greater than the increment amount from the previous column. For example, the address bucket of the first data column in the first row is 0x001069e0. The address bucket of the second data column in the first row is 0x001069e4 and so on. Normally the header column address is the next bucket address; that is, the address of the last data column of the previous row plus the increment. All rows without any usage are suppressed. More than one such contiguous row can be suppressed, indicated with three periods at the header column (...).

```
hostname# show memory profile detail
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
...
0x001069e0 . 24462 . . . .
...
0x00106d88 . 1865870 . . . .
...
0x0010adf0 . 7788 . . . .
...
0x00113640 . . . . 433152 .
...
0x00116790 2480 . . . . .
<snip>
```

The following example shows collated output:

```
hostname# show memory profile collated
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
24462 0x001069e4
1865870 0x00106d8c
7788 0x0010adf4
433152 0x00113650
2480 0x00116790
<snip>
```

The following example shows the peak capture buffer:

```
hostname# show memory profile peak
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
```

The following example shows the peak capture buffer and the number of bytes that is held by the text/code that falls in the corresponding bucket address:

```
hostname# show memory profile peak detail
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
...
0x00404c8c . . 102400 . . .
```

The following example shows the current state of memory profiling and the peak capture buffer:

```
hostname# show memory profile status
InUse profiling: ON
Peak profiling: OFF
Memory used by profile buffers: 11518860 bytes
Profile:
0x00100020-0x00bfc3a8(00000004)
```

Related Commands

Command	Description
memory profile enable	Enables the monitoring of memory usage (memory profiling).
memory profile text	Configures a program text range of memory to profile.
clear memory profile	Clears the memory buffers held by the memory profiling function.

show memory tracking

To display currently allocated memory tracked by the tool, use the show memory tracking command in privileged EXEC mode.

show memory tracking [address | dump | detail]

Syntax Description

address	(Optional) Shows memory tracking by address.
detail	(Optional) Shows internal memory tracking state.
dump	(Optional) Dumps memory tracking address.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0(8)	This command was introduced.

Usage Guidelines

Use the **show memory tracking** command to show currently allocated memory tracked by the tool.

Examples

The following example shows the **show memory tracking** command out-put:

```
hostname# show memory tracking
memory tracking by caller:
17 bytes from 1 allocates by 0x080c50c2
37 bytes from 1 allocates by 0x080c50f6
57 bytes from 1 allocates by 0x080c5125
20481 bytes from 1 allocates by 0x080c5154
```

The following examples show the **show memory tracking address**, and **show memory tracking dump** outputs:

```
hostname# show memory tracking address
memory tracking by caller:
17 bytes from 1 allocates by 0x080c50c2
37 bytes from 1 allocates by 0x080c50f6
57 bytes from 1 allocates by 0x080c5125
20481 bytes from 1 allocates by 0x080c5154
```

```
memory tracking by address:
37 byte region @ 0xa893ae80 allocated by 0x080c50f6
57 byte region @ 0xa893aed0 allocated by 0x080c5125
20481 byte region @ 0xa8d7cc50 allocated by 0x080c5154
17 byte region @ 0xa8a6f370 allocated by 0x080c50c2

hostname# memory tracking dump 0xa893aed0
Tracking data for the 57 byte region at 0xa893aed0:
Timestamp: 05:59:36.309 UTC Sun Jul 29 2007
Traceback:
0x080c5125
0x080b3695
0x0873f606
0x08740573
0x080ab530
0x080ac788
0x080ad141
0x0805df8f
Dumping 57 bytes of the 57 byte region:
a893aed0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | ................
a893aee0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | ................
a893aef0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | ................
a893af00: 0c 0c 0c 0c 0c 0c 0c 0c 0c | .........
```

Related Commands

Command	Description
clear memory tracking	Clears all currently gathered information.
show memory tracking	Shows currently allocated memory.

show memory-caller address

To display the address ranges configured on the security appliance, use the **show memory-caller address** command in privileged EXEC mode.

show memory-caller address

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	This command was introduced.

Usage Guidelines

You must first configure an address ranges with the **memory caller-address** command before you can display them with the **show memory-caller address** command.

Examples

The following examples show the address ranges configured with the **memory caller-address** commands, and the resulting display of the **show memory-caller address** command:

```
hostname# memory caller-address 0x00109d5c 0x00109e08
hostname# memory caller-address 0x009b0ef0 0x009b0f14
hostname# memory caller-address 0x00cf211c 0x00cf4464

hostname# show memory-caller address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

If address ranges are not configured before entering the **show memory-caller address** command, no addresses display:

```
hostname# show memory-caller address
Move down stack frame for the addresses:
```

Related Commands

Command	Description
memory caller-address	Configures block of memory for the caller PC.

show mfib

To display MFIB in terms of forwarding entries and interfaces, use the **show mfib** command in user EXEC or privileged EXEC mode.

show mfib [*group* [*source*]] [**verbose**]

Syntax Description

group	(Optional) IP address of the multicast group.
source	(Optional) IP address of the multicast route source. This is a unicast IP address in four-part dotted-decimal notation.
verbose	(Optional) Displays additional information about the entries.

Defaults

Without the optional arguments, information for all groups is shown.

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
User EXEC or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following is sample output from the **show mfib** command:

```
hostname# show mfib 224.0.2.39
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

Related Commands

Command	Description
show mfib verbose	Displays detail information about the forwarding entries and interfaces.

show mfib active

To display active multicast sources, use the **show mfib active** command in user EXEC or privileged EXEC mode.

show mfib [*group*] **active** [*kbps*]

Syntax Description

group	(Optional) IP address of the multicast group.
kbps	(Optional) Limits the display to multicast streams that are greater-than or equal to this value.

This command has no arguments or keywords.

Defaults

The default value for *kbps* is 4. If a *group* is not specified, all groups are shown.

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
User EXEC or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The output for the show mfib active command displays either positive or negative numbers for the rate PPS. The security appliance displays negative numbers when RPF packets fail or when the router observes RPF packets with an interfaces out (OIF) list. This type of activity may indicate a multicast routing problem.

Examples

The following is sample output from the **show mfib active** command:

```
hostname# show mfib active
Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
   Source: 192.168.28.69 (mbone.ipd.anl.gov)
     Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)

Group: 224.2.201.241, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)
```

```
Group: 224.2.207.215, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

Related Commands

Command	Description
show mroute active	Displays active multicast streams.

show mfib count

To display MFIB route and packet count data, use the **show mfib count** command in user EXEC or privileged EXEC mode.

show mfib [*group* [*source*]] **count**

Syntax Description

group	(Optional) IP address of the multicast group.
source	(Optional) IP address of the multicast route source. This is a unicast IP address in four-part dotted-decimal notation.

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
User EXEC or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command displays packet drop statistics.

Examples

The following sample output from the **show mfib count** command:

```
hostname# show mfib count
MFIB global counters are :
* Packets [no input idb] : 0
* Packets [failed route lookup] : 0
* Packets [Failed idb lookup] : 0
* Packets [Mcast disabled on input I/F] : 0
```

Related Commands

Command	Description
clear mfib counters	Clears MFIB router packet counters.
show mroute count	Displays multicast route counters.

show mfib interface

To display packet statistics for interfaces that are related to the MFIB process, use the **show mfib interface** command in user EXEC or privileged EXEC mode.

show mfib interface [*interface*]

Syntax Description

interface	(Optional) Interface name. Limits the display to the specified interface.

Defaults

Information for all MFIB interfaces is shown.

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
User EXEC or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example is sample output from the **show mfib interface** command:

```
hostname# show mfib interface
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
MFIB interface       status    CEF-based output
                               [configured,available]
           Ethernet0   up    [        no,       no]
           Ethernet1   up    [        no,       no]
           Ethernet2   up    [        no,       no]
```

Related Commands

Command	Description
show mfib	Displays MFIB information in terms of forwarding entries and interfaces.

show mfib reserved

To display reserved groups, use the **show mfib reserved** command in user EXEC or privileged EXEC mode.

show mfib reserved [**count** | **verbose** | **active** [*kpbs*]]

Syntax Description

count	(Optional) Displays packet and route count data.
verbose	(Optional) Displays additional information.
active	(Optional) Displays active multicast sources.
kpbs	(Optional) Limits the display to active multicast sources greater-than or equal to this value.

Defaults

The default value for *kbps* is 4.

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**
User EXEC or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command displays MFIB entries in the range 224.0.0.0 through 224.0.0.225.

Examples

The following is sample output from the **show mfib reserved** command:

```
hostname# command example
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop Forwarding Counts: Pkt Count/Pkts per
second/Avg Pkt Size/Kbits per second Other counts: Total/RPF failed/Other drops Interface
Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.0.0/4) Flags: C K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/24) Flags: K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.1) Flags:
   Forwarding: 0/0/0/0, Other: 0/0/0
   outside Flags: IC
```

```
dmz Flags: IC
inside Flags: IC
```

Related Commands

Command	Description
show mfib active	Displays active multicast streams.

show mfib status

To display the general MFIB configuration and operational status, use the **show mfib status** command in user EXEC or privileged EXEC mode.

show mfib status

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
User EXEC or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following is sample output from the **show mfib status** command:

```
hostname# show mfib status
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
```

Related Commands

Command	Description
show mfib	Displays MFIB information in terms of forwarding entries and interfaces.

show mfib summary

To display summary information about the number of MFIB entries and interfaces, use the **show mfib summary** command in user EXEC or privileged EXEC mode.

show mfib summary

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
User EXEC or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following is sample output from the **show mfib summary** command:

```
hostname# show mfib summary
IPv6 MFIB summary:

  54     total entries [1 (S,G), 7 (*,G), 46 (*,G/m)]

  17     total MFIB interfaces
```

Related Commands

Command	Description
show mroute summary	Displays multicast routing table summary information.

show mfib verbose

To display detail information about the forwarding entries and interfaces, use the **show mfib verbose** command in user EXEC or privileged EXEC mode.

show mfib verbose

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
User EXEC or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following is sample output from the **show mfib verbose** command:

```
hostname# show mfib verbose
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.1.40) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/8) Flags: K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

Related Commands

Command	Description
show mfib	Displays MFIB information in terms of forwarding entries and interfaces.
show mfib summary	Displays summary information about the number of MFIB entries and interfaces.

show mgcp

To display MGCP configuration and session information, use the **show mgcp** command in privileged EXEC mode.

show mgcp {**commands** | **sessions**} [**detail**]

Syntax Description

commands	Lists the number of MGCP commands in the command queue.
sessions	Lists the number of existing MGCP sessions.
detail	(Optional) Lists additional information about each command (or session) in the output.

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.

Usage Guidelines

The **show mgcp commands** command lists the number of MGCP commands in the command queue. The **show mgcp sessions** command lists the number of existing MGCP sessions. The **detail** option includes additional information about each command (or session) in the output.

Examples

The following are examples of the **show mgcp** command options:

```
hostname# show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07

hostname# show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
        Gateway IP | host-pc-2
        Transaction ID  2052
        Endpoint name | aaln/1
        Call ID | 9876543210abcdef
        Connection ID |
        Media IP | 192.168.5.7
        Media port | 6058
```

```
hostname# show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11

hostname# show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
       Gateway IP | host-pc-2
       Call ID | 9876543210abcdef
       Connection ID | 6789af54c9
       Endpoint name | aaln/1
       Media lcl port  6166
       Media rmt IP | 192.168.5.7
       Media rmt port  6058
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug mgcp	Enables MGCP debug information.
inspect mgcp	Enables MGCP application inspection.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.
show conn	Displays the connection state for different connection types.

show mode

To show the security context mode for the running software image and for any image in Flash memory, use the **show mode** command in privileged EXEC mode.

show mode

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	This command was introduced.

Examples

The following is sample output from the **show mode** command. The following example shows the current mode and the mode for the non-running image "image.bin":

```
hostname# show mode flash:/image.bin
Firewall mode: multiple
```

The mode can be multiple or single.

Related Commands

Command	Description
context	Creates a security context in the system configuration and enters context configuration mode.
mode	Sets the context mode to single or multiple.

show module

To show information about the SSM on the ASA 5500 series adaptive security appliance as well as system information, use the **show module** command in user EXEC mode.

show module [*slot* [**details**] | **all** | **1 recover**]]

Syntax Description

all	(Default) Shows information for the SSM in slot 1 and the system in slot 0.
details	(Optional) Shows additional information, including remote management configuration for intelligent SSMs (for example the AIP SSM).
1 recover	(Optional) For intelligent SSMs, shows the settings for the **hw-module module recover** command.
slot	(Optional) Specifies the slot number, 0 or 1.

Defaults

Shows information for both slots.

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[1]	System
User EXEC	•	•	•	•	•

1. The **show module recover** command is only available in the system execution space.

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command shows information about the SSM as well as the system and built-in interfaces.

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show module** command. Slot 0 is the system, while slot 1 is an SSM.

```
hostname> show module
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            XXXXXXXXXXX
  1 ASA 5500 Series Security Services Module-20  ASA-SSM-20         XXXXXXXXXXX

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.c619 to 000b.fcf8.c61d  1.0          1.0(6)5      7.0(0)77
```

```
  1 000b.fcf8.019f to 000b.fcf8.019f  1.0          1.0(6)5      5.0(0.15)S91(0.15)

Mod Status
--- ------------------
  0 Up Sys
  1 Up
```

Table 22 shows each field description.

Table 7-27 show module Fields

Field	Description
Mod	The slot number, 0 or 1.
Card Type	For the system shown in slot 0, the type is the platform model. For the SSM in slot 1, the SSM type.
Model	The model for this slot.
Serial No.	The serial number.
MAC Address Range	The MAC address range for interfaces on this SSM or, for the system, the built-in interfaces.
Hw Version	The hardware version.
Fw Version	The firmware version.
Sw Version	The software version.
Status	For the system in slot 0, the status is Up Sys. The status of the SSM in slot 1 is as follows: • Initializing—The SSM is being detected and the control communication is being initialized by the system. • Up—The SSM has completed initialization by the system. • Unresponsive—The system encountered an error communicating with this SSM. • Reloading—For intelligent SSMs, the SSM is reloading. • Shutting Down—The SSM is shutting down. • Down—The SSM is shut down. • Recover—For intelligent SSMs, the SSM is attempting to download a recovery image.

The following is sample output from the **show module details** command:

```
hostname> show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:              ASA-SSM-20
Hardware version:   V1.0
Serial Number:      12345678
Firmware version:   1.0(7)2
Software version:   4.1(1.1)S47(0.1)
MAC Address Range:  000b.fcf8.0156 to 000b.fcf8.0156
Status:             Up
Mgmt IP addr:       10.89.147.13
Mgmt web ports:     443
```

```
Mgmt TLS enabled:   true
```

Table 23 shows each field description. See Table 22 for fields that are also shown for the **show module** command.

Table 7-28 show module details Fields

Field	Description
Mgmt IP addr	For intelligent SSMs, shows the IP address for the SSM management interface.
Mgmt web ports	For intelligent SSMs, shows the ports configured for the management interface.
Mgmt TLS enabled	For intelligent SSMs, shows whether transport layer security is enabled for connections to the management interface of the SSM (true or false).

The following is sample output from the **show module recover** command:

```
hostname> show module 1 recover
Module 1 recover parameters…
Boot Recovery Image: Yes
Image URL:           tftp://10.21.18.1/ids-oldimg
Port IP Address:     10.1.2.10
Port Mask :          255.255.255.0
Gateway IP Address:  10.1.2.254
```

Related Commands

Command	Description
debug module-boot	Shows debug messages about the SSM booting process.
hw-module module recover	Recovers an intelligent SSM by loading a recovery image from a TFTP server.
hw-module module reset	Shuts down an SSM and performs a hardware reset.
hw-module module reload	Reloads the intelligent SSM software.
hw-module module shutdown	Shuts down the SSM software in preparation for being powered off without losing configuration data.

show mrib client

To display information about the MRIB client connections, use the **show mrib client** command in user EXEC or privileged EXEC mode.

show mrib client [**filter**] [**name** *client_name*]

Syntax Description

filter	(Optional) Displays client filter. Used to view information about the MRIB flags that each client owns and the flags in which each clients is interested.
name *client_name*	(Optional) Name of a multicast routing protocol that acts as a client of MRIB, such as PIM or IGMP.

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
User EXEC or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **filter** option is used to display the route and interface level flag changes that various MRIB clients have registered. This command option also shows what flags are owned by the MRIB clients.

Examples

The following sample output from the **show mrib client** command using the **filter** keyword:

```
hostname# show mrib client filter
MFWD:0 (connection id 0)
interest filter:
entry attributes: S C IA D
interface attributes: F A IC NS DP SP
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
groups:
include 0.0.0.0/0
interfaces:
include All
igmp:77964 (connection id 1)
```

```
ownership filter:
interface attributes: II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
pim:49287 (connection id 5)
interest filter:
entry attributes: E
interface attributes: SP II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
entry attributes: L S C IA D
interface attributes: F A IC NS DP
groups:
include 0.0.0.0/0
interfaces:
include All
```

Related Commands

Command	Description
show mrib route	Displays MRIB table entries.

show mrib route

To display entries in the MRIB table, use the **show mrib route** command in user EXEC or privileged EXEC mode.

show mrib route [[*source* | *] [*group*[*/prefix-length*]]]

Syntax Description

*	(Optional) Display shared tree entries.
/prefix-length	(Optional) Prefix length of the MRIB route. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
group	(Optional) IP address or name of the group.
source	(Optional) IP address or name of the route source.

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
User EXEC or Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The MFIB table maintains a subset of entries and flags updated from MRIB. The flags determine the forwarding and signaling behavior according to a set of forwarding rules for multicast packets.

In addition to the list of interfaces and flags, each route entry shows various counters. Byte count is the number of total bytes forwarded. Packet count is the number of packets received for this entry. The **show mfib count** command displays global counters independent of the routes.

Examples

The following is sample output from the **show mrib route** command:

```
hostname# show mrib route
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
```

```
LD - Local Disinterest
(*,224.0.0.0/4) RPF nbr: 10.11.1.20 Flags: L C
   Decapstunnel0 Flags: NS

(*,224.0.0.0/24) Flags: D

(*,224.0.1.39) Flags: S

(*,224.0.1.40) Flags: S
   POS0/3/0/0 Flags: II LI

(*,238.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS LI
   Decapstunnel0 Flags: A

(*,239.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS
   Decapstunnel0 Flags: A
```

Related Commands

Command	Description
show mfib count	Displays route and packet count data for the MFIB table.
show mrib route summary	Displays a summary of the MRIB table entries.

show mroute

To display the IPv4 multicast routing table, use the **show mroute** command in privileged EXEC mode.

show mroute [*group* [*source*] | **reserved**] [**active** [*rate*] | **count** | **pruned** | **summary**]

Syntax Description

active *rate*	(Optional) Displays only active multicast sources. Active sources are those sending at the specified *rate* or higher. If the *rate* is not specified, active sources are those sending at a rate of 4 kbps or higher.
count	(Optional) Displays statistics about the group and source, including number of packets, packets per second, average packet size, and bits per second.
group	(Optional) IP address or name of the multicast group as defined in the DNS hosts table.
pruned	(Optional) Displays pruned routes.
reserved	(Optional) Displays reserved groups.
source	(Optional) Source hostname or IP address.
summary	(Optional) Displays a one-line, abbreviated summary of each entry in the multicast routing table.

Defaults

If not specified, the *rate* argument defaults to 4 kbps.

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	This command was introduced.

Usage Guidelines

The **show mroute** command displays the contents of the multicast routing table. The security appliance populates the multicast routing table by creating (S,G) and (*,G) entries based on PIM protocol messages, IGMP reports, and traffic. The asterisk (*) refers to all source addresses, the "S" refers to a single source address, and the "G" is the destination multicast group address. In creating (S, G) entries, the software uses the best path to that destination group found in the unicast routing table (through RPF).

To view the **mroute** commands in the running configuration, use the **show running-config mroute** command.

Examples

The following is sample output from the **show mroute** command:

```
hostname(config)# show mroute

Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 239.1.1.40), 08:07:24/never, RP 0.0.0.0, flags: DPC
  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Outgoing interface list:
    inside, Null, 08:05:45/never
    tftp, Null, 08:07:24/never

(*, 239.2.2.1), 08:07:44/never, RP 140.0.0.70, flags: SCJ
  Incoming interface: outside
  RPF nbr: 140.0.0.70
  Outgoing interface list:
    inside, Forward, 08:07:44/never
```

The following fields are shown in the **show mroute** output:

- **Flags**—Provides information about the entry.
  - **D—Dense**. Entry is operating in dense mode.
  - **S—Sparse**. Entry is operating in sparse mode.
  - **B—Bidir Group**. Indicates that a multicast group is operating in bidirectional mode.
  - **s—SSM Group**. Indicates that a multicast group is within the SSM range of IP addresses. This flag is reset if the SSM range changes.
  - **C—Connected**. A member of the multicast group is present on the directly connected interface.
  - **L—Local**. The security appliance itself is a member of the multicast group. Groups are joined locally by the **igmp join-group** command (for the configured group).
  - **I—Received Source Specific Host Report**. Indicates that an (S, G) entry was created by an (S, G) report. This (S, G) report could have been created by IGMP. This flag is set only on the DR.
  - **P—Pruned**. Route has been pruned. The software keeps this information so that a downstream member can join the source.
  - **R—RP-bit set**. Indicates that the (S, G) entry is pointing toward the RP.
  - **F—Register flag**. Indicates that the software is registering for a multicast source.
  - **T—SPT-bit set**. Indicates that packets have been received on the shortest path source tree.
  - **J—Join SPT**. For (*, G) entries, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold set for the group. (The default SPT-Threshold setting is 0 kbps.) When the J - Join shortest path tree (SPT) flag is set, the next (S, G) packet received down the shared tree triggers an (S, G) join in the direction of the source, thereby causing the security appliance to join the source tree.

For (S, G) entries, indicates that the entry was created because the SPT-Threshold for the group was exceeded. When the J - Join SPT flag is set for (S, G) entries, the security appliance monitors the traffic rate on the source tree and attempts to switch back to the shared tree for this source if the traffic rate on the source tree falls below the SPT-Threshold of the group for more than 1 minute.

Note The security appliance measures the traffic rate on the shared tree and compares the measured rate to the SPT-Threshold of the group once every second. If the traffic rate exceeds the SPT-Threshold, the J - Join SPT flag is set on the (*, G) entry until the next measurement of the traffic rate. The flag is cleared when the next packet arrives on the shared tree and a new measurement interval is started.

If the default SPT-Threshold value of 0 kbps is used for the group, the J - Join SPT flag is always set on (*, G) entries and is never cleared. When the default SPT-Threshold value is used, the security appliance immediately switches to the shortest path source tree when traffic from a new source is received.

- **Timers:Uptime/Expires**—Uptime indicates per interface how long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table. Expires indicates per interface how long (in hours, minutes, and seconds) until the entry will be removed from the IP multicast routing table.
- **Interface state**—Indicates the state of the incoming or outgoing interface.
  - **Interface**—The interface name listed in the incoming or outgoing interface list.
  - **State**—Indicates that packets will either be forwarded, pruned, or null on the interface depending on whether there are restrictions due to access lists or a time-to-live (TTL) threshold.
- **(*, 239.1.1.40)** and **(* , 239.2.2.1)**—Entries in the IP multicast routing table. The entry consists of the IP address of the source followed by the IP address of the multicast group. An asterisk (*) in place of the source indicates all sources.
- **RP**—Address of the RP. For routers and access servers operating in sparse mode, this address is always 224.0.0.0.
- **Incoming interface**—Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
- **RPF nbr**—IP address of the upstream router to the source.
- **Outgoing interface list**—Interfaces through which packets will be forwarded.

Related Commands

Command	Description
clear configure mroute	Removes the **mroute** commands from the running configuration.
mroute	Configures a static multicast route.
show mroute	Displays IPv4 multicast routing table.
show running-config mroute	Displays configured multicast routes.

show nameif

To view the interface name set using the **nameif** command, use the show nameif command in privileged EXEC mode.

show nameif [*physical_interface*[**.***subinterface*] | *mapped_name*]

Syntax Description

mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

If you do not specify an interface, the security appliance shows all interface names.

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.

Usage Guidelines

In multiple context mode, if you mapped the interface ID in the **allocate-interface** command, you can only specify the mapped name in a context. The output for this command shows only the mapped name in the Interface column.

Examples

The following is sample output from the **show nameif** command:

```
hostname# show nameif
Interface               Name                    Security
GigabitEthernet0/0      outside                 0
GigabitEthernet0/1      inside                  100
GigabitEthernet0/2      test2                   50
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
interface	Configures an interface and enters interface configuration mode.
nameif	Sets the interface name.
show interface ip brief	Shows the interface IP address and status.

show ntp associations

To view NTP association information, use the **show ntp associations** command in user EXEC mode.

show ntp associations [**detail**]

Syntax Description

detail	(Optional) Shows additional details about each association.

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**
User EXEC	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show ntp associations** command:

```
hostname> show ntp associations
     address         ref clock     st  when  poll  reach  delay  offset    disp
 ~172.31.32.2      172.31.32.1      5    29  1024  377     4.2   -8.59     1.6
+~192.168.13.33    192.168.1.111    3    69   128  377     4.1    3.48     2.3
*~192.168.13.57    192.168.1.111    3    32   128  377     7.9   11.18     3.6
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

Table 7-26 shows each field description.

Table 7-29 show ntp associations Fields

Field	Description
(leading characters in display lines)	The first characters in a display line can be one or more of the following characters: • * —Synchronized to this peer. • # —Almost synchronized to this peer. • + —Peer selected for possible synchronization. • - —Peer is a candidate for selection. • ~ —Peer is statically configured, but not synchronized.
address	The address of the NTP peer.
ref clock	The address of the reference clock of the peer.
st	The stratum of the peer.
when	The time since the last NTP packet was received from the peer.
poll	The polling interval (in seconds).
reach	The peer reachability (as a bit string, in octal).
delay	The round-trip delay to the peer (in milliseconds).
offset	The relative time of the peer clock to the local clock (in milliseconds).
disp	The dispersion value.

The following is sample output from the **show ntp associations detail** command:

```
hostname> show ntp associations detail
172.23.56.249 configured, our_master, sane, valid, stratum 4
ref ID 172.23.56.225, time c0212639.2ecfc9e0 (20:19:05.182 UTC Fri Feb 22 2002)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 38.04 msec, root disp 9.55, reach 177, sync dist 156.021
delay 4.47 msec, offset -0.2403 msec, dispersion 125.21
precision 2**19, version 3
org time c02128a9.731f127b (20:29:29.449 UTC Fri Feb 22 2002)
rcv time c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
xmt time c02128a9.6b3f729e (20:29:29.418 UTC Fri Feb 22 2002)
filtdelay =     4.47    4.58    4.97    5.63    4.79    5.52    5.87    0.00
filtoffset =   -0.24   -0.36   -0.37    0.30   -0.17    0.57   -0.74    0.00
filterror =     0.02    0.99    1.71    2.69    3.66    4.64    5.62    16000.0
```

Table 7-27 shows each field description.

Table 7-30 show ntp associations detail Fields

Field	Description
IP-address configured	The server (peer) IP address.
(status)	• our_master—The security appliance is synchronized to this peer. • selected—Peer is selected for possible synchronization. • candidate—Peer is a candidate for selection.

Table 7-30 show ntp associations detail Fields (continued)

Field	Description
(sanity)	• sane—The peer passes basic sanity checks. • insane—The peer fails basic sanity checks.
(validity)	• valid—The peer time is believed to be valid. • invalid—The peer time is believed to be invalid. • leap_add—The peer is signalling that a leap second will be added. • leap-sub—The peer is signalling that a leap second will be subtracted.
stratum	The stratum of the peer.
(reference peer)	unsynced—The peer is not synchronized to any other machine. ref ID—The address of the machine that the peer is synchronized to.
time	The last time stamp the peer received from its master.
our mode client	Our mode relative to the peer, which is always client.
peer mode server	The peer's mode relative to us, which is always server.
our poll intvl	Our poll interval to the peer.
peer poll intvl	The peer poll interval to us.
root delay	The delay along the path to the root (ultimate stratum 1 time source).
root disp	The dispersion of the path to the root.
reach	The peer reachability (as a bit string in octal).
sync dist	The peer synchronization distance.
delay	The round-trip delay to the peer.
offset	The offset of the peer clock relative to our clock.
dispersion	The dispersion of the peer clock.
precision	The precision of the peer clock (in hertz).
version	The NTP version number that the peer is using.
org time	The originate time stamp.
rcv time	The receive time stamp.
xmt time	The transmit time stamp.
filtdelay	The round-trip delay (in milliseconds) of each sample.
filtoffset	The clock offset (in milliseconds) of each sample.
filterror	The approximate error of each sample.

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Sets an encrypted authentication key to synchronize with an NTP server.
ntp server	Identifies an NTP server.

Command	Description
ntp trusted-key	Provides a key ID for the security appliance to use in packets for authentication with an NTP server.
show ntp status	Shows the status of the NTP association.

show ntp status

To show the status of each NTP association, use the **show ntp status** command in user EXEC mode.

show ntp status

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
User EXEC	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show ntp status** command:

```
hostname> show ntp status
Clock is synchronized, stratum 5, reference is 172.23.56.249
nominal freq is 99.9984 Hz, actual freq is 100.0266 Hz, precision is 2**6
reference time is c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
clock offset is -0.2403 msec, root delay is 42.51 msec
root dispersion is 135.01 msec, peer dispersion is 125.21 msec
```

Table 7-28 shows each field description.

Table 7-31 show ntp status Fields

Field	Description
Clock	• synchronized—The security appliance is synchronized to an NTP server. • unsynchronized—The security appliance is not synchronized to an NTP server.
stratum	NTP stratum of this system.

Table 7-31 show ntp status Fields

Field	Description
reference	The address of the NTP server to which the security appliance is synchronized.
nominal freq	The nominal frequency of the system hardware clock.
actual freq	The measured frequency of the system hardware clock.
precision	The precision of the clock of this system (in hertz).
reference time	The reference time stamp.
clock offset	The offset of the system clock to the synchronized peer.
root delay	The total delay along the path to the root clock.
root dispersion	The dispersion of the root path.
peer dispersion	The dispersion of the synchronized peer.

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Sets an encrypted authentication key to synchronize with an NTP server.
ntp server	Identifies an NTP server.
ntp trusted-key	Provides a key ID for the security appliance to use in packets for authentication with an NTP server.
show ntp associations	Shows the NTP servers with which the security appliance is associated.

show ospf

To display the general information about the OSPF routing processes, use the **show ospf** command in privileged EXEC mode.

show ospf [*pid* **[***area_id***]**]

Syntax Description

area_id	(Optional) ID of the area that is associated with the OSPF address range.
pid	(Optional) The ID of the OSPF process.

Defaults

Lists all OSPF processes if no *pid* is specified.

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.

Usage Guidelines

If the *pid* is included, only information for the specified routing process is included.

Examples

The following is sample output from the **show ospf** command, showing how to display general information about a specific OSPF routing process:

```
hostname# show ospf 5
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

The following is sample output from the **show ospf** command, showing how to display general information about all OSPF routing processes:

```
hostname# show ospf
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
```

```
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x     0
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0

Routing Process "ospf 12" with ID 172.23.59.232 and Domain ID 0.0.0.12
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x     0
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0
```

Related Commands

Command	Description
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf border-routers

To display the internal OSPF routing table entries to ABRs and ASBRs, use the **show ospf border-routers** command in privileged EXEC mode.

show ospf border-routers

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 **ospf border-routers** command:

```
hostname# show ospf border-routers

OSPF Process 109 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 192.168.97.53 [10] via 192.168.1.53, fifth, ABR, Area 0, SPF 20
i 192.168.103.51 [10] via 192.168.96.51, outside, ASBR, Area 192.168.12.0, SPF 14
i 192.168.103.52 [10] via 192.168.96.51, outside, ABR/ASBR, Area 192.168.12.0, SPF 14
```

Related Commands

Command	Description
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf database

To display the information contained in the OSPF topological database on the security appliance, use the **show ospf database** command in privileged EXEC mode.

show ospf [*pid* [*area_id*]] **database** [**router** | **network** | **summary** | **asbr-summary** | **external** | **nssa-external**] [*lsid*] [**internal**] [**self-originat**e | **adv-router** *addr*]

show ospf [*pid* [*area_id*]] **database database-summary**

Syntax Description

addr	(Optional) Router address.
adv-router	(Optional) Advertised router.
area_id	(Optional) ID of the area that is associated with the OSPF address range.
asbr-summary	(Optional) Displays an ASBR list summary.
database	Displays the database information.
database-summary	(Optional) Displays the complete database summary list.
external	(Optional) Displays routes external to a specified autonomous system.
internal	(Optional) Routes that are internal to a specified autonomous system.
lsid	(Optional) LSA ID.
network	(Optional) Displays the OSPF database information about the network.
nssa-external	(Optional) Displays the external not-so-stubby-area list.
pid	(Optional) ID of the OSPF process.
router	(Optional) Displays the router.
self-originate	(Optional) Displays the information for the specified autonomous system.
summary	(Optional) Displays a summary of the list.

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.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the security appliance. You do not need to be in an OSPF configuration mode to use the OSPF-related **show** commands.

Examples

The following is sample output from the **show ospf database** command:

```
hostname# show ospf database
OSPF Router with ID(192.168.1.11) (Process ID 1)

                Router Link States(Area 0)
Link ID   ADV Router   Age   Seq# Checksum Link count
192.168.1.8 192.168.1.8 1381 0x8000010D    0xEF60 2
192.168.1.11 192.168.1.11 1460 0x800002FE    0xEB3D 4
192.168.1.12 192.168.1.12 2027 0x80000090    0x875D 3
192.168.1.27 192.168.1.27 1323 0x800001D6    0x12CC 3

                Net Link States(Area 0)
Link ID ADV Router   Age   Seq# Checksum
172.16.1.27 192.168.1.27 1323 0x8000005B    0xA8EE
172.17.1.11 192.168.1.11 1461 0x8000005B    0x7AC

                Type-10 Opaque Link Area Link States (Area 0)
Link ID ADV Router   Age Seq# Checksum Opaque ID
10.0.0.0 192.168.1.11 1461 0x800002C8    0x8483   0
10.0.0.0 192.168.1.12 2027 0x80000080    0xF858   0
10.0.0.0 192.168.1.27 1323 0x800001BC    0x919B   0
10.0.0.1 192.168.1.11 1461 0x8000005E    0x5B43   1
```

The following is sample output from the **show ospf database asbr-summary** command:

```
hostname# show ospf database asbr-summary
OSPF Router with ID(192.168.239.66) (Process ID 300)
Summary ASB Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router)
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0
TOS: 0 Metric: 1
```

The following is sample output from the **show ospf database router** command:

```
hostname# show ospf database router
OSPF Router with id(192.168.239.66) (Process ID 300)
Router Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 10.187.21.6
Advertising Router: 10.187.21.6
LS Seq Number: 80002CF6
Checksum: 0x73B7
Length: 120
AS Boundary Router
Number of Links: 8
Link connected to: another Router (point-to-point)
(link ID) Neighboring Router ID: 10.187.21.5
```

```
(Link Data) Router Interface address: 10.187.21.6
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

The following is sample output from the **show ospf database network** command:

```
hostname# show ospf database network
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Net Link States(Area 0.0.0.0)
LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links
Link State ID: 10.187.1.3 (address of Designated Router)
Advertising Router: 192.168.239.66
LS Seq Number: 800000E7
Checksum: 0x1229
Length: 52
Network Mask: 255.255.255.0
Attached Router: 192.168.239.66
Attached Router: 10.187.241.5
Attached Router: 10.187.1.1
Attached Router: 10.187.54.5
Attached Router: 10.187.1.5
```

The following is sample output from the **show ospf database summary** command:

```
hostname# show ospf database summary
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Summary Net Link States(Area 0.0.0.0)
LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network)
Link State ID: 10.187.240.0 (summary Network Number)
Advertising Router: 10.187.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0 TOS: 0 Metric: 1
```

The following is sample output from the **show ospf database external** command:

```
hostname# show ospf database external
OSPF Router with id(192.168.239.66) (Autonomous system 300)

                  Displaying AS External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 172.16.0.0 (External Network Number)
Advertising Router: 10.187.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0

      Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 0
```

Related Commands

Command	Description
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf flood-list

To display a list of OSPF LSAs waiting to be flooded over an interface, use the **show ospf flood-list** command in privileged EXEC mode.

show ospf flood-list *interface_name*

Syntax Description

interface_name	The name of the interface for which to display neighbor information.

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.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the security appliance. You do not need to be in an OSPF configuration mode to use the OSPF-related **show** commands.

Examples

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

```
hostname# show ospf flood-list outside

  Interface outside, Queue length 20
  Link state flooding due in 12 msec

  Type  LS ID          ADV RTR          Seq NO       Age   Checksum
     5  10.2.195.0     192.168.0.163    0x80000009   0     0xFB61
     5  10.1.192.0     192.168.0.163    0x80000009   0     0x2938
     5  10.2.194.0     192.168.0.163    0x80000009   0     0x757
     5  10.1.193.0     192.168.0.163    0x80000009   0     0x1E42
     5  10.2.193.0     192.168.0.163    0x80000009   0     0x124D
     5  10.1.194.0     192.168.0.163    0x80000009   0     0x134C
```

Related Commands

Command	Description
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf interface

To display the OSPF-related interface information, use the **show ospf interface** command in privileged EXEC mode.

show ospf interface [*interface_name*]

Syntax Description

interface_name	(Optional) Name of the interface for which to display the OSPF-related information.

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.

Usage Guidelines

When used without the *interface_name* argument, the OSPF information for all interfaces is shown.

Examples

The following is sample output from the **show ospf interface** command:

```
hostname# show ospf interface inside
inside is up, line protocol is up
Internet Address 192.168.254.202, Mask 255.255.255.0, Area 0.0.0.0
AS 201, Router ID 192.77.99.1, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State OTHER, Priority 1
Designated Router id 192.168.254.10, Interface address 192.168.254.10
Backup Designated router id 192.168.254.28, Interface addr 192.168.254.28
Timer intervals configured, Hello 10, Dead 60, Wait 40, Retransmit 5
Hello due in 0:00:05
Neighbor Count is 8, Adjacent neighbor count is 2
  Adjacent with neighbor 192.168.254.28 (Backup Designated Router)
  Adjacent with neighbor 192.168.254.10 (Designated Router)
```

Related Commands

Command	Description
interface	Opens interface configuration mode.

show ospf neighbor

To display the OSPF-neighbor information on a per-interface basis, use the **show ospf neighbor** command in privileged EXEC mode.

show ospf neighbor [**detail** | *interface_name* [*nbr_router_id*]]

Syntax Description

detail	(Optional) Lists detail information for the specified router.
interface_name	(Optional) Name of the interface for which to display neighbor information.
nbr_router_id	(Optional) Router ID of the neighbor router.

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 ospf neighbor** command. It shows how to display the OSPF-neighbor information on a per-interface basis.

```
hostname# show ospf neighbor outside

Neighbor 192.168.5.2, interface address 10.225.200.28
    In the area 0 via interface outside
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.225.200.28 BDR is 10.225.200.30
    Options is 0x42
    Dead timer due in 00:00:36
    Neighbor is up for 00:09:46
  Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

Related Commands

Command	Description
neighbor	Configures OSPF routers interconnecting to non-broadcast networks.
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf request-list

To display a list of all LSAs that are requested by a router, use the **show ospf request-list** command in privileged EXEC mode.

show ospf request-list *nbr_router_id interface_name*

Syntax Description

interface_name	Name of the interface for which to display neighbor information. Displays the list of all LSAs that are requested by the router from this interface.
nbr_router_id	Router ID of the neighbor router. Displays the list of all LSAs that are requested by the router from this neighbor.

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 ospf request-list** command:

```
hostname# show ospf request-list 192.168.1.12 inside

          OSPF Router with ID (192.168.1.11) (Process ID 1)

  Neighbor 192.168.1.12, interface inside address 172.16.1.12

  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x8000020D   8     0x6572
```

Related Commands

Command	Description
show ospf retransmission-list	Displays a list of all LSAs waiting to be resent.

show ospf retransmission-list

To display a list of all LSAs waiting to be resent, use the **show ospf retransmission-list** command in privileged EXEC mode.

show ospf retransmission-list *nbr_router_id interface_name*

Syntax Description

interface_name	Name of the interface for which to display neighbor information.
nbr_router_id	Router ID of the neighbor router.

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.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the security appliance. You do not need to be in an OSPF configuration mode to use the OSPF-related **show** commands.

The *nbr_router_id* argument displays the list of all LSAs that are waiting to be resent for this neighbor.

The *interface_name* argument displays the list of all LSAs that are waiting to be resent for this interface.

Examples

The following is sample output from the **show ospf retransmission-list** command, where the *nbr_router_id* argument is 192.168.1.11 and the *if_name* argument is outside:

```
hostname# show ospf retransmission-list 192.168.1.11 outside

          OSPF Router with ID (192.168.1.12) (Process ID 1)

  Neighbor 192.168.1.11, interface outside address 172.16.1.11
  Link state retransmission due in 3764 msec, Queue length 2


  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x80000210   0     0xB196
```

Related Commands

Command	Description
show ospf request-list	Displays a list of all LSAs that are requested by a router.

show ospf summary-address

To display a list of all summary address redistribution information that is configured under an OSPF process, use the **show ospf summary-address** command in privileged EXEC mode.

show ospf summary-address

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 shows sample output from the **show ospf summary-address** command. It shows how to display a list of all summary address redistribution information before a summary address has been configured for an OSPF process with the ID of 5.

```
hostname# show ospf 5 summary-address

OSPF Process 2, Summary-address

10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 0
10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 10
```

Related Commands

Command	Description
summary-address	Creates aggregate addresses for OSPF.

show ospf virtual-links

To display the parameters and the current state of OSPF virtual links, use the **show ospf virtual-links** command in privileged EXEC mode.

show ospf virtual-links

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 ospf virtual-links** command:

```
hostname# show ospf virtual-links

Virtual Link to router 192.168.101.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

Related Commands

Command	Description
area virtual-link	Defines an OSPF virtual link.

show perfmon

To display information about the performance of the security appliance, use the **show perfmon** command.

show perfmon

Syntax Description

This command has no arguments or keywords.

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	Support for this command was introduced on the security appliance.
7.0(8)	The following rate outputs were added: TCP Intercept Established Conns, TCP Intercept Attempts, TCP Embryonic Conns Timeout, and Valid Conns Rate in Tcp Intercept.

Usage Guidelines

This command output does not display in a Telnet console session.

The **perfmon** command allows you to monitor the security appliance's performance. The **show perfmon** command allows you to display the information immediately.

Examples

This example shows how to display information about the security appliance performance:

```
hostname(config)# show perfmon
Context: my_context

PERFMON STATS:                     Current      Average
Xlates                               0/s          0/s
Connections                          0/s          0/s
TCP Conns                            0/s          0/s
UDP Conns                            0/s          0/s
URL Access                           0/s          0/s
URL Server Req                       0/s          0/s
TCP Fixup                            0/s          0/s
TCP Intercept Established Conns      0/s          0/s
TCP Intercept Attempts               0/s          0/s
TCP Embryonic Conns Timeout          0/s          0/s
```

```
HTTP Fixup                              0/s          0/s
FTP Fixup                               0/s          0/s
AAA Authen                              0/s          0/s
AAA Author                              0/s          0/s
AAA Account                             0/s          0/s

VALID CONNS RATE in TCP INTERCEPT:    Current      Average
                                       100.00%         100.00%
```

Related Commands

Command	Description
perfmon	Displays detailed performance monitoring information.

show pim df

To display the bidirectional DF "winner" for a rendezvous point (RP) or interface, use the **show pim df** command in user EXEC or privileged EXEC mode.

show pim df [**winner**] [*rp_address* | *if_name*]

Syntax Description

rp_address	Can be either one of the following: • Name of the RP, as defined in the Domain Name System (DNS) hosts table or with the domain **ipv4 host** command. • IP address of the RP. This is a multicast IP address in four-part dotted-decimal notation.
if_name	The physical or logical interface name.
winner	(Optional) Displays the DF election winner per interface per RP.

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
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command also displays the winner metric towards the RP.

Examples

The following is sample output from the **show pim df** command:

```
hostname# show df winner inside
RP           Interface   DF Winner   Metrics

172.16.1.3   Loopback3   172.17.3.2  [110/2]
172.16.1.3   Loopback2   172.17.2.2  [110/2]
172.16.1.3   Loopback1   172.17.1.2  [110/2]
172.16.1.3   inside      10.10.2.3   [0/0]
172.16.1.3   inside      10.10.1.2   [110/2]
```

show pim group-map

To display group-to-protocol mapping table, use the **show pim group-map** command in user EXEC or privileged EXEC mode.

show pim group-map [**info-source**] [*group*]

Syntax Description

group	(Optional) Can be either one of the following: • Name of the multicast group, as defined in the DNS hosts table or with the domain **ipv4 host** command. • IP address of the multicast group. This is a multicast IP address in four-part dotted-decimal notation.
info-source	(Optional) Displays the group range information source.

Defaults

Displays group-to-protocol mappings for all groups.

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
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command displays all group protocol address mappings for the RP. Mappings are learned on the security appliance from different clients.

The PIM implementation on the security appliance has various special entries in the mapping table. Auto-rp group ranges are specifically denied from sparse-mode group range. SSM group range also does not fall under sparse-mode. Link Local multicast groups (224.0.0.0–224.0.0.225, as defined by 224.0.0.0/24) are also denied from the sparse-mode group range. The last entry shows all remaining groups in Sparse-Mode with a given RP.

If multiple RPs are configured with the **pim rp-address** command, then the appropriate group range is displayed with their corresponding RPs.

Examples

The following is sample output form the **show pim group-map** command:

```
hostname# show pim group-map
Group Range      Proto   Client Groups   RP address   Info
```

```
224.0.1.39/32*   DM      static 1        0.0.0.0
224.0.1.40/32*   DM      static 1        0.0.0.0
224.0.0.0/24*    NO      static 0        0.0.0.0
232.0.0.0/8*     SSM     config 0        0.0.0.0
224.0.0.0/4*     SM      autorp 1        10.10.2.2    RPF: POS01/0/3,10.10.3.2
```

In lines 1 and 2, Auto-RP group ranges are specifically denied from the sparse mode group range.

In line 3, link-local multicast groups (224.0.0.0 to 224.0.0.255 as defined by 224.0.0.0/24) are also denied from the sparse mode group range.

In line 4, the PIM Source Specific Multicast (PIM-SSM) group range is mapped to 232.0.0.0/8.

The last entry shows that all the remaining groups are in sparse mode mapped to RP 10.10.3.2.

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.
pim rp-address	Configures the address of a PIM rendezvous point (RP).

show pim interface

To display interface-specific information for PIM, use the **show pim interface** command in user EXEC or privileged EXEC mode.

show pim interface [*if_name* | **state-off** | **state-on**]

Syntax Description

if_name	(Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.
state-off	(Optional) Displays interfaces with PIM disabled.
state-on	(Optional) Displays interfaces with PIM enabled.

Defaults

If you do not specify an interface, PIM information for all interfaces is shown.

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
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The PIM implementation on the security appliance considers the security appliance itself a PIM neighbor. Therefore, the neighbor count column in the output of this command shows one more than the actual number of neighbors.

Examples

The following example displays PIM information for the inside interface:

```
hostname# show pim interface inside
Address    Interface      Ver/     Nbr     Query      DR     DR
                          Mode     Count   Intvl      Prior
172.16.1.4 inside         v2/S     2       100 ms     1      172.16.1.4
```

Related Commands

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

show pim join-prune statistic

To display PIM join/prune aggregation statistics, use the **show pim join-prune statistics** command in user EXEC or privileged EXEC mode.

show pim join-prune statistics [*if_name*]

Syntax Description

if_name	(Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.

Defaults

If an interface is not specified, this command shows the join/prune statistics 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
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Clear the PIM join/prune statistics with the **clear pim counters** command.

Examples

The following is sample output from the **show pim join-prune statistic** command:

```
hostname# show pim join-prune statistic

PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface          Transmitted             Received

            inside   0 /    0 /    0         0 /    0 /    0
  GigabitEthernet1   0 /    0 /    0         0 /    0 /    0
         Ethernet0   0 /    0 /    0         0 /    0 /    0
         Ethernet3   0 /    0 /    0         0 /    0 /    0
  GigabitEthernet0   0 /    0 /    0         0 /    0 /    0
         Ethernet2   0 /    0 /    0         0 /    0 /    0
```

Related Commands

Command	Description
clear pim counters	Clears the PIM traffic counters.

show pim neighbor

To display entries in the PIM neighbor table, use the **show pim neighbor** command in user EXEC or privileged EXEc mode.

show pim neighbor [**count** | **detail**] [*interface*]

Syntax Description

interface	(Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.
count	(Optional) Displays the total number of PIM neighbors and the number of PIM neighbors on each interface.
detail	(Optional) Displays additional address of the neighbor learned through the upstream-detection hello option.

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command is used to determine the PIM neighbors known to this router through PIM hello messages. Also, this command indicates that an interface is a designated router (DR) and when the neighbor is capable of bidirectional operation.

The PIM implementation on the security appliance considers the security appliance itself to be a PIM neighbor. Therefore, the security appliance interface is shown in the output of this command. The IP address of the security appliance is indicated by an asterisk next to the address.

Examples

The following is sample output from the **show pim neighbor** command:

```
hostname# show pim neighbor inside
Neighbor Address    Interface    Uptime     Expires   DR  pri  Bidir
10.10.1.1           inside       03:40:36   00:01:41  1        B
10.10.1.2*          inside       03:41:28   00:01:32  1   (DR) B
```

Related Commands

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

show pim range-list

To display range-list information for PIM, use the **show pim range-list** command in user EXEC or privileged EXEC mode.

show pim range-list [*rp_address*]

Syntax Description

rp_address	Can be either one of the following: • Name of the RP, as defined in the Domain Name System (DNS) hosts table or with the domain **ipv4 host** command. • IP address of the RP. This is a multicast IP address in four-part dotted-decimal notation.

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
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command is used to determine the multicast forwarding mode to group mapping. The output also indicates the rendezvous point (RP) address for the range, if applicable.

Examples

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

```
hostname# show pim range-list
config SSM Exp: never Src: 0.0.0.0
  230.0.0.0/8 Up: 03:47:09
config BD RP: 172.16.1.3 Exp: never Src: 0.0.0.0
  239.0.0.0/8 Up: 03:47:16
config BD RP: 172.18.1.6 Exp: never Src: 0.0.0.0
  239.100.0.0/16 Up: 03:47:10
config SM RP: 172.18.2.6 Exp: never Src: 0.0.0.0
  235.0.0.0/8 Up: 03:47:09
```

Related Commands

Command	Description
show pim group-map	Displays group-to-PIM mode mapping and active RP information.

show pim topology

To display PIM topology table information, use the **show pim topology** command in user EXEC or privileged EXEC mode.

show pim topology [*group*] [*source*]

Syntax Description

group	(Optional) Can be one of the following: • Name of the multicast group, as defined in the DNS hosts table or with the domain **ipv4 host** command. • IP address of the multicast group. This is a multicast IP address in four-part dotted-decimal notation.
source	(Optional) Can be one of the following: • Name of the multicast source, as defined in the DNS hosts table or with the domain **ipv4 host** command. • IP address of the multicast source. This is a multicast IP address in four-part dotted-decimal notation.

Defaults

Topology information for all groups and sources is shown.

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
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use the PIM topology table to display various entries for a given group, (*, G), (S, G), and (S, G)RPT, each with its own interface list.

PIM communicates the contents of these entries through the MRIB, which is an intermediary for communication between multicast routing protocols, such as PIM, local membership protocols, such as Internet Group Management Protocol (IGMP), and the multicast forwarding engine of the system.

The MRIB shows on which interface the data packet should be accepted and on which interfaces the data packet should be forwarded, for a given (S, G) entry. Additionally, the Multicast Forwarding Information Base (MFIB) table is used during forwarding to decide on per-packet forwarding actions.

Note For forwarding information, use the **show mfib route** command.

Examples

The following is sample output from the **show pim topology** command:

```
hostname# show pim topology

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR
(*,224.0.1.40) DM Up: 15:57:24 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags: LH DSS
  outside            15:57:24  off LI LH

(*,224.0.1.24) SM Up: 15:57:20 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:20  fwd LI LH

(*,224.0.1.60) SM Up: 15:57:16 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:16  fwd LI LH
```

Related Commands

Command	Description
show mrib route	Displays the MRIB table.

show pim topology reserved

To display PIM topology table information for reserved groups, use the **show pim topology reserved** command in user EXEC or privileged EXEC mode.

show pim topology reserved

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
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

None.

Related Commands

Command	Description
show pim topology	Displays the PIM topology table.

show pim topology route-count

To display PIM topology table entry counts, use the **show pim topology route-count** command in user EXEC or privileged EXEC mode.

show pim topology route-count [**detail**]

Syntax Description

detail	(Optional) Displays more detailed count information on a per-group basis.

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**
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

This command displays the count of entries in the PIM topology table. To display more information about the entries, use the **show pim topology** command.

Examples

The following is sample output from the **show pim topology route-count** command:

```
hostname# show pim topology route-count

PIM Topology Table Summary
  No. of group ranges = 5
  No. of (*,G) routes = 0
  No. of (S,G) routes = 0
  No. of (S,G)RPT routes = 0
```

Related Commands

Command	Description
show pim topology	Displays the PIM topology table.

show pim traffic

To display PIM traffic counters, use the **show pim traffic** command in user EXEC or privileged EXEC mode.

show pim traffic

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
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Clear the PIM traffic counters with the **clear pim counters** command.

Examples

The following is sample output from the **show pim traffic** command:

```
hostname# show pim traffic

PIM Traffic Counters
Elapsed time since counters cleared: 3d06h

                                Received     Sent
Valid PIM Packets                      0        9485
Hello                                  0        9485
Join-Prune                             0           0
Register                               0           0
Register Stop                          0           0
Assert                                 0           0
Bidir DF Election                      0           0

Errors:
Malformed Packets                                  0
Bad Checksums                                      0
Send Errors                                        0
Packet Sent on Loopback Errors                     0
Packets Received on PIM-disabled Interface         0
Packets Received with Unknown PIM Version          0
```

Related Commands

Command	Description
clear pim counters	Clears the PIM traffic counters.

show pim tunnel

To display information about the PIM tunnel interfaces, use the **show pim tunnels** command in user EXEC or privileged EXEC mode.

show pim tunnels [*if_name*]

Syntax Description

if_name	(Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.

Defaults

If an interface is not specified, this command shows the PIM tunnel information 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
User EXEC or privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

PIM register packets are sent through the virtual encapsulation tunnel interface from the source first hop DR router to the RP. On the RP, a virtual decapsulation tunnel is used to represent the receiving interface of the PIM register packets. This command displays tunnel information for both types of interfaces.

Register tunnels are the encapsulated (in PIM register messages) multicast packets from a source that is sent to the RP for distribution through the shared tree. Registering applies only to SM, not SSM and bidirectional PIM.

Examples

The following is sample output from the **show pim tunnel** command:

```
hostname# show pim tunnel

Interface     RP Address Source Address


Encapstunnel0 10.1.1.1   10.1.1.1

Decapstunnel0 10.1.1.1   -
```

show priority-queue statistics

To display the priority-queue statistics for an interface, use the **show priority-queue statistics** command in privileged EXEC mode.

show priority-queue statistics [*interface-name*]

Syntax Description

interface-name	(Optional) Specifies the name of the interface for which you want to show the best-effort and low-latency queue details.

Defaults

If you omit the interface name, this command shows priority-queue statistics for all configured 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
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

This example shows the use of the **show priority-queue statistics** command for the interface named test, and the command output. In this output, BE indicates the best-effort queue, and LLQ represents the low-latency queue:

```
hostname# show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type      = BE
Packets Dropped   = 0
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0

Queue Type      = LLQ
Packets Dropped   = 0
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0
hostname#
```

Related Commands

Command	Description
clear configure priority-queue	Removes the priority-queue configuration from the named interface.
clear priority-queue statistics	Clears the priority-queue statistics counters for an interface or for all configured interfaces
priority-queue	Configures priority queueing on an interface.
show running-config priority-queue	Shows the current priority-queue configuration on the named interface.

show processes

To display a list of the processes that are running on the security appliance, use the **show processes** command in privileged EXEC mode.

show processes [cpu-hog | memory | internals]

Defaults

By default this command displays the processes running on 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
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0	Support for this command was introduced on the security appliance.

Usage Guidelines

The **show processes** command allows you to display a list of the processes that are running on the security appliance.

The command can also help determine what process is using the CPU, with the optional **cpu-hog** argument. A process is flagged if it is hogging the CPU for more than 100 milliseconds. The **show process cpu-hog** command displays the following columns when invoked:

- MAXHOG - Maximum CPU hog runtime in milliseconds.
- NUMHOG - Number of CPU hog runs.
- LASTHOG - Last CPU hog runtime in milliseconds.

Processes are lightweight threads requiring only a few instructions. In the listing, PC is the program counter, SP is the stack pointer, STATE is the address of a thread queue, Runtime is the number of milliseconds that the thread has been running based on CPU clock cycles, SBASE is the stack base address, Stack is the current number of bytes that are used and the total size of the stack, and Process lists the thread's function.

The optional **memory** argument displays the memory allocated by each process, to help track memory usage by process.

The optional **internals** argument displays the number of invoked calls and giveups. Invoked is the number of times the scheduler has invoked, or ran, the process. Giveups is the number of times the process yielded the CPU back to the scheduler.

Examples

This example shows how to display a list of processes that are running on the security appliance:

```
hostname(config)# show processes
```

```
    PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 00102aa0 0a63f288 0089b068     117460 0a63e2d4 3600/4096 arp_timer
Lsi 00102aa0 0a6423b4 0089b068         10 0a64140c 3824/4096 FragDBGC
Hwe 004257c8 0a7cacd4 0082dfd8          0 0a7c9d1c 3972/4096 udp_timer
Lwe 0011751a 0a7cc438 008ea5d0         20 0a7cb474 3560/4096 dbgtrace
<--- More --->
```

hostname(config)# show processes cpu

```
    MAXHOG             NUMHOG             LASTHOG             Process
--------------     ---------------     ---------------       ---------
      7720                 4                110              Dispatch Unit
      7870               331               1010              Checkheaps
(other lines deleted for brevity)
      6170                 1               6170              CTM message handle
```

hostname(config)# show processes memory

```
-------------------------------------------------------------
Allocs   Allocated       Frees         Freed         Process
          (bytes)                      (bytes)
-------------------------------------------------------------
23512    13471545        6             180           *System Main*
0        0               0             0             lu_rx
2        8324            16            19488         vpnlb_thread
(other lines deleted for brevity)
```

hostname# sho proc internals

```
     Invoked      Giveups  Process
           1            0  block_diag
    19108445     19108445  Dispatch Unit
           1            0  CF OIR
           1            0  Reload Control Thread
           1            0  aaa
           2            0  CMGR Server Process
           1            0  CMGR Timer Process
           2            0  dbgtrace
          69            0  557mcfix
    19108019     19108018  557poll
           2            0  557statspoll
           1            0  Chunk Manager
         135            0  PIX Garbage Collector
           6            0  route_process
           1            0  IP Address Assign
           1            0  QoS Support Module
           1            0  Client Update Task
        8973         8968  Checkheaps
           6            0  Session Manager
```

```
          237          235  uauth
(other lines deleted for brevity)
```

show reload

To display the reload status on the security appliance, use the **show reload** command in privileged EXEC mode.

show reload

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	This command was introduced.

Usage Guidelines

This command has no usage guidelines.

Examples

The following example shows that a reload is scheduled for 12:00 a.m. (midnight) on Saturday, April 20:

```
hostname# show reload
Reload scheduled for 00:00:00 PDT Sat April 20 (in 12 hours and 12 minutes)
```

Related Commands

Command	Description
reload	Reboots and reloads the configuration.

show resource types

To view the resource types for which the security appliance tracks usage, use the **show resource types** command in privileged EXEC mode.

show resource types

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	This command was introduced.

Examples

The following sample display shows the resource types:

```
hostname# show resource types

Absolute limit types:
  Conns             Connections
  Hosts             Hosts
  IPSec             IPSec Mgmt Tunnels
  SSH               SSH Sessions
  Telnet            Telnet Sessions
  Xlates            XLATE Objects
  All               All Resources
```

Related Commands

Command	Description
clear resource usage	Clears the resource usage statistics
context	Adds a security context.
show resource usage	Shows the resource usage of the security appliance.

show resource usage

To view the resource usage of the security appliance or for each context in mutliple mode, use the **show resource usage** command in privileged EXEC mode.

show resource usage [**context** *context_name* | **top** *n* | **all** | **summary** | **system**]
[**resource** {*resource_name* | **all**}] [**counter** *counter_name* [*count_threshold*]]

Syntax Description

context *context_name*	(Multiple mode only) Specifies the context name for which you want to view statistics. Specify **all** for all contexts; the security appliance lists the context usage for each context.
count_threshold	Sets the number above which resources are shown. The default is 1. If the usage of the resource is below the number you set, then the resource is not shown. If you specify **all** for the counter name, then the *count_threshold* applies to the current usage. **Note** To show all resources, set the *count_threshold* to **0**.
counter *counter_name*	Shows counts for the following counter types: • **current**—Shows the active concurrent instances or the current rate of the resource. • **peak**—Shows the peak concurrent instances, or the peak rate of the resource since the statistics were last cleared, either using the **clear resource usage** command or because the device rebooted. • **all**—(Default) Shows all statistics.
resource *resource_name*	Shows the usage of a specific resource. Specify **all** (the default) for all resources. Resources include the following types: • **conns**—TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts. • **hosts**—Hosts that can connect through the security appliance. • **ipsec**—(Single mode only) IPSec sessions. • **ssh**—SSH sessions. • **telnet**—Telnet sessions. • **xlates**—NAT translations.
summary	(Multiple mode only) Shows all context usage combined.
system	(Multiple mode only) Shows all context usage combined, but shows the system limits for resources instead of the combined context limits.
top *n*	(Multiple mode only) Shows the contexts that are the top *n* users of the specified resource. You must specify a single resource type, and not **resource all**, with this option.

Defaults

For multiple context mode, the default context is **all**, which shows resource usage for every context. For single mode, the context name is ignored and the output shows the "context" as "System."

The default resource name is **all**, which shows all resource types.

The default counter name is **all**, which shows all statistics.

The default count threshold is **1**.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following is sample output from the **show resource usage context** command, which shows the resource usage for the admin context:

```
hostname# show resource usage context admin

Resource              Current         Peak      Limit    Context
Telnet                      1            1          5    admin
Conns                      44           55        N/A    admin
Hosts                      45           56        N/A    admin
```

The following is sample output from the **show resource usage summary** command, which shows the resource usage for all contexts and all resources. This sample shows the limits for 6 contexts.

```
hostname# show resource usage summary

Resource              Current         Peak      Limit    Context
Telnet                      3            5         30    Summary
SSH                         5            7         30    Summary
Conns                      40           55        N/A    Summary
Hosts                      44           56        N/A    Summary
```

The following is sample output from the **show resource usage summary** command, which shows the limits for 25 contexts. Because the context limit for Telnet and SSH connections is 5 per context, then the combined limit is 125. The system limit is only 100, so the system limit is shown.

```
hostname# show resource usage summary

Resource              Current         Peak      Limit    Context
Telnet                      1            1       100[S] Summary
SSH                         2            2       100[S] Summary
Conns                      56           90        N/A    Summary
Hosts                      89          102        N/A    Summary
S = System limit: Combined context limits exceed the system limit; the system limit is
shown.
```

The following is sample output from the **show resource usage system** command, which shows the resource usage for all contexts, but it shows the system limit instead of the combined context limits:

```
hostname# show resource usage system
```

```
Resource                Current         Peak      Limit    Context
Telnet                        3            5        100    System
SSH                           5            7        100    System
Conns                        40           55        N/A    System
Hosts                        44           56        N/A    System
```

Related Commands

Command	Description
clear resource usage	Clears the resource usage statistics
context	Adds a security context.
show resource types	Shows a list of resource types.

show route

To display a default or static route for an interface, use the **show route** command in privileged EXEC mode.

show route [*interface_name ip_address netmask gateway_ip*]

Syntax Description

gateway_ip	(Optional) IP address of the gateway router (the next-hop address for this route).
interface_name	(Optional) Internal or external network interface name.
ip_address	(Optional) Internal or external network IP address.
netmask	(Optional) Network mask to apply to *ip_address*.

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 route** command:

```
hostname(config)# show route
C    10.30.10.0 255.255.255.0 is directly connected, outside
C    10.40.10.0 255.255.255.0 is directly connected, inside
C    192.168.2.0 255.255.255.0 is directly connected, faillink
C    192.168.3.0 255.255.255.0 is directly connected, statelink
```

Related Commands

Command	Description
clear configure route	Removes the **route** commands from the configuration that do not contain the **connect** keyword.
route	Specifies a static or default route for the an interface.
show running-config route	Displays configured routes.

show run fips

To verify the FIPS system location, system contact, and so forth, use the **show run fips** command.

show run fips

Syntax Description

fips	FIPS 140-2 compliance information

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(4)	This command was introduced.

Usage Guidelines

The show run fips command displays information about the system configuration.

Examples

```
sw8-ASA(config)# show run fips
```

Related Commands

Command	Description
clear configure fips	Clears the system or module FIPS configuration information stored in NVRAM.
crashinfo console disable	Disables the reading, writing and configuration of crash write info to flash.
fips enable	Enables or disablea policy-checking to enforce FIPS compliance on the system or module.
fips self-test poweron	Executes power-on self-tests.
service internal	Allows conditional commands that would otherwise be hidden to be shown.
show crashinfo console	Reads, writes, and configures crash write to flash.
show running-config fips	Displays the FIPS configuration that is running on the security appliance.

show running-config

To display the configuration that is running on the security appliance, use the **show running-config** command in privileged EXEC mode.

show running-config [**all**] [*command*]

Syntax Description

all	Displays the entire operating configuration, including defaults.
command	Displays the configuration associated with a specific command.

Defaults

If no arguments or keywords are specified, the entire non-default security appliance configuration displays.

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	This command was modified.

Usage Guidelines

The **show running-config** command displays the current running configuration on the security appliance.

You can use the **running-config** keyword only in the **show running-config** command. You cannot use this keyword with **no** or **clear**, or as a standalone command, because the CLI treats it as a nonsupported command. When you enter the **?**, **no ?**, or **clear ?** keywords, a **running-config** keyword is not listed in the command list.

Note The device manager commands appear in the configuration after you use it to connect to or configure the security appliance.

Examples

This example show how to display the configuration that is running on the security appliance:

```
hostname# show running-config
: Saved
:
XXX Version X.X(X)
names
!
```

```
interface Ethernet0
 nameif test
 security-level 10
 ip address 10.10.88.50 255.255.255.254
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.86.194.176 255.255.254.0
!
interface Ethernet2
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet3
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet4
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet5
 shutdown
 no nameif
 security-level 0
 no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname XXX
domain-name XXX.com
boot system flash:/cdisk.bin
ftp mode passive
pager lines 24
mtu test 1500
mtu inside 1500
monitor-interface test
monitor-interface inside
ASDM image flash:ASDM
no ASDM history enable
arp timeout 14400
route inside 0.0.0.0 0.0.0.0 10.86.194.1 1
timeout xlate 3:00:00
timeout conn 2:00:00 half-closed 1:00:00 udp 0:02:00 icmp 1:00:00 rpc 1:00:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02
:00
timeout uauth 0:00:00 absolute
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
fragment size 200 test
fragment chain 24 test
fragment timeout 5 test
fragment size 200 inside
fragment chain 24 inside
```

```
fragment timeout 5 inside
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 1440
ssh timeout 5
console timeout 0
group-policy todd internal
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map xxx_global_fw_policy
 class inspection_default
  inspect dns
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect http
  inspect ils
  inspect mgcp
  inspect netbios
  inspect rpc
  inspect rsh
  inspect rtsp
  inspect sip
  inspect skinny
  inspect sqlnet
  inspect tftp
  inspect xdmcp
  inspect ctiqbe
  inspect cuseeme
  inspect icmp
!
terminal width 80
service-policy xxx_global_fw_policy global
Cryptochecksum:bfecf4b9d1b98b7e8d97434851f57e14
: end
```

Related Commands

Command	Description
configure	Configures the security appliance from the terminal.

show running-config aaa

To show the AAA configuration in the running configuration, use the **show running-config aaa** command in privileged EXEC mode.

show running-config aaa [**accounting** | **authentication** | **authorization** | **mac-exempt** | **proxy-limit**]

Syntax Description

accounting	(Optional) Show accounting-related AAA configuration.
authentication	(Optional) Show authentication-related AAA configuration.
authorization	(Optional) Show authorization-related AAA configuration.
mac-exempt	(Optional) Show MAC address exemption AAA configuration.
proxy-limit	(Optional) Show the number of concurrent proxy connections allowed per user.

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	This command was introduced.

Examples

The following is sample output from the **show running-config aaa** command:

```
hostname# show running-config aaa
aaa authentication match infrastructure_authentication_radiusvrs infrastructure radiusvrs
aaa accounting match infrastructure_authentication_radiusvrs infrastructure radiusvrs
aaa authentication secure-http-client
aaa local authentication attempts max-fail 16
```

Related Commands

Command	Description
aaa authentication match	Enables authentication for traffic that is identified by an access list.
aaa authorization match	Enables authorization for traffic that is identified by an access list.

Command	Description
aaa accounting match	Enables accounting for traffic that is identified by an access list.
aaa max-exempt	Specifies the use of a predefined list of MAC addresses to exempt from authentication and authorization.
aaa proxy-limit	Configure the uauth session limit by setting the maximum number of concurrent proxy connections allowed per user.

show running-config aaa-server

To display AAA server configuration, use the **show running-config aaa-server** command in privileged EXEC mode.

show running-config [**all**] **aaa-server** [*server-tag*] [(*interface-name*)] [**host** *hostname*]

Syntax Description

all	(Optional) Shows the running configuration, including default configuration values.
host *hostname*	(Optional) The symbolic name or IP address of the particular host for which you want to display AAA server statistics.
(interface-name)	(Optional) The network interface where the AAA server resides.
server-tag	(Optional) The symbolic name of the server group.

Defaults

Omitting the *server-tag* value displays the configurations for all AAA servers.

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	This command was modified to adhere to CLI guidelines

Usage Guidelines

Use this command to display the settings for a particular server group. Use the **all** parameter to display the default as well as the explicitly configured values.

Examples

To display the running configuration for the default AAA server group, use the following command:

```
hostname(config)# show running-config default aaa-server

aaa-server group1 protocol tacacs+ accounting-mode simultaneous
reactivation-mode depletion deadtime 10
max-failed-attempts 4
```

Related Commands

Command	Description
show aaa-server	Displays AAA server statistics.
clear configure aaa-server	Clears the AAA server configuration.

show running-config aaa-server host

To display AAA server statistics for a particular server, use the **show running-config aaa-server** command in global configuration or privileged EXEC mode.

show/clear aaa-server

show running-config [**all**] **aaa-server** *server-tag* [(*interface-name*)] **host** *hostname*

Syntax Description

all	(Optional) Shows the running configuration, including default configuration values.
server-tag	The symbolic name of the server group.

Defaults

Omitting the default keyword displays only the explicitly configured configuration values, not the default 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	•	•	—	—	•
Global configuration	•	•	—	—	•

Command History

Release	Modification
7.0	This command was modified to adhere to CLI guidelines.

Usage Guidelines

Use this command to display the statistics for a particular server group. Use the default parameter to display the default as well as the explicitly configured values.

Examples

To display the running configuration for the server group svrgrp1, use the following command:

```
hostname(config)# show running-config default aaa-server svrgrp1
```

Related Commands

Command	Description
show running-config aaa-server	Displays AAA server settings for the indicated server, group, or protocol.
clear configure aaa	Removes the settings for all AAA servers across all groups.

show running-config access-group

To display the access group information, use the **show running-config access-group** command in privileged EXEC mode.

show running-config access-group

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 running-config access-group** command:

```
hostname# show running-config access-group
access-group 100 in interface outside
```

Related Commands

Command	Description
access-group	Binds an access list to an interface.
clear configure access-group	Removes access groups from all the interfaces.

show running-config access-list

To display the access-list configuration that is running on the security appliance, use the **show running-config access-list** command in privileged EXEC mode.

show running-config [**default**] **access-list** [**alert-interval** | **deny-flow-max**]

show running-config [**default**] **access-list** *id* [*saddr_ip*]

Syntax Description

alert-interval	Shows the alert interval for generating syslog message 106001, which alerts that the system has reached a deny flow maximum.
deny-flow-max	Shows the maximum number of concurrent deny flows that can be created.
id	Identifies the access list that is displayed.
saddr_ip	Shows the access list elements that contain the specified source IP address.

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	Added keyword **running-config**.

Usage Guidelines

The **show running-config access-list** command allows you to display the current running access list configuration on the security appliance.

Examples

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

```
hostname# show running-config access-list
access-list allow-all extended permit ip any any
```

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.

Command	Description
access-list ethertype	Configures an access list that controls traffic based on its EtherType.
clear access-list	Clears an access list counter.
clear configure access-list	Clears an access list from the running configuration.

show running-config alias

To display the overlapping addresses with dual NAT commands in the configuration, use the **show running-config alias** command in privileged EXEC mode.

show running-config alias {*interface_name*}

Syntax Description

interface_name	Internal network interface name that the destination_ip overwrites.

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
Global configuration	•	•	—	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

This example shows how to display alias information:

```
hostname# show running-config alias
```

Related Commands

Command	Description
alias	Creates an alias.
clear configure alias	Deletes an alias.

show running-config arp

To show static ARP entries created by the **arp** command in the running configuration, use the **show running-config arp** command in privileged EXEC mode.

show running-config 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	This command was introduced.

Examples

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

```
hostname# show running-config arp
arp inside 10.86.195.11 0008.023b.9893
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show arp	Shows the ARP table.
show arp statistics	Shows ARP statistics.

show running-config arp timeout

To view the ARP timeout configuration in the running configuration, use the **show running-config arp timeout** command in privileged EXEC mode.

show running-config arp timeout

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	This command was changed from **show arp timeout**.

Examples

The following is sample output from the **show running-config arp timeout** command:

```
hostname# show running-config arp timeout
arp timeout 20000 seconds
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp timeout	Sets the time before the security appliance rebuilds the ARP table.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show arp statistics	Shows ARP statistics.

show running-config arp-inspection

To view the ARP inspection configuration in the running configuration, use the **show running-config arp-inspection** command in privileged EXEC mode.

show running-config 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	This command was changed from **show arp timeout**.

Examples

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

```
hostname# show running-config arp-inspection

arp-inspection inside1 enable 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 configure arp-inspection	Clears the ARP inspection configuration.
firewall transparent	Sets the firewall mode to transparent.
show arp statistics	Shows ARP statistics.

show running-config asdm

To display the **asdm** commands in the running configuration, use the **show running-config asdm** command in privileged EXEC mode.

show running-config asdm [**group** | **location**]

Syntax Description

group	(Optional) Limits the display to the **asdm group** commands in the running configuration.
location	(Optional) Limits the display to the **asdm location** commands in the running configuration.

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	This command was changed from the **show running-config pdm** command to the **show running-config asdm** command.

Usage Guidelines

To remove the **asdm** commands from the configuration, use the **clear configure asdm** command.

Note On security appliances running in multiple context mode, the **show running-config asdm group** and **show running-config asdm location** commands are only available in the system execution space.

Examples

The following is sample output from the **show running-configuration asdm** command:

```
hostname# show running-config asdm
asdm image flash:/ASDM
asdm history enable
hostname#
```

Related Commands

Command	Description
show asdm image	Displays the current ASDM image file.

show running-config auth-prompt

To displays the current authentication prompt challenge text, use the show running-config auth-prompt command in global configuration mode.

show running-config [default] auth-prompt

Syntax Description

default	(Optional) Display the default authentication prompt challenge text.

Defaults

Display the configured authentication prompt challenge text.

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	This command was modified for this release to conform to CLI guidelines.

Usage Guidelines

After you configure the authentication prompt with the **auth-prompt** command, use the **show running-config auth-prompt** command to view the current prompt text.

Examples

The following example shows the output of the **show running-config auth-prompt** command:

```
hostname(config)# show running-config auth-prompt
auth-prompt prompt Please login:
auth-prompt accept You're in!
auth-prompt reject Try again.
```

Related Commands

auth-prompt	Set the user authorization prompts.
clear configure auth-prompt	Reset the user authorization prompts to the default value.

show running-config banner

To display the specified banner and all the lines that are configured for it, use the **show running-config banner** command in privileged EXEC mode.

show running-config banner [**exec | login | motd**]

Syntax Description

exec	(Optional) Displays the banner before the enable prompt.
login	(Optional) Displays the banner before the password login prompt when accessing the security appliance using Telnet.
motd	(Optional) Displays the message-of-the-day banner.

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	The **running-config** keyword was added.

Usage Guidelines

The **show running-config banner** command displays the specified banner keyword and all the lines configured for it. If a keyword is not specified, then all banners display.

Examples

This example shows how to display the message-of-the-day (motd) banner:

```
hostname# show running-config banner motd
```

Related Commands

Command	Description
banner	Creates a banner.
clear configure banner	Deletes a banner.

show running-config class-map

To display the information about the class map configuration, use the **show running-config class-map** command in privileged EXEC mode.

show running-config [**all**] **class-map** [*class_map_name*]

Syntax Description

all	(Optional) Show all running class map configuration, including default.
class_map_name	(Optional) Text for the class map name; the text can be up to 40 characters in length.

Defaults

The **class-map class-default** command, which contains a single **match any** command is the default class map.

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	Added keyword **running-config**.

Examples

The following is sample output from the **show running-config class-map** command:

```
hostname# show running-config class-map
class-map tcp-port
  match port tcp eq ftp
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
clear configure class-map	Removes all of the traffic map definitions.

show running-config clock

To show the clock configuration in the running configuration, use the **show running-config clock** command in privileged EXEC mode.

show running-config [**all**] **clock**

Syntax Description

all	(Optional) Shows all **clock** commands, including the commands you have not changed from the default.

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	This command was introduced.

Usage Guidelines

The **all** keyword also displays the exact day and time for the **clock summer-time** command, as well as the default setting for the offset, if you did not originally set it.

Examples

The following is sample output from the **show running-config clock** command. Only the **clock summer-time** command was set.

```
hostname# show running-config clock
clock summer-time EDT recurring
```

The following is sample output from the **show running-config all clock** command. The default setting for the unconfigured **clock timezone** command displays, and the detailed information for the **clock summer-time** command displays.

```
hostname# show running-config all clock
clock timezone UTC 0
clock summer-time EDT recurring 1 Sun Apr 2:00 last Sun Oct 2:00 60
```

Related Commands

Command	Description
clock set	Manually sets the clock on the security appliance.
clock summer-time	Sets the date range to show daylight saving time.
clock timezone	Sets the time zone.

show running-config command-alias

To display the command aliases that are configured, use the **show running-config command-alias** command in privileged EXEC mode.

show running-config [**all**] **command-alias**

Syntax Description

all	(Optional) Displays all command aliases configured, including defaults.

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	This command was introduced.

Usage Guidelines

If you do not enter the **all** keyword, only non-default command aliases display.

Examples

The following example displays all command aliases that are configured on the security appliance, *including* defaults:

```
hostname# show running-config all command-alias
command-alias exec h help
command-alias exec lo logout
command-alias exec p ping
command-alias exec s show
command-alias exec save copy running-config startup-config
```

The following example displays all command aliases that are configured on the security appliance, *excluding* defaults:

```
hostname# show running-config command-alias
command-alias exec save copy running-config startup-config
hostname#
```

Related Commands

Command	Description
command-alias	Creates a command alias.
clear configure command-alias	Deletes all non-default command aliases.

show running-config console timeout

To display the console connection timeout value, use the **show running-config console timeout** command in privileged EXEC mode.

show running-config console timeout

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	The **running-config** keyword was added.

Examples

The following example shows how to display the console connection timeout setting:

```
hostname# show running-config console timeout
console timeout 0
```

Related Commands

Command	Description
console timeout	Sets the idle timeout for a console connection to the security appliance.
clear configure console	Resets the console connection settings to defaults.

show running-config context

To show the context configuration in the system execution space, use the **show running-config context** command in privileged EXEC mode.

show running-config context

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	This command was introduced.

Examples

The following is sample output from the **show running-config context** command:

```
hostname# show running-config context

admin-context admin
context admin
  allocate-interface GigabitEthernet0/0
  config-url flash:/admin.cfg
!

context A
  allocate-interface GigabitEthernet0/1
  config-url flash:/A.cfg
!
```

Related Commands

Command	Description
admin-context	Sets the admin context.
allocate-interface	Assigns interfaces to a context.
changeto	Changes between contexts or the system execution space.
config-url	Specifies the location of the context configuration.
context	Creates a security context in the system configuration and enters context configuration mode.

show running-config crypto

To display the entire crypto configuration including IPSec, crypto maps, dynamic crypto maps, and ISAKMP, use the **show running-config crypto** command in global configuration or privileged EXEC mode.

show running-config crypto

Syntax Description

This command has no keywords or arguments.

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	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example entered in privileged EXEC mode, displays all crypto configuration information:

```
hostname# show running-config crypto map
crypto map abc 1 match address xyz
crypto map abc 1 set peer 209.165.200.225
crypto map abc 1 set transform-set ttt
crypto map abc interface test
isakmp enable inside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
hostname#
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.

Command	Description
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show isakmp sa	Displays IKE runtime SA database with additional information.

show running-config crypto dynamic-map

To view a dynamic crypto map, use the **show running-config crypto dynamic-map** command in global configuration or privileged EXEC mode.

show running-config crypto dynamic-map

Syntax Description

This command has no keywords or arguments.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example entered in global configuration mode, displays all configuration information about crypto dynamic maps:

```
hostname(config)# show running-config crypto dynamic-map

Crypto Map Template "dyn1" 10

        access-list 152 permit ip host 172.21.114.67 any
        Current peer: 0.0.0.0
        Security association lifetime: 4608000 kilobytes/120 seconds
        PFS (Y/N): N
        Transform sets={ tauth, t1, }
hostname(config)#
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show isakmp sa	Displays IKE runtime SA database with additional information.

show running-config crypto ipsec

To display the complete IPSec configuration, use the **show running-config crypto ipsec** command in global configuration or privileged EXEC mode.

show running-config crypto ipsec

Syntax Description

This command has no default behavior or values.

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	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example issued in global configuration mode, displays information about the IPSec configuration:

```
hostname(config)# show running-config crypto ipsec
crypto ipsec transform-set ttt esp-3des esp-md5-hmac
hostname(config)#
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show isakmp sa	Displays IKE runtime SA database with additional information.

show running-config crypto isakmp

To display the complete ISAKMP configuration, use the **show running-config crypto isakmp** command in global configuration or privileged EXEC mode.

show running-config crypto isakmp

Syntax Description

This command has no default behavior or values.

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	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example issued in global configuration mode, displays information about the ISKAKMP configuration:

```
hostname<config># show running-config crypto isakmp
isakmp enable inside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
hostname<config>#
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show isakmp sa	Displays IKE runtime SA database with additional information.

show running-config crypto map

To display all configuration for all crypto maps, use the **show running-config crypto map** command in global configuration or privileged EXEC mode.

show running-config crypto map

Syntax Description

This command has no keywords or arguments.

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	•	•	•	—	—
Privileged EXEC	•	•	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example entered in privileged EXEC mode, displays all configuration information for all crypto maps:

```
hostname# show running-config crypto map
crypto map abc 1 match address xyz
crypto map abc 1 set peer 209.165.200.225
crypto map abc 1 set transform-set ttt
crypto map abc interface test
hostname#
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show isakmp sa	Displays IKE runtime SA database with additional information.

show running-config dhcpd

To show the DHCP configuration, use the **show running-config dhcpd** command in privileged EXEC or global configuration mode.

show running-config dhcpd

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	This command was changed from the **show dhcpd** command to the **show running-config dhcpd** command.

Usage Guidelines

The **show running-config dhcpd** command displays the DHCP commands entered in the running configuration. To see DHCP binding, state, and statistical information, use the **show dhcpd** command.

Examples

The following is sample output from the **show running-config dhcpd** command:

```
hostname# show running-config dhcpd

dhcpd address 10.0.1.100-10.0.1.108 inside
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd dns 209.165.201.2 209.165.202.129
dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
debug dhcpd	Displays debug information for the DHCP server.
show dhcpd	Displays DHCP binding, statistic, or state information.

show running-config dhcprelay

To view the current DHCP relay agent configuration, use the **show running-config dhcprelay** command in privileged EXEC mode.

show running-config dhcprelay

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.

Usage Guidelines

The **show running-config dhcprelay** command displays the current DHCP relay agent configuration. To show DHCP relay agent packet statistics, use the **show dhcprelay statistics** command.

Examples

The following example shows output from the **show running-config dhcprelay** command:

```
hostname(config)# show running-config dhcprelay

dhcprelay server 10.1.1.1
dhcprelay enable inside
dhcprelay timeout 90
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
clear dhcprelay statistics	Clears the DHCP relay agent statistic counters.
debug dhcprelay	Displays debug information for the DHCP relay agent.
show dhcprelay statistics	Displays DHCP relay agent statistic information.

show running-config dns

To show the DNS configuration in the running configuration, use the **show running-config dns** command in privileged EXEC mode.

show running-config dns

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	This command was introduced.

Examples

The following is sample output from the **show running-config dns** command:

```
hostname# show running-config dns
dns domain-lookup inside
dns name-server
dns retries 2
dns timeout 15
dns name-server 10.1.1.1
```

Related Commands

Command	Description
dns domain-lookup	Enables the security appliance to perform a name lookup.
dns name-server	Configures a DNS server address.
dns retries	Specifies the number of times to retry the list of DNS servers when the security appliance does not receive a response.
dns timeout	Specifies the amount of time to wait before trying the next DNS server.
show dns-hosts	Shows the DNS cache.

show running-config domain-name

To show the domain name configuration in the running configuration, use the **show running-config domain-name** command in privileged EXEC mode.

show running-config domain-name

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	This command was changed from **show domain-name**.

Examples

The following is sample output from the **show running-config domain-name** command:

```
hostname# show running-config domain-name
example.com
```

Related Commands

Command	Description
domain-name	Sets the default domain name.
hostname	Sets the security appliance hostname.

show running-config enable

To show the encrypted enable passwords, use the **show running-config enable** command in privileged EXEC mode.

show running-config enable

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	This command was changed from the **show enable** command.

Usage Guidelines

The password is saved to the configuration in encrypted form, so you cannot view the original password after you enter it. The password displays with the **encrypted** keyword to indicate that the password is encrypted.

Examples

The following is sample output from the **show running-config enable** command:

```
hostname# show running-config enable
enable password 2AfK9Kjr3BE2/J2r level 10 encrypted
enable password 8Ry2YjIyt7RRXU24 encrypted
```

Related Commands

Command	Description
disable	Exits privileged EXEC mode.
enable	Enters privileged EXEC mode.
enable password	Sets the enable password.

show running-config established

To display the allowed inbound connections that are based on established connections, use the **show running-config established** command in privileged EXEC mode.

show running-config established

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	The keyword **running-config** was added.

Usage Guidelines

This command has no usage guidelines.

Examples

This example shows how to display inbound connections that are based on established connections:

```
hostname# show running-config established
```

Related Commands

Command	Description
established	Permits return connections on ports that are based on an established connection.
clear configure established	Removes all established commands.

show running-config failover

To display the **failover** commands in the configuration, use the **show running-config failover** command in privileged EXEC mode.

show running-config [**all**] **failover**

Syntax Description

all	(Optional) Shows all failover commands, including the commands you have not changed from the default.

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	This command was introduced.

Usage Guidelines

The **show running-config failover** command displays the **failover** commands in the running configuration. It does not display the **monitor-interface** or **join-failover-group** commands.

Examples

The following example shows the default failover configuration before failover has been configured:

```
hostname# show running-config all failover
no failover
failover lan unit secondary
failover polltime unit 15 holdtime 45
failover polltime interface 15
failover interface policy 1
hostname#
```

Related Commands

Command	Description
show failover	Displays failover state and statistics.

show running-config filter

To show the filtering configuration, use the **show running-config filter** command in privileged EXEC mode.

show running-config filter

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
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show running-config filter** command displays the filtering configuration for the security appliance.

Examples

The following is sample output from the **show running-config filter** command, and shows the filtering configuration for the security appliance:

```
hostname# show running-config filter
!
filter activex 80 10.86.194.170 255.255.255.255 10.1.1.0 255.255.255.224
!
```

This example shows ActiveX filtering is enabled on port80 for the address 10.86.194.170.

Related Commands

Commands	Description
filter activex	Removes ActiveX objects from HTTP traffic passing through the security appliance.
filter ftp	Identifies the FTP traffic to be filtered by a URL filtering server.
filter https	Identifies the HTTPS traffic to be filtered by a Websense server.
filter java	Removes Java applets from HTTP traffic passing through the security appliance.
filter url	Directs traffic to a URL filtering server.

show running-config fips

To display the FIPS configuration that is running on the security appliance, use the **show running-config fips** command.

show running-config fips

Syntax Description

fips	FIPS-2 compliance information

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**
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

The **show running-config fips** command allows you to display the current running fips configuration. You use the **running-config** keyword only in the **show running-config fips** command. You cannot use this keyword with no or clear, or as a standalone command as it is not supported. When you enter the **?**, **no ?**, or **clear ?** keywords, a **running-config** keyword is not listed in the command list.

Examples

```
sw8-ASA(config)# show running-config fips
```

Related Commands

Command	Description
clear configure fips	Clears the system or module FIPS configuration information stored in NVRAM.
crashinfo console disable	Disables the reading, writing and configuration of crash write info to flash.
fips enable	Enables or disablea policy-checking to enforce FIPS compliance on the system or module.
fips self-test poweron	Executes power-on self-tests.
show crashinfo console	Displays crashinfo console settings.

show running-config fragment

To display the current configuration of the fragment databases, use the **show running-config fragment** command in privileged EXEC mode.

show running-config fragment [*interface*]

Syntax Description

interface	(Optional) Specifies the security appliance interface.

Defaults

If an interface is not specified, the command applies to 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
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0	The keyword **running-config** was added.

Usage Guidelines

The **show running-config fragment** command displays the current configuration of the fragment databases. If you specify an interface name, only information for the database residing at the specified interface displays. If you do not specify an interface name, the command applies to all interfaces.

Use the **show running-config fragment** command to display this information:

- Size—Maximum number of packets set by the **size** keyword. This value is the maximum number of fragments that are allowed on the interface.
- Chain—Maximum number of fragments for a single packet set by the **chain** keyword.
- Timeout—Maximum number of seconds set by the **timeout** keyword. This is the maximum number of seconds to wait for an entire fragmented packet to arrive. The timer starts after the first fragment of a packet arrives. If all fragments of the packet do not arrive by the number of seconds specified, all fragments of the packet that were already received will be discarded.

Examples

The following example shows how to display the states of the fragment databases on all interfaces:

```
hostname# show running-config fragment
fragment size 200 inside
fragment chain 24 inside
fragment timeout 5 inside
fragment size 200 outside1
fragment chain 24 outside1
fragment timeout 5 outside1
```

```
fragment size 200 outside2
fragment chain 24 outside2
fragment timeout 5 outside2
fragment size 200 outside3
fragment chain 24 outside3
fragment timeout 5 outside3
```

The following example shows how to display the states of the fragment databases on interfaces that start with the name “outside”:

Note In this example, the interfaces named “outside1”, “outside2”, and “outside3” display.

```
hostname# show running-config fragment outside
fragment size 200 outside1
fragment chain 24 outside1
fragment timeout 5 outside1
fragment size 200 outside2
fragment chain 24 outside2
fragment timeout 5 outside2
fragment size 200 outside3
fragment chain 24 outside3
fragment timeout 5 outside3
```

The following example shows how to display the states of the fragment databases on the interfaces named “outside1” only:

```
hostname# show running-config fragment outside1
fragment size 200 outside1
fragment chain 24 outside1
fragment timeout 5 outside1
```

Related Commands

Command	Description
clear configure fragment	Resets all the IP fragment reassembly configurations to defaults.
clear fragment	Clears the operational data of the IP fragment reassembly module.
fragment	Provides additional management of packet fragmentation and improves compatibility with NFS.
show fragment	Displays the operational data of the IP fragment reassembly module.

show running-config ftp-map

To show the FTP maps that have been configured, use the **show running-config ftp-map** command in privileged EXEC mode.

show running-config ftp-map *map_name*

Syntax Description.

map_name	Displays configuration for the specified FTP map.

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	This command was introduced.

Usage Guidelines

The **show running-config ftp-map** command displays the FTP maps that have been configured.

Examples

The following is sample output from the **show running-config ftp-map** command:

```
hostname# show running-config ftp-map ftp-policy
!
ftp-map ftp-policy
request-command deny put stou appe
!
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
ftp-map	Defines an FTP map and enables FTP map configuration mode.
inspect ftp	Applies a specific FTP map to use for application inspection.
mask-syst-reply	Hides the FTP server response from clients.
request-command deny	Specifies FTP commands to disallow.

show running-config ftp mode

To show the client mode configured for FTP, use the **show running-config ftp mode** command in privileged EXEC mode.

show running-config ftp mode

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.

Usage Guidelines

The **show running-config ftp mode** command displays the client mode that is used by the security appliance when accessing an FTP server.

Examples

The following is sample output from the **show running-config ftp-mode** command:

```
hostname# show running-config ftp-mode
!
ftp-mode passive
!
```

Related Commands

Commands	Description
copy	Uploads or downloads image files or configuration files to or from an FTP server.
debug ftp client	Displays detailed information about FTP client activity.
ftp mode passive	Sets the FTP client mode used by the security appliance when accessing an FTP server.

show running-config global

To display the **global** commands in the configuration, use the **show running-config global** command in privileged EXEC mode.

show running-config global

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:

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

Command History

Release	Modification
7.0	Added keyword **running-config**.

Examples

The following is sample output from the **show running-config global** command:

```
hostname# show running-config global
global (outside1) 10 interface
```

Related Commands

Command	Description
clear configure global	Removes global commands from the configuration.
global	Creates entries from a pool of global addresses.

show running-config group-delimiter

To display the current delimiter to be used when parsing group names from the user names that are received when tunnels are being negotiated, use the **show running-config group-delimiter** command in global configuration mode.

show running-config group-delimiter

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use this command to display the currently configured group-delimiter.

Examples

This example shows a **show running-config group-delimiter** command and its output:

```
hostname(config)# show running-config group-delimiter
group-delimiter @
```

Related Commands

Command	Description
group-delimiter	Enables group-name parsing and specifies the delimiter to be used when parsing group names from the user names that are received when tunnels are being negotiated.

show running-config group-policy

To display the running configuration for a particular group policy, use the **show running-config group-policy** command in privileged EXEC mode and append the name of the group policy. To display the running configuration for all group policies, use this command without naming a specific group policy. To have either display include the default configuration, use the **default** keyword.

show running-config [default] group-policy [*name***]**

Syntax Description

default	Displays the running configuration including default values.
name	Specifies the name of the group policy.

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	•	—	•	—	—
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to display the running configuration, including default values, for the group policy named FirstGroup:

```
hostname# show running-config default group-policy FirstGroup
```

Related Commands

Command	Description
group-policy	Creates, edits, or removes a group policy.
group-policy attributes	Enters group-policy attributes mode, which lets you configure AVPs for a specified group policy.
clear config group-policy	Removes the configuration for a particular group policy or for all group policies.

show running-config gtp-map

To show the GTP maps that have been configured, use the **show running-config gtp-map** command in privileged EXEC mode.

show running-config gtp-map *map_name*

Syntax Description.

map_name	Displays configuration for the specified GTP map.

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	This command was introduced.

Usage Guidelines

The **show running-config gtp-map** command displays the GTP maps that have been configured.

Examples

The following is sample output from the **show running-config gtp-map** command:

```
hostname# show running-config gtp-map gtp-policy
!
gtp-map gtp-policy
 request-queue 300
 message-length min 20 max 300
 drop message 20
 tunnel-limit 10000
!
```

Related Commands

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

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

show running-config http

To display the current set of configured http commands, use the **show running-config http** command in privileged EXEC mode.

show running-config http

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	•	—	•	—	—
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Examples

The following sample output shows how to use the **show running-config http** command:

```
hostname# show running-config http
http server enabled
0.0.0.0 0.0.0.0 inside
```

Related Commands

Command	Description
clear http	Remove the HTTP configuration: disable the HTTP server and remove hosts that can access the HTTP server.
http	Specifies hosts that can access the HTTP server by IP address and subnet mask. Specifies the security appliance interface through which the host accesses the HTTP server.
http authentication-certificate	Requires authentication via certificate from users who are establishing HTTPS connections to the security appliance.
http redirect	Specifies that the security appliance redirect HTTP connections to HTTPS.
http server enable	Enables the HTTP server.

show running-config http-map

To show the HTTP maps that have been configured, use the **show running-config http-map** command in privileged EXEC mode.

show running-config http-map *map_name*

Syntax Description.

map_name	Displays configuration for the specified HTTP map.

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	This command was introduced.

Usage Guidelines

The **show running-config http-map** command displays the HTTP maps that have been configured.

Examples

The following is sample output from the **show running-config http-map** command:

```
hostname# show running-config http-map http-policy
!
http-map http-policy
content-length min 100 max 2000 action reset log
content-type-verification match-req-rsp reset log
max-header-length request bytes 100 action log reset
max-uri-length 100 action reset log
!
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug http-map	Displays detailed information about traffic associated with an HTTP map.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.

Commands	Description
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

show running-config icmp

To show the access rules configured for ICMP traffic, use the **show running-config icmp** command in privileged EXEC mode.

show running-config icmp *map_name*

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
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show running-config icmp** command displays the access rules configured for ICMP traffic.

Examples

The following is sample output from the **show running-config icmp** command:

```
hostname# show running-config icmp
!
icmp permit host 172.16.2.15 echo-reply outside
icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
icmp permit any unreachable outside
!
```

Related Commands

Commands	Description
clear configure icmp	Clears the ICMP configuration.
debug icmp	Enables the display of debug information for ICMP.
show icmp	Displays ICMP configuration.
timeout icmp	Configures the idle timeout for ICMP.

show running-config imap4s

To display the running configuration for IMAP4S, use the s**how running-config imap4s** command in privileged EXEC mode.

show running-config [all] imap4s

Syntax Description

all	(Optional) Displays the running configuration including default values.

Defaults

No default behavior or values.

Command History

Release	Modification
7.0	This command was introduced.

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	•	—	•	—	—

Examples

The following is sample output from the **show running-config imap4s** command:

```
hostname# show running-config imap4s

imap4s
 server 10.160.105.2
 authentication-server-group KerbSvr
 authentication aaa

hostname# show running-config all imap4s

imap4s
 port 993
 server 10.160.105.2
 outstanding 20
 name-separator :
 server-separator @
 authentication-server-group KerbSvr
 no authorization-server-group
 no accounting-server-group
 no default-group-policy
 authentication aaa
```

Related Commands

Command	Description
clear configure imap4s	Removes the IMAP4S configuration.
imap4s	Creates or edits an IMAP4S e-mail proxy configuration.

show running-config interface

To show the interface configuration in the running configuration, use the s**how running-config interface** command in privileged EXEC mode.

show running-config [**all**] **interface** [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

Syntax Description

all	(Optional) Shows all **interface** commands, including the commands you have not changed from the default.
interface_name	(Optional) Identifies the interface name set with the **nameif** command.
mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

If you do not specify an interface, this command shows the configuration 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
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You cannot use the interface name in the system execution space, because the **nameif** command is only available within a context. Similarly, if you mapped the interface ID to a mapped name using the **allocate-interface** command, you can only use the mapped name in a context.

Examples

The following is sample output from the **show running-config interface** command. The following example shows the running configuration for all interfaces. The GigabitEthernet0/2 and 0/3 interfaces have not been configured yet, and show the default configuration. The Management0/0 interface also shows the default settings.

```
formula_1# show running-config interface
!
interface GigabitEthernet0/0
```

```
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
!
interface GigabitEthernet0/1
 shutdown
 nameif test
 security-level 0
 ip address 10.10.4.200 255.255.0.0
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 security-level 0
 no ip address
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
clear configure interface	Clears the interface configuration.
interface	Configures an interface and enters interface configuration mode.
nameif	Sets the interface name.
show interface	Displays the runtime status and statistics of interfaces.

show running-config ip address

To show the IP address configuration in the running configuration, use the s**how running-config ip address** command in privileged EXEC mode.

show running-config ip address [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

Syntax Description

interface_name	(Optional) Identifies the interface name set with the **nameif** command.
mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

If you do not specify an interface, this command shows the IP address configuration 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
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

In multiple context mode, if you mapped the interface ID in the **allocate-interface** command, you can only specify the mapped name or the interface name in a context.

In transparent firewall mode, do not specify an interface because this command shows only the management IP address; the transparent firewall does not have IP addresses associated with interfaces.

This display also shows the **nameif** command and **security-level** command configuration.

Examples

The following is sample output from the **show running-config ip address** command:

```
hostname# show running-config ip address
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
```

```
 ip address 10.86.194.60 255.255.254.0
!
interface GigabitEthernet0/1
 nameif test
 security-level 0
 ip address 10.10.4.200 255.255.0.0
!
```

Related Commands

Command	Description
clear configure interface	Clears the interface configuration.
interface	Configures an interface and enters interface configuration mode.
ip address	Sets the IP address for the interface or sets the management IP address for a transparent firewall.
nameif	Sets the interface name.
security-level	Sets the security level for the interface.

show running-config ip audit attack

To show the **ip audit attack** configuration in the running configuration, use the **show running-config ip audit attack** command in privileged EXEC mode.

show running-config ip audit attack

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	This command was changed from **show ip audit attack**.

Examples

The following is sample output from the **show running-config ip audit attack** command:

```
hostname# show running-config ip audit attack
ip audit attack action drop
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit signature	Disables a signature.

show running-config ip audit info

To show the **ip audit info** configuration in the running configuration, use the **show running-config ip audit info** command in privileged EXEC mode.

show running-config ip audit info

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	This command was changed from **show ip audit info**.

Examples

The following is sample output from the **show running-config ip audit info** command:

```
hostname# show running-config ip audit info
ip audit info action drop
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit signature	Disables a signature.

show running-config ip audit interface

To show the **ip audit interface** configuration in the running configuration, use the **show running-config ip audit interface** command in privileged EXEC mode.

show running-config ip audit interface [*interface_name*]

Syntax Description

interface_name	(Optional) Specifies the interface name.

Defaults

If you do not specify an interface name, this command shows the configuration 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
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0	This command was changed from **show ip audit interface**.

Examples

The following is sample output from the **show running-config ip audit interface** command:

```
hostname# show running-config ip audit interface
ip audit interface inside insidepolicy
ip audit interface outside outsidepolicy
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit signature	Disables a signature.

show running-config ip audit name

To show the **ip audit name** configuration in the running configuration, use the **show running-config ip audit name** command in privileged EXEC mode.

show running-config ip audit name [*name* [**info** | **attack**]]

Syntax Description

attack	(Optional) Shows the named audit policy configuration for attack signatures.
info	(Optional) Shows the named audit policy configuration for informational signatures.
name	(Optional) Shows the configuration for the audit policy name created using the **ip audit name** command.

Defaults

If you do not specify a name, this command shows the configuration for all audit policies.

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	This command was changed from **show ip audit name**.

Examples

The following is sample output from the **show running-config ip audit name** command:

```
hostname# show running-config ip audit name
ip audit name insidepolicy1 attack action alarm
ip audit name insidepolicy2 info action alarm
ip audit name outsidepolicy1 attack action reset
ip audit name outsidepolicy2 info action alarm
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit signature	Disables a signature.

show running-config ip audit signature

To show the **ip audit signature** configuration in the running configuration, use the **show running-config ip audit signature** command in privileged EXEC mode.

show running-config ip audit signature [*signature_number*]

Syntax Description

signature_number	(Optional) Shows the configuration for the signature number, if present. See the **ip audit signature** command for a list of supported signatures.

Defaults

If you do not specify a number, this command shows the configuration for all signatures.

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	This command was changed from **show ip audit signature**.

Examples

The following is sample output from the **show running-config ip audit signature** command:

```
hostname# show running-config ip audit signature
ip audit signature 1000 disable
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit signature	Disables a signature.

show running-config ip local pool

To display IP address pools, use the **show running-config ip local pool** command in privileged EXEC mode.

show running-config ip local pool [*poolname*]

Syntax Description

poolname	(Optional) Specifies the name of the IP address pool.

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
EXEC	•	—	•	—	—
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following is sample output from the **show running-config ip local pool** command:

```
hostname(config)# show running-config ip local pool firstpool

Pool            Begin           End             Mask            Free    In use
firstpool               10.20.30.40     10.20.30.50     255.255.255.0      11
    0
Available Addresses:
10.20.30.40
10.20.30.41
10.20.30.42
10.20.30.43
10.20.30.44
10.20.30.45
10.20.30.46
10.20.30.47
10.20.30.48
10.20.30.49
10.20.30.50

hostname(config)#
```

Related Commands

Command	Description
clear configure ip local pool	Removes all ip local pools
ip local pool	Configures an IP address pool.

show running-config ip verify reverse-path

To show the **ip verify reverse-path** configuration in the running configuration, use the **show running-config ip verify reverse-path** command in privileged EXEC mode.

show running-config ip verify reverse-path [interface *interface_name*]

Syntax Description

interface *interface_name*	(Optional) Shows the configuration for the specified interface.

Defaults

This command shows the configuration 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
Privileged EXEC	•	—	•	•	—

Command History

Release	Modification
7.0	This command was changed from **show ip verify reverse-path**.

Examples

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

```
hostname# show running-config ip verify reverse-path
ip verify reverse-path interface inside
ip verify reverse-path interface outside
ip verify reverse-path interface dmz
```

Related Commands

Command	Description
clear configure ip verify reverse-path	Clears the **ip verify reverse-path** configuration.
clear ip verify statistics	Clears the Unicast RPF statistics.
ip verify reverse-path	Enables the Unicast Reverse Path Forwarding feature to prevent IP spoofing.
show ip verify statistics	Shows the Unicast RPF statistics.

show running-config ipv6

To display the IPv6 commands in the running configuration, use the **show running-config ipv6** command in privileged EXEC mode.

show running-config [**all**] **ipv6**

Syntax Description

all	(Optional) Shows all **ipv6** commands, including the commands you have not changed from the default, in the running configuration.

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	This command was introduced.

Examples

The following is sample output from the **show running-config ipv6** command:

```
hostname# show running-config ipv6
ipv6 unicast-routing
ipv6 route vlan101 ::/0 fec0::65:0:0:a0a:6575
ipv6 access-list outside_inbound_ipv6 permit ip any any
ipv6 access-list vlan101_inbound_ipv6 permit ip any any
hostname#
```

Related Commands

Command	Description
debug ipv6	Displays IPv6 debug messages.
show ipv6 access-list	Displays the IPv6 access list.
show ipv6 interface	Displays the status of the IPv6 interfaces.
show ipv6 route	Displays the contents of the IPv6 routing table.
show ipv6 traffic	Displays IPv6 traffic statistics.

show running-config isakmp

To display the complete ISAKMP configuration, use the **show running-config isakmp** command in global configuration or privileged EXEC mode.

show running-config isakmp

Syntax Description

This command has no default behavior or values.

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	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example issued in global configuration mode, displays information about the ISKAKMP configuration:

```
hostname(config)# show running-config isakmp
isakmp enable inside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
hostname(config)#
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show isakmp sa	Displays IKE runtime SA database with additional information.

show running-config logging

To display all currently running logging configuration, use the **show runnig-config logging** command in privileged EXEC mode.

show running-config [all] logging [level | disabled]

Syntax Description

all	(Optional) Displays the logging configuration, including commands that you have not changed from the default.
disabled	(Optional) Displays only the disabled system log message configuration.
level	(Optional) Displays only the configuration for system log messages with a non-default severity level.

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	This command was changed from the **show logging** command.

Examples

The following is an example of the **show running-config logging disabled** command:

```
hostname# show running-config logging disabled

no logging message 720067
```

Related Commands

Command	Description
logging message	Configures logging.
show logging	Shows the log buffer and other logging settings.

show logging rate-limit

To display the disallowed messages to the original set, use the **show logging rate-limit** command.

show logging rate-limit

Syntax Description

This command has no arguments or keywords.

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	Support for this command was introduced on the security appliance.

Usage Guidelines

After the information is cleared, nothing more displays until the hosts reestablish their connections.

Examples

This example shows how to display the disallowed messages:

```
hostname(config)# show logging rate-limit
```

Related Commands

Command	Description
show logging	Displays the enabled logging options.

show running-config mac-address-table

To view the **mac-address-table static** and **mac-address-table aging-time** configuration in the running configuration, use the **show running-config mac-address-table** command in privileged EXEC mode.

show running-config mac-address-table

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	This command was introduced.

Examples

The following is sample output from the **show running-config mac-learn** command:

```
hostname# show running-config mac-address-table
mac-address-table aging-time 50
mac-address-table static inside1 0010.7cbe.6101
```

Related Commands

Command	Description
firewall transparent	Sets the firewall mode to transparent.
mac-address-table aging-time	Sets the timeout for dynamic MAC address entries.
mac-address-table static	Adds static MAC address entries to the MAC address table.
mac-learn	Disables MAC address learning.
show mac-address-table	Shows the MAC address table, including dynamic and static entries.

show running-config mac-learn

To view the **mac-learn** configuration in the running configuration, use the **show running-config mac-learn** command in privileged EXEC mode.

show running-config mac-learn

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	This command was introduced.

Examples

The following is sample output from the **show running-config mac-learn** command:

```
hostname# show running-config mac-learn
mac-learn disable
```

Related Commands

Command	Description
firewall transparent	Sets the firewall mode to transparent.
mac-address-table static	Adds static MAC address entries to the MAC address table.
mac-learn	Disables MAC address learning.
show mac-address-table	Shows the MAC address table, including dynamic and static entries.

show running-config mac-list

To display a list of MAC addresses previously specified in a **mac-list** command with the indicated MAC list number, use the **show running-config mac-list** command in privileged EXEC mode.

show running-config mac-list *id*

Syntax Description

id	A hexadecimal MAC address list number.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was modified to conform to CLI guidelines.

Usage Guidelines

The **show running-config aaa** command displays the **mac-list** command statements as part of the AAA configuration.

Examples

The following example shows how to display a MAC address list with the *id* equal to adc:

```
hostname(config)# show running-config mac-list adc
mac-list adc permit 00a0.cp5d.0282 ffff.ffff.ffff
mac-list adc deny 00a1.cp5d.0282 ffff.ffff.ffff
mac-list ac permit 0050.54ff.0000 ffff.ffff.0000
mac-list ac deny 0061.54ff.b440 ffff.ffff.ffff
mac-list ac deny 0072.54ff.b440 ffff.ffff.ffff
```

Related Commands

Command	Description
mac-list	Add a list of MAC addresses using a first-match search.
clear configure mac-list	Remove the indicated **mac-list** command statements.
show running-config aaa	Display the running AAA configuration values.

show running-config management-access

To display the name of the internal interface configured for management access, use the **show running-config management-access** command in privileged EXEC mode.

show running-config management-access

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.

Usage Guidelines

The **management-access** command lets you define an internal management interface using the IP address of the firewall interface specified in *mgmt_if*. (The interface names are defined by the **nameif** command and displayed in quotes, " ", in the output of the **show interface** command.)

Examples

The following example shows how to configure a firewall interface named "inside" as the management access interface and display the result:

```
hostname# management-access inside
hostname# show running-config management-access
management-access inside
```

Related Commands

Command	Description
clear configure management-access	Removes the configuration of an internal interface for management access of the security appliance.
management-access	Configures an internal interface for management access.

show running-config mgcp-map

To show the MGCP maps that have been configured, use the **show running-config mgcp-map** command in privileged EXEC mode.

show running-config mgcp-map *map_name*

Syntax Description.

map_name	Displays configuration for the specified MGCP map.

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	This command was introduced.

Usage Guidelines

The **show running-config mgcp-map** command displays the MGCP maps that have been configured.

Examples

The following is sample output from the **show running-config mgcp-map** command:

```
hostname# show running-config mgcp-map mgcp-policy
!
mgcp-map mgcp-policy
call-agent 10.10.11.5 101
call-agent 10.10.11.6 101
call-agent 10.10.11.7 102
call-agent 10.10.11.8 102
gateway 10.10.10.115 101
gateway 10.10.10.116 102
gateway 10.10.10.117 102
command-queue 150
```

Related Commands

Commands	Description
debug mgcp	Enables MGCP debug information.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.

Commands	Description
show conn	Displays the connection state for different connection types.
show mgcp	Displays information about MGCP sessions established through the security appliance.
timeout	Sets the maximum idle time duration for different protocols and session types.

show running-config mroute

To display the static multicast route table in the configuration use the **show running-config mroute** command in privileged EXEC mode.

show running-config mroute [*dst* [*src*]]

Syntax Description

dst	The Class D address of the multicast group.
src	The IP address of the multicast source.

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	Added keyword **running-config**.

Examples

The following is sample output from the **show running-config mroute** command:

```
hostname# show running-config mroute
```

Related Commands

Command	Description
mroute	Configures a static multicast route.

show running-config mtu

To display the current maximum transmission unit block size, use the **show running-config mtu** command in privileged EXEC mode.

show running-config mtu [*interface_name*]

Syntax Description

interface_name	(Optional) Internal or external network interface name.

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
Privileged EXEC	—	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

The following is sample output from the **show running-config mtu** command:

```
hostname# show running-config mtu
mtu outside 1500
mtu inside 1500
mtu dmz 1500
hostname# show running-config mtu outside
mtu outside 1500
```

Related Commands

Command	Description
clear configure mtu	Clears the configured maximum transmission unit values on all interfaces.
mtu	Specifies the maximum transmission unit for an interface.

show running-config multicast-routing

To display the **multicast-routing** command, if present, in the running configuration, use the **show running-config multicast-routing** command in privileged EXEC mode.

show running-config multicast-routing

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	This command was introduced.

Usage Guidelines

The **show running-config multicast-routing** command displays the **multicast-routing** command in the running configuration. Enter the **clear configure multicast-routing** command to remove the **multicast-routing** command from the running configuration.

Examples

The following is sample output from the **show running-config multicast-routing** command:

```
hostname# show running-config multicast-routing

multicast-routing
```

Related Commands

Command	Description
clear configure multicast-routing	Removes the **multicast-routing** command from the running configuration.
multicast-routing	Enables multicast routing on the security appliance.

show running-config name

To display a list of names associated with IP addresses (configured with the **name** command), use the **show running-config name** command in privileged EXEC mode.

show running-config name

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	The **running-config** keyword was added.

Examples

This example shows how to display a list of names associated with IP addresses:

```
hostname# show running-config name
name 192.168.42.3 sa_inside
name 209.165.201.3 sa_outside
```

Related Commands

Command	Description
clear configure name	Clears the list of names from the configuration.
name	Associates a name with an IP address.

show running-config nameif

To show the interface name configuration in the running configuration, use the s**how running-config nameif** command in privileged EXEC mode.

show running-config nameif [*physical_interface*[**.***subinterface*] | *mapped_name*]

Syntax Description

mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.

Defaults

If you do not specify an interface, this command shows the interface name configuration 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
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0	This command was changed from **show nameif**.

Usage Guidelines

In multiple context mode, if you mapped the interface ID in the **allocate-interface** command, you can only specify the mapped name in a context.

This display also shows the **security-level** command configuration.

Examples

The following is sample output from the **show running-config nameif** command:

```
hostname# show running-config nameif
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
!
interface GigabitEthernet0/1
 nameif test
 security-level 0
!
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
clear configure interface	Clears the interface configuration.
interface	Configures an interface and enters interface configuration mode.
nameif	Sets the interface name.
security-level	Sets the security level for the interface.

show running-config names

To display the IP address-to-name conversions, use the **show running-config names** command in privileged EXEC mode.

show running-config names

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	The keyword **running-config** was added.

Usage Guidelines

Use with the **names** command.

Examples

The following example shows how to display the IP address-to-name conversion:

```
hostname# show running-config names
name 192.168.42.3 sa_inside
name 209.165.201.3 sa_outside
```

Related Commands

Command	Description
clear configure name	Clears the list of names from the configuration.
name	Associates a name with an IP address.
names	Enables IP address-to-name conversions that you can configured with the **name** command.
show running-config name	Displays a list of names associated with IP addresses.

show running-config nat

To display a pool of global IP addresses that are associated with a network, use the **show running-config nat** command in privileged EXEC mode.

show running-config nat [*interface_name*] [*nat_id*]

Syntax Description

interface_name	(Optional) Name of the network interface.
nat_id	(Optional) ID of the group of host or networks.

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	Added keyword **running-config**.

Usage Guidelines

This command displays the maximum connection value for the UDP protocol. Every time the UPD maximum connection value is not set, the value will be displayed as 0 by default and will not be applied.

Note In transparent mode, only NAT ID 0 is valid.

Examples

This example shows how to display a pool of global IP addresses that are associated with a network:

```
hostname# show running-config nat
nat (inside) 1001 10.7.2.0 255.255.255.224 0 0
nat (inside) 1001 10.7.2.32 255.255.255.224 0 0
nat (inside) 1001 10.7.2.64 255.255.255.224 0 0
nat (inside) 1002 10.7.2.96 255.255.255.224 0 0
nat (inside) 1002 10.7.2.128 255.255.255.224 0 0
nat (inside) 1002 10.7.2.160 255.255.255.224 0 0
nat (inside) 1003 10.7.2.192 255.255.255.224 0 0
nat (inside) 1003 10.7.2.224 255.255.255.224 0 0
```

Related Commands

Command	Description
clear configure nat	Removes the NAT configuration.
nat	Associates a network with a pool of global IP addresses.

show running-config nat-control

To show the NAT configuration requirement, use the **show running-config nat-control** command in privileged EXEC mode.

show running-config nat-control

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:

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following is sample output from the **show running-config nat-control** command:

```
hostname# show running-config nat-control
no nat-control
```

Related Commands

Command	Description
nat	Defines an address on one interface that is translated to a global address on another interface.
nat-control	Allows inside hosts to communicate with outside networks without configuring a NAT rule.

show running-config ntp

To show the NTP configuration in the running configuration, use the **show running-config ntp** command in privileged EXEC mode.

show running-config ntp

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	This command was introduced.

Examples

The following is sample output from the **show running-config ntp** command:

```
hostname# show running-config ntp
ntp authentication-key 1 md5 test2
ntp authentication-key 2 md5 test
ntp trusted-key 1
ntp trusted-key 2
ntp server 10.1.1.1 key 1
ntp server 10.2.1.1 key 2 prefer
```

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Sets an encrypted authentication key to synchronize with an NTP server.
ntp server	Identifies an NTP server.
ntp trusted-key	Provides a key ID for the security appliance to use in packets for authentication with an NTP server.
show ntp status	Shows the status of the NTP association.

show running-config object-group

To display the current object groups, use the **show running-config object-group** command in privileged EXEC mode.

show running-config [**all**] **object-group** [**protocol** | **service** | **network** | **icmp-type** | **id** *obj_grp_id*]

Syntax Description

icmp-type	(Optional) Displays ICMP type object groups.
id obj_grp_id	(Optional) Displays the specified object group.
network	(Optional) Displays network object groups.
protocol	(Optional) Displays protocol object groups.
service	(Optional) Displays service object groups.

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 running-config object-group** command:

```
hostname# show running-config object-group
object-group protocol proto_grp_1
    protocol-object udp
    protocol-object tcp
object-group service eng_service tcp
    port-object eq smtp
    port-object eq telnet
object-group icmp-type icmp-allowed
    icmp-object echo
    icmp-object time-exceeded
```

Related Commands

Command	Description
clear configure object-group	Removes all the **object group** commands from the configuration.
group-object	Adds network object groups.
network-object	Adds a network object to a network object group.
object-group	Defines object groups to optimize your configuration.
port-object	Adds a port object to a service object group.

show running-config passwd

To show the encrypted login passwords, use the **show running-config passwd** command in privileged EXEC mode.

show running-config {**passwd** | **password**}

Syntax Description

passwd | **password**	You can enter either command; they are aliased to each other.

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	This command was changed from the **show passwd** command.

Usage Guidelines

The password is saved to the configuration in encrypted form, so you cannot view the original password after you enter it. The password displays with the **encrypted** keyword to indicate that the password is encrypted.

Examples

The following is sample output from the **show running-config passwd** command:

```
hostname# show running-config passwd
passwd 2AfK9Kjr3BE2/J2r encrypted
```

Related Commands

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

show running-config pim

To display the PIM commands in the running configuration, use the **show running-config pim** command in privileged EXEC mode.

show running-config pim

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	This command was introduced.

Usage Guidelines

The **show running-config pim** command displays the **pim** commands entered in global configuration mode. It does not show the **pim** commands entered in interface configuration mode. To see the **pim** commands entered in interface configuration mode, enter the **show running-config interface** command.

Examples

The following is sample output from the **show running-config pim** command:

```
hostname# show running-config pim

pim old-register-checksum
pim spt-threshold infinity
```

Related Commands

Command	Description
clear configure pim	Removes the **pim** commands from the running configuration.
show running-config interface	Displays interface configuration commands entered in interface configuration mode.

show running-config policy-map

To display all the policy-map configurations or the default policy-map configuration, use the **show running-config policy-map** command in privileged EXEC mode.

show running-config [all] policy-map

Syntax Description

all	(Optional) Display the default policy-map configuration.

Defaults

Omitting the **all** keyword displays only the explicitly configured policy-map configuration.

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	This command was introduced.

Usage Guidelines

Specifying the **all** keyword displays the default policy-map configuration as well as the explicitly configured policy-map configuration.

Examples

This example shows the use of the show running-config policy-map command for the policy map named localmap1,and the command output:

```
hostname# show running-config policy-map
!
policy-map localmap1
    description this is a test.
    class firstclass
    priority
    ids promiscuous fail0close
    set connection random-seq# enable
    class class-default
!
```

Related Commands

Command	Description

policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
clear configure policy-map	Removes the entire policy configuration.

show running-config pop3s

To display the running configuration for POP3S, use the s**how running-config pop3s** command in privileged EXEC mode. To have the display include the default configuration, use the **all** keyword.

show running-config [all] pop3s

Syntax Description

all	Displays the running configuration including default values.

Defaults

No default behavior or values.

Command History

Release	Modification
7.0	This command was introduced.

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	•	—	•	—	—
Global configuration	•	—	•	—	—

Examples

The following is sample output from the **show running-config pop3s** command:

```
hostname# show running-config pop3s

pop3s
 server 10.160.102.188
 authentication-server-group KerbSvr
 authentication aaa

hostname# show running-config all pop3s

pop3s
 port 995
 server 10.160.102.188
 outstanding 20
 name-separator :
 server-separator @
 authentication-server-group KerbSvr
 no authorization-server-group
 no accounting-server-group
 no default-group-policy
 authentication aaa
```

Related Commands

Command	Description
clear configure pop3s	Removes the POP3S configuration.
pop3s	Creates or edits a POP3S e-mail proxy configuration.

show running-config port-forward

To display the set(s) of applications that WebVPN users can access over forwarded TCP ports, use the **show running-config port-forward** command in privileged EXEC mode.

show running-config [all] port-forward

Syntax Description

all	(Optional) Displays the running configuration including default 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	This command was introduced.

Examples

The following is sample output from the **show running-config port-forward** command:

```
hostname# show running-config port-forward

port-forward Telnet 3500 10.148.1.5 23
port-forward Telnet 3501 10.148.1.81 23
port-forward Telnet 3502 10.148.1.82 23
port-forward SSH2 4976 10.148.1.81 22
port-forward SSH2 4977 10.148.1.85 22
port-forward Apps1 10143 flask.CompanyA.com 143
port-forward Apps1 10110 flask.CompanyA.com 110
port-forward Apps1 10025 flask.CompanyA.com 25
port-forward Apps1 11533 sametime-im.CompanyA.com 1533
port-forward Apps1 10022 ddts.CompanyA.com 22
port-forward Apps1 54000 10.148.1.5 23
port-forward Apps1 58000 vpn3060-1 23
port-forward Apps1 58001 vpn3005-1 23
hostname#
```

Related Commands

Command	Description
clear configure port-forward	Removes all port forwarding commands from the configuration. If you include the listname, the security appliance removes only the commands for that list.
port-forward	Configures the set of applications that WebVPN users can access.
port-forward (webvpn)	Enables WebVPN application access for a user or group policy.

show running-config prefix-list

To display the **prefix-list** command in the running configuration, use the **show running-config prefix-list** command in privileged EXEC mode.

show running-config prefix-list

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	This command was changed from the **show prefix-list** command to the **show running-config prefix-list** command.

Usage Guidelines

The **prefix-list description** commands always appear before their associated **prefix-list** commands in the running configuration. It does not matter what order you entered them.

Examples

The following is sample output from the **show running-config prefix-list** command:

```
hostname# show running-config prefix-list

!
prefix-list abc description A sample prefix list
prefix-list abc seq 5 permit 192.168.0.0/8 le 24
prefix-list abc seq 10 deny 10.0.0.0/8 le 32
!
```

Related Commands

Command	Description
clear configure prefix-list	Clears the **prefix-list** commands from the running configuration.

show running-config priority-queue

To display the priority queue configuration details for an interface, use the **show running-config priority-queue** command in privileged EXEC mode.

show running-config priority-queue *interface-name*

Syntax Description

interface-name	Specifies the name of the interface for which you want to show the priority queue details

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	This command was introduced.

Examples

This example shows the use of the show running-config priority-queue command for the interface named test, and the command output:

```
hostname# show running-config priority-queue test
priority-queue test
  queue-limit   50
  tx-ring-limit 10
hostname#
```

Related Commands

Command	Description
clear configure priority-queue	Removes the priority-queue configuration from the named interface.
priority-queue	Configures priority queueing on an interface.
show priority-queue statistics	Shows the statistics for the priority queue configured on the named interface.

show running-config privilege

To display the privileges for a command or a set of commands, use the **show running-config privilege** command in privileged EXEC mode.

show running-config [all] privilege [**all | command** *command* **| level** *level*]

Syntax Description

all	(Optional) First occurrence -- Displays the default privilege level.
all	(Optional) Second occurrence -- Displays the privilege level for all commands.
command *command*	(Optional) Displays the privilege level for a specific command.
level *level*	(Optional) Displays the commands that are configured with the specified level; valid values are from 0 to 15.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was modified for this release to conform to CLI guidelines.

Usage Guidelines

Use the **show running-config privilege** command to view the current privilege level.

Examples

```
hostname(config)# show running-config privilege level 0
privilege show level 0 command checksum
privilege show level 0 command curpriv
privilege configure level 0 mode enable command enable
privilege show level 0 command history
privilege configure level 0 command login
privilege configure level 0 command logout
privilege show level 0 command pager
privilege clear level 0 command pager
privilege configure level 0 command pager
privilege configure level 0 command quit
privilege show level 0 command version
```

Related Commands

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

show running-config rip

To display the information about the RIP configuration, use the **show running-config rip** command in privileged EXEC mode.

show running-config [**all**] **rip** [*interface_name*]

Syntax Description

all	(Optional) Shows all RIP commands, including the commands you have not changed from the default.
interface_name	(Optional) Displays only the RIP commands for the specified 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**
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.0	This command was changed from **show rip** to **show running-config rip**.

Examples

This example shows how to display RIP information:

```
hostname# show running-config rip
rip outside passive version 2 authentication md5 thisisakey 2
rip outside default version 2 authentication md5 thisisakey 2
rip inside passive version 1
rip dmz passive version 2
```

Related Commands

Command	Description
clear configure rip	Clears all RIP commands from the running configuration.
debug rip	Displays debug information for RIP.
rip	Configures RIP on the specified interface.

show running-config route

To display the route configuration that is running on the security appliance, use the **show running-config route** command in privileged EXEC mode.

show running-config [**all**] **route**

Syntax Description

No default behavior or values.

Defaults

This command has no arguments or keywords.

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	Added keyword **running-config**.

Examples

The following is sample output from the **show running-config route** command:

```
hostname# show running-config route
route outside 10.30.10.0 255.255.255.0 1
```

Related Commands

Command	Description
clear configure route	Removes the **route** commands from the configuration that do not contain the **connect** keyword.
route	Specifies a static or default route for the an interface.
show route	Displays route information.

show running-config route-map

To display the information about the route map configuration, use the **show running-config route-map** command in privileged EXEC mode.

show running-config route-map [*map_tag*]

Syntax Description

map_tag	(Optional) Text for the route-map tag.

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	Added keyword **running-config**.

Usage Guidelines

To show all route-maps defined in the configuration, use the **show running-config route-map** command. To show individual route-maps by name, use the **show running-config route-map** *map_tag* command, where *map_tag* is the name of the route-map. Multiple route maps may share the same map tag name.

Examples

The following is sample output from the **show running-config route-map** command:

```
hostname# show running-config route-map
route-map maptag1 permit sequence 10
    set metric 5
    match metric 3
route-map maptag1 permit sequence 12
    set metric 5
    match interface backup
    match metric 3
route-map maptag2 deny sequence 10
    match interface dmz
```

Related Commands

Command	Description
clear configure route-map	Removes the conditions for redistributing the routes from one routing protocol into another routing protocol.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.

show running-config router

To display the global commands in the router configuration, use the **show running-config router** command in privileged EXEC mode.

show running-config [all] **router** [**ospf** [*process_id*]]

Syntax Description

all	Shows all router commands, including the commands you have not changed from the default.
ospf	(Optional) Displays only the OSPF commands in the configuration.
process_id	(Optional) Displays the commands for the selected OSPF process.

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	This command was changed from the **show router** command to the **show running-config router** command.

Examples

The following is sample output from the **show running-config router** command:

```
hostname# show running-config router ospf 1
router ospf 1
  log-adj-changes detail
  ignore lsa mospf
  no compatible rfc1583
  distance ospf external 200
  timers spf 10 20
  timers lsa-group-pacing 60
```

Related Commands

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

show running-config same-security-traffic

To display the same-security interface communication, use the **show running-config same-security-traffic** command in privileged EXEC mode.

show running-config same-security-traffic

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:

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following is sample output from the **show running-config same-security-traffic** command:

```
hostname# show running-config same-security-traffic
```

Related Commands

Command	Description
same-security-traffic	Permits communication between interfaces with equal security levels.

show running-config service

To display the system services, use the **show running-config service** command in privileged EXEC mode.

show running-config service

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	The keyword **running-config** was added.

Examples

This command shows how to display the system services:

```
hostname# show running-config service
service resetoutside
```

Related Commands

Command	Description
service	Enables system services.

show running-config service-policy

To display all currently running service policy configurations, use the **show runnig-config service-policy** command in global configuration mode.

show running-config service-policy

Syntax Description

default	Displays the default service policy.

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	This command was introduced.

Examples

The following is an example of the **show running-config service-policy** command:

```
hostname# show running-config service-policy
```

Related Commands

Command	Description
show service-policy	Displays the service policy.
service-policy	Configures service policies.
clear service-policy	Clears service policy configurations.
clear configure service-policy	Clears service policy configurations.

show running-configuration smtps

To display the running configuration for smpts, use the s**how running-configuration smtps** command in privileged EXEC mode. To have the display include the default configuration, use the **all** keyword.

show running-configuration [all] smtps

Syntax Description

all	Displays the running configuration including default values.

Defaults

No default behavior or values.

Command History

Release	Modification
7.0	This command was introduced.

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	•	—	•	—	—
Global configuration	•	—	•	—	—

Examples

The following is sample output from the **show running-config smtps** command:

```
hostname# show running-configuration smtps

smtps
server 10.1.1.21
 authentication-server-group KerbSvr
 authentication aaa

hostname# show running-config all smtps

smtps
 port 995
 server 10.1.1.21
 outstanding 20
 name-separator :
 server-separator @
 authentication-server-group KerbSvr
 no authorization-server-group
 no accounting-server-group
 no default-group-policy
 authentication aaa
hostname#
```

Related Commands

Command	Description
clear configure smtps	Removes the SMTPS configuration.
smtps	Creates or edits an SMTPS e-mail proxy configuration

show running-config snmp-map

To show the SNMP maps that have been configured, use the **show running-config snmp-map** command in privileged EXEC mode.

show running-config snmp-map *map_name*

Syntax Description.

map_name	Displays configuration for the specified SNMP map.

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	This command was introduced.

Usage Guidelines

The **show running-config snmp-map** command displays the SNMP maps that have been configured.

Examples

The following is sample output from the **show running-config snmp-map** command:

```
hostname# show running-config snmp-map snmp-policy
!
snmp-map snmp-policy
deny version 1
!
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
deny version	Disallows traffic using a specific version of SNMP.
inspect snmp	Enable SNMP application inspection.
snmp-map	Defines an SNMP map and enables SNMP map configuration mode.

show running-config snmp-server

To display all currently running SNMP server configurations, use the **show runnig-config snmp-server** command in global configuration mode.

show running-config [default] snmp-server

Syntax Description

default	Displays the default snmp server configuration.

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
PIX Version 7.0	This command was introduced.

Examples

The following is an example of the **show running-config snmp-server** command:

```
hostname# show running-config snmp-server
```

Related Commandsh

Command	Description
snmp-server	Configures the SNMP server.
clear snmp-server	Clears the SNMP server configuration.
show snmp-server statistics	Displays SNMP server configuration.

show running-config ssh

To show the SSH commands in the current configuration, use the **show running-config ssh** command in privileged EXEC mode.

show running-config [**default**] **ssh** [**timeout** | **version**]

show run [**default**] **ssh** [**timeout**]

Syntax Description

default	(Optional) Displays the default SSH configuration values along with the configured values.
timeout	(Optional) Displays the current SSH session timeout value.
version	(Optional) Displays the version of SSH currently being supported.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	The command was changed from the **show ssh** command to the **show running-config ssh** command.

Usage Guidelines

This command shows the current ssh configuration. To display only the SSH session timeout value, use the **timeout** option. To see a list of active SSH sessions, use the **show ssh sessions** command.

Examples

The following example displays the SSH session timeout:

```
hostname# show running-config timeout
ssh timeout 5 minutes
hostname#
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
ssh	Allows SSH connectivity to the security appliance from the specified client or network.
ssh scopy enable	Enables a secure copy server on the security appliance.
ssh timeout	Sets the timeout value for idle SSH sessions.
ssh version	Restricts the security appliance to using either SSH Version 1 or SSH Version 2.

show running-config ssl

To display the current set of configured ssl commands, use the **show running-config ssl** command in privileged EXEC mode.

show running-config ssl

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	•	•	•	•	•
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following is sample output from the **show running-config ssl** command:

```
hostname# show running-config ssl
ssl server-version  tlsv1
ssl client-version tlsv1-only
ssl encryption 3des-sha1
ssl trust-point Firstcert
```

Related Commands

Command	Description
clear config ssl	Removes all ssl commands from the configuration, reverting to the default values.
ssl client-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a client.
ssl server-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a server
ssl trust-point	Specifies the certificate trust point that represents the SSL certificate for an interface.

show running-config static

To display all **static** commands in the configuration, use the **show running-config static** command in privileged EXEC mode.

show running-config static

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	The keyword **running-config** was added.

Usage Guidelines

This command displays the maximum connections value for the UDP protocol. If the UDP maximum connections value is “0” or not set, the limit enforcement is disabled.

Examples

This example shows how to display all static commands in the configuration:

```
hostname# show running-config static
static (inside,outside) 192.150.49.91 10.1.1.91 netmask 255.255.255.255
static (inside,outside) 192.150.49.200 10.1.1.200 netmask 255.255.255.255 tcp 255 0
```

Note No UDP value connection limit is shown.

Related Commands

Command	Description
clear configure static	Removes all the **static** commands from the configuration.
static	Configures a persistent one-to-one address translation rule by mapping a local IP address to a global IP address.

show running-config sunrpc-server

To display the information about the SunRPC configuration, use the **show running-config sunrpc-server** command in privileged EXEC mode.

show running-config sunrpc-server *interface_name ip_addr mask* **service** *service_type* **protocol** [**TCP** | **UDP**] **port** *port* [**-** *port*] **timeout** *hh:mm:ss*

Syntax Description

interface_name	Server interface.
ip_addr	Server IP address.
mask	Network mask.
port *port* **-** *port*	SunRPC protocol port range and optionally, a second port.
protocol	SunRPC transport protocol.
service	Specifies a service.
service_type	Sets the SunRPC service program type.
timeout *hh:mm:ss*	Specifies the timeout idle time after which the access for the SunRPC service traffic is closed.
TCP	(Optional) Specifies TCP.
UDP	(Optional) Specifies UDP.

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	This command was introduced.

Usage Guidelines

The *service_type* is specified in the **sunrpcinfo** command.

Examples

The following is sample output from the **show running-config sunrpc-server** command:

```
hostname# show running-config sunrpc-server
inside 30.26.0.23 255.255.0.0 service 2147483647 protocol TCP port 2222 timeout 0:03:00
```

Related Commands

Command	Description
clear configure sunrpc-server	Clears the SunRPC services from the security appliance.
debug sunrpc	Enables debug information for SunRPC.
show conn	Displays the connection state for different connection types, including SunRPC.
sunrpc-server	Creates the SunRPC services table.
timeout	Sets the maximum idle time duration for different protocols and session types, including SunRPC.

show running-config sysopt

To show the **sysopt** command configuration in the running configuration, use the **show running-config sysopt** command in privileged EXEC mode.

show running-config sysopt

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	This command was changed from the **show sysopt** command.

Examples

The following is sample output from the **show running-config sysopt** command:

```
hostname# show running-config sysopt
no sysopt connection timewait
sysopt connection tcpmss 1200
sysopt connection tcpmss minimum 400
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt connection permit-ipsec
```

Related Commands

Command	Description
clear configure sysopt	Clears the **sysopt** command configuration.
sysopt connection permit-ipsec	Permits any packets that come from an IPSec tunnel without checking any ACLs for interfaces.
sysopt connection tcpmss	Overrides the maximum TCP segment size or ensures that the maximum is not less than a specified size.
sysopt connection timewait	Forces each TCP connection to linger in a shortened TIME_WAIT state after the final normal TCP close-down sequence.
sysopt nodnsalias	Disables alteration of the DNS A record address when you use the **alias** command.

show running-config tcp-map

To display the information about the TCP map configuration, use the **show running-config tcp-map** command in privileged EXEC mode.

show running-config tcp-map [*tcp_map_name*]

Syntax Description

tcp_map_name	(Optional) Text for the TCP map name; the text can be up to 58 characters in length.

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	This command was introduced.

Examples

The following is sample output from the **show running-config tcp-map** command:

```
hostname# show running-config tcp-map
tcp-map localmap
```

Related Commands

Command	Description
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.
clear configure tcp-map	Clears the TCP map configuration.

show running-config telnet

To display the current list of IP addresses that are authorized to use Telnet connections to the security appliance, use the **show running-config telnet** command in privileged EXEC mode. You can also use this command to display the number of minutes that a Telnet session can remain idle before being closed by the security appliance.

show running-config telnet [**timeout**]

Syntax Description

timeout	(Optional) Displays the number of minutes that a Telnet session can be idle before being closed by the security appliance.

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	The keyword **running-config** was added.

Examples

This example shows how to display the current list of IP addresses that are authorized for use by Telnet connections to the security appliance:

```
hostname# show running-config telnet
2003 Jul 15 14:49:36 %MGMT-5-LOGIN_FAIL:User  failed to
log in from 128.107.183.22 through Telnet
2003 Jul 15 14:50:27 %MGMT-5-LOGIN_FAIL:User  failed to log in from 128.107.183.
22 through Telnet
```

Related Commands

Command	Description
clear configure telnet	Removes the Telnet connection from the configuration.
telnet	Adds Telnet access to the console and sets the idle timeout.

show running-config terminal

To display the current terminal settings, use the **show running-config terminal** command in privileged EXEC mode.

show running-config terminal

Syntax Description

This command has no keywords or arguments.

Defaults

The default display width is 80 columns.

Command Modes

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

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

Command History

Release	Modification
7.0	The **running-config** keyword was added.

Examples

The following example clears the page length setting:

```
hostname# show running-config terminal

Width = 80, no monitor
```

Related Commands

Command	Description
clear configure terminal	Clears the terminal display width setting.
terminal	Sets the terminal line parameters.
terminal width	Sets the terminal display width.

show running-config tftp-server

To display the default TFTP server address and directory, use the **show running-config tftp-server** command in global configuration mode.

show running-config tftp-server

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	The **running-config** keyword was added.

Examples

This example shows how to display the IP/IPv6 address of the default TFTP server and the directory of the configuration file:

```
hostname(config)# show running-config tftp-server
tftp-server inside 10.1.1.42 /temp/config/test_config
```

Related Commands

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

show running-config timeout

To display the timeout value of all protocols, or just a specific one, use the **show running-config timeout** command in privileged EXEC mode.

show running-config timeout *protocol*

Syntax Description

protocol	(Optional) Displays the timeout value of the specified protocol. Supported protocols are: **xlate**, **conn, udp**, **icmp**, **rpc**, **h323**, **h225**, **mgcp**, **mgcp-pat**, **sip**, **sip_media**, and **uauth**.

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	The **running-config** and **mgcp-pat** keywords were added.

Examples

This example shows how to display the timeout values for the system:

```
hostname(config)# show timeout
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02
:00
timeout uauth 0:00:00 absolute
```

Related Commands

Command	Description
clear configure timeout	Restores the default idle time durations.
timeout	Sets the maximum idle time duration.

show running-config tunnel-group

To display tunnel group information about all or a specified tunnel group and tunnel-group attributes, use the **show running-config tunnel-group** command in global configuration or privileged EXEC mode.

show running-config [**all**] **tunnel-group** [*name* [**general-attributes | ipsec-attributes | ppp-attributes**]]

Syntax Description

all	[Optional] Displays all tunnel-group commands, including the commands you have not changed from the default.
general-attributes	Displays configuration information for general attributes.
ipsec-attributes	Displays configuration information for IPSec attributes.
name	Specifies the name of the tunnel group.
ppp-attributes	Displays configuration information for PPP attributes.

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	•		•		
Privileged EXEC	•		•		

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example entered in global configuration mode, displays the current configuration for all tunnel groups:

```
hostname<config># show running-config tunnel-group
tunnel-group 209.165.200.225 type IPSec_L2L
tunnel-group 209.165.200.225 ipsec-attributes
    pre-shared-key xyzx
hostname<config>#
```

Related Commands

Command	Description
clear configure tunnel-group	Removes tunnel-group configuration
tunnel-group general-attributes	Enters subconfiguration mode for specifying general attributes for specified tunnel group.
tunnel-group ipsec-attributes	Enters subconfiguration mode for specifying IPSec attributes for specified tunnel group.
tunnel-group	Enters tunnel-group subconfiguration mode for the specified type.

show running-config url-block

To show the configuration for buffers and memory allocation used by URL filtering, use the **show running-config url-block** command in privileged EXEC mode.

show running-config url-block [**block** | **url-mempool** | **url-size**]

Syntax Description

block	Displays the configuration for the maximum number of blocks that will be buffered.
url-mempool	Displays the configuration for the maximum allow URL size (in KB).
url-size	Displays the configuration for the memory resource (in KB) allocated for the long URL buffer.

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
Prexisting	This command was previously existing.

Usage Guidelines

The **show running-config url-block** command displays the configuration for buffers and memory allocation used by URL filtering.

Examples

The following is sample output from the **show running-config url-block** command:

```
hostname# show running-config url-block
!
url-block block 56
!
```

Related Commands

Commands	Description
clear url-block block statistics	Clears the block buffer usage counters.
show url-block	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-block	Manage the URL buffers used for web server responses.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

show running-config url-cache

To show the cache configuration used by URL filtering, use the **show running-config url-cache** command in privileged EXEC mode.

show running-config url-cache

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 previously existing.

Usage Guidelines

The **show running-config url-cache** command displays the cache configuration used by URL filtering.

Examples

The following is sample output from the **show running-config url-cache** command:

```
hostname# show running-config url-cache
!
url-cache src_dst 128
!
```

Related Commands

Commands	Description
clear url-cache statistics	Removes **url-cache** command statements from the configuration.
filter url	Directs traffic to a URL filtering server.
show url-cache statistics	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

show running-configuration url-list

To display the set(s) of URLs that WebVPN users can access, use the **show running-configuration url-list** command in privileged EXEC mode.

show running-configuration url-list

Syntax Description

This command has no arguments or keywords.

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	•	—	•	—	—
Global configuration	•	—	•	—	—
Webvpn	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following is sample output from the **show running-configuration url-list** command:

```
hostname# show running-configuration url-list
url-list userURL "SW Engineering" http://10.1.1.2
url-list userURL "My Company" http://www.mycompany.com
url-list userURL "401K Program" https://401k.com
url-list userURL "Exchange5.5 Mail" http://10.1.1.11/exchange
url-list URLlist2 "OWA-2000" http://10.1.1.7/exchange
```

Related Commands

Command	Description
clear configuration url-list	Removes all url-list commands from the configuration. If you include the listname, the security appliance removes only the commands for that list.
url-list	Configures the set of URLs that WebVPN users can access.
url-list	Enables WebVPN URL access for a specific group policy or user.

show running-config url-server

To show the URL filtering server configuration, use the **show running-config url-server** command in privileged EXEC mode.

show running-config url-server

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 previously existing.

Usage Guidelines

The **show running-config url-server** command displays the URL filtering server configuration.

Examples

The following is sample output from the **show running-config url-server** command:

```
hostname# show running-config url-server
!
url-server (perimeter) vendor websense host 10.0.1.1
!
```

Related Commands

Commands	Description
clear url-server	Clears the URL filtering server statistics.
show url-server	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense filtering server.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

show running-config username

To display the running configuration for a particular user, use the **show running-config username** command in privileged EXEC mode with the username appended. To display the running configuration for all users, use this command without a username.

show running-config [**all**] **username** [*name*] [**attributes**]]

Syntax Description

attributes	Displays the specific AVPs for the user(s)
all	(Optional) Displays all username commands, including the commands you have not changed from the default.
name	Provides the name of the user.

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	•	—	•	—	—
Global configuration	•	—	•	—	—
Username	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following is sample output from the show the running-config username for a user named anyuser:

```
hostname# show running-config username anyuser
username anyuser password .8T1d6ik58/lzXS5 encrypted privilege 3
username anyuser attributes
vpn-group-policy DefaultGroupPolicy
vpn-idle-timeout 10
vpn-session-timeout 120
vpn-tunnel-protocol IPSec
```

Related Commands

Command	Description
clear config username	Clears the username database.
username	Adds a user to the security appliance database.
username attributes	Lets you configure attributes for specific users.

show running-config virtual

To display the IP address of the security appliance virtual server, use the **show running-config virtual** command in privileged EXEC mode.

show running-config [**all**] **virtual**

Syntax Description

all	Display the virtual server IP address of all virtual servers.

Defaults

Omitting the **all** keyword displays the explicitly configured IP address of the current virtual server or servers.

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	This command was modified to conform to CLI guidelines.

Usage Guidelines

You must be in privileged EXEC mode to use this command.

Examples

This example displays the **show running-config virtual** command output for a situation in which there is a previously configured HTTP virtual server:

```
hostname(config)# show running-config virtual
virtual http 192.168.201.1
```

Related Commands

Command	Description
clear configure virtual	Removes **virtual** command statements from the configuration.
virtual	Displays the address for authentication virtual servers.

show running-config vpn load-balancing

To display the current VPN load-balancing virtual cluster configuration, use the **show running-config vpn-load-balancing** command in global configuration, privileged EXEC, or VPN load-balancing mode.

show running-config [**all**] **vpn load-balancing**

Syntax Description

all	Display both the default and the explicitly configured VPN load-balancing configuration.

Defaults

Omitting the **all** keyword displays the explicitly configured VPN load-balancing configuration.

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	•	—	•	—	—
Privileged EXEC	•	—	•	—	—
vpn load-balancing	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **show running-config vpn load-balancing** command also displays configuration information for the following related commands: **cluster encryption**, **cluster ip address**, **cluster key**, **cluster port**, **nat**, **participate**, and **priority**.

Examples

This example displays **show running-config vpn load-balancing** command and its output, with the **all** option enabled:

```
hostname(config)# show running-config all vpn load-balancing
vpn load-balancing
 no nat
 priority 9
 interface lbpublic test
 interface lbprivate inside
 no cluster ip address
 no cluster encryption
 cluster port 9023
 no participate
```

Related Commands

Command	Description
clear configure vpn load-balancing	Removes **vpn load-balancing** command statements from the configuration.
show vpn load-balancing	Displays the VPN load-balancing runtime statistics.
vpn load-balancing	Enters vpn load-balancing mode.

show running-configuration vpn-sessiondb

To display the current set of configured vpnsessiondb commands, use the **show running-configuration vpn-sessiondb** command in privileged EXEC mode.

show running-configuration [all] vpn-sessiondb

Syntax Description

all	(Optional) Displays all **vpn-sessionddb** commands, including the commands you have not changed from the default

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	This command was introduced.

Usage Guidelines

As of Release 7.0, this command displays only the VPN maximum sessions limit, if configured.

Examples

The following is sample output for the **show running-configuration vpn-sessiondb** command:

```
hostname# show running-configuration vpn-sessiondb
```

Related Commands

Command	Description
show vpn-sessiondb	Displays sessions with or without extended details, optionally filtered and sorted by criteria you specify.
show vpn-sessiondb summary	Displays a session summary, including total current session, current sessions of each type, peak and total cumulative, maximum concurrent sessions

show running-configuration webvpn

To display the running configuration for webvpn, use the s**how running-configuration webvpn** command in privileged EXEC mode. To have the display include the default configuration, use the **all** keyword.

show running-configuration [all] webvpn

Syntax Description

all	Displays the running configuration including default values.

Defaults

No default behavior or values.

Command History

Release	Modification
7.0	This command was introduced.

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	•	—	•	—	—
Global configuration	•	—	•	—	—

Examples

The following is sample output from the **show running-config webvpn** command:

```
hostname# show running-configuration webvpn
webvpn
 title WebVPN Services for ASA-4
 title-color green
 default-idle-timeout 0
 nbns-server 10.148.1.28 master timeout 2 retry 2
 accounting-server-group RadiusACS1
 authentication-server-group RadiusACS2
 authorization-dn-attributes CN

hostname#(config-webvpn)# show running-config all webvpn

webvpn
 title WebVPN Services for ASA-4
 username-prompt Username
 password-prompt Password
 login-message Please enter your username and password
 logout-message Goodbye
 no logo
 title-color green
 secondary-color #CCCCFF
```

```
 text-color white
 secondary-text-color black
 default-idle-timeout 0
 no http-proxy
 no https-proxy
 nbns-server 10.148.1.28 master timeout 2 retry 2
 accounting-server-group RadiusACS1
 authentication-server-group RadiusACS2
 no authorization-server-group
 default-group-policy DfltGrpPolicy
 authentication aaa
 no authorization-required
 authorization-dn-attributes CN
hostname#
```

Related Commands

Command	Description
clear configure smtps	Removes the smtps configuration.
smtps	Creates or edits an SMTPS e-mail proxy configuration

show service-policy

To display the configured service policies, use the **service-policy** command in global configuration mode.

show service-policy [**global** | **interface** *intf*] [**inspect** | **ips** | **police** | **priority** | **set connection**]

show service-policy [**global** | **interface** *intf*] [**flow** *protocol* {**host** *src_host* | *src_ip src_mask*} [**eq** *src_port*] {**host** *dest_host* | *dest_ip dest_mask*} [**eq** *dest_port*] [*icmp_number* | *icmp_control_message*]]

Syntax Description

dest_ip	The destination IP address of the traffic flow.
dest_mask	The subnet mask of the traffic flow destination IP address.
dest_port	(Optional) The destination port used in the traffic flow.
eq	(Optional) The equals operator, requiring the source or destination port, as applicable, to match the port number that follows.
flow	(Optional) Specifies a traffic flow for which you want to see the policies that the security appliance would apply to the flow. The arguments and keywords following the **flow** keyword specify the flow in ip-5-tuple format.
global	(Optional) Limits output to the global policy, which applies to all interfaces.
host *dest_host*	The host destination IP address of the traffic flow.
host *src_host*	The host source IP address of the traffic flow.
icmp_control_message	(Optional) Specifies an ICMP control message of the traffic flow. Valid values for the *icmp_control_message* argument are listed in the "Usage Guidelines" section, below.
icmp_number	(Optional) Specifies the ICMP protocol number of the traffic flow.
inspect	(Optional) Limits the output to policies that include an **inspect** command.
interface *intf*	(Optional) Displays policies applied to the interface specified by the *intf* argument, where *intf* is the interface name given by the **nameif** command.
ips	Limits output to policies that include the **ips** command.
police	Limits output to policies that include the **police** command.
priority	Limits output to policies that include the **priority** command.
set connection	Limits output to policies that include the **set connection** command.
protocol	The protocol used in the traffic flow. Valid values for the *protocol* argument are listed in the "Usage Guidelines" section, below.
src_ip	The source IP address used in the traffic flow.
src_mask	The source IP netmask used in the traffic flow.
src_port	The source port used in the traffic flow.

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		
	Routed	Transparent	Single	Multiple Context	Multiple System
Global configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **flow** keyword lets you determine, for any flow that you can describe, the policies that the security appliance would apply to that flow. You can use this to check that your service policy configuration will provide the services you want for specific connections. The arguments and keywords following the **flow** keyword specifies the flow in ip-5-tuple format with no object grouping.

Because the flow is described in ip-5-tuple format, not all match criteria are supported. Following are the list of match criteria that are supported for flow match:

- **match access-list**
- **match port**
- **match rtp**
- **match default-inspection-traffic**

The **priority** keyword is used to display the aggregate counter values of packets transmitted through an interface.

The number of embryonic connections displayed in the **show service-policy** command output indicates the current number of embryonic connections to an interface for traffic matching that defined by the **class-map** command. The `embryonic-conn-max` field shows the maximum embryonic limit configured for the traffic class using the Modular Policy Framework. If the current embryonic connections displayed equals or exceeds the maximum, TCP intercept is applied to new TCP connections that match the traffic type defined by the **class-map** command.

protocol Argument Values

The following are valid values for the *protocol* argument:

- *number*—The protocol number (0 - 255).
- **ah**
- **eigrp**
- **esp**
- **gre**
- **icmp**
- **icmp6**
- **igmp**
- **igrp**
- **ip**
- **ipinip**

- **ipsec**
- **nos**
- **ospf**
- **pcp**
- **pim**
- **pptp**
- **snp**
- **tcp**
- **udp**

icmp_control_message Argument Values

The following are valid values for the *icmp_control_message* argument:

- **alternate-address**
- **conversion-error**
- **echo**
- **echo-reply**
- **information-reply**
- **information-request**
- **mask-reply**
- **mask-request**
- **mobile-redirect**
- **parameter-problem**
- **redirect**
- **router-advertisement**
- **router-solicitation**
- **source-quench**
- **time-exceeded**
- **timestamp-reply**
- **timestamp-request**
- **traceroute**
- **unreachable**

Examples

The following example shows the syntax of the **show service-policy** command:

```
hostname# show service-policy global

Global policy:
  Service-policy: inbound_policy
    Class-map: ftp-port
      Inspect: ftp strict inbound_ftp, packet 0, drop 0, reset-drop 0
hostname# show service-policy priority
```

```
Interface outside:

Global policy:
  Service-policy: sa_global_fw_policy

Interface outside:
  Service-policy: ramap
    Class-map: clientmap
      Priority:
        Interface outside: aggregate drop 0, aggregate transmit 5207048
    Class-map: udpmap
      Priority:
        Interface outside: aggregate drop 0,  aggregate transmit 5207048
    Class-map: cmap


hostname# show service-policy flow udp host 209.165.200.229 host 209.165.202.158 eq 5060

Global policy:
  Service-policy: f1_global_fw_policy
    Class-map: inspection_default
      Match: default-inspection-traffic
      Action:
        Input flow:  inspect sip

Interface outside:
  Service-policy: test
    Class-map: test
      Match: access-list test
        Access rule: permit ip 209.165.200.229 255.255.255.224 209.165.202.158
255.255.255.224
      Action:
        Input flow:  ids inline
        Input flow:  set connection conn-max 10 embryonic-conn-max 20
```

Related Commands

Command	Description
clear configure service-policy	Clears service policy configurations.
clear service-policy	Clears all service policy configurations.
service-policy	Configures the service policy.
show running-config service-policy	Displays the service policies configured in the running configuration.

show service-policy inspect gtp

To display the GTP configuration, use the **show service-policy inspect gtp** command in privileged EXEC mode.

show service-policy [**interface** *int*] **inspect gtp** {**pdp-context** [**apn** *ap_name* | **detail** | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num*] | **pdpmcb** | **requests** | **statistics** [**gsn** *IP_address*] }

Syntax Description.

apn	(Optional) Displays the detailed output of the PDP contexts based on the APN specified.
ap_name	Identifies the specific access point name for which statistics are displayed.
detail	(Optional) Displays the detailed output of the PDP contexts.
imsi	Displays the detailed output of the PDP contexts based on the IMSI specified.
IMSI_value	Hexadecimal value that identifies the specific IMSI for which statistics are displayed.
interface	(Optional) Identifies a specific interface.
int	Identifies the interface for which information will be displayed.
gsn	(Optional) Identifies the GPRS support node, which is interface between the GPRS wireless data network and other networks.
gtp	(Optional) Displays the service policy for GTP.
IP_address	IP address for which statistics are displayed.
ms-addr	(Optional) Displays the detailed output of the PDP contexts based on the MS Address specified.
pdp-context	(Optional) Identifies the Packet Data Protocol context
pdpmcb	(Optional) Displays the status of the PDP master control block.
requests	(Optional) Displays status of GTP requests.
statistics	(Optional) Displays GTP statistics.
tid	(Optional) Displays the detailed output of the PDP contexts based on the TID specified.
tunnel_ID	Hexadecimal value that identifies the specific tunnel for which statistics are displayed.
version	(Optional) Displays the detailed output of the PDP contexts based on the GTP version.
version_num	Specifies the version of the PDP context for which statistics are displayed. The valid range is 0 to 255.

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	This command was introduced.

Usage Guidelines

You can use the vertical bar | to filter the display. Type | for more display filtering options.

The **show pdp-context** command displays PDP context-related information.

The Packet Data Protocol context is identified by the tunnel ID, which is a combination of IMSI and NSAPI. A GTP tunnel is defined by two associated PDP Contexts in different GSN nodes and is identified with a Tunnel ID. A GTP tunnel is necessary to forward packets between an external packet data network and a mobile station user.

The **show gtp requests** command displays current requests in the request queue.

Examples

The following is sample output from the **show gtp requests** command:

```
hostname# show gtp requests
0 in use, 0 most used, 200 maximum allowed
```

You can use the vertical bar | to filter the display, as in the following example:

```
hostname# show service-policy gtp statistics | grep gsn
```

This example shows the GTP statistics with the word gsn in the output.

The following command shows the statistics for GTP inspection:

```
hostname# show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support | 0 | msg_too_short | 0
  unknown_msg | 0 | unexpected_sig_msg | 0
  unexpected_data_msg | 0 | ie_duplicated | 0
  mandatory_ie_missing | 0 | mandatory_ie_incorrect | 0
  optional_ie_incorrect | 0 | ie_unknown | 0
  ie_out_of_order | 0 | ie_unexpected | 0
  total_forwarded | 0 | total_dropped | 0
  signalling_msg_dropped | 0 | data_msg_dropped | 0
  signalling_msg_forwarded | 0 | data_msg_forwarded | 0
  total created_pdp | 0 | total deleted_pdp | 0
  total created_pdpmcb | 0 | total deleted_pdpmcb | 0
  pdp_non_existent | 0
```

The following command displays information about the PDP contexts:

```
hostname# show service-policy inspect gtp pdp-context
1 in use, 1 most used, timeout 0:00:00

Version TID | MS Addr | SGSN Addr | Idle | APN
```

```
v1 | 1234567890123425 | 1.1.1.1 | 11.0.0.2 0:00:13  gprs.cisco.com

 | user_name (IMSI): 214365870921435 | MS address: | 1.1.1.1
 | primary pdp: Y | nsapi: 2
 | sgsn_addr_signal: | 11.0.0.2 | sgsn_addr_data: | 11.0.0.2
 | ggsn_addr_signal: | 9.9.9.9 | ggsn_addr_data: | 9.9.9.9
 | sgsn control teid: | 0x000001d1 | sgsn data teid: | 0x000001d3
 | ggsn control teid: | 0x6306ffa0 | ggsn data teid: | 0x6305f9fc
 | seq_tpdu_up: | 0 | seq_tpdu_down: | 0
 | signal_sequence: | 0
 | upstream_signal_flow: | 0 | upstream_data_flow: | 0
 | downstream_signal_flow: | 0 | downstream_data_flow: | 0
 | RAupdate_flow: | 0
```

Table 7-29 describes each column the output from the **show service-policy inspect gtp pdp-context** command.

Table 7-32 PDP Contexts

Column Heading	Description
Version	Displays the version of GTP.
TID	Displays the tunnel identifier.
MS Addr	Displays the mobile station address.
SGSN Addr	Displays the serving gateway service node.
Idle	Displays the time for which the PDP context has not been in use.
APN	Displays the access point name.

Related Commands

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

show shun

To display shun information, use the **show shun** command in privileged EXEC mode.

show shun [*src_ip* | *statistics*]

Syntax Description

src_ip	(Optional) Displays the information for that address.
statistics	(Optional) Displays the interface counters only.

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 shun** command:

```
hostname# show shun
shun (outside) 10.1.1.27 10.2.2.89 555 666 6
shun (inside1) 10.1.1.27 10.2.2.89 555 666 6
```

Related Commands

Command	Description
clear shun	Disables all the shuns that are currently enabled and clears the shun statistics.
shun	Enables a dynamic response to an attacking host by preventing new connections and disallowing packets from any existing connection.

show sip

To display SIP sessions, use the **show sip** command in privileged EXEC mode.

show sip

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.

Usage Guidelines

The **show sip** command assists in troubleshooting SIP inspection engine issues and is described with the **inspect protocol sip udp 5060** command. The **show timeout sip** command displays the timeout value of the designated protocol.

The **show sip** command displays information for SIP sessions established across the security appliance. Along with the **debug sip** and **show local-host** commands, this command is used for troubleshooting SIP inspection engine issues.

Note We recommend that you configure the **pager** command before using the **show sip** command. If there are a lot of SIP session records and the **pager** command is not configured, it will take a while for the **show sip** command output to reach its end.

Examples

The following is sample output from the **show sip** command:

```
hostname# show sip
Total: 2
call-id c3943000-960ca-2e43-228f@10.130.56.44
 state Call init, idle 0:00:01
call-id c3943000-860ca-7e1f-11f7@10.130.56.45
 state Active, idle 0:00:06
```

This sample shows two active SIP sessions on the security appliance (as shown in the `Total` field). Each `call-id` represents a call.

The first session, with the `call-id c3943000-960ca-2e43-228f@10.130.56.44,` is in the state `Call Init`, which means the session is still in call setup. Call setup is complete only when the ACK is seen. This session has been idle for 1 second.

The second session is in the state `Active`, in which call setup is complete and the endpoints are exchanging media. This session has been idle for 6 seconds.

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug sip	Enables debug information for SIP.
inspect sip	Enables SIP application inspection.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

show skinny

To troubleshoot SCCP (Skinny) inspection engine issues, use the **show skinny** command in privileged EXEC mode.

show skinny

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.

Usage Guidelines

The **show skinny** command assists in troubleshooting SCCP (Skinny) inspection engine issues.

Examples

The following is sample output from the **show skinny** command under the following conditions. There are two active Skinny sessions set up across the security appliance. The first one is established between an internal Cisco IP Phone at local address 10.0.0.11 and an external Cisco CallManager at 172.18.1.33. TCP port 2000 is the CallManager. The second one is established between another internal Cisco IP Phone at local address 10.0.0.22 and the same Cisco CallManager.

```
hostname# show skinny

        LOCAL                   FOREIGN                 STATE

-----------------------------------------------------------------

1       10.0.0.11/52238         172.18.1.33/2000                1

  MEDIA 10.0.0.11/22948         172.18.1.22/20798

2       10.0.0.22/52232         172.18.1.33/2000                1

  MEDIA 10.0.0.22/20798         172.18.1.11/22948
```

The output indicates a call has been established between both internal Cisco IP Phones. The RTP listening ports of the first and second phones are UDP 22948 and 20798 respectively.

The following is the xlate information for these Skinny connections:

```
hostname# show xlate debug
2 in use, 2 most used
Flags: D|DNS, d|dump, I|identity, i|inside, n|no random,
|o|outside, r|portmap, s|static
NAT from inside:10.0.0.11 to outside:172.18.1.11 flags si idle 0:00:16 timeout 0:05:00
NAT from inside:10.0.0.22 to outside:172.18.1.22 flags si idle 0:00:14 timeout 0:05:00
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug skinny	Enables SCCP debug information.
inspect skinny	Enables SCCP application inspection.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

show snmp-server statistics

To display information about the SNMP server statistics, use the **show snmp-server statistics** command in privileged EXEC mode.

show snmp-server statistics

Syntax Description

This command has no arguments or keywords.

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	This command was introduced.

Examples

This example shows how to display the SNMP server statistics:

```
hostname# show snmp-server statistics
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
```

Related Commands

Command	Description
snmp-server	Provides the security appliance event information through SNMP.
clear configure snmp-server	Disables the Simple Network Management Protocol (SNMP) server.
show running-config snmp-server	Displays the SNMP server configuration.

show ssh sessions

To display information about the active SSH session on the security appliance, use the **show ssh sessions** command in privileged EXEC mode.

show ssh sessions [*ip_address*]

Syntax Description

ip_address	(Optional) Displays session information for only the specified IP address.

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.

Usage Guidelines

The SID is a unique number that identifies the SSH session. The Client IP is the IP address of the system running an SSH client. The Version is the protocol version number that the SSH client supports. If the SSH only supports SSH version 1, then the Version column displays 1.5. If the SSH client supports both SSH version 1 and SSH version 2, then the Version column displays 1.99. If the SSH client only supports SSH version 2, then the Version column displays 2.0. The Encryption column shows the type of encryption that the SSH client is using. The State column shows the progress that the client is making as it interacts with the security appliance. The Username column lists the login username that has been authenticated for the session.

Examples

The following example demonstrates the output of the **show ssh sessions** command:

```
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
```

Related Commands

Command	Description
ssh disconnect	Disconnects an active SSH session.
ssh timeout	Sets the timeout value for idle SSH sessions.

show startup-config

To show the startup configuration, use the show startup-config command in privileged EXEC mode.

show startup-config

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.

Usage Guidelines

In multiple context mode, this command shows the startup configuration for your current execution space: the system configuration or the security context.

Examples

The following is sample output from the **show startup-config** command:

```
hostname# show startup-config
: Saved
: Written by enable_15 at 01:44:55.598 UTC Thu Apr 17 2003

Version 7.0(0)28
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
!
interface GigabitEthernet0/1
 shutdown
 nameif test
 security-level 0
 ip address 10.10.4.200 255.255.0.0
!

...
!
```

```
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname firewall1
domain-name example.com
boot system disk0:/cdisk.bin
ftp mode passive
names
name 10.10.4.200 outside
access-list xyz extended permit ip host 192.168.0.4 host 150.150.0.3
!
ftp-map ftp_map
!
ftp-map inbound_ftp
 deny-request-cmd appe stor stou
!

...

Cryptochecksum:4edf97923899e712ed0da8c338e07e63
```

Related Commands

Command	Description
show running-config	Shows the running configuration.

show sunrpc-server active

To display the pinholes open for Sun RPC services, use the **show sunrpc-server active** command in privileged EXEC mode.

show sunrpc-server active

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.

Usage Guidelines

Use the **show sunrpc-server active** command to display the pinholes open for Sun RPC services, such as NFS and NIS.

Examples

To display the pinholes open for Sun RPC services, enter the **show sunrpc-server active** command. The following is sample output from the **show sunrpc-server active** command:

```
hostname# show sunrpc-server active
        LOCAL           FOREIGN                 SERVICE TIMEOUT
        -----------------------------------------------
        192.168.100.2/0 209.165.200.5/32780     100005 00:10:00
```

Related Commands

Command	Description
clear configure sunrpc-server	Clears the Sun remote processor call services from the security appliance.
clear sunrpc-server active	Clears the pinholes opened for Sun RPC services, such as NFS or NIS.
inspect sunrpc	Enables or disables Sun RPC application inspection and configures the port used.
show running-config sunrpc-server	Displays information about the SunRPC services configuration.

show tcpstat

To display the status of the security appliance TCP stack and the TCP connections that are terminated on the security appliance (for debugging), use the **show tcpstat** command in privileged EXEC mode. This command supports IPv4 and IPv6 addresses.

show tcpstat

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.

Usage Guidelines

The **show tcpstat** command allows you to display the status of the TCP stack and TCP connections that are terminated on the security appliance. The TCP statistics displayed are described in Table 7-30.

Table 7-33 TCP Statistics in the show tcpstat Command

Statistic	Description
tcb_cnt	Number of TCP users.
proxy_cnt	Number of TCP proxies. TCP proxies are used by user authorization.
tcp_xmt pkts	Number of packets that were transmitted by the TCP stack.
tcp_rcv good pkts	Number of good packets that were received by the TCP stack.
tcp_rcv drop pkts	Number of received packets that the TCP stack dropped.
tcp bad chksum	Number of received packets that had a bad checksum.
tcp user hash add	Number of TCP users that were added to the hash table.
tcp user hash add dup	Number of times a TCP user was already in the hash table when trying to add a new user.
tcp user srch hash hit	Number of times a TCP user was found in the hash table when searching.

Table 7-33 TCP Statistics in the show tcpstat Command (continued)

Statistic	Description
tcp user srch hash miss	Number of times a TCP user was not found in the hash table when searching.
tcp user hash delete	Number of times that a TCP user was deleted from the hash table.
tcp user hash delete miss	Number of times that a TCP user was not found in the hash table when trying to delete the user.
lip	Local IP address of the TCP user.
fip	Foreign IP address of the TCP user.
lp	Local port of the TCP user.
fp	Foreign port of the TCP user.
st	State (see RFC 793) of the TCP user. The possible values are as follows: 1 CLOSED 2 LISTEN 3 SYN_SENT 4 SYN_RCVD 5 ESTABLISHED 6 FIN_WAIT_1 7 FIN_WAIT_2 8 CLOSE_WAIT 9 CLOSING 10 LAST_ACK 11 TIME_WAIT
rexqlen	Length of the retransmit queue of the TCP user.
inqlen	Length of the input queue of the TCP user.
tw_timer	Value of the time_wait timer (in milliseconds) of the TCP user.
to_timer	Value of the inactivity timeout timer (in milliseconds) of the TCP user.
cl_timer	Value of the close request timer (in milliseconds) of the TCP user.
per_timer	Value of the persist timer (in milliseconds) of the TCP user.
rt_timer	Value of the retransmit timer (in milliseconds) of the TCP user.
tries	Retransmit count of the TCP user.

Examples

This example shows how to display the status of the TCP stack on the security appliance:

```
hostname# show tcpstat
                CURRENT MAX      TOTAL
tcb_cnt         2       12       320
proxy_cnt       0       0        160

tcp_xmt pkts = 540591
tcp_rcv good pkts = 6583
tcp_rcv drop pkts = 2
```

```
tcp bad chksum = 0
tcp user hash add = 2028
tcp user hash add dup = 0
tcp user srch hash hit = 316753
tcp user srch hash miss = 6663
tcp user hash delete = 2027
tcp user hash delete miss = 0

lip = 172.23.59.230 fip = 10.21.96.254 lp = 443 fp = 2567 st = 4 rexqlen = 0
in0
  tw_timer = 0 to_timer = 179000 cl_timer = 0 per_timer = 0
rt_timer = 0
tries 0
```

Related Commands

Command	Description
show conn	Displays the connections used and those that are available.

show tech-support

To display the information that is used for diagnosis by technical support analysts, use the **show tech-support** command in privileged EXEC mode.

show tech-support [**detail** | **file** | **no-config**]

Syntax Description

detail	(Optional) Lists detailed information.
file	(Optional) Writes the output of the command to a file.
no-config	(Optional) Excludes the output of the running configuration.

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	The **detail** and **file** keywords were added.

Usage Guidelines

The **show tech-suppor**t command lets you list information that technical support analysts need to help you diagnose problems. This command combines the output from the **show** commands that provide the most information to a technical support analyst.

Examples

The following example shows how to display information that is used for technical support analysis, excluding the output of the running configuration:

```
hostname# show tech-support no-config

Cisco XXX Firewall Version X.X(X)
Cisco Device Manager Version X.X(X)

Compiled on Fri 15-Apr-05 14:35 by root

XXX up 2 days 8 hours

Hardware:   XXX, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB

0: ethernet0: address is 0003.e300.73fd, irq 10
```

```
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited

This XXX has a Restricted (R) license.

Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 23:05:24.264 UTC Sat Nov 16 2002

------------------ show clock ------------------

00:08:14.911 UTC Sun Apr 17 2005

------------------ show memory ------------------

Free memory:        50708168 bytes
Used memory:        16400696 bytes
-------------     ----------------
Total memory:       67108864 bytes

------------------ show conn count ------------------

0 in use, 0 most used

------------------ show xlate count ------------------

0 in use, 0 most used

------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550   1188    795    919

------------------ show interface ------------------

interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0003.e300.73fd
  IP address 172.23.59.232, subnet mask 255.255.0.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        1267 packets input, 185042 bytes, 0 no buffer
        Received 1248 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        20 packets output, 1352 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 9 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (13/128) software (0/2)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
  Hardware is i82559 ethernet, address is 0003.e300.73fe
```

```
  IP address 10.1.1.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1 packets output, 60 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        1 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet2 "intf2" is administratively down, line protocol is down
  Hardware is i82559 ethernet, address is 00d0.b7c8.139e
  IP address 127.0.0.1, subnet mask 255.255.255.255
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)

------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

------------------ show process ------------------


    PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 001e3329 00763e7c 0053e5c8          0 00762ef4 3784/4096 arp_timer
Lsi 001e80e9 00807074 0053e5c8          0 008060fc 3832/4096 FragDBGC
Lwe 00117e3a 009dc2e4 00541d18          0 009db46c 3704/4096 dbgtrace
Lwe 003cee95 009de464 00537718          0 009dc51c 8008/8192 Logger
Hwe 003d2d18 009e155c 005379c8          0 009df5e4 8008/8192 tcp_fast
Hwe 003d2c91 009e360c 005379c8          0 009e1694 8008/8192 tcp_slow
Lsi 002ec97d 00b1a464 0053e5c8          0 00b194dc 3928/4096 xlate clean
Lsi 002ec88b 00b1b504 0053e5c8          0 00b1a58c 3888/4096 uxlate clean
Mwe 002e3a17 00c8f8d4 0053e5c8          0 00c8d93c 7908/8192 tcp_intercept_times
Lsi 00423dd5 00d3a22c 0053e5c8          0 00d392a4 3900/4096 route_process
Hsi 002d59fc 00d3b2bc 0053e5c8          0 00d3a354 3780/4096 XXX Garbage Collecr
Hwe 0020e301 00d5957c 0053e5c8          0 00d55614 16048/16384 isakmp_time_keepr
Lsi 002d377c 00d7292c 0053e5c8          0 00d719a4 3928/4096 perfmon
Hwe 0020bd07 00d9c12c 0050bb90          0 00d9b1c4 3944/4096 IPSec
Mwe 00205e25 00d9e1ec 0053e5c8          0 00d9c274 7860/8192 IPsec timer handler
Hwe 003864e3 00db26bc 00557920          0 00db0764 6952/8192 qos_metric_daemon
Mwe 00255a65 00dc9244 0053e5c8          0 00dc8adc 1436/2048 IP Background
Lwe 002e450e 00e7bb94 00552c30          0 00e7ad1c 3704/4096 XXX/trace
Lwe 002e471e 00e7cc44 00553368          0 00e7bdcc 3704/4096 XXX/tconsole
Hwe 001e5368 00e7ed44 00730674          0 00e7ce9c 7228/8192 XXX/intf0
Hwe 001e5368 00e80e14 007305d4          0 00e7ef6c 7228/8192 XXX/intf1
Hwe 001e5368 00e82ee4 00730534       2470 00e8103c 4892/8192 XXX/intf2
H*  0011d7f7 0009ff2c 0053e5b0        780 00e8511c 13004/16384 ci/console
Csi 002dd8ab 00e8a124 0053e5c8          0 00e891cc 3396/4096 update_cpu_usage
Hwe 002cb4d1 00f2bfbc 0051e360          0 00f2a134 7692/8192 uauth_in
Hwe 003d17d1 00f2e0bc 00828cf0          0 00f2c1e4 7896/8192 uauth_thread
Hwe 003e71d4 00f2f20c 00537d20          0 00f2e294 3960/4096 udp_timer
Hsi 001db3ca 00f30fc4 0053e5c8          0 00f3004c 3784/4096 557mcfix
Crd 001db37f 00f32084 0053ea40  121094970 00f310fc 3744/4096 557poll
Lsi 001db435 00f33124 0053e5c8          0 00f321ac 3700/4096 557timer
Hwe 001e5398 00f441dc 008121e0          0 00f43294 3912/4096 fover_ip0
```

```
Cwe 001dcdad 00f4523c 00872b48         20 00f44344 3528/4096 ip/0:0
Hwe 001e5398 00f4633c 008121bc          0 00f453f4 3532/4096 icmp0
Hwe 001e5398 00f47404 00812198          0 00f464cc 3896/4096 udp_thread/0
Hwe 001e5398 00f4849c 00812174          0 00f475a4 3832/4096 tcp_thread/0
Hwe 001e5398 00f495bc 00812150          0 00f48674 3912/4096 fover_ip1
Cwe 001dcdad 00f4a61c 008ea850          0 00f49724 3832/4096 ip/1:1
Hwe 001e5398 00f4b71c 0081212c          0 00f4a7d4 3912/4096 icmp1
Hwe 001e5398 00f4c7e4 00812108          0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4          0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0          0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534          0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c          0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078          0 00f50c8c 3896/4096 udp_thread/2
Hwe 001e5398 00f52c5c 00812054          0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8          0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8          0 00f786c4 7640/8192 Crypto CA

------------------ show failover ------------------

No license for Failover

------------------ show traffic ------------------

outside:
        received (in 205213.390 secs):
                1267 packets    185042 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 205213.390 secs):
                20 packets      1352 bytes
                0 pkts/sec      0 bytes/sec
inside:
        received (in 205215.800 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 205215.800 secs):
                1 packets       60 bytes
                0 pkts/sec      0 bytes/sec
intf2:
        received (in 205215.810 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 205215.810 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec

------------------ show perfmon ------------------


PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
TCPIntercept         0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
```

Related Commands

Command	Description
show clock	Displays the clock for use with the Syslog Server (PFSS) and the Public Key Infrastructure (PKI) protocol.
show conn count	Displays the connections used and available.
show cpu	Display the CPU utilization information.
show failover	Displays the status of a connection and which security appliance is active
show memory	Displays a summary of the maximum physical memory and current free memory that is available to the operating system.
show perfmon	Displays information about the performance of the security appliance
show processes	Displays a list of the processes that are running.
show running-config	Displays the configuration that is currently running on the security appliance.
show xlate	Displays information about the translation slot.

show traffic

To display interface transmit and receive activity, use the **show traffic** command in privileged EXEC mode.

show traffic

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.

Usage Guidelines

The **show traffic** command lists the number of packets and bytes moving through through each interface since the last show traffic command was entered or since the security appliance came online. The number of seconds is the duration the security appliance has been online since the last reboot, unless the **clear traffic** command was entered since the last reboot. If this is the case, then the number of seconds is the duration since that command was entered.

Examples

The following example shows output from the **show traffic** command:

```
hostname# show traffic
outside:
        received (in 102.080 secs):
                2048 packets 204295 bytes
                20 pkts/sec 2001 bytes/sec
        transmitted (in 102.080 secs):
                2048 packets 204056 bytes
                20 pkts/sec 1998 bytes/sec

Ethernet0:
        received (in 102.080 secs):
                2049 packets 233027 bytes
                20 pkts/sec 2282 bytes/sec
        transmitted (in 102.080 secs):
                2048 packets 232750 bytes
                20 pkts/sec 2280 bytes/sec
```

Related Commands

Command	Description
clear traffic	Resets the counters for transmit and receive activity.

show uauth

To display one or all currently authenticated users, the host IP to which they are bound, and any cached IP and port authorization information, use the **show uauth** command in privileged EXEC mode.

show uauth [*username*]

Syntax Description

username	(Optional) Specifies, by username, the user authentication and authorization information to display.

Defaults

Omitting username displays the authorization information for all users.

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.

Usage Guidelines

The **show uauth** command displays the AAA authorization and authentication caches for one user or for all users.

This command is used with the **timeout** command.

Each user host IP address has an authorization cache attached to it. The cache allows up to 16 address and service pairs for each user host. If the user attempts to access a service that has been cached from the correct host, the security appliance considers it preauthorized and immediately proxies the connection. Once you are authorized to access a website, for example, the authorization server is not contacted for each image as it is loaded (assuming the images come from the same IP address). This process significantly increases performance and reduces the load on the authorization server.

The output from the **show uauth** command displays the username that is provided to the authorization server for authentication and authorization purposes, the IP address to which the username is bound, and whether the user is authenticated only or has cached services.

Note When you enable Xauth, an entry is added to the uauth table (as shown by the **show uauth** command) for the IP address that is assigned to the client. However, when using Xauth with the Easy VPN Remote feature in Network Extension Mode, the IPSec tunnel is created from network to network, so that the users behind the firewall cannot be associated with a single IP address. For this reason, a uauth entry

cannot be created upon completion of Xauth. If AAA authorization or accounting services are required, you can enable the AAA authentication proxy to authenticate users behind the firewall. For more information on AAA authentication proxies, see to the **aaa** commands.

Use the **timeout uauth** command to specify how long the cache should be kept after the user connections become idle. Use the **clear uauth** command to delete all the authorization caches for all the users, which will cause them to have to reauthenticate the next time that they create a connection.

Examples

This example shows sample output from the **show uauth** command when no users are authenticated and one user authentication is in progress:

```
hostname(config)# show uauth
                        Current    Most Seen
Authenticated Users       0          0
Authen In Progress        0          1
```

This example shows sample output from the **show uauth** command when three users are authenticated and authorized to use services through the security appliance:

```
hostname(config)# show uauth
user 'pat' from 209.165.201.2 authenticated
user 'robin' from 209.165.201.4 authorized to:
   port 192.168.67.34/telnet    192.168.67.11/http     192.168.67.33/tcp/8001
        192.168.67.56/tcp/25    192.168.67.42/ftp
user 'terry' from 209.165.201.7 authorized to:
   port 192.168.1.50/http     209.165.201.8/http
```

Related Commands

Command	Description
clear uauth	Remove current user authentication and authorization information.
timeout	Set the maximum idle time duration.

show url-block

To display the number of packets held in the url-block buffer and the number (if any) dropped due to exceeding the buffer limit or retransmission, use the **show url-block** command in privileged EXEC mode.

show url-block [**block statistics**]

Syntax Description

block statistics	(Optional) Displays block buffer usage statistics.

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.

Usage Guidelines

The **show url-block block statistics** command displays the number of packets held in the url block buffer and the number (if any) dropped due to exceeding the buffer limit or retransmission.

Examples

The following is sample output from the **show url-block** command:

```
hostname# show url-block
|url-block url-mempool 128|url-block url-size 4|url-block block 128
```

This shows the configuration of the URL block buffer.

The following is sample output from the **show url-block block statistics** command:

```
hostname# show url-block block statistics

URL Pending Packet Buffer Stats with max block  128|
Cumulative number of packets held:|896
Maximum number of packets held (per URL):|3
Current number of packets held (global):|38
Packets dropped due to
|exceeding url-block buffer limit:|7546
|HTTP server retransmission:|10
Number of packets released back to client:|0
```

Related Commands

Commands	Description
clear url-block block statistics	Clears the block buffer usage counters.
filter url	Directs traffic to a URL filtering server.
url-block	Manage the URL buffers used for web server responses.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

show url-cache statistics

To display information about the url-cache, which is used for URL responses received from an N2H2 or Websense filtering server, use the **show url-cache statistics** command in privileged EXEC mode.

show url-cache 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.

Usage Guidelines

The **show url-cache statistics** command displays the following entries:

- Size—The size of the cache in kilobytes, set with the **url-cache** *size* option.
- Entries—The maximum number of cache entries based on the cache size.
- In Use—The current number of entries in the cache.
- Lookups—The number of times the security appliance has looked for a cache entry.
- Hits—The number of times the security appliance has found an entry in the cache.

You can view additional information about N2H2 Sentian or Websense filtering activity with the **show perfmon** command.

Examples

The following is sample output from the **show url-cache statistics** command:

```
hostname# show url-cache statistics

URL Filter Cache Stats
----------------------
 Size :     1KB
 Entries :      36
  In Use :      30
 Lookups :      300
 Hits :      290
```

Related Commands

Commands	Description
clear url-cache statistics	Removes **url-cache** command statements from the configuration.
filter url	Directs traffic to a URL filtering server.
url-block	Manage the URL buffers used for web server responses.
url-cache	Enables URL caching for responses received from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

show url-server

To display information about the URL filtering server, use the **show url-server** command in privileged EXEC mode.

show url-server 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.

Usage Guidelines

The **show url-server statistics** command displays the URL server vendor; number of URLs total, allowed, and denied; number of HTTPS connections total, allowed, and denied; number of TCP connections total, allowed, and denied; and the URL server status.

The **show url-server** command displays the following information:

- For N2H2, **url-server** (*if_name*) **vendor n2h2 host** *local_ip* **port** *number* **timeout** *seconds* **protocol [{TCP | UDP}{version 1 | 4}]**
- For Websense, **url-server** (*if_name*) **vendor websense host** *local_ip* **timeout** *seconds* **protocol [{TCP | UDP}]**

Examples

The following is sample output from the **show url-server statistics** command:

```
hostname## show url-server statistics

URL Server Statistics: |
Vendor websense
HTTPs total/allowed/denied 0/0/0
HTTPSs total/allowed/denied 0/0/0
FTPs total/allowed/denied 0/0/0 |
URL Server Status: |
172.23.58.103 UP |
URL Packets Send and Receive Stats: |
Message Send Receive
```

```
STATUS_REQUEST 200 200
LOOKUP_REQUEST 10 10
LOG_REQUEST 20 NA
```

Related Commands

Commands	Description
clear url-server	Clears the URL filtering server statistics.
filter url	Directs traffic to a URL filtering server.
url-block	Manage the URL buffers used for web server responses.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

show version

To display the software version, hardware configuration, license key, and related uptime data, use the **show version** command in user EXEC mode.

show version

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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show version** command allows you to display the software version, operating time since the last reboot, processor type, Flash partition type, interface boards, serial number (BIOS ID), activation key value, license type (R or UR), and time stamp for when the configuration was last modified.

The serial number listed with the **show version** command is for the Flash partition BIOS. This number is different from the serial number on the chassis. When you get a software upgrade, you will need the serial number that appears in the **show version** command, not the chassis number.

Note The uptime value indicates how long a failover set has been running. If one unit stops running, the uptime value will continue to increase as long as the other unit continues to operate.

Examples

The following example shows how to display the software version, hardware configuration, license key, and related uptime information:

```
hostname# show version

Cisco PIX Security Appliance Software Version 7.0(4)
Device Manager Version 5.0(4)

Compiled on Tue 27-Sep-05 10:41 by root
System image file is "flash:/cdisk.bin"
```

```
Config file at boot was "startup-config"

pix2 up 7 days 7 hours

Hardware:   PIX-515E, 128 MB RAM, CPU Pentium II 433 MHz
Flash E28F128J3 @ 0xfff00000, 16MB
BIOS Flash AM29F400B @ 0xfffd8000, 32KB

 0: Ext: Ethernet0           : address is 0011.2094.1d2b, irq 10
 1: Ext: Ethernet1           : address is 0011.2094.1d2c, irq 11

Licensed features for this platform:
Maximum Physical Interfaces : 6
Maximum VLANs               : 25
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Enabled
Cut-through Proxy           : Enabled
Guards                      : Enabled
URL Filtering               : Enabled
Security Contexts           : 5
GTP/GPRS                    : Enabled
VPN Peers                   : Unlimited

This platform has an Unrestricted (UR) license.

Serial Number: 808184143
Running Activation Key: 0xcf22f25d 0xec1c3174 0x8cb138a0 0xaad8b878 0x4f32fd90
Configuration last modified by enable_15 at 14:18:26.103 UTC Thu Oct 6 2005
hostname#
```

Related Commands

Command	Description
show hardware	Displays detail hardware information.
show serial	Displays the hardware serial information.
show uptime	Displays how long the security appliance has been up.

show vpn load-balancing

To display the runtime statistics for the VPN load-balancing virtual cluster configuration, use the **show vpn-load-balancing** command in global configuration, privileged EXEC, or VPN load-balancing mode.

show vpn load-balancing

Syntax Description

This command has no variables or arguments.

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	•	—	•	—	—
Privileged EXEC	•	—	•	—	—
vpn load-balancing	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **show vpn load-balancing** command displays statistical information for the virtual VPN load-balancing cluster. If the local device is not participating in the VPN load-balancing cluster, this command indicates that VPN load balancing has not been configured for this device.

Examples

This example displays **show vpn load-balancing** command and its output for a situation in which the local device is participating in the VPN load-balancing cluster:

```
hostname(config-load-balancing)# show vpn load-balancing

Status: enabled
Role: Master
Failover: n/a
Encryption: enabled
Cluster IP: 192.168.1.100
Peers: 1
Public IP Role Pri Model Load (%) Sessions
-------------------------------------------------------------
* 192.168.1.40 Master 10 PIX-515 0 0
192.168.1.110 Backup 5 PIX-515 0 0
hostname(config-load-balancing)#
```

If the local device is not participating in the VPN load-balancing cluster, the **show vpn load-balancing** command shows a different result:

```
hostname(config)# show vpn load-balancing
VPN Load Balancing has not been configured.
```

Related Commands

Command	Description
clear configure vpn load-balancing	Removes **vpn load-balancing** command statements from the configuration.
show running-config vpn load-balancing	Displays the the current VPN load-balancing virtual cluster configuration.
vpn load-balancing	Enters vpn load-balancing mode.

show vpn-sessiondb

To display information about VPN sessions, use the show **vpn-sessiondb** command in privileged EXEC mode. The command includes options for displaying information in full or in detail, lets you specify type of sessions to display, and provides options to filter and sort the information. The syntax table and usage notes organize the choices accordingly.

show vpn-sessiondb [detail] [full] {remote | l2l | index *indexnumber* **| webvpn | svc | email-proxy}**
[filter {name *username* **| ipaddress** *IPaddr* **| a-ipaddress** *IPaddr* **| p-ipaddress** *IPaddr* **|**
tunnel-group *groupname* **| protocol** *protocol-name* **| encryption** *encryption-algo***}]**
[sort {name | ipaddress | a-ipaddress | p-ip address | tunnel-group | protocol | encryption}]

Syntax Descriptions

Granularity of Display	
detail	Displays extended details about a session. For example, using the **detail** option for an IPSec session displays additional details such as the IKE hashing algorithm, authentication mode, and rekey interval. If you choose **detail**, and the **full** option, the security appliance displays the detailed output in a machine-readable format.
filter	Filters the output to display only the information you specify by using one or more of the filter options. For more information, see usage notes.
full	Displays streamed, untruncated output. Output is delineated by | characters and a || string between records.
sort	Sorts the output according to the sort option you specify. For more information, see usage notes.
Session Type to Display	
email-proxy	Displays email-proxy sessions. You can display this information for e-mail proxy sessions, or you can filter it by using the following filter and sort options: **name** (connection name), **ipaddress** (client), **encryption**.
index *indexnumber*	Displays a single session by index number. Specify the index number for the session, 1 - 750. Filter and sort options do not apply.
l2l	Displays VPN LAN-to-LAN session information. You can display this information for all groups or you can filter it by using the following filter and sort options: **name**, **ipaddress**, **protocol, encryption**.
remote	Displays remote-access sessions. You can display this information for all groups or you can filter it by using the following filter options: **name**, **a-ipaddress**, **p-ipaddress, tunnel-group**, **protocol**, **encryption**.
svc	Displays SVC sessions. You can display this information for all groups or you can filter it by using the following filter options: **a-ipaddress**, **encryption**, **name**, **p-ipaddress**.
vpn-lb	Displays VPN Load Balancing Management sessions. You can display this information for all groups or you can filter it by using the following filter options: **encryption**, **ipaddress**, **name**, **protocol**.
webvpn	Displays information about WebVPN sessions. You can display this information for all groups or you can filter it by using the following filter and sort options: **name**, **ipaddress**, **encryption**.

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	This command was introduced.

Usage Guidelines You can use the following options to filter and to sort the session display:

Filter/Sort Option	Meaning
filter a-ipaddress *IPaddr*	Filters the output to display information for the specified assigned IP address or addresses only.
sort a-ipaddress	Sorts the display by assigned IP addresses.
filter encryption *encryption-algo*	Filters the output to display information for sessions using the specified encryption algorithm(s) only.
sort encryption	Sorts the display by encryption algorithm. Encryption algorithms include: aes128 des aes192 3des aes256 rc4
filter ipadddress *IPaddr*	Filters the output to display information for the specified inside IP address or addresses only.
sort ipaddress	Sorts the display by inside IP addresses.
filter name *username*	Filters the output to display sessions for the specified username(s).
sort name	Sorts the display by usernames in alphabetical order.
filter p-address *IPaddr*	Filters the output to display information for the specified outside IP address only.
sort p-address	Sorts the display by the specified outside IP address or addresses.
filter protocol *protocol-name*	Filters the output to display information for sessions using the specified protocol(s) only.
sort protocol	Sorts the display by protocol. Protocols include:

Filter/Sort Option	Meaning	
	IKE	IPSecoverTCP
	IMAP4S	IPSecOverUDP
	IPSec	SMTPS
	IPSecLAN2LAN	userHTTPS
	IPSecLAN2LANOverNatT	vcaLAN2LAN
	IPSecOverNatT	
filter tunnel-group *groupname*	Filters the output to display information for the specified tunnel group(s) only.	
sort tunnel-group	Sorts the display by tunnel group.	
| character	Modifies the output, using the following arguments: {begin | include | exclude | grep | [-v]} {reg_exp}	
<cr>	Sends the output to the console.	

The following example, entered in privileged EXEC mode, shows detailed information about LAN-to-LAN sessions:

```
hostname# show vpn-sessiondb detail l2l
Session Type: LAN-to-LAN Detailed
Connection   : 172.16.0.1
Index        : 1                    IP Addr      : 172.16.0.1
Protocol     : IPSecLAN2LAN         Encryption   : AES256
Bytes Tx     : 48484156             Bytes Rx     : 875049248
Login Time   : 09:32:03 est Mon Aug 2 2004
Duration     : 6:16:26
Filter Name  :

IKE Sessions: 1 IPSec Sessions: 2

IKE:
  Session ID   : 1
  UDP Src Port : 500                  UDP Dst Port : 500
  IKE Neg Mode : Main                 Auth Mode    : preSharedKeys
  Encryption   : AES256               Hashing      : SHA1
  Rekey Int (T): 86400 Seconds        Rekey Left(T): 63814 Seconds
  D/H Group    : 5

IPSec:
  Session ID   : 2
  Local Addr   : 10.0.0.0/255.255.255.0
  Remote Addr  : 209.165.201.30/255.255.255.0
  Encryption   : AES256               Hashing      : SHA1
  Encapsulation: Tunnel               PFS Group    : 5
  Rekey Int (T): 28800 Seconds        Rekey Left(T): 10903 Seconds
  Bytes Tx     : 46865224             Bytes Rx     : 2639672
  Pkts Tx      : 1635314              Pkts Rx      : 37526


IPSec:
  Session ID   : 3
  Local Addr   : 10.0.0.1/255.255.255.0
  Remote Addr  : 209.165.201.30/255.255.255.0
  Encryption   : AES256               Hashing      : SHA1
  Encapsulation: Tunnel               PFS Group    : 5
  Rekey Int (T): 28800 Seconds        Rekey Left(T): 6282 Seconds
```

```
  Bytes Tx     : 1619268                Bytes Rx     : 872409912
  Pkts Tx      : 19277                  Pkts Rx      : 1596809

hostname#
```

Related Commands

Command	Description
show running-configuration vpn-sessiondb	Displays the VPN session database running configuration.
show vpn-sessiondb ratio	Displays VPN session encryption or protocol ratios.
show vpn-sessiondb summary	Displays a summary of all VPN sessions.

show vpn-sessiondb ratio

To display the ratio of current sessions as a percentage by protocol or encryption algorithm, use the **show vpn-sessiondb ratio** command in privileged EXEC mode.

show vpn-sessiondb ratio {protocol | encryption} [filter *groupname***]**

Syntax Description

encryption	Identifies the encryption protocols you want to display. Refers to phase 2 encryption. Encryption algorithms include:	
	aes128	des
	aes192	3des
	aes256	rc4
filter *groupname*	Filters the output to include session ratios only for the tunnel group you specify.	
protocol	Identifies the protocols you want to display. Protocols include:	
	IKE	SMTPS
	IMAP4S	userHTTPS
	IPSec	vcaLAN2LAN
	IPSecLAN2LAN	
	IPSecLAN2LANOverNatT	
	IPSecOverNatT	
	IPSecoverTCP	
	IPSecOverUDP	

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	This command was introduced.

Examples

The following is sample output for the **show vpn-sessiondb ratio** command, with **encryption** as the argument:

```
hostname# show vpn-sessiondb ratio enc
Filter Group         : All
Total Active Sessions: 5
Cumulative Sessions  : 9

Encryption               Sessions       Percent
none                     0               0%
DES                      1              20%
3DES                     0               0%
AES128                   4        80%
AES192                   0               0%
AES256                   0               0%
```

The following is sample output for the **show vpn-sessiondb ratio** command with **protocol** as the argument:

```
hostname# show vpn-sessiondb ratio protocol
Filter Group         : All
Total Active Sessions: 6
Cumulative Sessions  : 10

Protocol                 Sessions       Percent
IKE                      0               0%
IPSec                    1              20%
IPSecLAN2LAN             0               0%
IPSecLAN2LANOverNatT     0               0%
IPSecOverNatT            0               0%
IPSecOverTCP             1 20%
IPSecOverUDP             0               0%
vpnLoadBalanceMgmt       0               0%
userHTTPS                0               0%
IMAP4S                   3 30%
POP3S                    0               0%
SMTPS                    3 30%
```

Related Commandss

Command	Description
show vpn-sessiondb	Displays sessions with or without extended details, optionally filtered and sorted by criteria you specify.
show vpn-sessiondb summary	Displays a session summary, including total current session, current sessions of each type, peak and total cumulative, maximum concurrent sessions

show vpn-sessiondb summary

To display the a summary of current VPN sessions, use the **show vpn-sessiondb summary** command in privileged EXEC mode. The session summary includes total current sessions, current sessions of each type, peak and total cumulative sessions, and maximum concurrent sessions.

show vpn-sessiondb summary

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	This command was introduced.

Examples

The following is sample output for the **show vpn-sessiondb summary** command:

```
hostname# show vpn-sessiondb summary

Active Sessions:              Session Information:
  LAN-to-LAN : 2                 Peak Concurrent : 7
  Remote Access : 5              Concurrent Limit: 2000
  WebVPN : 0                     Cumulative Sessions: 12
  Email Proxy : 0
```

Related Commands

Command	Description
show vpn-sessiondb	Displays sessions with or without extended details, optionally filtered and sorted by criteria you specify.
show vpn-sessiondb ratio	Displays VPN session encryption or protocol ratios.

show xlate

To display information about the translation slots, use the **show xlate** command in privileged EXEC mode.

show xlate [**global** *ip1*[**-***ip2*] [**netmask** *mask*]] [**local** *ip1*[**-***ip2*] [**netmask** *mask*]] [**gport** *port1*[**-***port2*]] [**lport** *port1*[**-***port2*]] [**interface** *if_name*] [**state** *state*] [**debug**] [**detail**]

show xlate count

Syntax Description

count	Displays the translation count.
debug	(Optional) Displays xlate debug information.
detail	(Optional) Displays detail xlate information.
global *ip1*[**-***ip2*]	(Optional) Displays the active translations by global IP address or range of addresses.
gport *port1*[*-port2*]	Displays the active translations by the global port or range of ports.
interface *if_name*	(Optional) Displays the active translations by interface.
local *ip1*[**-***ip2*]	(Optional) Displays the active translations by local IP address or range of addresses.
lport *port1*[*-port2*]	Displays the active translations by local port or range of ports.
netmask *mask*	(Optional) Specifies the network mask to qualify the global or local IP addresses.
state *state*	(Optional) Displays the active translations by state. You can enter one or more of the following states: • **static**—specifies **static** translations. • **portmap**—specifies PAT global translations. • **norandomseq**—specifies a **nat** or **static** translation with the **norondomseq** setting. • **identity**—specifies **nat 0** identity address translations. When specifying more than one state, separate the states with a space.

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.

Usage Guidelines

The **show xlate** command displays the contents of the translation slots. The **show xlate detail** command displays the following information:

- {**ICMP**|**TCP**|**UDP**} **PAT from** *interface*:*real-address*/*real-port* **to** *interface*:*mapped-address*/*mapped-port* **flags** *translation-flags*
- **NAT from** *interface*:*real-address*/*real-port to interface*:*mapped-address*/*mapped-port* **flags** *translation-flags*

The translation flags are defined in Table 7-31.

Table 7-34 Translation Flags

Flag	Description
s	Static translation slot
d	Dump translation slot on next cleaning cycle
r	Port map translation (Port Address Translation)
n	No randomization of TCP sequence number
i	Inside address translation
D	DNS A RR rewrite
I	Identity translation from **nat 0**

Note When the **vpnclient** configuration is enabled and the inside host is sending out DNS requests, the **show xlate** command may list multiple xlates for a static translation.

Examples

The following is sample output from the **show xlate** command. It shows how translation slot information with three active PATs.

```
hostname# show xlate

3 in use, 3 most used
PAT Global 192.150.49.1(0) Local 10.1.1.15 ICMP id 340
PAT Global 192.150.49.1(1024) Local 10.1.1.15(1028)
PAT Global 192.150.49.1(1024) Local 10.1.1.15(516)
```

The following is sample output from the **show xlate detail** command.It shows the translation type and interface information with three active PATs.

The first entry is a TCP PAT for host port (10.1.1.15, 1025) on the inside network to host-port (192.150.49.1, 1024) on the outside network. The r flag indicates that the translation is a PAT. The i flag indicates that the translation applies to the inside address port.

The second entry is a UDP PAT for host port (10.1.1.15, 1028) on the inside network to host port (192.150.49.1, 1024) on the outside network. The r flag indicates that the translation is a PAT. The i flag indicates that the translation applies to the inside address port.

The third entry is an ICMP PAT for host-ICMP-id (10.1.1.15, 21505) on the inside network to host-ICMP-id (192.150.49.1, 0) on the outside network. The r flag indicates that the translation is a PAT. The i flag indicates that the translation applies to the inside address ICMP ID.

The inside address fields appear as source addresses on packets traversing from the more secure interface to the less secure interface. They appear as destination addresses on packets traversing from the less secure interface to the more secure interface.

```
hostname# show xlate detail

3 in use, 3 most used
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
       r - portmap, s - static
TCP PAT from inside:10.1.1.15/1026 to outside:192.150.49.1/1024 flags ri
UDP PAT from inside:10.1.1.15/1028 to outside:192.150.49.1/1024 flags ri
ICMP PAT from inside:10.1.1.15/21505 to outside:192.150.49.1/0 flags ri
```

The following is sample output from the **show xlate** command. It shows two static translations. The first translation has one associated connection (called “nconns”), and the second translation has four associated connections.

```
hostname# show xlate
Global 209.165.201.10 Local 209.165.201.10 static nconns 1 econns 0
Global 209.165.201.30 Local 209.165.201.30 static nconns 4 econns 0
```

Related Commands

Command	Description
clear xlate	Clears current translation and connection information.
show conn	Displays all active connections.
show local-host	Displays the local host network information.
show uauth	Displays the currently authenticated users.

shun

To block connections from an attacking host, use the **shun** command in privileged EXEC mode. To disable a shun, use the **no** form of this command.

shun *source_ip* [*dest_ip source_port dest_port* [*protocol*]] [**vlan** *vlan_id*]

no shun *source_ip* [**vlan** *vlan_id*]

Syntax Description

dest_port	(Optional) Specifies the destination port of a current connection that you want to drop when you place the shun on the source IP address.
dest_ip	(Optional) Specifies the destination address of a current connection that you want to drop when you place the shun on the source IP address.
protocol	(Optional) Specifies the IP protocol of a current connection that you want to drop when you place the shun on the source IP address, such as UDP or TCP. By default, the protocol is 0 (any protocol).
source_ip	Specifies the address of the attacking host. If you only specify the source IP address, all future connections from this address are dropped; current connections remain in place. To drop a current connection and also place the shun, specify the additional parameters of the connection. Note that the shun remains in place for all future connections from the source IP address, regardless of destination parameters.
source_port	(Optional) Specifies the source port of a current connection that you want to drop when you place the shun on the source IP address.
vlan_id	(Optional) Specifies the VLAN ID where the source host resides.

Defaults

The default protocol is 0 (any protocol).

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.

Usage Guidelines

The **shun** command lets you block connections from an attacking host. All future connections from the source IP address are dropped and logged until the blocking function is removed manually or by the Cisco IPS sensor. The blocking function of the **shun** command is applied whether or not a connection with the specified host address is currently active.

If you specify the destination address, source and destination ports, and the protocol, then you drop the matching connection as well as placing a shun on all future connections from the source IP address; all future connections are shunned, not just those that match these specific connection parameters.

You can only have one **shun** command per source IP address.

Because the **shun** command is used to block attacks dynamically, it is not displayed in the security appliance configuration.

Whenever an interface configuration is removed, all shuns that are attached to that interface are also removed. If you add a new interface or replace the same interface (using the same name), then you must add that interface to the IPS sensor if you want the IPS sensor to monitor that interface.

Examples

The following example shows that the offending host (10.1.1.27) makes a connection with the victim (10.2.2.89) with TCP. The connection in the security appliance connection table reads as follows:

```
10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP
```

Apply the **shun** command using the following options:

```
hostname# shun 10.1.1.27 10.2.2.89 555 666 tcp
```

The command deletes the specific current connection from the security appliance connection table and also prevents all future packets from 10.1.1.27 from going through the security appliance.

Related Commands

Command	Description
clear shun	Disables all the shuns that are currently enabled and clears the shun statistics.
show conn	Shows all active connections.
show shun	Displays the shun information.

shutdown

To disable an interface, use the **shutdown** command in interface configuration mode. To enable an interface, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

All physical interfaces are shut down by default. Allocated interfaces in security contexts are not shut down in the configuration.

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	This command was moved from a keyword of the **interface** command to an interface configuration mode command.

Usage Guidelines

By default, all physical interfaces are shut down. You must enable the physical interface before any traffic can pass through an enabled subinterface. For multiple context mode, if you allocate a physical interface or subinterface to a context, the interfaces are enabled by default in the context. However, before traffic can pass through the context interface, you must also enable the interface in the system configuration. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.

Note This command only disables the software interface. The physical link remains up, and the directly connected device is still recognized as being up even when the corresponding interface is configured with the **shutdown** command.

Examples\

The following example enables a main interface:

```
hostname(config)# interface gigabitethernet0/2
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
```

```
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
```

The following example enables a subinterface:

```
hostname(config)# interface gigabitethernet0/2.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

The following example shuts down the subinterface:

```
hostname(config)# interface gigabitethernet0/2.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# shutdown
```

Related Commands

Command	Description
clear xlate	Resets all translations for existing connections, causing the connections to be reset.
interface	Configures an interface and enters interface configuration mode.

smtps

To enter SMTPS configuration mode, use the **smtps** command in global configuration mode. To remove any commands entered in SMTPS command mode, use the **no** version of this command. SMTPS is a TCP/IP protocol that lets you to send e-mail over an SSL connection.

smtps

no smtps

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to enter SMTPS configuration mode:

```
hostname(config)# smtps
hostname(config-smtps)#
```

Related Commands

Command	Description
clear configure smtps	Removes the SMTPS configuration.
show running-config smtps	Displays the running configuration for SMTPS.

smtp-server

To configure an SMTP server, use the **smtp-server** command in global configuration mode. To remove the attribute from the configuration, use the **no** version of this command.

The security appliance includes an internal SMTP client that the Events system can use to notify external entities that a certain event has occurred. You can configure SMTP servers to receive these event notices, and then forward them to specified e-mail addresses. The SMTP facility is active only when you enable E-mail events an the security appliance.

smtp-server {*primary_server*} [*backup_server*]

no smtp-server

Syntax Description

primary_server	Identifies the primary SMTP server. Use either an IP address or DNS name
backup_server	Identifies a backup SMTP server to relay event messages in the event the primary SMTP server is unavailable. Use either an IP address or DNS name.

Defaults

No SMTP server is configured 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	This command was introduced.

Usage Guidelines

Examples

The following example shows how to set an SMTP server with an IP address of 10.1.1.24, and a backup SMTP server with an IP address of 10.1.1.34:

```
hostname(config)# smtp-server 10.1.1.24 10.1.1.34
```

Related Commands

Command	Description

snmp-server

To provide the security appliance event information through SNMP, use the **snmp-server** command in privileged EXEC mode. To disable the SNMP commands, use the **no** form of this command.

snmp-server {community | contact | location} *text*}

no snmp-server {community | contact | location} *text*}

snmp-server host *interface_name ip_addr* **[community** *commstr*] [**trap | poll**] [**version** *vers*] [**udp-port** *udp_port*]

no snmp-server host *interface_name ip_addr* **[community** *commstr*] [**trap | poll**] [**version** *vers*] [**udp-port** *udp_port*]

snmp-server enable [traps [**all** | *feature* [*trap1* ... [*trapn*]]]

no snmp-server enable [traps [**all** | *feature* [*trap1* ... [*trapn*]]]

snmp-server listen-port *lport*

no snmp-server listen-port *lport*

Syntax Description

community *text*	Specifies the security appliance community string to the SNMP management station.
contact *text*	Specifies the name of the contact person or the PIX system administrator.
location *text*	Specifies the security appliance location.
host	Specifies an IP address of the SNMP management station to which traps should be sent and/or from which the SNMP requests come.
interface_name	Interface name where the SNMP management station resides.
ip_addr	IP address of a host to which SNMP traps should be sent and/or from which the SNMP requests come.
trap	(Optional) Specifies that only traps are sent and that this host is not allowed to poll.
poll	(Optional) Specifies that this host is allowed to poll.
enable	Enable specific SNMP trap notifications.
enable traps	Enables sending log messages as SNMP trap notifications.
all	Enable or disable traps for all features.
community	Specifies the community string of the security appliance.
commstr	The community string for a specific host.
feature	The feature for which traps are enabled.
trapn	A specific trap to enable.
listen-port	Override the default port (161) for incoming SNMP requests.[1]
lport	The port on which incoming requests will be accepted.
udp-port *udp_port*	Configure port to which notifications will be sent

1. The **listen-port** keyword is only available in admin context because the **snmp-server** command is not available in the system context.

Defaults

By default, both traps and polls are acted upon.

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.

Usage Guidelines

The **snmp-server** command allows you to identify the site, management station, community string, and user information.

Enter the password key in use at the SNMP management station. The SNMP community string is a shared secret among the SNMP management station and the network nodes being managed. The security appliance uses the key to determine if the incoming SNMP request is valid. For example, you could designate a site with a community string and then configure the routers, security appliance, and the management station with this same string. The security appliance uses this string and does not respond to requests with an invalid community string.

The **contact** *text* is case sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.

The **location** *text* is case sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.

You can specify up to 32 SNMP management stations.

When configuring a host using the **snmp-server host** command, specifying the **trap** option will cause the device to reject incoming requests from the host.

The **clear configure snmp-server** and **no snmp-server** commands disable the SNMP commands in the configuration as follows:

```
hostname(config)# no snmp-server location
hostname(config)# no snmp-server contact
hostname(config)# snmp-server community public
hostname(config)# no snmp-server enable traps
```

Examples

This example shows the commands that you would enter to start receiving SNMP requests from a management station:

```
hostname(config)# snmp-server community wallawallabingbang
hostname(config)# snmp-server location Building 42, Sector 54
hostname(config)# snmp-server contact Sherlock Holmes
hostname(config)# snmp-server host perimeter 10.1.2.42
```

Related Commands

Command	Description
clear configure snmp-server	Disables the Simple Network Management Protocol (SNMP) server.
show snmp-server statistics	Displays information about the SNMP server.
show running-config snmp-server	Displays the SNMP server configuration.

snmp-map

To identify a specific map for defining the parameters for SNMP inspection, use the **snmp-map** command in global configuration mode. To remove the map, use the **no** form of this command.

snmp-map *map_name*

no snmp-map *map_name*

Syntax Description

map_name	The name of the SNMP map.

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	This command was introduced.

Usage Guidelines

Use the **snmp-map** command to identify a specific map to use for defining the parameters for SNMP inspection. When you enter this command, the system enters the SNMP map configuration mode, which lets you enter the different commands used for defining the specific map. After defining the SNMP map, you use the **inspect snmp** command to enable the map. Then you use the **class-map**, **policy-map**, and **service-policy** commands to define a class of traffic, to apply the **inspect** command to the class, and to apply the policy to one or more interfaces.

Examples

The following example shows how to identify SNMP traffic, define a SNMP map, define a policy, and apply the policy to the outside interface.

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
hostname(config-pmap-c)# inspect snmp inbound_snmp
```

```
hostname(config-pmap-c)# exit
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
deny version	Disallows traffic using a specific version of SNMP.
inspect snmp	Enable SNMP application inspection.
policy-map	Associates a class map with specific security actions.

snmp-server enable trap remote-access

To enable threshold trapping, use the **snmp-server enable trap remote-access** command in global configuration mode. To disable threshold trapping, use the **no** version of this command. This command lets the security appliance send traps when remote access sessions reach the number set with the **remote-access threshold session-threshold-exceeded** command**.**

snmp-server enable trap remote-access session-threshold-exceeded

no **snmp-server enable trap remote-access**

Syntax Description

session-threshold-exceeded	Session threshold is exceeded.

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	This command was introduced.

Examples

The following example shows how to enable threshold trapping:

```
hostname# snmp-server enable trap remote-access session-threshold-exceeded
```

Related Commands

Command	Description
remote-access threshold session-threshold-exceeded	Specifies a number of active, concurrent, remote access sessions, at which point the security appliance sends traps.

speed

To set the speed of a copper (RJ-45) Ethernet interface, use the **speed** command in interface configuration mode. To restore the speed setting to the default, use the **no** form of this command.

speed {**auto** | **10** | **100** | **1000** | **nonegotiate**}

no speed [**auto** | **10** | **100** | **1000** | **nonegotiate**]

Syntax Description

10	Sets the speed to 10BASE-T.
100	Sets the speed to 100BASE-T.
1000	Sets the speed to 1000BASE-T. For copper Gigabit Ethernet only.
auto	Auto detects the speed.
nonegotiate	For fiber interfaces, sets the speed to 1000 Mbps and does not negotiate link parameters. This command and the **no** form of this command are the only settings available for fiber interfaces. When you set the value to **no speed nonegotiate** (the default), the interface enables link negotiation, which exchanges flow-control parameters and remote fault information.

Defaults

For copper interfaces, the default is **speed auto**.

For fiber interfaces, the default is **no speed nonegotiate**.

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	This command was moved from a keyword of the **interface** command to an interface configuration mode command.

Usage Guidelines

Set the speed on the physical interface only.

If your network does not support auto detection, set the speed to a specific value.

For RJ-45 interfaces on the ASA 5500 series adaptive security appliance, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled.

Examples

The following example sets the speed to 1000BASE-T:

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
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
```

Related Commands

Command	Description
clear configure interface	Clears all configuration for an interface.
duplex	Sets the duplex mode.
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.
show running-config interface	Shows the interface configuration.

split-dns

To enter a list of domains to be resolved through the split tunnel, use the **split-dns** command in group-policy configuration mode. To delete a list, use the **no** form of this command.

To delete all split tunneling domain lists, use the **no split-dns** command without arguments. This deletes all configured split tunneling domain lists, including a null list created by issuing the **split-dns none** command.

When there are no split tunneling domain lists, users inherit any that exist in the default group policy. To prevent users from inheriting such split tunneling domain lists, use the **split-dns none** command.

split-dns {**value** *domain-name1 domain-name2 domain-nameN* | **none**}

no split-dns [*domain-name domain-name2 domain-nameN*]

Syntax Description

value *domain-name*	Provides a domain name that the security appliance resolves through the split tunnel.
none	Indicates that there is no split DNS list. Sets a split DNS list with a null value, thereby disallowing a split DNS list. Prevents inheriting a split DNS list from a default or specified group policy.

Defaults

Split DNS is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use a single space to separate each entry in the list of domains. There is no limit on the number of entries, but the entire string can be no longer than 255 characters. You can use only alphanumeric characters, hyphens (-), and periods (.).

The **no split-dns** command, when used without arguments, deletes all current values, including a null value created by issuing the **split-dns none** command.

Note The AnyConnect VPN client and the SSL VPN Client do not support split DNS.

Examples

The following example shows how to configure the domains Domain1, Domain2, Domain3 and Domain4 to be resolved through split tunneling for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

Related Commands

Command	Description
default-domain	Specifies a default domain name that he IPSec client uses the for DNS queries that omit the domain field.
split-dns	Provides a list of domains to be resolved through the split tunnel.
split-tunnel-network-list	Identifies the access list the security appliance uses to distinguish networks that require tunneling and those that do not.
split-tunnel-policy	Lets an IPSec client conditionally direct packets over an IPSec tunnel in encrypted form, or to a network interface in cleartext form

split-tunnel-network-list

To create a network list for split tunneling, use the **split-tunnel-network-list** command in group-policy configuration mode. To delete a network list, use the **no** form of this command.

To delete all split tunneling network lists, use the **no split-tunnel-network-list** command without arguments. This deletes all configured network lists, including a null list created by issuing the **split-tunnel-network-list none** command.

When there are no split tunneling network lists, users inherit any network lists that exist in the default or specified group policy. To prevent users from inheriting such network lists, use the **split-tunnel-network-list none** command.

Split tunneling network lists distinguish networks that require traffic to travel across the tunnel from those that do not require tunneling.

split-tunnel-network-list {value *access-list name* **| none}**

no split-tunnel-network-list value [*access-list name*]

Syntax Description

value *access-list name*	Identifies an access list that enumerates the networks to tunnel or not tunnel.
none	Indicates that there is no network list for split tunneling; the security appliance tunnels all traffic. Sets a split tunneling network list with a null value, thereby disallowing split tunneling. Prevents inheriting a default split tunneling network list from a default or specified group policy.

Defaults

By default, there are no split tunneling network lists.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The security appliance makes split tunneling decisions on the basis of a network list, which is a standard ACL that consists of a list of addresses on the private network.

The **no split-tunnel-network-list** command, when used without arguments, deletes all current network lists, including a null value created by issuing the **split-tunnel-network-list none** command.

Examples

The following example shows how to set a network list called FirstList for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-network-list FirstList
```

Related Commands

Command	Description
access-list	Creates an access list, or uses a downloadable access list.
default-domain	Specifies a default domain name that he IPSec client uses the for DNS queries that omit the domain field.
split-dns	Provides a list of domains to be resolved through the split tunnel.
split-tunnel-policy	Lets an IPSec client conditionally direct packets over an IPSec tunnel in encrypted form, or to a network interface in cleartext form.

split-tunnel-policy

To set a split tunneling policy, use the **split-tunnel-policy** command in group-policy configuration mode. To remove the split-tunnel-policy attribute from the running configuration, use the **no** form of this command. This enables inheritance of a value for split tunneling from another group policy.

Split tunneling lets a remote-access IPSec client conditionally direct packets over an IPSec tunnel in encrypted form, or to a network interface in cleartext form. With split-tunneling enabled, packets not bound for destinations on the other side of the IPSec tunnel do not have to be encrypted, sent across the tunnel, decrypted, and then routed to a final destination.

This command applies this split tunneling policy to a specific network.

split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}

no split-tunnel-policy

Syntax Description

excludespecified	Defines a list of networks to which traffic goes in the clear. This feature is useful for remote users who want to access devices on their local network, such as printers, while they are connected to the corporate network through a tunnel. This option applies only to the Cisco VPN Client.
split-tunnel-policy	Indicates that you are setting rules for tunneling traffic.
tunnelall	Specifies that no traffic goes in the clear or to any other destination than the security appliance. Remote users reach internet networks through the corporate network and do not have access to local networks.
tunnelspecified	Tunnels all traffic from or to the specified networks. This option enables split tunneling. It lets you create a network list of addresses to tunnel. Data to all other addresses travels in the clear, and is routed by the remote user's internet service provider.

Defaults

Split tunneling is disabled by default, which is tunnelall.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Split tunneling is primarily a traffic management feature, not a security feature. In fact, for optimum security, we recommend that you not enable split tunneling.

Examples

The following example shows how to set a split tunneling policy of tunneling only specified networks for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-policy tunnelspecified
```

Related Commands

Command	Description
default-domain	Specifies a default domain name that he IPSec client uses the for DNS queries that omit the domain field.
split-dns	Provides a list of domains to be resolved through the split tunnel.
split-tunnel-network-list none	Indicates that no access list exists for split tunneling. All traffic travels across the tunnel.
split-tunnel-network-list value	Identifies the access list the security appliance uses to distinguish networks that require tunneling and those that do not.

ssh

To add SSH access to the security appliance, use the **ssh** command in global configuration mode. To disable SSH access to the security appliance, use the **no** form of this command. This command supports IPv4 and IPv6 addresses.

ssh {*ip_address mask* | *ipv6_address*/*prefix*} *interface*

no ssh {*ip_address mask* | *ipv6_address*/*prefix*} *interface*

Syntax Description

interface	The security appliance interface on which SSH is enabled. If not specified, SSH is enabled on all interfaces except the outside interface.
ip_address	IPv4 address of the host or network authorized to initiate an SSH connection to the security appliance. For hosts, you can also enter a host name.
ipv6_address/*prefix*	The IPv6 address and prefix of the host or network authorized to initiate an SSH connection to the security appliance.
mask	Network mask for *ip_address*.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **ssh** *ip_address* command specifies hosts or networks that are authorized to initiate an SSH connection to the security appliance. You can have multiple ssh commands in the configuration. The **no** form of the command removes a specific SSH command from the configuration. Use the **clear configure ssh** command to remove all SSH commands.

Before you can begin using SSH to the security appliance, you must generate a default RSA key using the **crypto key generate rsa** command.

The following security algorithms and ciphers are supported on the security appliance:

- 3DES and AES ciphers for data encryption
- HMAC-SHA and HMAC-MD5 algorithms for packet integrity

- RSA public key algorithm for host authentication
- Diffie-Hellman Group 1 algorithm for key exchange

The following SSH Version 2 features are not supported on the security appliance:

- X11 forwarding
- Port forwarding
- SFTP support
- Kerberos and AFS ticket passing
- Data compression

Examples

The following example shows how to configure the inside interface to accept SSH version 2 connections from a management console with the IP address 10.1.1.1. The idle session timeout is set to 60 minutes and SCP is enabled.

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
crypto key generate rsa	Generates RSA key pairs for identity certificates.
debug ssh	Displays debug information and error messages for SSH commands.
show running-config ssh	Displays the current SSH commands in the running configuration.
ssh scopy enable	Enables a secure copy server on the security appliance.
ssh version	Restricts the security appliance to using either SSH Version 1 or SSH Version 2.

ssh disconnect

To disconnect an active SSH session, use the **ssh disconnect** command in privileged EXEC mode.

ssh disconnect *session_id*

Syntax Description

session_id	Disconnects the SSH session specified by the ID number.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You must specify a session ID. Use the **show ssh sessions** command to obtain the ID of the SSH session you want to disconnect.

Examples

The following example shows an SSH session being disconnected:

```
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
hostname# ssh disconnect 2
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.29    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
```

Related Commands

Command	Description
show ssh sessions	Displays information about active SSH sessions to the security appliance.
ssh timeout	Sets the timeout value for idle SSH sessions.

ssh scopy enable

To enable Secure Copy (SCP) on the security appliance, use the **ssh scopy enable** command in global configuration mode. To disable SCP, use the **no** form of this command.

ssh scopy enable

no ssh scopy enable

Syntax Description

This command has no keywords or arguments.

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	This command was introduced.

Usage Guidelines

SCP is a server-only implementation; it will be able to accept and terminate connections for SCP but can not initiate them. The security appliance has the following restrictions:

- There is no directory support in this implementation of SCP, limiting remote client access to the security appliance internal files.
- There is no banner support when using SCP.
- SCP does not support wildcards.
- The security appliance license must have the VPN-3DES-AES feature to support SSH version 2 connections.

Examples

The following example shows how to configure the inside interface to accept SSH Version 2 connections from a management console with the IP address 10.1.1.1. The idle session timeout is set to 60 minutes and SCP is enabled.

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
debug ssh	Displays debug information and error messages for SSH commands.
show running-config ssh	Displays the current SSH commands in the running configuration.
ssh	Allows SSH connectivity to the security appliance from the specified client or network.
ssh version	Restricts the security appliance to using either SSH Version 1 or SSH Version 2.

ssh timeout

To change the default SSH session idle timeout value, use the **ssh timeout** command in global configuration mode. To restore the default timeout value, use the **no** form of this command.

ssh timeout *number*

no ssh timeout

Syntax Description

number	Specifies the duration in minutes that an SSH session can remain inactive before being disconnected. Valid values are from 1 to 60 minutes.

Defaults

The default session timeout value is 5 minutes.

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 **ssh timeout** command specifies the duration in minutes that a session can be idle before being disconnected. The default duration is 5 minutes.

Examples

The following example shows how to configure the inside interface to accept only SSH version 2 connections from a management console with the IP address 10.1.1.1. The idle session timeout is set to 60 minutes and SCP is enabled.

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
show running-config ssh	Displays the current SSH commands in the running configuration.

Command	Description
show ssh sessions	Displays information about active SSH sessions to the security appliance.
ssh disconnect	Disconnects an active SSH session.

ssh version

To restrict the version of SSH accepted by the security appliance, use the **ssh version** command in global configuration mode. To restore the default value, use the **no** form of this command. The default values permits SSH Version 1 and SSH Version 2 connections to the security appliance.

ssh version {**1** | **2**}

no ssh version [**1** | **2**]

Syntax Description

1	Specifies that only SSH Version 1 connections are supported.
2	Specifies that only SSH Version 2 connections are supported.

Defaults

By default, both SSH Version 1 and SSH Version 2 are supported.

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	This command was introduced.

Usage Guidelines

1 and 2 specify which version of SSH the security appliance is restricted to using. The **no** form of the command returns the security appliance to the default stance, which is compatible mode (both version can be used).

Examples

The following example shows how to configure the inside interface to accept SSH Version 2 connections from a management console with the IP address 10.1.1.1. The idle session timeout is set to 60 minutes and SCP is enabled.

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
debug ssh	Displays debug information and error messages for SSH commands.
show running-config ssh	Displays the current SSH commands in the running configuration.
ssh	Allows SSH connectivity to the security appliance from the specified client or network.

ssl client-version

To specify the SSL/TLS protocol version the security appliance uses when acting as a client, use the **ssl client-version** command in global configuration mode. To revert to the default, **any**, use the **no** version of this command. This command lets you restrict the versions of SSL/TLS that the security appliance sends.

ssl client-version [*any* | *sslv3-only* | *tlsv1-only*]

no ssl client-version

Syntax Description

any	The security appliance sends SSL version3 hellos, and negotiates either SSL version 3 or TLS version 1.
sslv3-only	The security appliance sends SSL version 3 hellos, and accepts only SSL version 3.
tlsv1-only	The security appliance sends TLSv1 client hellos, and accepts only TLS version 1.

Defaults

The default value is **any**.

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	This command was introduced.

Usage Guidelines

TCP Port Forwarding does not work when a WebVPN user connects with some SSL versions, as follows:

Negotiate SSLv3	Java downloads
Negotiate SSLv3/TLSv1	Java downloads
Negotiate TLSv1	Java does NOT download
TLSv1Only	Java does NOT download
SSLv3Only	Java does NOT download

The issue is that JAVA only negotiates SSLv3 in the client Hello packet when you launch the Port Forwarding application.

Examples

The following example shows how to configure the security appliance to communicate using only TLSv1 when acting as an SSL client:

```
hostname(config)# ssl client-version tlsv1-only
```

Related Commands

Command	Description
clear config ssl	Removes all SSL commands from the configuration, reverting to the default values.
ssl encryption	Specifies the encryption algorithms that the SSL/TLS protocol uses.
show running-config ssl	Displays the current set of configured SSL commands.
ssl server-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a server.
ssl trust-point	Specifies the certificate trust point that represents the SSL certificate for an interface.

ssl encryption

To specify the encryption algorithms that the SSL/TLS protocol uses, use the **ssl encryption** command in global configuration mode**.** Issuing the command again overwrites the previous setting. The ordering of the algorithms determines preference for their use. You can add or remove algorithms to meet the needs of your environment. To restore the default, which is the complete set of encryption algorithms, use the **no** version of the command.

ssl encryption [*3des-sha1*] [*des-sha1*] [*rc4-md5*] [*possibly others*]

no ssl encryption

Syntax Description

3des-sha1	Specifies triple DES encryption with Secure Hash Algorithm 1.
des-sha1	Specifies DES encryption with Secure Hash Algorithm 1.
rc4-md5	Specifies RC4 encryption with an MD5 hash function.
possibly others	Indicates that more encryption algorithms may be added in future releases.

Defaults

The default is to have all algorithms available in the following order:

[*3des-sha1***] [***des-sha1***] [***rc4-md5***] [***possibly others***]**

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	This command was introduced.

Examples

The following example shows how to configure the security appliance to use the 3des-sha1 and des-sha1 encryption algorithms:

```
hostname(config)# ssl encryption 3des-sha1 des-sha1
```

Related Commands

Command	Description
clear config ssl	Removes all SSL commands from the configuration, reverting to the default values.
show running-config ssl	Displays the current set of configured SSL commands.

Command	Description
ssl client-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a client.
ssl server-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a server.
ssl trust-point	Specifies the certificate trust point that represents the SSL certificate for an interface.

ssl server-version

To specify the SSL/TLS protocol version the security appliance uses when acting as a server, use the **ssl server-version** command in global configuration mode. To revert to the default, any, use the **no** version of this command. This command lets you restrict the versions of SSL/TSL that the security appliance accepts.

ssl server-version [*any* | *sslv3* | *tlsv1* | *sslv3-only* | *tlsv1-only*]

no ssl server-version

Syntax Description

any	The security appliance accepts SSL version 2 client hellos, and negotiates either SSL version 3 or TLS version 1.
sslv3	The security appliance accepts SSL version 2 client hellos, and negotiates to SSL version 3.
sslv3-only	The security appliance accepts only SSL version 3 client hellos, and uses only SSL version 3.
tlsv1	The security appliance accepts SSL version 2 client hellos, and negotiates to TLS version 1.
tlsv1-only	The security appliance accepts only TLSv1 client hellos, and uses only TLS version 1.

Defaults

The default value is **any**.

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	This command was introduced.

Usage Guidelines

TCP Port Forwarding does not work when a WebVPN user connects with some SSL versions, as follows:

Negotiate SSLv3	Java downloads
Negotiate SSLv3/TLSv1	Java downloads
Negotiate TLSv1	Java does NOT download
TLSv1Only	Java does NOT download
SSLv3Only	Java does NOT download

If you configure e-mail proxy, do not set thhe SSL version to TLSv1 Only. Outlook and Outlook Express do not support TLS.

Examples

The following example shows how to configure the security appliance to communicate using only TLSv1 when acting as an SSL server:

```
hostname(config)# ssl server-version tlsv1-only
```

Related Commands

Command	Description
clear config ssl	Removes all ssl commands from the configuration, reverting to the default values.
show running-config ssl	Displays the current set of configured ssl commands.
ssl client-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a client.
ssl encryption	Specifies the encryption algorithms that the SSL/TLS protocol uses.
ssl trust-point	Specifies the certificate trust point that represents the SSL certificate for an interface.

ssl trust-point

To specify the certificate trustpoint that represents the SSL certificate for an interface, use the **ssl trust-point** command with the *interface* argument in global configuration mode. If you do not specify an interface, this command creates the fallback trustpoint for all interfaces that do not have a trustpoint configured. To remove an SSL trustpoint from the configuration that does not specify an interface, use the **no** version of this command. To remove an entry that does specify an interface, use the **no ssl trust-point {***trustpoint [interface]***}** version of the command.

ssl trust-point {*trustpoint [interface]***}**

no ssl trust-point

Syntax Description

interface	The name for the interface to which the trustpoint applies. The **nameif** command specifies the name of the interface.
trustpoint	The *name* of the CA trustpoint as configured in the **crypto ca trustpoint** {*name*} command.

Defaults

The default is no trustpoint association. The security appliance uses the default self-generated RSA key-pair certificate.

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	This command was introduced.

Usage Guidelines

Observe these guidelines when using this command:

- The value for *trustpoint* must be the name of the CA trustpoint as configured in the **crypto ca trustpoint {*name*}** command.
- The value for *interface* must be the *nameif* name of a previously configured interface.
- Removing a trustpoint also removes any **ssl trust-point** entries that reference that trustpoint.
- You can have one **ssl trustpoint** entry for each interface and one that specifies no interfaces.
- You can reuse the same trustpoint for multiple entries.

The following example explains how to use the **no** versions of this command:

The configuration includes these SSL trustpoints:

```
ssl trust-point tp1
ssl trust-point tp2 outside
```

Issue the command:

no ssl trust-point

Then show run ssl will have:

ssl trust-point tp2 outside

Examples

The following example shows how to configure an ssl trustpoint called FirstTrust for the inside interface, and a trustpoint called DefaultTrust with no associated interface.

```
hostname(config)# ssl trust-point FirstTrust inside
hostname(config)# ssl trust-point DefaultTrust
```

The next example shows how to use the **no** version of the command to delete a trustpoint that has no associated interface:

```
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
hostname(config)# no ssl trust-point
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
```

The next example shows how to delete a trustpoint that does have an associated interface:

```
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
hostname(config)# no ssl trust-point FirstTrust inside
hostname(config)# show running-configuration ssl
ssl trust-point DefaultTrust
```

Command	Description
clear config ssl	Removes all SSL commands from the configuration, reverting to the default values.
show running-config ssl	Displays the current set of configured SSL commands.
ssl client-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a client.
ssl encryption	Specifies the encryption algorithms that the SSL/TLS protocol uses.
ssl server-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a server.

static

To configure a persistent one-to-one address translation rule by mapping a real IP address to a mapped IP address, use the **static** command in global configuration mode. To restore the default settings, use the **no** form of this command.

For static NAT:

static (*real_ifc*,*mapped_ifc*) {*mapped_ip* | **interface**} {*real_ip* [**netmask** *mask*] | **access-list** *access_list_name*} [**dns**] [**norandomseq** [**nailed**]] [[**tcp**] {*max_conns* {*emb_lim*}} [**udp** *udp_max_conns*]]

no static (*real_ifc*,*mapped_ifc*) {*mapped_ip* | **interface**} {*real_ip* [**netmask** *mask*] | **access-list** *access_list_name*} [**dns**] [**norandomseq** [**nailed**]] [[**tcp**] {*max_conns* {*emb_lim*}} [**udp** *udp_max_conns*]]

For static PAT:

static (*real_ifc*,*mapped_ifc*) {**tcp** | **udp**} {*mapped_ip* | **interface**} *mapped_port* {*real_ip real_port* [**netmask** *mask*]} | {**access-list** *access_list_name*} [**dns**] [**norandomseq** [**nailed**]] [[**tcp**] {*max_conns* {*emb_lim*}} [**udp** *udp_max_conns*]]

no static (*real_ifc*,*mapped_ifc*) {**tcp** | **udp**} {*mapped_ip* | **interface**} *mapped_port* {*real_ip real_port* [**netmask** *mask*]} | {**access-list** *access_list_name*} [**dns**] [**norandomseq** [**nailed**]] [[**tcp**] {*max_conns* {*emb_lim*}} [**udp** *udp_max_conns*]]

Syntax Description

access-list *access_list_name*	Lets you identify real addresses for NAT by specifying the real and destination addresses (or ports). This feature is known as policy NAT. The subnet mask used in the access list is also used for the *mapped_ip*. You can only include **permit** statements in the access list. You can also specify the real and destination ports in the access list using the **eq** operator. Policy NAT does not consider the **inactive** or **time-range** keywords; all ACEs are considered to be active for policy NAT configuration.
dns	(Optional) Rewrites the A record, or address record, in DNS replies that match this static. For DNS replies traversing from a mapped interface to a real interface, the A record is rewritten from the mapped value to the real value. Inversely, for DNS replies traversing from a real interface to a mapped interface, the A record is rewritten from the real value to the mapped value.
emb_lim	(Optional) Specifies the maximum number of embryonic connections per host. The default is 0, which means unlimited embryonic connections. Limiting the number of embryonic connections protects you from a DoS attack. The security appliance uses the embryonic 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. This option does not apply to outside NAT. The TCP intercept feature applies only to hosts or servers on a higher security level. If you set the embryonic limit for outside NAT, the embryonic limit is ignored.

interface	Uses the interface IP address as the mapped address. Use this keyword if you want to use the interface address, but the address is dynamically assigned using DHCP. **Note** You must use the interface keyword instead of specifying the actual IP address when you want to include the IP address of an interface in a static PAT entry. Otherwise, an error message is generated.
mapped_ifc	Specifies the name of the interface connected to the mapped IP address network.
mapped_ip	Specifies the address to which the real address is translated.
mapped_port	Specifies the mapped TCP or UDP port. You can specify ports by either a literal name or a number in the range of 0 to 65535. You can view valid port numbers online at the following website: http://www.iana.org/assignments/port-numbers
nailed	(Optional) Allows TCP sessions for asymmetrically routed traffic. This option allows inbound traffic to traverse the security appliance without a corresponding outbound connection to establish the state. This command is used in conjunction with the **failover timeout** command. The **failover timeout** command specifies the amount of time after a system boots or becomes active that the nailed sessions are accepted. If not configured, the connections cannot be reestablished. **Note** Adding the **nailed** option to the **static** command causes TCP state tracking and sequence checking to be skipped for the connection. Using the **asr-group** command to configure asymmetric routing support is more secure than using the **static** command with the **nailed** option and is the recommended method for configuring asymmetric routing support.
netmask *mask*	Specifies the subnet mask for the real and mapped addresses. For single hosts, use 255.255.255.255. If you do not enter a mask, then the default mask for the IP address class is used, with one exception. If a host-bit is non-zero after masking, a host mask of 255.255.255.255 is used. If you use the **access-list** keyword instead of the *real_ip*, then the subnet mask used in the access list is also used for the *mapped_ip*.
norandomseq	(Optional) Disables TCP ISN randomization protection. 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.
real_ifc	Specifies the name of the interface connected to the real IP address network.
real_ip	Specifies the real address that you want to translate.

real_port	Specifies the real TCP or UDP port. You can specify ports by either a literal name or a number in the range of 0 to 65535. You can view valid port numbers online at the following website: http://www.iana.org/assignments/port-numbers
tcp	For static PAT, specifies the protocol as TCP.
tcp *max_conns*	Specifies the maximum number of simultaneous TCP and UDP connections for the entire subnet. The default is 0, which means unlimited connections. (Idle connections are closed after the idle timeout specified by the **timeout conn** command.) This option does not apply to outside NAT. The security appliance only tracks connections from a higher security interface to a lower security interface.
udp	For static PAT, specifies the protocol as UDP.
udp *udp_max_conns*	(Optional) Used with the **udp** keyword to set the maximum number of simultaneous UDP connections the *real_ip* hosts are each allowed to use.

Defaults

The defaults are as follows:

- No embryonic limit.
- No connection limits.

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

Static NAT creates a fixed translation of real address(es) to mapped address(es).With dynamic NAT and PAT, each host uses a different address or port for each subsequent translation. Because the mapped address is the same for each consecutive connection with static NAT, and a persistent translation rule exists, static NAT allows hosts on the destination network to initiate traffic to a translated host (if there is an access list that allows it).

Note For static policy NAT, in undoing the translation, the ACL in the **static** command is not used. If the destination address in the packet matches the mapped address in the static rule, the static rule is used to untranslate the address.

The main difference between dynamic NAT and a range of addresses for static NAT is that static NAT allows a remote host to initiate a connection to a translated host (if there is an access list that allows it), while dynamic NAT does not. You also need an equal number of mapped addresses as real addresses with static NAT.

Static PAT is the same as static NAT, except it lets you specify the protocol (TCP or UDP) and port for the real and mapped addresses.

This feature lets you identify the same mapped address across many different static statements, so long as the port is different for each statement (you cannot use the same mapped address for multiple static NAT statements).

You cannot use the same real or mapped address in multiple **static** commands between the same two interfaces. Do not use a mapped address in the **static** command that is also defined in a **global** command for the same mapped interface.

When you specify the ports in policy NAT for applications that require application inspection for secondary channels (FTP, VoIP, etc.), the security appliance automatically translates the secondary ports.

NAT, in the conventional sense, is not available in transparent firewall mode. In transparent firewall mode, you can use the **static** command to configure maximum connections, maximum embryonic connections, and TCP sequence randomization. In this case, both the real and mapped IP addresses are the same.

You can alternatively configure maximum connections, maximum embryonic connections, and TCP sequence randomization using the **set connection** commands. 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.

If you specify a network for translation (for example, 10.1.1.0 255.255.255.0), then the security appliance translates the .0 and .255 addresses. If you want to prevent access to these addresses, be sure to configure an access list to deny access.

After changing or removing a static command statement, use the **clear xlate** command to clear the translations.

Examples

Static NAT Examples

For example, the following policy static NAT example shows a single real address that is translated to two mapped addresses depending on the destination address:

```
hostname(config)# access-list NET1 permit ip host 10.1.2.27 209.165.201.0 255.255.255.224
hostname(config)# access-list NET2 permit ip host 10.1.2.27 209.165.200.224
255.255.255.224
hostname(config)# static (inside,outside) 209.165.202.129 access-list NET1
hostname(config)# static (inside,outside) 209.165.202.130 access-list NET2
```

The following command maps an inside IP address (10.1.1.3) to an outside IP address (209.165.201.12):

```
hostname(config)# static (inside,outside) 209.165.201.12 10.1.1.3 netmask 255.255.255.255
```

The following command maps the outside address (209.165.201.15) to an inside address (10.1.1.6):

```
hostname(config)# static (outside,inside) 10.1.1.6 209.165.201.15 netmask 255.255.255.255
```

The following command statically maps an entire subnet:

```
hostname(config)# static (inside,dmz) 10.1.1.0 10.1.2.0 netmask 255.255.255.0
```

This example shows how to permit a finite number of users to call in through H.323 using Intel Internet Phone, CU-SeeMe, CU-SeeMe Pro, MeetingPoint, or Microsoft NetMeeting. The **static** command maps addresses 209.165.201.0 through 209.165.201.30 to local addresses 10.1.1.0 through 10.1.1.30 (209.165.201.1 maps to 10.1.1.1, 209.165.201.10 maps to 10.1.1.10, and so on).

```
hostname(config)# static (inside, outside) 209.165.201.0 10.1.1.0 netmask 255.255.255.224
hostname(config)# access-list acl_out permit tcp any 209.165.201.0 255.255.255.224 eq h323
hostname(config)# access-group acl_out in interface outside
```

This example shows the commands that are used to disable Mail Guard:

```
hostname(config)# static (dmz1,outside) 209.165.201.1 10.1.1.1 netmask 255.255.255.255
hostname(config)# access-list acl_out permit tcp any host 209.165.201.1 eq smtp
hostname(config)# access-group acl_out in interface outside
hostname(config)# no fixup protocol smtp 25
```

In the example, the **static** command allows you to set up a global address to permit outside hosts access to the 10.1.1.1 mail server host on the dmz1 interface. You shoud set the MX record for DNS to point to the 209.165.201.1 address so that mail is sent to this address. The **access-list** command allows the outside users to access the global address through the SMTP port (25). The **no fixup protocol** command disables Mail Guard.

Static PAT Examples

For example, for Telnet traffic initiated from hosts on the 10.1.3.0 network to the security appliance outside interface (10.1.2.14), you can redirect the traffic to the inside host at 10.1.1.15 by entering the following commands:

```
hostname(config)# access-list TELNET permit tcp host 10.1.1.15 eq telnet 10.1.3.0
255.255.255.0 eq telnet
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet access-list TELNET
```

For HTTP traffic initiated from hosts on the 10.1.3.0 network to the security appliance outside interface (10.1.2.14), you can redirect the traffic to the inside host at 10.1.1.15 by entering:

```
hostname(config)# access-list HTTP permit tcp host 10.1.1.15 eq http 10.1.3.0
255.255.255.0 eq http
hostname(config)# static (inside,outside) tcp 10.1.2.14 http access-list HTTP
```

To redirect Telnet traffic from the security appliance outside interface (10.1.2.14) to the inside host at 10.1.1.15, enter the following command:

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet netmask
255.255.255.255
```

If you want to allow the preceding real Telnet server to initiate connections, though, then you need to provide additional translation. For example, to translate all other types of traffic, enter the following commands. The original **static** command provides translation for Telnet to the server, while the **nat** and **global** commands provide PAT for outbound connections from the server.

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet netmask
255.255.255.255
hostname(config)# nat (inside) 1 10.1.1.15 255.255.255.255
hostname(config)# global (outside) 1 10.1.2.14
```

If you also have a separate translation for all inside traffic, and the inside hosts use a different mapped address from the Telnet server, you can still configure traffic initiated from the Telnet server to use the same mapped address as the **static** statement that allows Telnet traffic to the server. You need to create a more exclusive **nat** statement just for the Telnet server. Because **nat** statements are read for the best

match, more exclusive **nat** statements are matched before general statements. The following example shows the Telnet **static** statement, the more exclusive **nat** statement for initiated traffic from the Telnet server, and the statement for other inside hosts, which uses a different mapped address.

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet netmask
255.255.255.255
hostname(config)# nat (inside) 1 10.1.1.15 255.255.255.255
hostname(config)# global (outside) 1 10.1.2.14
hostname(config)# nat (inside) 2 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 2 10.1.2.78
```

To translate a well-known port (80) to another port (8080), enter the following command:

```
hostname(config)# static (inside,outside) tcp 10.1.2.45 80 10.1.1.16 8080 netmask
255.255.255.255
```

Related Commands

Command	Description
clear configure static	Removes **static** commands from the configuration.
clear xlate	Clears all translations.
nat	Configures dynamic NAT.
show running-config static	Displays all **static** commands in the configuration.
timeout conn	Sets the timeout for connections.

strict-http

To allow forwarding of non-compliant HTTP traffic, use the **strict-http** command in HTTP map configuration mode, which is accessible using the **http-map** command. To reset this feature to its default behavior, use the **no** form of the command.

strict-http action {**allow** | **reset** | **drop**} [**log**]

no **strict-http action** {**allow** | **reset** | **drop**} [**log**]

Syntax Description

action	The action taken when a message fails this command inspection.
allow	Allows the message.
drop	Closes the connection.
log	(Optional) Generate a syslog.
reset	Closes the connection with a TCP reset message to client and server.

Defaults

This command is enabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Although strict HTTP inspection cannot be disabled, the **strict-http action allow** command causes the security appliance to allow forwarding of non-compliant HTTP traffic. This command overrides the default behavior, which is to deny forwarding of non-compliant HTTP traffic.

Examples

The following example allows forwarding of non-compliant HTTP traffic:

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# strict-http allow
hostname(config-http-map)# exit
```

Related Commands

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

strip-group

This command applies only to usernames received in the form user@realm. A realm is an administrative domain appended to a username with the @ delimiter (juser@abc).

To enable or disable strip-group processing, use the **strip-group** command in tunnel-group general-attributes mode. The security appliance selects the tunnel group for PPP connections by obtaining the group name from the username presented by the VPN client. When strip-group processing is enabled, the security appliance sends only the user part of the username for authorization/authentication. Otherwise (if disabled), the security appliance sends the entire username including the realm.

To disable strip-group processing, use the **no** form of this command.

strip-group

no strip-group

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting for this command 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
Tunnel-group general attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You can apply this attribute only to the IPSec remote access tunnel-type.

Examples

The following example configures a remote access tunnel group named “remotegrp” for type IPSec remote access, then enters general configuration mode, sets the tunnel group named “remotegrp” as the default group policy, and then enables strip group for that tunnel group:

```
hostname(config)# tunnel-group remotegrp type IPSec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-general)# default-group-policy remotegrp
hostname(config-general)# strip-group
hostname(config-general)
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
group-delimiter	Enables group-name parsing and specifies the delimiter to be used when parsing group names from the user names that are received when tunnels are being negotiated.
show running-config tunnel group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group-map default group	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

strip-realm

To enable or disable strip-realm processing, use the **strip-realm** command in tunnel-group general-attributes configuration mode. Strip-realm processing removes the realm from the username when sending the username to the authentication or authorization server. A realm is an administrative domain appended to a username with the @ delimiter (username@realm). If the command is enabled, the security appliance sends only the user part of the username authorization/authentication. Otherwise, the security appliance sends the entire username.

To disable strip-realm processing, use the **no** form of this command.

strip-realm

no strip-realm

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting for this command 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
Tunnel-group general attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You can apply this attribute only to the IPSec remote access tunnel-type.

Examples

The following example configures a remote access tunnel group named “remotegrp” for type IPSec remote access, then enters general configuration mode, sets the tunnel group named “remotegrp” as the default group policy, and then enables strip realm for that tunnel group:

```
hostname(config)# tunnel-group remotegrp type IPSec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-general)# default-group-policy remotegrp
hostname(config-general)# strip-realm
```

neral)

ostname(config-ge

Related Commands

h

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the indicated certificate map entry.
tunnel-limit	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

subject-name (crypto ca certificate map)

To indicate that rule entry is applied to the subject DN of the IPSec peer certificate, use the **subject-name** command in CA certificate map configuration mode. To remove an subject-name, use the **no** form of the command.

subject-name [**attr** *tag*] **eq | ne |co | nc** *string*

no subject-name [**attr** *tag*] **eq | ne |co | nc** *string*

Syntax Description

attr *tag*	Indicates that only the specified attribute value from the certificate DN will be compared to the rule entry string. The tag values are as follows: DNQ = DN qualifier GENQ = Generational qualifier I = Initials GN = Given name N = Name SN = Surname IP = IP address SER = Serial number UNAME = Unstructured name EA = Email address T = Title O = Organization Name L = Locality SP = State/Province C = Country OU = Organizational unit CN = Common name
co	Specifies that the rule entry string must be a substring in the DN string or indicated attribute.
eq	Specifies that the DN string or indicated attribute must match the entire rule string.
nc	Specifies that the rule entry string must not be a substring in theDN string or indicated attribute.
ne	Specifies that the DN string or indicated attribute must not match the entire rule string.
string	Specifies the value to be matched.

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
Crypto ca certificate map configuration	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example enters the CA certificate map mode for certificate map 1 and creates a rule entry indicating that the Organization attribute of the certificate subject name must be equal to Central.

```
hostname(config)# crypto ca certificate map 1
hostname(ca-certificate-map)# subject-name attr o eq central
hostname(ca-certificate-map)# exit
```

Related Commands

Command	Description
crypto ca certificate map	Enters CA certificate map mode.
issuer-name	Identifies the DN from the CA certificate that is to be compared to the rule entry string.
tunnel-group-map	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

subject-name (crypto ca trustpoint)

To include the indicated subject DN in the certificate during enrollment, use the **subject-name** command in crypto ca trustpoint configuration mode. This is the person or system that uses the certificate. To restore the default setting, use the **no** form of the command.

subject-name *X.500_name*

no subject-name

Syntax Description

X.500_name	Defines the X.500 distinguished name, for example: cn=crl,ou=certs,o=CAName,c=US. The maximum length is 1K characters (effectively unbounded).

Defaults

The default setting is not to include the subject name.

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 sets up automatic enrollment at the URL https//:frog.phoobin.com and includes the subject DN OU tiedye.com in the the enrollment request for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment url http://frog.phoobin.com/
hostname(ca-trustpoint)# subject-name ou=tiedye.com
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.
enrollment url	Specifies the URL for enrolling with a CA.

summary-address

To create aggregate addresses for OSPF, use the **summary-address** command in router configuration mode. To remove the summary address or specific summary address options, use the **no** form of this command.

summary-address *addr mask* [**not-advertise**] [**tag** *tag_value*]

no summary-address *addr mask* [**not-advertise**] [**tag** *tag_value*]

Syntax Description

addr	Value of the summary address that is designated for a range of addresses.
mask	IP subnet mask that is used for the summary route.
not-advertise	(Optional) Suppresses routes that match the specified prefix/mask pair.
tag *tag_value*	(Optional) A 32-bit decimal value attached to each external route. This value is not used by OSPF itself. It may be used to communicate information between ASBRs. If none is specified, then the remote autonomous system number is used for routes from BGP and EGP; for other protocols, zero (0) is used. Valid values range from 0 to 4294967295.

Defaults

The defaults are as follows:

- *tag_value* is 0.
- Routes that match the specified prefix/mask pair are not suppressed.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Routes learned from other routing protocols can be summarized. Using this command for OSPF causes an OSPF Autonomous System Boundary Router (ASBR) to advertise one external route as an aggregate for all redistributed routes that are covered by the address. This command summarizes only routes from other routing protocols that are being redistributed into OSPF. Use the **area range** command for route summarization between OSPF areas.

To remove a **summary-address** command from the configuration, use the no form of the command without specifying any of the optional keywords or arguments. To remove an option from a summary command in the configuration, use the **no** form of the command with the options that you want removed. See the "Examples" section for more information.

Examples

The following example configures route summarization with a **tag** set to 3:

```
hostname(config-router)# summary-address 1.1.0.0 255.255.0.0 tag 3
hostname(config-router)#
```

The following example shows how to use the **no** form of the **summary-address** command with an option to set that option back to the default value. In this example, the **tag** value, set to 3 in the previous example, is removed from the **summary-address** command.

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0 tag 3
hostname(config-router)#
```

The following example removes the **summary-address** command from the configuration:

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0
hostname(config-router)#
```

Related Commands

Command	Description
area range	Consolidates and summarizes routes at an area boundary.
router ospf	Enters router configuration mode.
show ospf summary-address	Displays the summary address settings for each OSPF routing process.

sunrpc-server

To create entries in the SunRPC services table, use the **sunrpc-server** command in global configuration mode. To remove SunRPC services table entries from the configuration, use the **no** form of this command.

sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **protocol** [**tcp** | **udp**] **port** *port* [**-** *port*] **timeout** *hh:mm:ss*

no sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **protocol** [**tcp** | **udp**] **port** *port* [*- port]* **timeout** *hh:mm:ss*

no sunrpc-server active service *service_type* **server** *ip_addr*

Syntax Description

ifc_name	Server interface name.
ip_addr	SunRPC server IP address.
mask	Network mask.
port *port* [- *port*]	Specifies the SunRPC protocol port range.
port- *port*	(Optional) Specifies the SunRPC protocol port range.
protocol tcp	Specifies the SunRPC transport protocol.
protocol udp	Specifies the SunRPC transport protocol.
service	Specifies a service.
service_type	Sets the SunRPC service program number as specified in the **sunrpcinfo** command.
timeout *hh:mm:ss*	Specifies the timeout idle time after which the access for the SunRPC service traffic is closed.

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	This command was introduced.

Usage Guidelines

The SunRPC services table is used to allow SunRPC traffic through the security appliance based on an established SunRPC session for the duration specified by the timeout.

Examples

The following example shows how to create an SunRPC services table:

```
hostname(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100003 protocol TCP
port 111 timeout 0:11:00
hostname(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100005 protocol TCP
port 111 timeout 0:11:00
```

Related Commands

Command	Description
clear configure sunrpc-server	Clears the Sun remote processor call services from the security appliance.
show running-config sunrpc-server	Displays the information about the SunRPC configuration.

support-user-cert-validation

To validate a remote user certificate based on the current trustpoint, provided that this trustpoint is authenticated to the CA that issued the remote certificate, use the **support-user-cert-validation** command in crypto ca trustpoint configuration mode. To restore the default setting, use the **no** form of the command.

support-user-cert-validation

no support-user-cert-validation

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is to support user certificate validation.

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.

Usage Guidelines

The security appliance can have two trustpoints with the same CA resulting in two different identity certificates from the same CA. This option is automatically disabled if the trustpoint is authenticated to a CA that is already associated with another trustpoint that has enabled this feature. This prevents ambiguity in the choice of path-validation parameters. If the user attempts to activate this feature on a trustpoint that has been authenticated to a CA already associated with another trustpoint that has enabled this feature, the action is not permitted. No two trustpoints can have this setting enabled and be authenticated to the same CA.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and enables the trustpoint central to accept user validation:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# support-user-cert-validation
hostname(ca-trustpoint)#
```

Related Commands

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

syn-data

To allow or drop SYN packets with data, use the **syn-data** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

syn-data {**allow** | **drop**}

no syn-data {**allow** | **drop**}

Syntax Description

allow	Allows SYN packets that contain data.
drop	Drops SYN packets that contain data.

Defaults

Packets with SYN data are allowed by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

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

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **syn-data** command in tcp-map configuration mode to drop packets with data in SYN packets.

According to the TCP specification, TCP implementations are required to accept data contained in a SYN packet. Because this is a subtle and obscure point, some implementations may not handle this correctly. To avoid any vulnerabilities to insertion attacks involving incorrect end-system implementations, you may choose to drop packets with data in SYN packets.

Examples

The following example shows how to drop SYN packets with data on all TCP flows:

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# syn-data drop
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
```

```
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

Related Commands

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

sysopt connection permit-ipsec

For traffic that enters the security appliance through an IPSec tunnel and is then decrypted, use the **sysopt connection permit-ipsec** command in global configuration mode to allow the traffic to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic. To disable this feature, use the **no** form of this command.

sysopt connection permit-ipsec

no sysopt connection permit-ipsec

Syntax Description

This command has no arguments or keywords.

Defaults

This feature 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 is now enabled by default. Also, only interface access lists are bypassed; group policy or per-user access lists remain in force.

Usage Guidelines

You might want to bypass interface access lists for decrypted traffic to simplify configuration and to maximize the security appliance performance. If you disable this feature, you must apply an access list to the ingress interface that permits decrypted IPSec packets from all IPSec peers (see the the **access-list** and **access-group** commands).

Examples

The following example lets IPSec traffic bypass interface access lists:

```
hostname(config)# sysopt connection permit-ipsec
```

Related Commands

Command	Description
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.

Command	Description
sysopt connection tcpmss	Overrides the maximum TCP segment size or ensures that the maximum is not less than a specified size.
sysopt connection timewait	Forces each TCP connection to linger in a shortened TIME_WAIT state after the final normal TCP close-down sequence.

sysopt connection tcpmss

To ensure that the maximum TCP segment size does not exceed the value you set and that the maximum is not less than a specified size, use the **sysopt connection tcpmss** command in global configuration mode. To restore the default setting, use the **no** form of this command.

sysopt connection tcpmss [**minimum**] *bytes*

no sysopt connection tcpmss [**minimum**] [*bytes*]

Syntax Description

bytes	Sets the maximum TCP segment size in bytes, between 48 and any maximum number. The default value is 1380 bytes. You can disable this feature by setting *bytes* to 0. For the **minimum** keyword, the *bytes* represent the smallest maximum value allowed.
minimum	Overrides the maximum segment size to be no less than *bytes*, between 48 and 65535 bytes. This feature is disabled by default (set to 0).

Defaults

The default maximum value is 1380 bytes. The minimum feature is disabled by default (set to 0).

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Both the host and the server can set the maximum segment size when they first establish a connection. If either maximum exceeds the value you set with the **sysopt connection tcpmss** command, then the security appliance overrides the maximum and inserts the value you set. If either maximum is less than the value you set with the **sysopt connection tcpmss minimum** command, then the security appliance overrides the maximum and inserts the "minimum" value you set (the minimum value is actually the smallest maximum allowed). For example, if you set a maximum size of 1200 bytes and a minimum size of 400 bytes, when a host requests a maximum size of 1300 bytes, then the security appliance alters the packet to request 1200 bytes (the maximum). If another host requests a maximum value of 300 bytes, then the security appliance alters the packet to request 400 bytes (the minimum).

The default of 1380 bytes allows room for header information so that the total packet size does not exceed 1500 bytes, which is the default MTU for Ethernet. See the following calculation:

1380 data + 20 TCP + 20 IP + 24 AH + 24 ESP_CIPHER + 12 ESP_AUTH + 20 IP = 1500 bytes

If the host or server does not request a maximum segment size, the security appliance assumes that the RFC 793 default value of 536 bytes is in effect.

If you set the maximum size to be greater than 1380, packets might become fragmented, depending on the MTU size (which is 1500 by default). Large numbers of fragments can impact the performance of the security appliance when it uses the Frag Guard feature. Setting the minimum size prevents the TCP server from sending many small TCP data packets to the client and impacting the performance of the server and the network.

Note Although not advised for normal use of this feature, if you encounter the syslog IPFRAG messages 209001 and 209002, you can raise the *bytes* value.

Examples

The following example sets the maximum size to 1200 and the minimum to 400:

```
hostname(config)# sysopt connection tcpmss 1200
hostname(config)# sysopt connection tcpmss minimum 400
```

Related Commands

Command	Description
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.
sysopt connection permit-ipsec	Permits any packets that come from an IPSec tunnel without checking any ACLs for interfaces.
sysopt connection timewait	Forces each TCP connection to linger in a shortened TIME_WAIT state after the final normal TCP close-down sequence.

sysopt connection timewait

To force each TCP connection to linger in a shortened TIME_WAIT state of at least 15 seconds after the final normal TCP close-down sequence, use the **sysopt connection timewait** command in global configuration mode. To disable this feature, use the **no** form of this command. You might want to use this feature if an end host application default TCP terminating sequence is a simultaneous close.

sysopt connection timewait

Syntax Description

This command has no arguments or keywords.

Defaults

This feature 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
Preexisting	This command was preexisting.

Usage Guidelines

The default behavior of the security appliance is to track the shutdown sequence and release the connection after two FINs and the ACK of the last FIN segment. This quick release heuristic enables the security appliance to sustain a high connection rate, based on the most common closing sequence, known as the normal close sequence. However, in a simultaneous close, both ends of the transaction initiate the closing sequence, as opposed to the normal close sequence where one end closes and the other end acknowledges prior to initiating its own closing sequence (see RFC 793). Thus, in a simultaneous close, the quick release forces one side of the connection to linger in the CLOSING state. Having many sockets in the CLOSING state can degrade the performance of an end host. For example, some WinSock mainframe clients are known to exhibit this behavior and degrade the performance of the mainframe server. Using the **sysopt connection timewait** command creates a window for the simultaneous close down sequence to complete.

Examples

The following example enables the timewait feature:

```
hostname(config)# sysopt connection timewait
```

Related Commands

Command	Description
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.
sysopt connection permit-ipsec	Permits any packets that come from an IPSec tunnel without checking any ACLs for interfaces.
sysopt connection tcpmss	Overrides the maximum TCP segment size or ensures that the maximum is not less than a specified size.

sysopt nodnsalias

To disable DNS inspection that alters the DNS A record address when you use the **alias** command, use the **sysopt nodnsalias** command in global configuration mode. To disable this feature, use the **no** form of this command. You might want to disable DNS application inspection if you want the **alias** command to perform only NAT, and DNS packet alteration is undesirable.

sysopt nodnsalias {**inbound** | **outbound**}

no sysopt nodnsalias {**inbound** | **outbound**}

Syntax Description

inbound	Disables DNS record alteration for packets from lower security interfaces to higher security interfaces specified by an **alias** command.
outbound	Disables DNS record alteration for packets from higher security interfaces specified by an **alias** command to lower security interfaces.

Defaults

This feature is disabled by default (DNS record address alteration is enabled).

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 **alias** command performs NAT and DNS A record address alteration. In some cases, you might want to disable the DNS record alteration.

Examples

The following example disables the DNS address alteration for inbound packets:

```
hostname(config)# sysopt nodnsalias inbound
```

Related Commands

Command	Description
alias	Translates an outside address and alters the DNS records to accommodate the translation.
clear configure sysopt	Clears the **sysopt** command configuration.

Command	Description
show running-config sysopt	Shows the **sysopt** command configuration.
sysopt noproxyarp	Disables proxy ARP on an interface.

sysopt noproxyarp

To disable proxy ARP for NAT global addresses on an interface, use the **sysopt noproxyarp** command in global configuration mode. To reenable proxy ARP for global addresses, use the **no** form of this command.

sysopt noproxyarp *interface_name*

no sysopt noproxyarp *interface_name*

Syntax Description

interface_name	The interface name for which you want to disable proxy ARP.

Defaults

Proxy ARP for global addresses is enabled by default.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

In rare circumstances, you might want to disable proxy ARP for global addresses.

When a host sends IP traffic to another device on the same Ethernet network, the host needs to know the MAC address of the device. ARP is a Layer 2 protocol that resolves an IP address to a MAC address. A host sends an ARP request asking "Who is this IP address?" The device owning the IP address replies, "I own that IP address; here is my MAC address."

Proxy ARP is when a device responds to an ARP request with its own MAC address, even though the device does not own the IP address. The security appliance uses proxy ARP when you configure NAT and specify a global address that is on the same network as the security appliance interface. The only way traffic can reach the hosts is if the security appliance uses proxy ARP to claim that the security appliance MAC address is assigned to destination global addresses.

Examples

The following example disables proxy ARP on the inside interface:

```
hostname(config)# sysopt noproxyarp inside
```

Related Commands

Command	Description
alias	Translates an outside address and alters the DNS records to accommodate the translation.
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.
sysopt nodnsalias	Disables alteration of the DNS A record address when you use the **alias** command.

sysopt radius ignore-secret

To ignore the authentication key in RADIUS accounting responses, use the **sysopt radius ignore-secret** command in global configuration mode. To disable this feature, use the **no** form of this command. You might need to ignore the key for compatibility with some RADIUS servers.

sysopt radius ignore-secret

no sysopt radius ignore-secret

Syntax Description

This command has no arguments or keywords.

Defaults

This feature 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
Preexisting	This command was preexisting.

Usage Guidelines

Some RADIUS servers fail to include the key in the authenticator hash within the accounting acknowledgment response. This usage caveat can cause the security appliance to continually retransmit the accounting request. Use the **sysopt radius ignore-secret** command to ignore the key in these acknowledgments, thus avoiding the retransmit problem. (The key identified here is the same one you set with the **aaa-server host** command.)

Examples

The following example ignores the authentication key in accounting responses:

```
hostname(config)# sysopt radius ignore-secret
```

Related Commands

Command	Description
aaa-server host	Identifies a AAA server.
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.

sysopt uauth allow-http-cache

To let the web browser supply a username and password from its cache when it reauthenticates with the virtual HTTP server on the security appliance (see the **virtual http** command), use the **sysopt uauth allow-http-cache** command in global configuration mode. If you do not allow the HTTP cache, then after your authentication session times out, the next time you connect to the virtual HTTP server, you are prompted again for your username and password. To disable this feature, use the **no** form of this command.

sysopt uauth allow-http-cache

no sysopt uauth allow-http-cache

Syntax Description

This command has no arguments or keywords.

Defaults

This feature 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
Preexisting	This command was preexisting.

Examples

The following example allows the HTTP cache to be used:

```
hostname(config)# sysopt uauth allow-http-cache
```

Related Commands

Command	Description
virtual http	When you use HTTP authentication on the security appliance, and the HTTP server also requires authentication, this command allows you to authenticate separately with the security appliance and with the HTTP server. Without virtual HTTP, the same username and password you used to authenticate with the security appliance is sent to the HTTP server; you are not prompted separately for the HTTP server username and password.
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.