



## **same-security-traffic through show asdm sessions Commands**

---

# same-security-traffic

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

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

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

## Syntax Description

<b>inter-interface</b>	Permits communication between different interfaces that have the same security level.
<b>intra-interface</b>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				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

We recommend that you do not make the outside interface (for example, where you access the Internet) on the same security level as your inside interfaces. On the FWSM, all connections have an associated xlate entry (even when you do not explicitly configure NAT). Xlates are normally created for connections between the inside interface and any lower security interface. In a same-security-traffic configuration, the FWSM randomly chooses which same-security interface is the “inside” interface for the sake of creating xlates. This selection may change later after a reload or after a software upgrade. 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 (see the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* for xlate limits). After that, the FWSM will stop creating new xlates, logging error message %FWSM-3-305006: (“translation creation failed”) for every new connection. The **show resource usage** command will show the number of active xlates equal or close to the limit. The **clear xlate** command will temporarily recover connectivity.

To avoid this situation, we recommend that the outside interface should always have security level lower than any other FWSM interface. This configuration guarantees that the FWSM always considers the ISP link as an outside interface. In this case, only one xlate will be created for every application or virus scanning Internet hosts from the inside network. No xlates will be created for Internet hosts being scanned.

---

### 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
<b>show running-config same-security-traffic</b>	Displays the <b>same-security-traffic</b> 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

<i>host</i>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>aaa-server host</b>	Enter AAA server host configuration mode so that you can configure AAA server parameters that are host-specific.
	<b>clear configure aaa-server</b>	Removes all AAA server configurations.
	<b>sdi-version</b>	Specifies the version of SDI to use for this host connection.
	<b>show running-config aaa-server</b>	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

<i>version</i>	Specify the version of SDI to use. Valid values are: <ul style="list-style-type: none"> <li><b>sdi-5</b>—SDI version 5.0 (default)</li> <li><b>sdi-pre-5</b>—SDI versions prior to 5.0</li> </ul>
----------------	---

## Defaults

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

## Command Modes

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

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

## 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
<b>aaa-server host</b>	Enter AAA server host configuration mode so that you can configure AAA server parameters that are host-specific.

---

<b>clear configure aaa-server</b>	Remove all AAA configurations.
<b>show running-config aaa-server</b>	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

---

# 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

<b>disable</b>	Disables secure unit authentication.
<b>enable</b>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				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**

<b>Command</b>	<b>Description</b>
<b>ip-phone-bypass</b>	Lets IP phones connect without undergoing user authentication. Secure unit authentication remains in effect.
<b>leap-bypass</b>	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.
<b>user-authentication</b>	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:

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

## Command History

Release	Modification
3.1(1)	This command was introduced. It moved from a keyword of the <b>nameif</b> 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 some 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 some 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 some 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 some 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
<b>clear local-host</b>	Resets all connections.
<b>interface</b>	Configures an interface and enters interface configuration mode.
<b>nameif</b>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				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
	<b>crypto ca trustpoint</b>	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

<i>port-number</i>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				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
<b>aaa-server host</b>	Configures host-specific AAA server parameters.

---

<b>clear configure aaa-server</b>	Removes all AAA-server configuration.
<b>show running-config aaa-server</b>	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 resetinbound

To send a reset to inbound TCP connections when they are denied, use the **service** 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:

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

## Command History

Release	Modification
1.1(1)	This command was introduced.

## Usage Guidelines

The **service** 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.

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
```

The following is the expected behavior of traffic on the FWSM 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.

### Examples

This example shows how to enable system services:

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

### Related Commands

Command	Description
<b>show running-config</b>	Displays the system services.
<b>service</b>	

# 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

<i>policymap_name</i>	A unique alphanumeric policy map identifier.
<b>global</b>	Applies the policy map to all interfaces.
<b>interface</b>	Applies the policy map to a specific interface
<i>intf</i>	The interface name defined in the <b>nameif</b> command.

## 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
3.1(1)	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

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

# set connection

To set the maximum TCP and UDP connections or to enable 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, thereby allowing unlimited connections, use the **no** form of this command.

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

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

## Syntax Description

<b>conn-max</b> <i>number</i>	Sets the maximum number of simultaneous TCP and UDP connections.
<b>disable</b>	Turns off TCP sequence number randomization.
<b>enable</b>	Turns on TCP sequence number randomization.
<b>random-seq#</b>	<p>Enables or disables TCP sequence number randomization. TCP initial sequence number randomization can be disabled if another in-line firewall is also randomizing the initial sequence numbers, because there is no need for both firewalls to be performing this action. However, leaving ISN randomization enabled on both firewalls does not affect the traffic.</p> <p>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 the outbound direction. If the connection is between two interfaces with the same security level, then the ISN will be randomized in the SYN in both directions.</p> <p>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.</p>

## Defaults

For the **conn-max** keyword, the default value of *number* 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		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	•	•	•	•	—

## Command History

Release	Modification
3.1(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** command to set connections for that class map.

**Note**

When you identify a **match access-list** command for the class map, then the **set connection** actions are performed separately for each ACE in the access list and not for the access list as a whole. For example, you match an access list with 2 ACEs such as the following, and apply a connection limit of 2 connections:

```
access-list testACL extended permit tcp host 10.2.1.1 any eq 21
access-list testACL extended permit tcp host 10.2.1.1 any eq 23
```

```
class-map testclass
  match access-list testACL
```

```
policy-map testpolicy
  class testclass
    set connection conn-max 2
```

The FWSM allows the creation of 2 connections for Telnet sessions (ACE 1) and 2 connections for FTP sessions (ACE 2).

**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 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 random-seq# disable
```

**Related Commands**

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

## set connection timeout

To configure the timeout period after which an embryonic, half-closed, or 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 {[embryonic hh:mm:ss] [half-closed hh:mm:ss] [tcp hh:mm:0]}
```

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

### Syntax Description

<b>embryonic</b> <i>hh:mm:ss</i>	Defines the timeout period in seconds until an 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 <b>set connection</b> command, you can set the timeout using this command.
<b>half-closed</b> <i>hh:mm:ss</i>	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. The FWSM does not send a reset when taking down half-closed connections.
<b>tcp</b> <i>hh:mm:ss</i>	Defines the idle time after which a TCP established connection closes, between 0:5:0 and 1092:15:0. The default is 0:60:0. You can also set the value to 0, which means the connection never times out.
<b>Note</b>	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 **tcp** connection timeout value is 60 minutes.

### Command Modes

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

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

### Command History

Release	Modification
3.1(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 timeout** command to set connection timeouts for that class map.

**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.

**Examples**

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

```
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 tcp 2:0:0
```

**Related Commands**

Command	Description
<b>class</b>	Identifies a class map in the policy map.
<b>class-map</b>	Creates a class map for use in a service policy.
<b>policy-map</b>	Configures a policy map that associates a class map and one or more actions.
<b>service-policy</b>	Assigns a policy map to an interface.
<b>set connection</b>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				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

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

# 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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				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
<b>match interface</b>	Distributes any routes that have their next hop out one of the interfaces specified,
<b>match ip next-hop</b>	Distributes any routes that have a next-hop router address that is passed by one of the access lists specified.
<b>route-map</b>	Defines the conditions for redistributing routes from one routing protocol into another.

# 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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple 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 <b>yes</b> or <b>no</b> . If you enter <b>yes</b> , the setup dialog continues. If <b>no</b> , the setup dialog stops and the global configuration prompt (hostname(config)#) appears.
Firewall Mode [Routed]:	Enter <b>routed</b> or <b>transparent</b> . 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 <b>yes</b> or <b>no</b> . If you enter <b>yes</b> , the inside interface is enabled and the requested configuration is written to the Flash partition.  If you enter <b>no</b> , the setup dialog repeats, beginning with the first question: Pre-configure Firewall now through interactive prompts [yes]?  Enter <b>no</b> to exit the setup dialog or <b>yes</b> 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
<b>asdm</b>	Configures the communication between the FWSM and a browser running the device manager.

# 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.
	<i>groupname</i>	(Optional) Shows statistics for servers in a group.
	<b>host</b> <i>hostname</i>	(Optional) Shows statistics for a particular server in the group.
	<b>protocol</b> <i>protocol</i>	(Optional) Shows statistics for servers of the specified protocol: <ul style="list-style-type: none"> <li>• <b>kerberos</b></li> <li>• <b>ldap</b></li> <li>• <b>nt</b></li> <li>• <b>radius</b></li> <li>• <b>sdi</b></li> <li>• <b>tacacs+</b></li> </ul>

## Defaults

By default, all AAA server statistics display.

## 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
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 <b>aaa-server</b> command.
Server Protocol	The server protocol for the server group specified by the <b>aaa-server</b> 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 <b>authentication-port</b> command. You can specify the RADIUS accounting port using the <b>accounting-port</b> command. For non-RADIUS servers, the port is set by the <b>server-port</b> command.
Server status	<p>The status of the server. You see one of the following values:</p> <ul style="list-style-type: none"> <li>ACTIVE—The FWSM will communicate with this AAA server.</li> <li>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.</li> </ul> <p>You also see the date and time of the last transaction in the following form:</p> <pre><b>Last transaction</b> ({<b>success</b>   <b>failure</b>}) at <i>time</i> <i>timezone</i> <i>date</i></pre> <p>If the FWSM has never communicated with the server, the message shows as the following:</p> <pre><b>Last transaction at Unknown</b></pre>
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: <ul style="list-style-type: none"> <li>The “authenticator” string in the RADIUS packet is corrupted (rare).</li> <li>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.</li> </ul> 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
<b>show running-config aaa-server</b>	Display statistics for all servers in the indicated server group or for a particular server.
<b>clear aaa-server statistics</b>	Clear the AAA server statistics.

# show aaa local user

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

`show aaa local user [locked]`

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

Defaults	No default behavior or values.
----------	--------------------------------

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

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

Command History	Release	Modification
	3.1(1)	This command was introduced.

Usage Guidelines	If you omit the optional keyword <b>locked</b> , 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 <b>show aaa local user</b> 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
<b>aaa local authentication attempts max-fail</b>	Configures the maximum number of times a user can enter a wrong password before being locked out.
<b>clear aaa local user fail-attempts</b>	Resets the number of failed attempts to 0 without modifying the lockout status.
<b>clear aaa local user lockout</b>	Clears the lockout status of the specified user or all users and sets their failed attempts counters to 0.

# 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	<i>id</i>	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:
---------------	---

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

Command History	Release	Modification
	1.1(1)	This command was introduced.

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 <b>show access-list</b> 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 hexadecimal identifier for each ACE at the end of each line.

### Related Commands

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				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 confirmation. 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: Oxyadayada Oxyadayada Oxyadayada
Oxyadayada Oxyadayada
```

```
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
<b>activation-key</b>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				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
<b>admin-context</b>	Sets the admin context.
<b>changeto</b>	Changes between contexts or the system execution space.
<b>clear configure context</b>	Removes all contexts.
<b>mode</b>	Sets the context mode to single or multiple.
<b>show context</b>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple 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.fcfc.8c4ad
  inside 10.86.194.168 000c.ce6f.9b7e
```

### Related Commands

Command	Description
<b>arp</b>	Adds a static ARP entry.
<b>arp-inspection</b>	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
<b>clear arp statistics</b>	Clears ARP statistics.
<b>show arp statistics</b>	Shows ARP statistics.
<b>show running-config arp</b>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple 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
	<b>arp</b>	Adds a static ARP entry.
	<b>arp-inspection</b>	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
	<b>clear arp statistics</b>	Clears ARP statistics.
	<b>show arp statistics</b>	Shows ARP statistics.
	<b>show running-config arp</b>	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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple 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
<b>arp-inspection</b>	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
<b>clear arp statistics</b>	Clears ARP statistics and resets the values to zero.
<b>show arp</b>	Shows the ARP table.
<b>show running-config arp</b>	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	
<b>asdmclient</b>	(Optional) Displays the ASDM history data formatted for the ASDM client.
<b>feature</b> <i>feature</i>	(Optional) Limits the history display to the specified feature. The following are valid values for the <i>feature</i> argument: <ul style="list-style-type: none"> <li>• <b>all</b>—Displays the history for all features (default).</li> <li>• <b>blocks</b>—Displays the history for the system buffers.</li> <li>• <b>cpu</b>—Displays the history for CPU usage.</li> <li>• <b>failover</b>—Displays the history for failover.</li> <li>• <b>ids</b>—Displays the history for IDS.</li> <li>• <b>interface</b> <i>if_name</i>—Displays the history for the specified interface. The <i>if_name</i> argument is the name of the interface as specified by the <b>nameif</b> command.</li> <li>• <b>memory</b>—Displays memory usage history.</li> <li>• <b>perfmon</b>—Displays performance history.</li> <li>• <b>sas</b>—Displays the history for Security Associations.</li> <li>• <b>tunnels</b>—Displays the history for tunnels.</li> <li>• <b>xlates</b>—Displays translation slot history.</li> </ul>
<b>snapshot</b>	(Optional) Displays only the last ASDM history data point.
<b>view</b> <i>timeframe</i>	(Optional) Limits the history display to the specified time period. Valid values for the <i>timeframe</i> argument are: <ul style="list-style-type: none"> <li>• <b>all</b>—all contents in the history buffer (default).</li> <li>• <b>12h</b>—12 hours</li> <li>• <b>5d</b>—5 days</li> <li>• <b>60m</b>—60 minutes</li> <li>• <b>10m</b>—10 minutes</li> </ul>

## 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
1.1(1)	This command was introduced (as <b>show pdm history</b> ).
3.1(1)	This command was changed from the <b>show pdm history</b> command to the <b>show asdm history</b> 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 0
Underruns:
[ 10s:12:46:41 Mar 1 2005 ] 0 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 0
Collisions:
[ 10s:12:46:41 Mar 1 2005 ] 0 0 0 0 0 0 0 0
LCOLL:
[ 10s:12:46:41 Mar 1 2005 ] 0 0 0 0 0 0 0 0
Reset:
[ 10s:12:46:41 Mar 1 2005 ] 0 0 0 0 0 0 0 0
Deferred:
[ 10s:12:46:41 Mar 1 2005 ] 0 0 0 0 0 0 0 0
Lost Carrier:
[ 10s:12:46:41 Mar 1 2005 ] 0 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 0
Hardware Output Queue:
[ 10s:12:46:41 Mar 1 2005 ] 0 0 0 0 0 0 0 0
Software Output Queue:
[ 10s:12:46:41 Mar 1 2005 ] 0 0 0 0 0 0 0 0
Drop KPacket Count:
[ 10s:12:46:41 Mar 1 2005 ] 0 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|751|751|751|751|751|751|751|751|751|751|751|7
51|751|751|751|751|751|752|752|752|752|752|752|752|752|752|752|752|752|752|752|752|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|56|56|56|56|56|56|56|56|56|
MH|IBR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|7127|5155|6202|3545|5408|3979|4
381|9492|3033|4962|4571|4226|3760|5923|3265|6494|3441|3542|3162|4076|4744|2726|4847|4292|5
401|5166|3735|6659|3837|5260|4186|5728|4932|4515|3764|2843|3397|10768|3080|6309|5969|4472|
2780|4492|3540|3664|3800|3002|6258|5567|4044|4059|4548|3713|3265|4159|3630|8235|6934|4298|
MH|OBR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|82791|57|1410|588|57|639|0|4698
|5068|4992|6495|3292|3292|3352|5061|4808|5205|3931|3298|3349|5064|3439|3356|3292|3343|3349
|5067|3883|3356|4500|3301|3349|5212|3298|3349|3292|7316|116896|5072|3881|3356|3931|3298|33
49|5064|3292|3349|3292|3292|3349|5061|3883|3356|3931|3452|3356|5064|3292|3349|3292|
MH|IPR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|12|8|6|5|7|5|6|14|5|7|7|5|6|9|5
|8|6|5|5|7|6|5|6|5|6|7|6|8|6|6|6|8|6|7|6|4|5|19|5|8|7|6|4|7|5|6|6|5|7|8|6|6|7|5|5|7|6|9|7|
6|
MH|OPR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|12|0|1|0|0|0|0|4|0|2|2|0|0|0|0|
1|1|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
|

```



```
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
L呢COLL: [ 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
L呢COLL: [ 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 Authorization 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
<b>asdm history enable</b>	Enables ASDM history tracking.

---

# 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:

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

### Command History

Release	Modification
1.1(1)	This command was introduced (as <b>show pdm sessions</b> ).
3.1(1)	This command was changed from the <b>show pdm sessions</b> command to the <b>show asdm sessions</b> 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
<b>asdm disconnect</b>	Terminates an active ASDM session.