CHAPTER 24

same-security-traffic through show asdmsessions Commands

same-security-traffic

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

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

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

Syntax Description

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

Defaults

By default, these behaviors are disabled.

Command Modes

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

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

Command History

Release	Modification
2.2(1)	This command with the inter-interface keyword was introduced.
2.3(1)	Support for the intra-interface keyword was added.

Usage Guidelines

Allowing communication between same security interfaces (enabled by the **same-security-traffic inter-interface** command) lets you 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).

If you enable NAT control, you do not need to configure NAT between same security level interfaces.

The **same-security-traffic intra-interface** command lets traffic enter and exit the same interface, which is normally not allowed.

Note If you use a same-security interface for both the outside and inside interfaces, you might want to enable the **xlate-bypass** command; in some situations, you can exceed the maximum number of xlates using that configuration (see the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* for limits). For example, without **xlate-bypass**, the FWSM creates xlates for all connections (even if you do not configure NAT). In a same-security-traffic configuration, the FWSM randomly chooses which same-security interface is the "inside" interface for the sake of creating xlates. If the FWSM considers the outside same-security interface as the "inside" interface, it creates

xlates for every Internet host being accessed through it. If there is any application (or a virus) on the internal network that scans thousands of Internet hosts, all entries in the xlate table may be quickly exhausted.

Examples

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

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

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

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

Related Commands

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

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
3.1(1)	This command was introduced.

Usage Guidelines

This command is available for any host in an SDI AAA server group, 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 FWSM 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
```

Related Commands

Command	Description
aaa-server host	Enter AAA server host configuration mode so that 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
3.1(1)	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
```

Related Commands

Command	Description
aaa-server host	Enter AAA server host configuration mode so that 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
3.1(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example configures failover group 1 with the primary unit as the higher priority and failover group 2 with the secondary unit as the higher priority. Both failover groups are configured with the **preempt** command so that 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)# 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.

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 {**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
3.1(1)	This command was introduced.

Usage Guidelines

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 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 FWSM, 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 FWSM 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 FWSM 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
3.1(1)	This command was introduced. It moved from a keyword of the **nameif** command to an interface configuration mode command.

Usage Guidelines

The level controls the following behavior:

- 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 FWSM.
- 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
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 gigabitethernet1
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.

serial-number

To include the FWSM 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
3.1(1)	This command was introduced.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and includes the FWSM 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-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
3.1(1)	This command was introduced.

Examples

The following example configures an SDI AAA server named “svrgrp1” to use server port number 8888:

```
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)# server-port 8888
```

Related Commands

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

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

service reset no-connection

To send a reset for a TCP packet for which the FWSM does not have any connection history, use the **service reset no-connection** command in global configuration mode. To disable sending a reset, use the **no** form of this command.

service reset no-connection

no service reset no-connection

Syntax Description

This command has no arguments or keywords.

Defaults

By default, resets are sent.

Command Modes

The 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
4.0(1)	This command was introduced.

Usage Guidelines

If the FWSM receives an ACK or SYN-ACK packet without first receiving a SYN packet, then the FWSM does not have any connection history for the packet. By default, the FWSM sends a RST for the packet. To disable the sending of the RST, enter the **no service reset no-connectio**n command.

See the **service resetinbound** command to set the reset bahavior for SYN packets that attempt to establish a connection with the FWSM but are denied based on access lists or AAA configuration.

Note This command is only available in the admin context.

Examples

The following example shows how to disable the sending of the RST:

```
hostname(config)# no service reset no-connection
```

Related Commands

Command	Description
service resetinbound	Sets whether to send a reset for TCP SYN packets that are denied.
show running-config service	Displays the system services.

service resetinbound

To send a reset to inbound TCP connections when they are denied, use the **service resetinbound** command in global configuration mode. To not send a reset, use the **no** form of this command.

service resetinbound

no service resetinbound

Syntax Description

This command has no arguments or keywords.

Defaults

By default, no resets are sent.

Command Modes

The 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
1.1(1)	This command was introduced.

Usage Guidelines

The **service resetinbound** command works with all inbound TCP connections 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 FWSM drops the packet without returning an RST.

To configure whether to send a reset for packets that do not have a connection on the FWSM, see the **service reset no-connection** command. For example, if the FWSM receives an ACK or SYN-ACK packet without first receiving a SYN packet, then the FWSM does not have any connection history for the packet. The **service resetinbound** command applies only to SYN packets that attempt to establish a connection with the FWSM.

The FWSM 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 FWSM sends a syslog message stating that the incoming connection was denied. Without entering the **service resetinbound** command, the FWSM 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 FWSM. 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
```

Examples

This example shows how to enable system services:

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

Related Commands

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

service-policy

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Interface service policies take precedence over the global service policy.

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

The default service policy includes the following command:

```
service-policy global_policy global
```

Examples

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

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

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

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

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.

set boot device (Catalyst OS)

By default, the FWSM boots from the **cf:4** application partition. However, you can choose to boot from the **cf:5** application partition or into the **cf:1** maintenance partition. To change the default boot partition, enter the **set boot device** command in privileged EXEC mode.

set boot device cf:*n mod_num*

Syntax Description

mod_num	Specifies the module number. Use the **show module** command to view installed modules and their numbers.
cf:*n*	Sets the boot partition. Application partitions include **cf:4** and **cf:5**. The maintenance partition is **cf:1**.

Defaults

The default boot partition is cf:4.

Command Modes

Privileged EXEC.

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Each application partition has its own startup configuration.

To view the current module, enter the **show module** command:

```
Console> show module
Mod Slot Ports Module-Type               Model               Sub Status
--- ---- ----- ------------------------- ------------------- --- ------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1A-2GE    yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC         no  ok
4   4    2     Intrusion Detection Syste WS-X6381-IDS        no  ok
5   5    6     Firewall Module           WS-SVC-FWM-1        no  ok
6   6    8     1000BaseX Ethernet        WS-X6408-GBIC       no  ok
```

Examples

The following example shows how to set the boot partition to the maintenance partition:

```
Console> (enable) set boot device cf:1 1
```

Related Commands

Command	Description
boot device module	Changes the default boot partition.
reset	Resets the module.
show module	Shows all installed modules.

set connection

To set the maximum TCP and UDP connections, connection rate limits, or disable TCP sequence number randomization for a traffic class, use the **set connection** command in class configuration mode. The class configuration mode is accessible from the policy-map configuration mode. To remove these specifications, use the **no** form of this command.

set connection {[**conn-max** *number*] [**conn-rate-limit** *number*] [**random-seq#** {**enable** | **disable**}]}

no set connection {[**conn-max** *number*] [**conn-rate-limit** *number*] [**random-seq#** {**enable** | **disable**}]}

Syntax Description

conn-max *number*	Sets the maximum number of simultaneous TCP and UDP connections, between 0 and 65535. The default is 0, which means no limit on connections.
conn-rate-limit *number*	Sets the maximum TCP and/or UDP connections per second between 0 and 65535. The default is 0, which means no limit on the connection rate.
disable	Turns off TCP sequence number randomization.
enable	Turns on TCP sequence number randomization.
random-seq#	Enables or disables TCP sequence number randomization. Each TCP connection has two ISNs: one generated by the client and one generated by the server. The FWSM 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 predicting 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 FWSM, and the eBGP peers are using MD5. Randomization breaks the MD5 checksum. • You use a WAAS device that requires the FWSM not to randomize the sequence numbers of connections. **Note** Because of the way TCP sequence randomization is implemented, if you enable Xlate Bypass using the **xlate-bypass** command), then disabling TCP sequence randomization only works for control connections, and not data connections; for data connections, the TCP sequence continues to be randomized.

Defaults

For the **conn-max** keyword, the default value of *number* is 0, which allows unlimited connections.

For the **conn-rate-limit** keyword, the default value of *number* is 0, which allows unlimited connections per second.

Sequence number randomization is enabled by default.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.
4.0(1)	The **conn-rate-limit** keyword was added. Also, when you match an access list in the class map, the set connection actions are performed for the access list as a whole instead of independently for each ACE.

Usage Guidelines

After you identify the traffic using the **class-map** command, enter the **policy-map** command to identify the actions associated with each class map. Enter the **class** command to identify the class map, and then enter the **set connection** command to set connections for that class map.

Note You can also configure maximum connections and TCP sequence randomization in the NAT configuration (the **nat** and **static** commands). If you configure these settings for the same traffic using both methods, then the FWSM uses the lower limit. For TCP sequence randomization, if it is disabled using either method, then the FWSM disables TCP sequence randomization.

Unlike the **set connection** command, NAT also lets you configure embryonic connection limits, which triggers TCP Intercept to prevent a DoS attack.

Examples

The following example configures the maximum number of simultaneous connections as 256, the maximum rate as 50 per second, and disables TCP sequence number randomization:

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection conn-max 256 conn-rate-limit 50 random-seq#
disable
```

Related Commands

Command	Description
class	Identifies a class map in the policy map.
class-map	Creates a class map for use in a service policy.
policy-map	Configures a policy map that associates a class map and one or more actions.

service-policy	Assigns a policy map to an interface.
set connection timeout	Sets the connection timeouts.

set connection advanced-options tcp-state-bypass

To enable TCP state bypass, use the **set connection advanced-options** command in class configuration mode. The class configuration mode is accessible from the policy-map configuration mode. To disable TCP state bypass, use the **no** form of this command.

set connection advanced-options tcp-state-bypass

no set connection advanced-options tcp-state-bypass

Syntax Description

This command has no arguments or keywords.

Defaults

By default, TCP state bypass 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
Class configuration	•	•	•	•	—

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

After you identify the traffic using the **class-map** command, enter the **policy-map** command to identify the actions associated with each class map. Enter the **class** command to identify the class map, and then enter the **set connection advanced-options** command to enable TCP state bypass for that class map.

Allowing Outbound and Inbound Flows through Separate FWSMs

By default, all traffic that goes through the FWSM is inspected using the Adaptive Security Algorithm and is either allowed through or dropped based on the security policy. The FWSM maximizes the firewall performance by checking the state of each packet (is this a new connection or an established connection?) and assigning it to either the session management path (a new connection SYN packet), the fast path (an established connection), or the control plane path (advanced inspection).

TCP packets that match existing connections in the fast path can pass through the FWSM without rechecking every aspect of the security policy. This feature maximizes performance. However, the method of establishing the session in the fast path using the SYN packet, and the checks that occur in the fast path (such as TCP sequence number), can stand in the way of asymmetrical routing solutions: both the outbound and inbound flow of a connection must pass through the same FWSM.

For example, a new connection goes to FWSM 1. The SYN packet goes through the session management path, and an entry for the connection is added to the fast path table. If subsequent packets of this connection go through FWSM 1, then the packets will match the entry in the fast path, and are passed

through. But if subsequent packets go to FWSM 2, where there was not a SYN packet that went through the session management path, then there is no entry in the fast path for the connection, and the packets are dropped.

If you have asymmetric routing configured on upstream routers, and traffic alternates between two FWSMs, then you can configure TCP state bypass for specific traffic. TCP state bypass alters the way sessions are established in the fast path and disables the fast path checks. This feature treats TCP traffic much as it treats a UDP connection: when a non-SYN packet matching the specified networks enters the FWSM, and there is not a fast path entry, then the packet goes through the session management path to establish the connection in the fast path. Once in the fast path, the traffic bypasses the fast path checks.

Application Inspection Unsupported

Application inspection requires both inbound and outbound traffic to go through the same FWSM, so application inspection is not supported with TCP state bypass.

Compatibility with NAT

Because the translation session is established separately for each FWSM, be sure to configure static NAT on both FWSMs for TCP state bypass traffic; if you use dynamic NAT, the address chosen for the session on FWSM 1 will differ from the address chosen for the session on FWSM 2.

Connection Timeout

If there is no traffic on a given connection for 2 minutes, the connection times out. You can override this default using the **set connection timeout tcp** command. Normal TCP connections timeout by default after 60 minutes.

Examples

The following is an example configuration for TCP state bypass:

```
hostname(config)# access-list tcp extended permit tcp 10.1.1.0 255.255.255.0 10.2.1.0
255.255.255.0

hostname(config)# class-map tcp_bypass
hostname(config-cmap)# description "TCP traffic that bypasses stateful firewall"
hostname(config-cmap)# match access-list tcp_bypass

hostname(config-cmap)# policy-map tcp_bypass_policy
hostname(config-pmap)# class tcp_bypass
hostname(config-pmap-c)# set connection advanced-options tcp-state-bypass

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

Related Commands

Command	Description
class	Identifies a class map in the policy map.
class-map	Creates a class map for use in a service policy.
policy-map	Configures a policy map that associates a class map and one or more actions.
service-policy	Assigns a policy map to an interface.
set connection timeout	Sets the connection timeouts.

set connection timeout

To configure the timeout period after which an embryonic, half-closed, or idle connection is disconnected, use the **set connection timeout** command in class configuration mode. To remove the timeout, use the **no** form of this command.

set connection timeout {[[**embryonic** *hh:mm:ss*] [**half-closed** *hh:mm:ss*] [**tcp** *hh:mm***:0**]] | **idle** *hh:mm***:0**}

no set connection timeout {[[**embryonic** *hh:mm:ss*] [**half-closed** *hh:mm:ss*] [**tcp** *hh:mm***:0**]] | **idle** *hh:mm***:0**}

Syntax Description

embryonic *hh:mm:ss*	Defines the timeout period until a TCP embryonic connection is closed, between 0:0:1 and 0:4:15. The default is 0:0:20. You can also set the value to 0, which means the connection never times out. Although you cannot set the maximum embryonic connections using the **set connection** command, you can set the timeout using this command.
half-closed *hh:mm:ss*	Defines the timeout period until a TCP half-closed connection is freed, between 0:0:1 and 0:4:15. The default is 0:0:20. You can also set the value to 0, which means the connection never times out.
idle *hh:mm***:0**	Defines the idle time after which an established connection of any protocol closes, between 0:5:0 and 1092:15:0. The default is 1:00:0. You can also set the value to 0, which means the connection never times out. **Note** This command ignores the value you set for seconds; you can only specify the hours and minutes. Therefore, you should set the seconds to be 0.
tcp *hh:mm***:0**	Defines the idle time after which a TCP established connection closes, between 0:5:0 and 1092:15:0. The default is 1:00:0. You can also set the value to 0, which means the connection never times out. This keyword has been replaced by the **idle** keyword, which applies to all protocols and not just to TCP. However, if you still have this command in your configuration, it is accepted. See the "Usage Guidelines" for more information about using both commands in the same policy. **Note** This command ignores the value you set for seconds; you can only specify the hours and minutes. Therefore, you should set the seconds to be 0.

Defaults

The default **embryonic** connection timeout value is 20 seconds.

The default **half-closed** connection timeout value is 20 seconds.

The default **idle** connection timeout value is 1 hour.

The default **tcp** connection timeout value is 1 hour.

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 configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.
3.2(1)	Support for the **idle** keyword was introduced.

Usage Guidelines

Configure this command using Modular Policy Framework. First define the traffic to which you want to apply the timeout using the **class-map** command. Then enter the **policy-map** command to define the policy, and enter the **class** command to reference the class map. In class configuration mode, you can enter the **set connection timeout** command. Finally, apply the policy map to an interface using the **service-policy** command. For more information about how Modular Policy Framework works, see the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*.

Note This command does not affect secondary connections created by an inspection engine. For example, you cannot change the connection settings for secondary flows like SQL*Net, FTP data flows, and so on using the **set connection timeout** command. For these connections, use the global **timeout conn** command to change the idle time. Note that the **timeout conn** command affects *all* traffic flows unless you otherwise use the **set connection timeout** command for eligible traffic.

You can enter the **tcp** keyword, **embryonic** keyword, and **half-closed** keyword together, however you must enter the **idle** keyword separately.

If you remove a timeout using the **no** form of the command, then all timeouts are removed. To change the value of a timeout, reenter the command with the new value instead of using the **no** form.

If you configure the **set connection timeout tcp** and **set connection timeout idle** commands for the same class, then the **idle** command (which sets the timeout for all types of connections) is used instead of the **tcp** command (which sets the timeout for TCP connections only) when the class map does not specifically match TCP traffic. If the class map matches an access list that specifies TCP traffic explicitly, then the **tcp** command is used instead of the **idle** command for TCP traffic; other traffic that matches the access list uses the **idle** command. The following example creates an access list with an ACE that specifically matches TCP traffic. Therefore, TCP traffic uses the **tcp** command, while UDP and ICMP traffic uses the **idle** command:

```
access-list ip_traffic extended permit tcp any any
access-list ip_traffic extended permit udp any any
access-list ip_traffic extended permit icmp any any

class-map c1
   match access-list ip_traffic

policy-map p1
   class c1
      set connection timeout idle 3:0:0
```

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

service-policy p1 global
```

The following example has an access list that matches all IP traffic, and it does not specifically match TCP traffic. Therefore, even though the **tcp** command is present in the configuration, it is ignored in favor of the **idle** command for all traffic, including TCP traffic:

```
access-list ip_traffic extended permit ip any any

class-map c1
   match access-list ip_traffic

policy-map p1
   class c1
      set connection timeout idle 3:0:0
      set connection timeout tcp 2:0:0

service-policy p1 global
```

Examples

The following example sets the maximum TCP and UDP connections to 5000, and sets the maximum embryonic timeout to 40 seconds, the half-closed timeout to 20 minutes, and the idle timeout to 2 hours for traffic going to 10.1.1.1:

```
hostname(config)# access-list CONNS permit ip any host 10.1.1.1

hostname(config)# class-map conns
hostname(config-cmap)# match access-list CONNS

hostname(config-cmap)# policy-map conns
hostname(config-pmap)# class conns
hostname(config-pmap-c)# set connection conn-max 5000
hostname(config-pmap-c)# set connection timeout embryonic 0:0:40 half-closed 0:20:0
hostname(config-pmap-c)# set connection timeout idle 2:0:0

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

Related Commands

Command	Description
class	Identifies a class map in the policy map.
class-map	Creates a class map for use in a service policy.
policy-map	Configures a policy map that associates a class map and one or more actions.
service-policy	Assigns a policy map to an interface.
set connection	Configures the maximum TCP and UDP connections.

set metric

To set the metric value for the destination 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
1.1(1)	This command was introduced.

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 metric for the destination routing protocol, 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 the FWSM through interactive prompts, enter the **setup** command in global configuration mode.

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
1.1(1)	This command was introduced.

Usage Guidelines

The FWSM requires some initial configuration before ASDM can connect to it. Before you enter the **setup** command, you must first name an interface "inside" with the **nameif** command. The FWSM does not have a default inside interface.

Once you enter the **setup** command, you are asked for the setup information in Table 24-1.

Table 24-1 Setup Information

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.
`Firewall Mode [Routed]:`	Enter **routed** or **transparent**. The firewall mode prompt is available only in single mode or in a context.
`Enable password:`	Enter an enable password. (The password must have at least three characters.)
`Inside IP address:`	Enter the network interface IP address of the FWSM.

Table 24-1 Setup Information (continued)

`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, 255.255.0.0, or 255.255.x.x. Use 0.0.0.0 to specify a default route. You can abbreviate the 0.0.0.0 netmask as 0.
`Host name:`	Enter the host name that you want to display in the command line prompt.
`Domain name:`	Enter the domain name of the network on which the FWSM runs.
`IP address of host running Device Manager:`	Enter the IP address on which ASDM connects to the FWSM.
`Use this configuration and write to flash [yes]?`	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.

The host and domain names are used to generate the default certificate for the Secure Socket Layer (SSL) connection.

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
Inside IP address [192.168.1.1]: 192.168.1.1
Inside network mask [255.255.255.0]: 255.255.255.0
Host name [tech_pubs]: tech_pubs
Domain name [your_company.com]: your_company.com
IP address of host running Device Manager:

The following configuration will be used:
Enable password: writer
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

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

Related Commands

Command	Description
asdm	Configures the communication between the FWSM and a browser running the device manager.

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
3.1(1)	This command was introduced.

Usage Guidelines

If you omit the optional keyword **locked**, the FWSM 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       augry13
    -                   1       N       cisco
    -                   4       N       newuser
hostname(config)#
```

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

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

Related Commands

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

show aaa-server

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

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

Syntax Description

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

Defaults

By default, all AAA server statistics display.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.
2.2(1)	This command was modified to support a LOCAL method.

Examples

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

```
hostname(config)# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: ACTIVE. Last transaction (success) at 11:10:08 UTC  Fri Aug 22
Number of pending requests        20
```

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

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

Field	Description
Server Group	The server group name specified by the **aaa-server** command.
Server Protocol	The server protocol for the server group specified by the **aaa-server** command.
Server Address	The IP address of the AAA server.
Server port	The communication port used by the FWSM and the AAA server. You can specify the RADIUS authentication port using the **authentication-port** command. You can specify the RADIUS accounting port using the **accounting-port** command. For non-RADIUS servers, the port is set by the **server-port** command.
Server status	The status of the server. You see one of the following values: • ACTIVE—The FWSM will communicate with this AAA server. • FAILED—The FWSM cannot communicate with the AAA server. Servers that are put into this state remain there for some period of time, depending on the policy configured, and are then reactivated. You also see the date and time of the last transaction in the following form: **Last transaction ({success | failure}) at** *time timezone date* If the FWSM has never communicated with the server, the message shows as the following: **Last transaction at Unknown**
Number of pending requests	The number of requests that are still in progress.
Average round trip time	The average time that it takes to complete a transaction with the server.
Number of authentication requests	The number of authentication requests sent by the FWSM. This value does not include retransmissions after a timeout.

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

Related Commands

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

show access-list

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

show access-list [*id*] [**optimization** [**detail**] [**range** *low high*]]

Syntax Description

detail	Shows detailed access list optimization information.
id	Identifies the access list.
optimization	Shows access list optimization information.
range *low high*	Shows the specified access list range.

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
1.1(1)	This command was introduced.
4.0(1)	Keywords **optimization**, **detail**, and **range** were added.

Usage Guidelines

An ACL only denies SYN packets, so if another type of packet comes in, that packet will not show up in the access-list hit counters. TCP packet types other than SYN packets (including RST, SYN-ACK, ACK, PSH, and FIN) are dropped by the FWSM before they can be dropped by an access list. Only SYN packets can create a session in the Adaptive Security Algorithm, so only SYN packets are assessed by the access list.

Examples

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

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

```
access-list 101 line 6 extended permit udp any lt ntp any (hitcnt=0) 0x8983c43 access-list
101 line 7 extended permit udp any any lt ntp (hitcnt=0) 0xf361ffb6
access-list 101 line 8 extended permit udp any any range ntp biff (hitcnt=0) 0x219581
access-list 101 line 9 extended permit icmp any any (hitcnt=0) 0xe8fa08e1
access-list 101 line 10 extended permit icmp any any echo (hitcnt=0) 0x2eb8deea
access-list 102; 1 elements access-list 102 line 1 extended permit icmp any any echo
(hitcnt=0) 0x59e2fea8
```

The output contains a unique hexamdecimal identifier for each ACE at the end of each line.

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
3.1(1)	Support for this command was introduced.

Usage Guidelines

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

- If the activation key in the FWSM Flash file system is the same as the activation key running on the FWSM, 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 FWSM Flash file system is different from the activation key running on the FWSM, 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 FWSM 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 FWSM 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
2.2(1)	This command was introduced.

Examples

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

```
hostname# show admin-context
Admin: admin disk:/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. This command shows dynamic and manual ARP entries, but does not identify the origin of each entry.

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
1.1(1)	This command was introduced.

Examples

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

```
hostname# show arp
        inside 10.86.195.205 0008.023b.9892
        inside 10.86.194.170 0001.023a.952d
        inside 10.86.194.172 0001.03cf.9e79
        inside 10.86.194.1 00b0.64ea.91a2
        inside 10.86.194.146 000b.fcf8.c4ad
        inside 10.86.194.168 000c.ce6f.9b7e
```

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
1.1(1)	This command was introduced.

Examples

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

```
hostname# show arp statistics
        Number of ARP entries:
        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 24-2 shows each field description.

Table 24-2 show arp statistics Fields

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

Table 24-2 show arp statistics Fields (continued)

Field	Description
Queued blocks	The number of blocks currently queued in the ARP module.
Interface collision ARPs received	The number of ARP packets received at all FWSM interfaces that were from the same IP address as that of a FWSM interface.
ARP-defense gratuitous ARPs sent	The number of gratuitous ARPs sent by the FWSM 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 FWSM 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 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
2.2(1)	This command was introduced.

Examples

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

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

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

Related Commands

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

show asdm history

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

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

Syntax Description

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

Defaults

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

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced (as **show pdm history**).
3.1(1)	This command was changed from the **show pdm history** command to the **show asdm history** command.

Usage Guidelines

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

Examples

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

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

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

```
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Underruns:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Output Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Collisions:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
LCOLL:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Reset:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Deferred:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Lost Carrier:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]   128   128   128   128   128   128   128
Software Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Software Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Drop KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
hostname#
```

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

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

MH|IBC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|62439|62445|62453|62457|62464|6
2469|62474|62486|62489|62496|62501|62506|62511|62518|62522|62530|62534|62539|62542|62547|6
2553|62556|62562|62568|62574|62581|62585|62593|62598|62604|62609|62616|62622|62628|62633|6
2636|62640|62653|62657|62665|62672|62678|62681|62686|62691|62695|62700|62704|62711|62718|6
2723|62728|62733|62738|62742|62747|62751|62761|62770|62775|
MH|OBC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|25023|25023|25025|25025|25025|2
5026|25026|25032|25038|25044|25052|25056|25060|25064|25070|25076|25083|25087|25091|25096|2
5102|25106|25110|25114|25118|25122|25128|25133|25137|25143|25147|25151|25157|25161|25165|2
5169|25178|25321|25327|25332|25336|25341|25345|25349|25355|25359|25363|25367|25371|25375|2
5381|25386|25390|25395|25399|25403|25410|25414|25418|25422|
MH|IPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|749|749|749|749|749|750|750|750
|750|750|750|750|750|750|750|750|750|750|750|751|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|
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|
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|
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|
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|
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|
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|
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|
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|
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|
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|
|
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|
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|
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|
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|
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|
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|
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|
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 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
3.1(1)	This command was introduced.

Usage Guidelines

Each active ASDM session has one or more associated ASDM logging sessions. ASDM uses the logging session to retrieve syslog messages from the FWSM. 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
1.1(1)	This command was introduced (as **show pdm sessions**).
3.1(1)	This command was changed from the **show pdm sessions** command to the **show asdm sessions** command.

Usage Guidelines

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

Examples

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

```
hostname# show asdm sessions

0 192.168.1.1
1 192.168.1.2
```

Related Commands

Command	Description
asdm disconnect	Terminates an active ASDM session.