CHAPTER 2

aaa accounting command through accounting-server-group Commands

aaa accounting command

To send accounting messages to the TACACS+ accounting server when you enter any command other than **show** commands at the CLI, use the **aaa accounting command** command in global configuration mode. To disable support for command accounting, use the **no** form of this command.

aaa accounting command [**privilege** *level*] *server-tag*

no aaa accounting command [**privilege** *level*] *server-tag*

Syntax Description

privilege *level*	If you customize the command privilege level using the **privilege** command, you can limit which commands the FWSM accounts for by specifying a minimum privilege level. The FWSM does not account for commands that are below the minimum privilege level. **Note** If you enter a deprecated command and enabled the **privilege** keyword, then the FWSM does not send accounting information for the deprecated command. If you want to account for deprecated commands, be sure to disable the **privilege** keyword. Many deprecated commands are still accepted at the CLI, and are often converted into the currently-accepted command at the CLI; they are not included in CLI help or this guide.
server-tag	Specifies the server or group of TACACS+ servers to which accounting records are sent, as specified by the **aaa-server protocol** command.

Defaults

The default privilege level is 0.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

When you configure the **aaa accounting command** command, each command other than **show** commands entered by an administrator is recorded and sent to the accounting server or servers.

Examples

The following example specifies that accounting records will be generated for any supported command, and that these records are sent to the server from the group named adminserver.

```
hostname(config)# aaa accounting command adminserver
```

Related Commands

Command	Description
aaa accounting	Enables or disables TACACS+ or RADIUS user accounting (on a server designated by the **aaa-server** command).
clear configure aaa	Remove/reset the configured AAA accounting values.
show running-config aaa	Display the AAA configuration.

aaa accounting console

To enable support for AAA accounting for administrative access, use the **aaa accounting console** command in global configuration mode. To disable support for accounting for administrative access, use the **no** form of this command.

aaa accounting {telnet | ssh | enable} console *server-tag*

no aaa accounting {telnet | ssh | enable} console *server-tag*

Syntax Description

enable	Enables accounting records to mark the entry to and exit from privileged EXEC mode.
server-tag	Specifies the server or group of servers to which accounting records are sent. Valid server group protocols are RADIUS and TACACS+. You must specify the name of the server group, previously specified in an **aaa-server** command.
ssh	Enables accounting records to mark the establishment and termination of admin sessions created over SSH.
telnet	Enables accounting records to mark the establishment and termination of admin sessions created over Telnet. This command does not account for sessions from the switch to the FWSM (system execution space).s

Defaults

By default, AAA accounting for administrative access 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
Global configuration	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced on the FWSM.
2.2(1)	This command was modified to support fallback to LOCAL.

Usage Guidelines

Sessions from the switch to the FWSM are not accounted for in the admin context, even if you have Telnet authentication enabled.

Examples

The following example specifies that accounting records will be generated for enable access, and that these records are sent to the server named adminserver.

```
hostname(config)# aaa accounting enable console adminserver
```

Related Commands

Command	Description
aaa accounting match	Enables or disables TACACS+ or RADIUS user accounting.
aaa accounting command	Specifies that each command, or commands of a specified privilege level or higher, entered by an administrator/user is recorded and sent to the accounting server or servers.
clear configure aaa	Removes/resets the configured AAA accounting values.
show running-config aaa	Display the AAA configuration.

aaa accounting include, exclude

To enable accounting for connections through the FWSM, use the **aaa accounting include** command in global configuration mode. To exclude addresses from accounting, use the **aaa accounting exclude** command. To disable accounting, use the **no** form of this command.

aaa accounting {**include** | **exclude**} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

no aaa accounting {**include** | **exclude**} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

Syntax Description

exclude	Excludes the specified service and address from accounting if it was already specified by an **include** command.
include	Specifies the services and IP addresses that require accounting. Traffic that is not specified by an **include** statement is not processed.
inside_ip	Specifies the IP address on the higher security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the destination address. If you apply the command to the higher security interface, then this address is the source address. Use 0 to mean all hosts.
inside_mask	Specifies the network mask for the inside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
interface_name	Specifies the interface name from which users require accounting.
outside_ip	(Optional) Specifies the IP address on the lower security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the source address. If you apply the command to the higher security interface, then this address is the destination address. Use 0 to mean all hosts.
outside_mask	(Optional) Specifies the network mask for the outside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
server_tag	Specifies the AAA server group defined by the **aaa-server host** command.
service	Specifies the services that require accounting. You can specify one of the following values: • **any** or **tcp/0** (specifies all TCP traffic) • **ftp** • **http** • **https** • **ip** • **ssh** • **telnet** • **tcp/***port* • **udp/***port*

Defaults

By default, AAA accounting for administrative access 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
Global configuration	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The FWSM can send accounting information to a RADIUS or TACACS+ server about any TCP or UDP traffic that passes through the FWSM. If that traffic is also authenticated, then the AAA server can maintain accounting information by username. If the traffic is not authenticated, the AAA server can maintain accounting information by IP address. Accounting information includes when sessions start and stop, username, the number of bytes that pass through the FWSM for the session, the service used, and the duration of each session.

Before you can use this command, you must first designate a AAA server with the **aaa-server** command.

To enable accounting for traffic that is specified by an access list, use the **aaa accounting match** command. You cannot use the **match** command in the same configuration as the **include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

You cannot use the **aaa accounting include** and **exclude** commands between same-security interfaces. For that scenario, you must use the **aaa accounting match** command.

Examples

The following example enables accounting on all TCP connections:

```
hostname(config)# aaa-server mygroup protocol tacacs+
hostname(config)# aaa-server mygroup (inside) host 192.168.10.10 thekey timeout 20
hostname(config)# aaa accounting include any inside 0 0 0 0 mygroup
```

Related Commands

Command	Description
aaa accounting match	Enables accounting for traffic specified by an access list.
aaa accounting command	Enables accounting of administrative access.
aaa-server host	Configures the AAA server.
clear configure aaa	Clears the AAA configuration.
show running-config aaa	Displays the AAA configuration.

aaa accounting match

To enable accounting for TCP and UDP connections through the FWSM, use the **aaa accounting match** command in global configuration mode. To disable accounting for traffic, use the **no** form of this command.

aaa accounting match *acl_name interface_name server_tag*

no aaa accounting match *acl_name interface_name server_tag*

Syntax Description

acl_name	Specifies the traffic that requires accounting my matching an **access-list** name. Permit entries in the access list are accounted, while deny entries are exempt from accounting. This command is only supported for TCP and UDP traffic. A warning message is displayed if you enter this command and it references an access list that permits other protocols.
interface_name	Specifies the interface name from which users require accounting.
server_tag	Specifies the AAA server group tag defined by the **aaa-server** command.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The FWSM can send accounting information to a RADIUS or TACACS+ server about any TCP or UDP traffic that passes through the FWSM. If that traffic is also authenticated, then the AAA server can maintain accounting information by username. If the traffic is not authenticated, the AAA server can maintain accounting information by IP address. Accounting information includes when sessions start and stop, username, the number of bytes that pass through the FWSM for the session, the service used, and the duration of each session.

Before you can use this command, you must first designate a AAA server with the **aaa-server** command.

Accounting information is sent only to the active server in a server group unless you enable simultaneous accounting using the **accounting-mode** command in aaa-server protocol configuration mode.

You cannot use the **aaa accounting match** command in the same configuration as the **aaa accounting include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

Examples

The following example enables accounting for traffic matching a specific access list acl2:

```
hostname(config)# access-list acl12 extended permit tcp any any
hostname(config)# aaa accounting match acl2 outside radserver1
```

Related Commands

Command	Description
aaa accounting include, exclude	Enables accounting by specifying the IP addresses directly in the command.
access-list extended	Creates an access list.
clear configure aaa	Removes AAA configuration.
show running-config aaa	Displays the AAA configuration.

aaa authentication challenge disable

To disable authentication challenge for FTP, Telnet, HTTP, or HTTPS, use the **aaa authentication challenge disable** command in global configuration mode. To reset the FWSM to default authentication, use the **no** form of this command.

aaa authentication {**ftp | telnet | http | https** } **challenge disable**

no aaa authentication {**ftp | telnet | http | https** } **challenge disable**

Syntax Description

ftp	Disables the authentication challenge for FTP connections.
http	Disables the authentication challenge for HTTP connections.
https	Disables the authentication challenge for HTTPS connections.
telnet	Disables the authentication challenge for Telnet connections.

Defaults

By default, if you enable authentication using the **aaa authentication match** or **aaa authentication** [**include | exclude**] commands, authentication challenge is enabled for FTP, Telnet, HTTP, and HTTPS.

Command Modes

The 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

You can configure whether the FWSM challenges users for a username and password. By default, the FWSM prompts the user when a AAA rule enforces authentication for traffic in a new session and the protocol of the traffic is FTP, Telnet, HTTP, or HTTPS. In some cases, you may want to disable the authentication challenge for one or more of these protocols. You can use the **aaa authentication challenge** command to do so.

If you disable challenge authentication for a particular protocol, traffic using that protocol is allowed only if the traffic belongs to a session previously authenticated. This authentication can be accomplished by traffic using a protocol whose authentication challenge remains enabled. For example, if you disable challenge authentication for FTP, the FWSM denies a new session using FTP if the traffic is included in an authentication rule. If the user establishes the session with a protocol whose authentication challenge is enabled (such as HTTP), FTP traffic is allowed.

Examples

The following example permits inbound access to a TCP IP address in the range of 209.165.201.1 through 209.165.201.30 indicated by the 209.165.201.0 network address (subnet mask 255.255.255.224). All services are permitted by the **access-list** command, and the **aaa authentication** command requires authentication. The authentication server is at IP address 10.16.1.20 on the inside interface. The final command disables challenge authentication for FTP, which means that users whose sessions are identifed by the **aaa authentication include** command must be authenticated by Telnet, HTTP, or HTTPS, and not by FTP.

```
hostname(config)# aaa-server AuthIn protocol tacacs+
hostname(config)# aaa-server AuthIn (inside) host 10.16.1.20 thisisakey timeout 20
hostname(config)# access-list acl-out permit tcp 10.16.1.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-group acl-out in interface outside
hostname(config)# aaa authentication include tcp inside 0 0 0 0 AuthIn
hostname(config)# aaa authentication ftp challenge disable
```

Related Commands

Command	Description
aaa authentication	Enables or disables authentication by including or excluding traffic.
aaa authentication match	Specifies the name of an access list, previously defined in an access-list command, that must be matched, and then provides authentication for that match.
aaa authentication secure-http-client	Provides a secure method for user authentication to the FWSM prior to allowing HTTP requests to traverse the FWSM.
aaa-server protocol	Configures group-related server attributes.
aaa-server host	Configures host-related attributes.

aaa authentication clear-conn

To force any active connections to close immediately after the user authentication times out or when you clear the authentication session with the **clear uauth** command, use the **aaa authentication clear-conn** command in global configuration mode. To disable this feature, use the **no** form of this command. Without this command, active connections are not terminated even though the user authentication session expired.

aaa authentication clear-conn *interface-name source_ip source_mask*

no aaa authentication clear-conn *interface-name source_ip source_mask*

Syntax Description

interface-name	Sets the interface name connected to the source IP address.
source_ip	Specifies the source IP address of the user for which you want to terminate connections.
source_mask	Specifies the source IP subnet mask.

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
3.2(1)	This command was introduced.

Usage Guidelines

To set the authentication timeout values, see the **timeout uauth** command.

When a connection is ended because of this command, system log message 109036 is generated.

Examples

The following example authenticates users on the inside interface from the 10.0.0.0/24 network when they access 192.168.2.0/24. These same user connections are terminated when their authentication times out.

```
hostname(config)# access-list mylist permit tcp 10.0.0.0 255.255.255.0 192.168.2.0
255.255.255.0
hostname(config)# aaa authentication mylist inside radius1
hostname(config)# aaa authentication clear-conn inside 10.0.0.0 255.255.255.0
```

Related Commands

Command	Description
aaa authentication match	Enables authentication for traffic through the FWSM.
clear configure aaa	Removes AAA configuration.
clear uauth	Clears the authentication sessions.
show running-config aaa	Displays the AAA configuration.
timeout uauth	Sets the timeout for the authentication sessions.

aaa authentication console

To authenticate users who access the FWSM CLI over an SSH, HTTP (ASDM), or Telnet connection, or to authenticate users who access privileged EXEC mode using the **enable** command, use the **aaa authentication console** command in global configuration mode. To disable authentication, use the **no** form of this command.

aaa authentication {**enable | telnet | ssh | http**} **console** {**LOCAL** | *server_group* [**LOCAL**]}

no aaa authentication {**enable | telnet | ssh | http**} **console** {**LOCAL** | *server_group* [**LOCAL**]}

Syntax Description

enable	Authenticates users who access privileged EXEC mode when they use the **enable** command.
http	Authenticates ASDM users who access the FWSM over HTTPS. You only need to configure HTTPS authentication if you want to use a RADIUS or TACACS+ server. By default, ASDM uses the local database for authentication even if you do not configure this command.

LOCAL	Uses the local database for authentication. **LOCAL** is case sensitive. If the local database is empty, the following warning message appears:
	`Warning:local database is empty! Use 'username' command to define local users.`
	If the local database becomes empty when **LOCAL** is still present in the configuration, the following warning message appears:
	`Warning:Local user database is empty and there are still commands using 'LOCAL' for authentication.`

server_group [**LOCAL**]	Specifies the AAA server group tag defined by the **aaa-server** command. You can use a RADIUS or TACACS+ server group. If you use the **LOCAL** keyword in addition to the *server_group*, you can configure the FWSM to use the local database as a fallback method if the AAA server is unavailable. **LOCAL** is case sensitive. We recommend that you use the same username and password in the local database as the AAA server because the FWSM prompt does not give any indication which method is being used.
ssh	Authenticates users who access the FWSM using SSH.
telnet	Authenticates users who access the FWSM using Telnet. If you enter this command in the admin context in multiple context mode, then authentication also applies to sessions from the switch to the FWSM (which enters the system execution space). You cannot enter any AAA commands directly in the system execution space.

Defaults

By default, fallback to the local database is disabled.

If the **aaa authentication telnet console** command is not defined, you can gain access to the FWSM CLI with the FWSM login password (set with the **password** command). If you enter the **aaa authentication telnet console** command in the admin context in multiple context mode, then authentication also applies to sessions from the switch to the FWSM (which enters the system execution space). You cannot enter any AAA commands directly in the system execution space.

If a **aaa authentication http console** command is not defined, you can gain access to the FWSM (via ASDM) with no username and the FWSM enable password (set with the **enable password** command). If the **aaa** commands are defined, but the HTTP authentication requests a time out, which implies the AAA servers might be down or not available, you can gain access to the FWSM using the default administrator username and the enable password. By default, the enable password is not set.

If a **aaa authentication ssh console** command is not defined, you can gain access to the FWSM CLI with the username **pix** and with the FWSM enable password (set with the **enable password** command). By default, the enable password is blank. This behavior differs from when you log into the FWSM without AAA configured; in that case, you use the login password (set by the **passwd** command).

Command Modes

The 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.
2.2(1)	This command was modified to support fallback to LOCAL.
3.2(1)	Support for Telnet authentication (sessioning from the switch to the FWSM) was added for the system execution space when you configure this command in the admin context.

Usage Guidelines

Before the FWSM can authenticate a Telnet or SSH user, you must first configure access to the FWSM using the **telnet** or **ssh** commands. These commands identify the IP addresses that are allowed to communicate with the FWSM. The exception is for access to the system in multiple context mode; a session from the switch to the FWSM is a Telnet session, but the **telnet** command is not required.

After you connect to the FWSM, you log in and access user EXEC mode.

- If you do not enable any authentication for Telnet, you do not enter a username; you enter the login password (set with the **password** command). For SSH, you enter “pix” as the username, and enter the login password.
- If you enable Telnet or SSH authentication according to this section, you enter the username and password as defined on the AAA server or local user database.

To enter privileged EXEC mode, enter the **enable** command or the **login** command (if you are using the local database only).

- If you do not configure enable authentication, enter the system enable password when you enter the **enable** command (set by the **enable password** command). However, if you do not use enable authentication, after you enter the **enable** command, you are no longer logged in as a particular user. To maintain your username, use enable authentication.
- If you configure enable authentication, the FWSM prompts you for your username and password.

For authentication using the local database, you can use the **login** command, which maintains the username but requires no configuration to turn on authentication.

By default, you can log in to ASDM with a blank username and the enable password set by the **enable password** command. However, if you enter a username and password at the login screen (instead of leaving the username blank), ASDM checks the local database for a match.

Although you can configure HTTP authentication using this command and specify the local database, that functionality is always enabled by default. You should only configure HTTP authentication if you want to use a RADIUS or TACACS+ server for authentication. The maximum username prompt for HTTP authentication is 30 characters. The maximum password length is 16 characters.

In multiple context mode, you cannot configure any AAA commands in the system configuration. However, if you configure Telnet authentication in the admin context, then authentication also applies to sessions from the switch to the FWSM (which enters the system execution space).

As the following table shows, the action of the prompts for authenticated access to the FWSM CLI differ, depending on the option you choose with the **aaa authentication console** command.

Option	Number of Login Attempts Allowed
enable	3 tries before access is denied
ssh	3 tries before access is denied
telnet	Continual until success
http	Continual until success

Examples

The following example shows use of the **aaa authentication console** command for a Telnet connection to a RADIUS server with the server tag “radius”:

```
hostname(config)# aaa authentication telnet console radius
```

The following example identifies the server group “AuthIn” for enable authentication:

```
hostname(config)# aaa authentication enable console AuthIn
```

The following example shows use of the **aaa authentication console** command with fallback to the LOCAL user database if all the servers in the group “svrgrp1” fail:

```
hostname(config)# aaa-server svrgrp1 protocol tacacs
hostname(config)# aaa authentication ssh console svrgrp1 LOCAL
```

Related Commands

Command	Description
aaa authentication match	Enables user authentication.
aaa-server host	Specifies the AAA server to use for user authentication.
clear configure aaa	Clears the AAA configuration.
show running-config aaa	Displays the AAA configuration.

aaa authentication include, exclude

To enable authentication for connections through the FWSM, use the **aaa authentication include** command in global configuration mode. To exclude addresses from authentication, use the **aaa authentication exclude** command. To disable authentication, use the **no** form of this command.

aaa authentication {include | exclude} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] {*server_tag* | **LOCAL**}

no aaa authentication {include | exclude} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

Syntax Description

exclude	Excludes the specified service and address from authentication if it was already specified by an **include** command.
include	Specifies the services and IP addresses that require authentication. Traffic that is not specified by an **include** statement is not processed.
inside_ip	Specifies the IP address on the higher security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the destination address. If you apply the command to the higher security interface, then this address is the source address. Use 0 to mean all hosts.
inside_mask	Specifies the network mask for the inside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
interface_name	Specifies the interface name from which users require authentication.
LOCAL	Specifies the local user database.
outside_ip	(Optional) Specifies the IP address on the lower security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the source address. If you apply the command to the higher security interface, then this address is the destination address. Use 0 to mean all hosts.
outside_mask	(Optional) Specifies the network mask for the outside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.

server_tag	Specifies the AAA server group defined by the **aaa-server** command.
service	Specifies the services that require authentication. You can specify one of the following values: • **any** or **tcp/0** (specifies all TCP traffic) • **ftp** • **http** • **https** • **ip** • **ssh** • **telnet** • **tcp/***port* • **udp/***port* • **icmp/***type* • *protocol*[**/***port*] Although you can configure the FWSM to require authentication for network access to any protocol or service, users can authenticate directly with HTTP, HTTPS, Telnet, or FTP only. A user must first authenticate with one of these services before the FWSM allows other traffic requiring authentication. See "Usage Guidelines" for more information.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

To enable authentication for traffic that is specified by an access list, use the **aaa authentication match** command. You cannot use the **match** command in the same configuration as the **include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

You cannot use the **aaa authentication include** and **exclude** commands between same-security interfaces. For that scenario, you must use the **aaa authentication match** command.

TCP sessions might have their sequence numbers randomized even if you disable sequence randomization. This occurs when a AAA server proxies the TCP session to authenticate the user before permitting access.

For HTTP, when you need to use a separate username and password for the AAA server and for the destination web server, use the **virtual http** command.

One-Time Authentication

A user at a given IP address only needs to authenticate one time for all rules and types, until the authentication session expires. (See the **timeout uauth** command for timeout values.) For example, if you configure the FWSM to authenticate Telnet and FTP, and a user first successfully authenticates for Telnet, then as long as the authentication session exists, the user does not also have to authenticate for FTP.

For HTTP or HTTPS authentication, once authenticated, a user never has to reauthenticate, no matter how low the **timeout uauth** command is set, because the browser caches the string "Basic=Uuhjksdkfhk==" in every subsequent connection to that particular site. This can be cleared only when the user exits *all* instances of the web browser and restarts. Flushing the cache is of no use.

Applications Required to Receive an Authentication Challenge

Although you can configure the FWSM to require authentication for network access to any protocol or service, users can authenticate directly with HTTP, HTTPS, Telnet, or FTP only. A user must first authenticate with one of these services before the FWSM allows other traffic requiring authentication.

The authentication ports that the FWSM supports for AAA are fixed:

- Port 21 for FTP
- Port 23 for Telnet
- Port 80 for HTTP
- Port 443 for HTTPS

For Telnet and FTP, the FWSM generates an authentication prompt. After you authenticate correctly, the FWSM redirects you to your original destination. If the destination server also has its own authentication, you enter another username and password.

For HTTP, you log in using basic HTTP authentication supplied by the browser. For HTTPS, the FWSM generates custom login windows.

Note If you use HTTP authentication without using the **aaa authentication secure-http-client** command, the username and password are sent from the client to the FWSM in clear text. We recommend that you use the **aaa authentication secure-http-client** command whenever you enable HTTP authentication.

For FTP, a user has the option of entering the FWSM username followed by an at sign (@) and then the FTP username (name1@name2). For the password, the user enters the FWSM password followed by an at sign (@) and then the FTP password (password1@password2). For example, enter the following text.

```
name> jang@jgray
password> letmein@he110
```

This feature is useful when you have cascaded firewalls that require multiple logins. You can separate several names and passwords by multiple at signs (@).

The number of login attempts allowed differs between the supported protocols:

Protocol	Number of Login Attempts Allowed
FTP	Incorrect password causes the connection to be dropped immediately.
HTTP HTTPS	Continual reprompting until successful login.
Telnet	4 tries before dropping the connection.

Static PAT and HTTP

For HTTP authentication, the FWSM checks real ports when static PAT is configured. If it detects traffic destined for real port 80, regardless of the mapped port, the FWSM intercepts the HTTP connection and enforces authentication.

For example, assume that outside TCP port 889 is translated to port 80 (www) and that any relevant access lists permit the traffic:

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask 255.255.255.255
```

Then when users try to access 10.48.66.155 on port 889, the FWSM intercepts the traffic and enforces HTTP authentication. Users see the HTTP authentication page in their web browsers before the FWSM allows HTTP connection to complete.

If the local port is different than port 80, as in the following example:

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask 255.255.255.255
```

Then users do not see the authentication page. Instead, the FWSM sends to the web browser an error message indicating that the user must be authenticated prior using the requested service.

Authenticating Directly with the FWSM

If you do not want to allow HTTP(S), Telnet, or FTP through the FWSM but want to authenticate other types of traffic, you can configure virtual Telnet or virtual SSH. With virtual Telnet or SSH, the user connects using Telnet or SSH to a given IP address configured on the FWSM, and the FWSM provides a prompt. See the **virtual telnet** and **virtual ssh** commands.

Examples

The following example includes for authentication TCP traffic on the outside interface, with an inside IP address of 192.168.0.0 and a netmask of 255.255.0.0, with an outside IP address of all hosts, and using a server named “tacacs+”. The second command line excludes Telnet traffic on the outside interface with a local address of 192.168.38.0, with a remote/foreign IP address of all hosts:

```
hostname(config)# aaa authentication include tcp outside 192.168.0.0 255.255.0.0 0.0.0.0
0.0.0.0 tacacs+
hostname(config)# aaa authentication exclude telnet outside 192.168.38.0 255.255.255.0
0.0.0.0 0.0.0.0 tacacs+
```

Example 2:

The following examples demonstrate ways to use the *interface-name* parameter. The FWSM has an inside network of 192.168.1.0, an outside network of 209.165.201.0 (subnet mask 255.255.255.224), and a perimeter network of 209.165.202.128 (subnet mask 255.255.255.224).

This example enables authentication for connections originated from the inside network to the outside network:

```
hostname(config)# aaa authentication include tcp inside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

Example 3:

This example enables authentication for connections originated from the inside network to the perimeter network:

```
hostname(config)#aaa authentication include tcp inside 192.168.1.0 255.255.255.0
209.165.202.128 255.255.255.224 tacacs+
```

Example 4:

This example enables authentication for connections originated from the outside network to the inside network:

```
hostname(config)# aaa authentication include tcp outside 209.165.201.0 255.255.255.224
192.168.1.0 255.255.255.0 tacacs+
```

Example 5:

This example enables authentication for connections originated from the outside network to the perimeter network:

```
hostname(config)# aaa authentication include tcp outside 209.165.201.0 255.255.255.224
209.165.202.128 255.255.255.224 tacacs+
```

Example 6:

This example enables authentication for connections originated from the perimeter network to the outside network:

```
hostname(config)#aaa authentication include tcp inside 209.165.202.128 255.255.255.224
209.165.201.0 255.255.255.224 tacacs+
```

Example 7:

This example specifies that IP addresses 10.0.0.1 through 10.0.0.254 must be authenticated by the FWSM when establishing connections through the outside interface. In this example, the first **aaa authentication** command requires authentication of all FTP, HTTP, and Telnet sessions. The second **aaa authentication** command lets host 10.0.0.42 start outbound connections without being authenticated. This example uses a server group named **tacacs+**.

```
hostname(config)# nat (inside) 1 10.0.0.0 255.255.255.0
hostname(config)# aaa authentication include tcp inside 0 0 tacacs+
hostname(config)# aaa authentication exclude tcp inside 10.0.0.42 255.255.255.255 tacacs+
```

Example 8:

This example permits inbound access to a TCP IP address in the range of 209.165.201.1 through 209.165.201.30 indicated by the 209.165.201.0 network address (subnet mask 255.255.255.224). All services are permitted by the **access-list** command, and the **aaa authentication** command requires authentication on HTTP. The authentication server is at IP address 10.16.1.20 on the inside interface.

```
hostname(config)# aaa-server AuthIn protocol tacacs+
hostname(config)# aaa-server AuthIn (inside) host 10.16.1.20 thisisakey timeout 20
hostname(config)# access-list acl-out permit tcp 10.16.1.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-group acl-out in interface outside
hostname(config)# aaa authentication include http inside 0 0 0 0 AuthIn
```

Related Commands

Command	Description
aaa authentication console	Enables or disables authentication on entry to privileged mode or requires authentication verification to access the FWSM via the specified type of connection.
aaa authentication match	Specifies the name of an access list, previously defined in an **access-list** command, that must be matched, and then provides authentication for that match.
aaa authentication secure-http-client	Provides a secure method for user authentication to the FWSM prior to allowing HTTP requests to traverse the FWSM.
aaa-server protocol	Configures group-related server attributes.
aaa-server host	Configures host-related attributes.

aaa authentication match

To enable authentication for connections through the FWSM, use the **aaa authentication match** command in global configuration mode. To disable authentication, use the **no** form of this command.

aaa authentication match *acl_name interface_name* {*server_tag* | **LOCAL**}

no aaa authentication match *acl_name interface_name* {*server_tag* | **LOCAL**}

Syntax Description

acl_name	Specifies an extended access list name.
interface_name	Specifies the interface name from which to authenticate users.
LOCAL	Specifies the local user database.
server_tag	Specifies the AAA server group tag defined by the **aaa-server** command.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

You cannot use the **aaa authentication match** command in the same configuration as the **include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

TCP sessions might have their sequence numbers randomized even if you disable sequence randomization. This occurs when a AAA server proxies the TCP session to authenticate the user before permitting access.

For HTTP, when you need to use a separate username and password for the AAA server and for the destination web server, use the **virtual http** command.

One-Time Authentication

A user at a given IP address only needs to authenticate one time for all rules and types, until the authentication session expires. (See the **timeout uauth** command for timeout values.) For example, if you configure the FWSM to authenticate Telnet and FTP, and a user first successfully authenticates for Telnet, then as long as the authentication session exists, the user does not also have to authenticate for FTP.

For HTTP or HTTPS authentication, once authenticated, a user never has to reauthenticate, no matter how low the **timeout uauth** command is set, because the browser caches the string "Basic=Uuhjksdkfhk==" in every subsequent connection to that particular site. This can be cleared only when the user exits *all* instances of the web browser and restarts. Flushing the cache is of no use.

Applications Required to Receive an Authentication Challenge

Although you can configure the FWSM to require authentication for network access to any protocol or service, users can authenticate directly with HTTP, HTTPS, Telnet, or FTP only. A user must first authenticate with one of these services before the FWSM allows other traffic requiring authentication.

The authentication ports that the FWSM supports for AAA are fixed:

- Port 21 for FTP
- Port 23 for Telnet
- Port 80 for HTTP
- Port 443 for HTTPS

For Telnet and FTP, the FWSM generates an authentication prompt. After you authenticate correctly, the FWSM redirects you to your original destination. If the destination server also has its own authentication, you enter another username and password.

For HTTP, you log in using basic HTTP authentication supplied by the browser. For HTTPS, the FWSM generates custom login windows.

Note If you use HTTP authentication without using the **aaa authentication secure-http-client** command, the username and password are sent from the client to the FWSM in clear text. We recommend that you use the **aaa authentication secure-http-client** command whenever you enable HTTP authentication.

For FTP, a user has the option of entering the FWSM username followed by an at sign (@) and then the FTP username (name1@name2). For the password, the user enters the FWSM password followed by an at sign (@) and then the FTP password (password1@password2). For example, enter the following text.

```
name> jang@jgray
password> letmein@he110
```

This feature is useful when you have cascaded firewalls that require multiple logins. You can separate several names and passwords by multiple at signs (@).

The number of login attempts allowed differs between the supported protocols:

Protocol	Number of Login Attempts Allowed
FTP	Incorrect password causes the connection to be dropped immediately.
HTTP HTTPS	Continual reprompting until successful login.
Telnet	4 tries before dropping the connection.

Static PAT and HTTP

For HTTP authentication, the FWSM checks real ports when static PAT is configured. If it detects traffic destined for real port 80, regardless of the mapped port, the FWSM intercepts the HTTP connection and enforces authentication.

For example, assume that outside TCP port 889 is translated to port 80 (www) and that any relevant access lists permit the traffic:

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask 255.255.255.255
```

Then when users try to access 10.48.66.155 on port 889, the FWSM intercepts the traffic and enforces HTTP authentication. Users see the HTTP authentication page in their web browsers before the FWSM allows HTTP connection to complete.

If the local port is different than port 80, as in the following example:

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask 255.255.255.255
```

Then users do not see the authentication page. Instead, the FWSM sends to the web browser an error message indicating that the user must be authenticated prior using the requested service.

Authenticating Directly with the FWSM

If you do not want to allow HTTP(S), Telnet, or FTP through the FWSM but want to authenticate other types of traffic, you can configure virtual Telnet or virtual SSH. With virtual Telnet or SSH, the user connects using Telnet or SSH to a given IP address configured on the FWSM, and the FWSM provides a prompt. See the **virtual telnet** and **virtual ssh** commands.

Examples

The following set of examples illustrates how to use the **aaa authentication match** command:

```
hostname(config)# show access-list
access-list mylist permit tcp 10.0.0.0 255.255.255.0 192.168.2.0 255.255.255.0 (hitcnt=0)
access-list yourlist permit tcp any any (hitcnt=0)

hostname(config)# show running-config aaa
aaa authentication match mylist outbound TACACS+
```

In this context, the following command:

```
hostname(config)# aaa authentication match yourlist outbound tacacs
```

is equivalent to this command:

```
hostname(config)# aaa authentication include TCP/0 outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs
```

The **aaa** command statement list is order-dependent between **access-list** command statements. If you enter the following command:

```
hostname(config)# aaa authentication match mylist outbound TACACS+
```

before this command:

```
hostname(config)# aaa authentication match yourlist outbound tacacs
```

the FWSM tries to find a match in the **mylist access-list** command statement group before it tries to find a match in the **yourlist access-list** command statement group.

Related Commands

Command	Description
aaa authorization	Enables or disable LOCAL or TACACS+ user authorization services.
access-list extended	Creates an access list or use a downloadable access list.

clear configure aaa	Removes/resets the configured AAA accounting values.
show running-config aaa	Display the AAA configuration.

aaa authentication secure-http-client

To enable SSL and secure username and password exchange between HTTP clients and the FWSM, use the **aaa authentication secure-http-client** command in global configuration mode. To disable this function, use the **no** form of this command. The **aaa authentication secure-http-client** command offers a secure method for user authentication to the FWSM prior to allowing user HTTP-based web requests to traverse the FWSM.

aaa authentication secure-http-client

no aaa authentication secure-http-client

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
2.3(1)	This command was introduced.

Usage Guidelines

The **aaa authentication secure-http-client command** secures HTTP client authentication (through SSL). This command is used for HTTP cut-through proxy authentication.

The **aaa authentication secure-http-client** command has the following limitations:

- A maximum of 128 concurrent HTTPS authentication processes is allowed. If all 128 HTTPS authentication processes are running, any new HTTPS connections requiring authentication are not allowed.
- When **uauth timeout 0** is configured (the **uauth timeout** is set to 0), HTTPS authentication might not work. If a browser initiates multiple TCP connections to load a web page after HTTPS authentication, the first connection is let through, but the subsequent connections trigger authentication. As a result, users are continuously presented with an authentication page, even if the correct username and password are entered each time. To work around this, set the **uauth timeout** to 1 second with the **timeout uauth 0:0:1** command. However, this workaround opens a 1-second window of opportunity that might allow non-authenticated users to go through the firewall if they are coming from the same source IP address.

- Because HTTPS authentication occurs on the SSL port 443, users must not configure an **access-list** command statement to block traffic from the HTTP client to HTTP server on port 443. Furthermore, if static PAT is configured for web traffic on port 80, it must also be configured for the SSL port. In the following example, the first line configures static PAT for web traffic and the second line must be added to support the HTTPS authentication configuration:

```
static (inside,outside) tcp 10.132.16.200 www 10.130.16.10 www
static (inside,outside) tcp 10.132.16.200 443 10.130.16.10 443
```

- HTTP users see a pop-up window generated by the browser itself if **aaa authentication secure-http-client** is not configured. If **aaa authentication secure-http-client** is configured, a form loads in the browser to collect username and password. In either case, if a user enters an incorrect password, the user is reprompted. When the web server and the authentication server are on different hosts, use the **virtual** command to get the correct authentication behavior.

Examples

The following example configures HTTP traffic to be securely authenticated:

```
hostname(config)# aaa authentication secure-http-client
hostname(config)# aaa authentication include http...
```

where "..." represents your values for *authen_service if_name local_ip local_mask* [*foreign_ip foreign_mask*] *server_tag*.

The following command configures HTTPS traffic to be securely authenticated:

```
hostname (config)# aaa authentication include https...
```

where "..." represents your values for *authentication -service interface-name local-ip local-mask* [*foreign-ip foreign-mask*] *server-tag*.

Note The **aaa authentication secure-https-client** command is not needed for HTTPS traffic.

Related Commands

Command	Description
aaa authentication	Enables user authentication.
virtual telnet	Accesses the FWSM virtual server.

aaa authorization command

The **aaa authorization command** command specifies whether command execution at the CLI is subject to authorization. To enable command authorization, use the **aaa authorization command** command in global configuration mode. To disable command authorization, use the **no** form of this command.

aaa authorization command {LOCAL | *server_tag* [LOCAL]}

no aaa authorization command {**LOCAL | *server_tag* [LOCAL]}**

Syntax Description

LOCAL	Specifies the use of the FWSM local user database for local command authorization (using privilege levels). If **LOCAL** is specified after a TACACS+ server group tag, the local user database is used for command authorization only as a fallback when the TACACS+ server group is unavailable.
server_tag	Specifies a predefined server group tag for the TACACS+ authorization server. The AAA server group tag as defined by the **aaa-server** command.

Defaults

Fallback to the local database for authorization is disabled by default.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.
2.2(1)	Support added for fallback to LOCAL authorization when a TACACS+ server group is temporarily unavailable.

Usage Guidelines

You can use one of two command authorization methods:

- Local database—Configure the command privilege levels on the FWSM using the **privilege** command. When a local user authenticates with the **enable** command (or logs in with the **login** command), the FWSM places that user in the privilege level that is defined by the local database. The user can then access commands at the user privilege level and below.

  You can use local command authorization without any users in the local database and without CLI or enable authentication. To do so, when you enter the **enable** command, use the system enable password, and the FWSM places you in level 15 as the default “enable_15” username. You can create enable passwords for every level, so that when you enter **enable** *n* (2 to 15), the FWSM places you in level *n*. These levels are not used unless you turn on local command authorization.

- TACACS+ server—On the TACACS+ server, configure the commands that a user or group can use after they authenticate for CLI access. Every command that a user enters at the CLI is checked with the TACACS+ server.

Security Contexts and Command Authorization

The following are important points to consider when implementing command authorization with multiple security contexts:

- AAA settings are discrete per context, not shared between contexts.

  When configuring command authorization, you must configure each security context separately. This provides you the opportunity to enforce different command authorizations for different security contexts.

  When switching between security contexts, administrators should be aware that the commands permitted for the username specified when they login may be different in the new context session or that command authorization may not be configured at all in the new context. Failure to understand that command authorizations may differ between security contexts could confuse an administrator. This behavior is further complicated by the next point.

- New context sessions started with the **changeto** command always use the default "enable_15" username as the administrator identity, regardless of what username was used in the previous context session. This behavior can lead to confusion if command authorization is not configured for the enable_15 user or if authorizations are different for the enable_15 user than for the user in the previous context session.

  This behavior also affects command accounting, which is useful only if you can accurately associate each command that is issued with a particular administrator. Because all administrators with permission to use the **changeto** command can use the enable_15 username in other contexts, command accounting records may not readily identify who was logged in as the enable_15 username. If you use different accounting servers for each context, tracking who was using the enable_15 username requires correlating the data from several servers.

  When configuring command authorization, consider the following:

  – An administrator with permission to use the **changeto** command effectively has permission to use all commands permitted to the enable_15 user in each of the other contexts.

  – If you intend to authorize commands differently per context, ensure that in each context the enable_15 username is denied use of commands that are also denied to administrators who are permitted use of the **changeto** command.

  When switching between security contexts, administrators can exit privileged EXEC mode and enter the **enable** command again to use the username they need.

Note The system execution space does not support AAA commands; therefore, command authorization is not available in the system execution space.

TACACS+ Command Authorization

If you enable TACACS+ command authorization, and a user enters a command at the CLI, the FWSM sends the command and username to the TACACS+ server to determine if the command is authorized.

When configuring command authorization with a TACACS+ server, do not save your configuration until you are sure it works the way you want. If you get locked out because of a mistake, you can usually recover access by restarting the FWSM.

Be sure that your TACACS+ system is completely stable and reliable. The necessary level of reliability typically requires that you have a fully redundant TACACS+ server system and fully redundant connectivity to the FWSM. For example, in your TACACS+ server pool, include one server connected to interface 1, and another to interface 2. You can also configure local command authorization as a fallback method if the TACACS+ server is unavailable. In this case, you need to configure local users and command privilege levels.

Examples

The following example shows how to enable command authorization using a TACACS+ server group named tplus1:

```
hostname(config)# aaa authorization command tplus1
```

The following example shows how to configure administrative authorization to support fallback to the local user database if all servers in the tplus1 server group are unavailable.

```
hostname(config)# aaa authorization command tplus1 LOCAL
```

Related Commands

Command	Description
aaa authorization	Enables or disables user authorization.
aaa-server host	Configures host-related attributes.
aaa-server	Configures group-related server attributes.
clear configure aaa	Removes/resets the configured AAA accounting values.
show running-config aaa	Displays the AAA configuration.

aaa authorization include, exclude

To enable authorization for connections through the FWSM, use the **aaa authorization include** command in global configuration mode. To exclude addresses from authorization, use the **aaa authorization exclude** command. To disable authorization, use the **no** form of this command.

aaa authorization {include | exclude} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

no aaa authorization {include | exclude} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

Syntax Description

exclude	Excludes the specified service and address from authorization if it was already specified by an **include** command.
include	Specifies the services and IP addresses that require authorization. Traffic that is not specified by an **include** statement is not processed.
inside_ip	Specifies the IP address on the higher security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the destination address. If you apply the command to the higher security interface, then this address is the source address. Use 0 to mean all hosts.
inside_mask	Specifies the network mask for the inside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
interface_name	Specifies the interface name from which users require authorization.
outside_ip	(Optional) Specifies the IP address on the lower security interface. This address might be the source or the destination address, depending on the interface to which you apply this command. If you apply the command to the lower security interface, then this address is the source address. If you apply the command to the higher security interface, then this address is the destination address. Use 0 to mean all hosts.
outside_mask	(Optional) Specifies the network mask for the outside IP address. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.

server_tag	Specifies the AAA server group defined by the **aaa-server** command.
service	Specifies the services that require authorization. You can specify one of the following values: • **any** or **tcp/0** (specifies all TCP traffic) • **ftp** • **http** • **https** • **ip** • **ssh** • **telnet** • **tcp/***port*[**-***port*] • **udp/***port*[**-***port*] • **icmp/***type* • *protocol*[**/***port*[**-***port*]]

Defaults

An IP address of **0** means "all hosts." Setting the local IP address to **0** lets the authorization server decide which hosts are authorized.

Fallback to the local database for authorization is disabled by default.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

To enable authorization for traffic that is specified by an access list, use the **aaa authorization match** command. You cannot use the **match** command in the same configuration as the **include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

You cannot use the **aaa authorization include** and **exclude** commands between same-security interfaces. For that scenario, you must use the **aaa authorization match** command.

You can configure the FWSM to perform network access authorization with TACACS+. Authentication and authorization statements are independent; however, any unauthenticated traffic matched by an authorization statement will be denied. For authorization to succeed, a user must first authenticate with

the FWSM. Because a user at a given IP address only needs to authenticate one time for all rules and types, if the authentication session has not expired, authorization can occur even if the traffic is matched by an authentication statement.

After a user authenticates, the FWSM checks the authorization rules for matching traffic. If the traffic matches the authorization statement, the FWSM sends the username to the TACACS+ server. The TACACS+ server responds to the FWSM with a permit or a deny for that traffic, based on the user profile. The FWSM enforces the authorization rule in the response.

See the documentation for your TACACS+ server for information about configuring network access authorizations for a user.

For each IP address, one **aaa authorization include** command is permitted.

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 follows.

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

Note Specifying a port range might produce unexpected results at the authorization server. The FWSM sends the port range to the server as a string, with the expectation that the server will parse it out into specific ports. Not all servers do this. In addition, you might want users to be authorized on specific services, which does not occur if a range is accepted.

Examples

The following example uses the TACACS+ protocol:

```
hostname(config)# aaa-server tplus1 protocol tacacs+
hostname(config)# aaa-server tplus1 (inside) host 10.1.1.10 thekey timeout 20
hostname(config)# aaa authentication include any inside 0 0 0 0 tplus1
hostname(config)# aaa authorization include any inside 0 0 0 0
hostname(config)# aaa accounting include any inside 0 0 0 0 tplus1
hostname(config)# aaa authentication ssh console tplus1
```

In this example, the first command statement creates a server group named tplus1 and specifies the TACACS+ protocol for use with this group. The second command specifies that the authentication server with the IP address 10.1.1.10 resides on the inside interface and is in the tplus1 server group. The next three command statements specify that any users starting connections through the outside interface to any foreign host will be authenticated using the tplus1 server group, that the users who are successfully authenticated are authorized to use any service, and that all outbound connection information will be logged in the accounting database. The last command statement specifies that SSH access to the FWSM console requires authentication from the tplus1 server group.

The following example enables authorization for DNS lookups from the outside interface:

```
hostname(config)# aaa authorization include udp/53 outside 0.0.0.0 0.0.0.0
```

The following example enables authorization of ICMP echo-reply packets arriving at the inside interface from inside hosts:

```
hostname(config)# aaa authorization include 1/0 inside 0.0.0.0 0.0.0.0
```

This means that users cannot ping external hosts if they have not been authenticated using Telnet, HTTP, or FTP.

The following example enables authorization only for ICMP echoes (pings) that arrive at the inside interface from an inside host:

```
hostname(config)# aaa authorization include 1/8 inside 0.0.0.0 0.0.0.0
```

Related Commands

Command	Description
aaa authorization command	Specifies whether command execution is subject to authorization, or configure administrative authorization to support fallback to the local user database if all servers in the specified server group are disabled.
aaa authorization match	Enables or disables the LOCAL or TACACS+ user authorization services for a specific access-list command name.
clear configure aaa	Removes/resets the configured AAA accounting values.
show running-config aaa	Display the AAA configuration.

aaa authorization match

To enable authorization for connections through the FWSM, use the **aaa authorization match** command in global configuration mode. To disable authorization, use the **no** form of this command.

aaa authorization match *acl_name interface_name server_tag*

no aaa authorization match *acl_name interface_name server_tag*

Syntax Description

acl_name	Specifies an extended access list name. See the **access-list extended** command. The **permit** ACEs mark matching traffic for authorization, while **deny** entries exclude matching traffic from authorization.
interface_name	Specifies the interface name from which users require authentication.
server_tag	Specifies the AAA server group tag as defined by the **aaa-server** command.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was modified to support RADIUS servers for VPN management connection authorization.

Usage Guidelines

You cannot use the **aaa authorization match** command in the same configuration as the **include** and **exclude** commands. We suggest that you use the **match** command instead of the **include** and **exclude** commands; the **include** and **exclude** commands are not supported by ASDM.

You can configure the FWSM to perform network access authorization with TACACS+. RADIUS authorization with the **aaa authorization match** command only supports authorization of VPN management connections to the FWSM.

After a user authenticates, the FWSM checks the authorization rules for matching traffic. If the traffic matches the authorization statement, the FWSM sends the username to the TACACS+ server. The TACACS+ server responds to the FWSM with information that the FWSM treats as a dynamic access list for that traffic, based on the user profile. Note that for interface access lists, the **access-list per-user-override** keyword applies for authorized traffic.

Authentication and authorization statements are independent; however, any unauthenticated traffic matched by an authorization statement will be denied. For authorization to succeed, a user must first authenticate with the FWSM.

Note We suggest that you identify the same traffic for authentication as for authorization. Due to the way the FWSM uses the dynamic access list, if you have a more restrictive authorization statement than authentication, then some connections are unexpectedly denied. When a user first authenticates, if the connection matches the authentication statement and not the authorization statement, then later connections for that user that match the authorization statement are denied (for as long as the uauth session exists). Conversely, if the first connection matches the authorization statement, then later connections that do not match the authorization statement but that match the authentication statement are denied. Therefore, you need to match the authentication and authorization configurations.

See the documentation for your TACACS+ server for information about configuring network access authorizations for a user.

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 follows.

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

Note Specifying a port range might produce unexpected results at the authorization server. The FWSM sends the port range to the server as a string, with the expectation that the server will parse it out into specific ports. Not all servers do this. In addition, you might want users to be authorized on specific services, which does not occur if a range is accepted.

Examples

The following example uses the tplus1 server group with the **aaa** commands:

```
hostname(config)# access-list myacl extended permit ip any any
hostname(config)# aaa-server tplus1 protocol tacacs+
hostname(config)# aaa-server tplus1 (inside) host 10.1.1.10 thekey timeout 20
hostname(config)# aaa authentication match myacl inside tplus1
hostname(config)# aaa accounting match myacl inside tplus1
hostname(config)# aaa authorization match myacl inside tplus1
```

In this example, the first command statement defines the tplus1 server group as a TACACS+ group. The second command specifies that the authentication server with the IP address 10.1.1.10 resides on the inside interface and is in the tplus1 server group. The next three command statements specify that any connections traversing the inside interface to any foreign host are authenticated using the tplus1 server group, that all these connections are logged in the accounting database, and that they are authorized by the AAA servers in the tplus1 server group.

Related Commands

Command	Description
aaa authorization	Enables or disables user authorization.
clear configure aaa	Resets all aaa configuration parameters to the default values.
clear uauth	Deletes AAA authorization and authentication caches for one user or all users, which forces users to reauthenticate the next time that they create a connection.

Command	Description
show running-config aaa	Displays the AAA configuration.
show uauth	Displays the username provided to the authorization server for authentication and authorization purposes, the IP address to which the username is bound, and whether the user is only authenticated or has cached services.

aaa local authentication attempts max-fail

To limit the number of consecutive failed local login attempts that the FWSM allows any given user account, use the **aaa local authentication attempts max-fail** command in global configuration mode. This command only affects authentication with the local user database. To disable this feature and allow an unlimited number of consecutive failed local login attempts, use the **no** form of this command.

aaa local authentication attempts max-fail *number*

Syntax Description

number	The maximum number of times a user can enter a wrong password before being locked out. This number can be in the range 1-16.

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 this command, there is no limit on the number of times a user can enter an incorrect password when the local database is used for authentication.

After a user makes the configured number of attempts with the wrong password, the user is locked out and cannot log in successfully until an administrator unlocks the username. Locking or unlocking a username results in a syslog message.

The administrator cannot be locked out of the device.

The number of failed attempts resets to zero and the lockout status resets to No when the user successfully authenticates or when the FWSM reboots.

Examples

The following example shows use of the **aaa local authentication attempts max-limits** command to set the maximum number of failed attempts allowed to 2:

```
hostname(config)# aaa local authentication attempts max-limits 2
hostname(config)#
```

Related Commands

Command	Description
clear aaa local user lockout	Clears the lockout status of the specified users and set their failed-attempts counter to 0.
clear aaa local user fail-attempts	Resets the number of failed user authentication attempts to zero without modifying the locked-out status of the user.
show aaa local user	Shows the list of usernames that are currently locked.

aaa mac-exempt

To exempt MAC addresses from authentication and authorization (for through traffic only), use the **aaa mac-exempt** command in global configuration mode. You can only add one **aaa mac-exempt** command. To disable MAC exemption, use the **no** form of this command.

aaa mac-exempt match *id*

no aaa mac-exempt match *id*

Syntax Description

id	Specifies a MAC list number configured with the **mac-list** command.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The FWSM can exempt from authentication and authorization any through traffic from specific MAC addresses. For example, if the FWSM authenticates TCP traffic originating on a particular network but you want to allow unauthenticated TCP connections from a specific server, you would use a MAC exempt rule to exempt from authentication and authorization any traffic from the server specified by the rule.

This feature is particularly useful to exempt devices such as IP phones that cannot respond to authentication prompts.

This command exempts the list of MAC addresses for through-the-box connections only. For commands like Telnet to the FWSM, the authentication or authorization is not exempted even if the MAC address of the device is in the MAC list used by the **aaa mac-exempt** command.

Configure the MAC addresses you want to exempt using the **mac-list** command before using the **aaa mac-exempt** command. **permit** entries in the MAC list exempt the MAC addresses from authentication and authorization, while **deny** entries require authentication and authorization for the MAC address, if enabled. Because you can only add one instance of the **aaa mac-exempt** command, be sure that your MAC list includes all the MAC addresses you want to exempt.

Examples

The following example bypasses authentication for a single MAC address:

```
hostname(config)# mac-list abc permit 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# aaa mac-exempt match abc
```

The following entry bypasses authentication for all Cisco IP Phones, which have the hardware ID 0003.E3:

```
hostname(config)# mac-list acd permit 0003.E300.0000 FFFF.FF00.0000
hostname(config)# aaa mac-exempt match acd
```

The following example bypasses authentication for a a group of MAC addresses except for 00a0.c95d.02b2:

```
hostname(config)# mac-list 1 deny 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# mac-list 1 permit 00a0.c95d.0000 ffff.ffff.0000
hostname(config)# aaa mac-exempt match 1
```

Related Commands

Command	Description
aaa authentication	Enables user authentication.
aaa authorization	Enables user authorization services.
aaa mac-exempt	Exempts a list of MAC addresses from authentication and authorization.
show running-config mac-list	Displays a list of MAC addresses previously specified in the **mac-list** command.
mac-list	Specifies a list of MAC addresses to be used to exempt MAC addresses from authentication and/or authorization.

aaa proxy-limit

To set the maximum number of concurrent proxy connections allowed per user, use the **aaa proxy-limit** command in global configuration mode. To disable proxies, use the **disable** parameter. To return to the default proxy-limit value of 16 concurrent proxy connections per user, use the **no** form of this command.

aaa proxy-limit *proxy_limit*

aaa proxy-limit disable

no aaa proxy-limit

Syntax Description

disable	No proxies allowed.
proxy_limit	Specify the number of concurrent proxy connections allowed per user, from 1 to 128.

Defaults

The default proxy-limit value is 16.

Command Modes

The 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

If a source address is a proxy server, consider excluding this IP address from authentication or increasing the number of allowable outstanding AAA requests.

Examples

The following example shows how to set the maximum number of outstanding authentication requests allowed per user:

```
hostname(config)# aaa proxy-limit 6
```

Related Commands

Command	Description
aaa authentication	Enables, disables, or views LOCAL, TACACS+, or RADIUS user authentication, on a server designated by the **aaa-server** command, or ASDM user authentication.

aaa authorization	Enables or disables user authorization services.
aaa-server host	Specifies a AAA server.
clear configure aaa	Removes/resets the configured AAA accounting values.
show running-config aaa	Displays the AAA configuration.

aaa-server host

To configure or add a AAA server to a AAA server group or to configure AAA server parameters that are host-specific, use the **aaa-server host** command in global configuration mode. When you use the **aaa-server host** command, you enter aaa-server host configuration mode, from which you can specify and manage host-specific AAA server connection data. To remove a host configuration, use the **no** form of this command:

aaa-server *server_tag* [(*interface_name*)] **host** *server_ip* [*key*] [**timeout** *seconds*]

no aaa-server *server_tag* [(*interface_name*)] **host** *server_ip* [*key*] [**timeout** *seconds*]

Syntax Description

(*interface_name*)	The network interface where the authentication server resides. The parentheses are required in this parameter. If you do not enter an interface, the interface named “inside” is used. If you do not have an interface named “inside,” then an error message displays, and you need to specify this argument.
key	(Optional) Specifies a case-sensitive, alphanumeric keyword of up to 127 characters that is the same value as the key on the AAA server. Any characters entered past 127 are ignored. The key is used between the FWSM and the server for encrypting data between them. the key must be the same on both the FWSM and server systems. Spaces are not permitted in the key, but other special characters are allowed. You can add or modify the key using the **key** command in aaa-server host configuration mode.
server_ip	Specifies the IP address of the AAA server.
server_tag	Specifies the name of the AAA server group as defined by the **aaa-server** command. Each server group is specific to one type of server: Kerberos, LDAP, NT, RADIUS, SDI, or TACACS+.
timeout *seconds*	(Optional) Specifies the timeout interval for the request. This is the time after which the FWSM gives up on the request to the primary AAA server. If there is a standby AAA server, the FWSM sends the request to the backup server. You can modify the timeout interval using the **timeout** command in host mode.

Defaults

The default timeout value is 10 seconds.

Command Modes

The 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.
3.1(1)	The **aaa-server** command is now two separate commands: the **aaa-server** command adds the group and specifies the protocol while the **aaa-server host** command adds a server IP address to the group.

Usage Guidelines

You can have up to 15 AAA server groups in single mode or 4 AAA server groups per context in multiple mode. Each group can have up to 16 servers in single mode or 4 servers in multiple mode.

When a user logs in, the servers are accessed one at a time starting with the first server you specify in the configuration, until a server responds.

If accounting is in effect, the accounting information goes only to the active server, unless you specify simultaneous accounting in the **aaa-server protocol** command.

Examples

The following example configures an SDI AAA server group named "svrgrp1" on host "209.165.200.225", sets the timeout interval to 6 seconds, sets the retry interval to 7 seconds, and configures the SDI version to version 5.

```
hostname(config)# aaa-server svrgrp1 protocol sdi
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 209.165.200.225
hostname(config-aaa-server-host)# timeout 6
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# sdi-version sdi-5
hostname(config-aaa-server-host)# exit
hostname(config)#
```

Related Commands

Command	Description
aaa-server protocol	Configures group-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.

aaa-server

To create a AAA server group and define parameters that are group-specific and common to all hosts, use the **aaa-server** command in global configuration mode. To remove the designated group, use the **no** form of this command.

aaa-server *server_tag* **protocol** {**kerberos** | **ldap** | **nt** | **radius** | **sdi** | **tacacs+**}

no aaa-server *server_tag* **protocol** *server-protocol*

Syntax Description

kerberos	Specifies the Kerberos server type.
ldap	Specifies the LDAP server type.
nt	Specifies the Windows NT server type.
radius	Specifies the RADIUS server type.
sdi	Specifies the SDI server type.
server_tag	Specifies the name of the server group. Other AAA commands make reference to the *server_tag* group.
tacacs+	Specifies the TACACS+ server type.

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.
3.1(1)	Additional server types were added to RADIUS and TACACS+. The **aaa-server** command is now two separate commands: the **aaa-server** command adds the group and specifies the protocol while the **aaa-server host** command adds a server IP address to the group.

Usage Guidelines

Use the **aaa-server host** command to add a AAA server to the AAA server group.

You can have up to 15 AAA server groups in single mode or 4 AAA server groups per context in multiple mode. Each group can have up to 16 servers in single mode or 4 servers in multiple mode.

When a user logs in, the servers are accessed one at a time starting with the first server you specify in the configuration, until a server responds.

If accounting is in effect, the accounting information goes only to the active server, unless you specify simultaneous accounting in the **aaa-server protocol** command.

Examples

The following example adds a TACACS+ server group and assigns the server at 10.1.1.1 to it:

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# accounting-mode simultaneous
hostname(config-aaa-server-group)# reactivation mode timed
hostname(config-aaa-server-group)# max-failed attempts 2
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 10.1.1.1
```

Related Commands

Command	Description
aaa-server host	Configures parameters for specific AAA servers.
accounting-mode	Indicates whether accounting messages are sent to a single server (single mode) or sent to all servers in the group (simultaneous mode).
reactivation-mode	Specifes the method by which failed servers are reactivated.
max-failed-attempts	Specifies the number of failures that will be tolerated for any given server in the server group before that server is deactivated.
clear configure aaa-server	Removes all AAA server 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.

absolute

To define an absolute time when a time range is in effect, use the **absolute** command in time-range configuration mode. To disable, use the **no** form of this command.

absolute [**end** *time date*] [**start** *time date*]

no absolute [**end** *time date*] [**start** *time date*]

Syntax Description

date	Specifies the date in the format day month year; for example, 1 January 2006. The valid range of years is 1993 through 2035.
time	Specifies the time in the format HH:MM. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.

Defaults

If no start time and date are specified, the permit or deny statement is in effect immediately and always on. Similarly, the maximum end time is 23:59 31 December 2035. If no end time and date are specified, the associated permit or deny statement is in effect indefinitely.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Time-range configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

To implement a time-based ACL, use the **time-range** command to define specific times of the day and week. Then use the with the **access-list extended time-range** command to bind the time range to an ACL.

Examples

The following example activates an ACL at 8:00 a.m. on 1 January 2006:

```
hostname(config-time-range)# absolute start 8:00 1 January 2006

Because no end time and date are specified, the associated ACL is in effect indefinitely.
```

Related Commands

Command	Description
access-list extended	Configures a policy for permitting or denying IP traffic through the FWSM.
default	Restores default settings for the **time-range** command **absolute** and **periodic** keywords.
periodic	Specifies a recurring (weekly) time range for functions that support the time-range feature.
time-range	Defines access control to the FWSM based on time.

accept-subordinates

To configure the FWSM to accept subordinate CA certificates if delivered during phase one IKE exchange when not previously installed on the device, use the **accept-subordinates** command in crypto ca trustpoint configuration mode. To restore the default setting, use the **no** form of this command.

accept-subordinates

no accept-subordinates

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is on (subordinate certificates are accepted).

Command Modes

The 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.

Usage Guidelines

During phase 1 processing, an IKE peer might pass both a subordinate certificate and an identity certificate. The subordinate certificate might not be installed on the FWSM. This command lets an administrator support subordinate CA certificates that are not configured as trustpoints on the device without requiring that all subordinate CA certificates of all established trustpoints be acceptable; in other words, this command lets the device authenticate a certificate chain without installing the entire chain locally.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and allows the FWSM to accept subordinate certificates for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# accept-subordinates
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.

access-group

To bind the access list to an interface, use the **access-group** command. To unbind the access list from the interface, use the **no** form of this command.

access-group *access-list* {**in** | **out**} **interface** *interface_name* [**per-user-override**]

no access-group *access-list* {**in** | **out**} **interface** *interface_name* [**per-user-override**]

Syntax Description

access-list	Specifies the **access-list** ID.
in	Filters the inbound packets at the specified interface. **Note** "Inbound" and "outbound" refer to the application of an access list on an interface, either to traffic entering the FWSM on an interface or traffic exiting the FWSM on an interface. These terms do not refer to the movement of traffic from a lower security interface to a higher security interface, commonly known as inbound, or from a higher to lower interface, commonly known as outbound.
interface *interface_name*	Specifies the name of the interface on which you want to control access.
out	Filters the outbound packets at the specified interface. You might want to use an outbound access list to simplify your access list configuration. For example, if you want to allow three inside networks on three different interfaces to access each other, you can create a simple inbound access list that allows all traffic on each inside interface.
per-user-override	(Optional) Allows per-user access lists downloaded from a RADIUS server to override the existing interface access lists. This keyword is only available for an inbound **access-group** command.

Defaults

By default without an **access-group** command, no traffic can enter an interface. The exception to this rule is if a packet is part of an existing TCP or UDP connection; then returning traffic is allowed back through the FWSM. An **access-group** command is not required in this case on the destination interface. For connectionless protocols, you need to apply the access list to the source and destination interfaces if you want traffic to pass in both directions.

Command Modes

The 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.
2.3(1)	The **per-user-override** keyword was added.

Usage Guidelines

The **access-group** command binds an access list to an interface. If you enter the **permit** option in an **access-list** command statement, the FWSM continues to process the packet. If you enter the **deny** option in an **access-list** command statement, the FWSM discards the packet and generates syslog message 106019.

You can apply one access list to each direction of the interface (in or out).

Traffic flowing across an interface in the FWSM can be controlled in two ways. Traffic that enters the FWSM can be controlled by attaching an inbound access list to the source interface (the **in** keyword). Traffic that exits the FWSM can be controlled by attaching an outbound access list to the destination interface (the **out** keyword). To allow any traffic to enter the FWSM, you must attach an inbound access list to an interface; otherwise, the FWSM automatically drops all traffic that enters that interface. By default, traffic can exit the FWSM on any interface unless you restrict it using an outbound access list, which adds restrictions to those already configured in the inbound access list.

The **per-user-override** keyword allows dynamic access lists that are downloaded for user authorization to override the access list assigned to the interface. For example, if the interface access list denies all traffic from 10.0.0.0, but the dynamic access list permits all traffic from 10.0.0.0, then the dynamic access list overrides the interface access list for that user.

Additionally, the following rules are observed:

- At the time a packet arrives, if there is no per-user access list associated with the packet, the interface access list will be applied.
- The per-user access list is governed by the timeout value specified by the **uauth** option of the **timeout** command, but it can be overridden by the AAA per-user session timeout value.
- Existing access list log behavior will be the same. For example, if user traffic is denied because of a per-user access list, syslog message 109025 will be logged. If user traffic is permitted, no syslog message is generated. The **log** option in the per-user access-list will have no effect.

Note If all of the **permit** and **deny** statements are removed from an **access-list** that is referenced by one or more **access-group** commands, the **access-group** commands are automatically removed from the configuration. The **access-group** command cannot reference empty access lists or access lists that contain only a remark.

Examples

The following example shows how to use the **access-group** command. The **static** command provides a global address of 209.165.201.3 for the web server at 10.1.1.3. The **access-list** command lets any host access the global address using port 80. The **access-group** command specifies that the **access-list** command applies to traffic entering the outside interface.

```
hostname (config)# static (inside,outside) 209.165.201.3 10.1.1.3
hostname (config)# access-list acl_out permit tcp any host 209.165.201.3 eq 80
hostname (config)# access-group acl_out in interface outside
```

Related Commands

Command	Description
access-list extended	Creates an access list, or uses a downloadable access list.
clear configure access-group	Removes access groups from all the interfaces.
show running-config access-group	Displays the context group members.

access-list alert-interval

To specify the time interval between deny flow maximum messages, use the **access-list alert-interval** command in global configuration mode. To return to the default settings, use the **no** form of this command.

access-list alert-interval *secs*

no access-list alert-interval

Syntax Description

secs	Time interval between deny flow maximum message generation; valid values are from 1 to 3600 seconds.

Defaults

The default is 300 seconds.

Command Modes

The 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 **access-list alert-interval** command sets the time interval for generating the syslog message 106101. The syslog message 106101 alerts you that the FWSM has reached a deny flow maximum. When the deny flow maximum is reached, another 106101 message is generated if at least *secs* seconds have occurred since the last 106101 message.

See the **access-list deny-flow-max** command for information about the deny flow maximum message generation.

Examples

The following example shows how to specify the time interval between deny flow maximum messages:

```
hostname(config)# access-list alert-interval 30
```

Related Commands

Command	Description
access-list deny-flow-max	Specifies the maximum number of concurrent deny flows that can be created.
access-list extended	Adds an access list to the configuration and is used to configure policy for IP traffic through the FWSM.
clear access-group	Clears an access list counter.
clear configure access-list	Clears access lists from the running configuration.
show access-list	Displays the access list entries by number.

access-list commit

To commit access lists when in manual-commit mode, use the **access-list commit** command in global configuration mode.

access-list commit

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
2.2(1)	This command was introduced.

Usage Guidelines

If you set the **access-list mode** command to manual-commit, then you must manually commit access lists a before they can be used by the FWSM.

Note Manual-commit mode only affects access lists that are not used or access lists that are used with the **access-group** command. Access lists used for other configuration commands are always committed automatically, except if the ACL mode is set to manual; then the uncommitted ACLs can not be used for the Commit feature, NAT, and AAA.

Examples

The following example shows how to commit an access list and other rules:

```
fwsm/context(config)# access-list commit
```

Related Commands

Command	Description
access-group	Binds an access list to an interface.
access-list extended	Adds an access list to the configuration and configures policy for IP traffic through the FWSM.

Command	Description
access-list mode	Switches the commitment mode for access lists between manual- and auto-commit.
clear access-list	Clears an access list counter.
object-group	Defines object groups that you can use to optimize your configuration.

access-list deny-flow-max

To specify the maximum number of concurrent deny flows that can be created, use the **access-list deny-flow-max** command in global configuration mode. To return to the default settings, use the **no** form of this command.

access-list deny-flow-max

no access-list deny-flow-max

Syntax Description

This command has no arguments or keywords.

Defaults

The default is 4096.

Command Modes

The 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 was introduced.

Usage Guidelines

Syslog message 106101 is generated when the FWSM has reached the maximum number, *n*, of ACL deny flows.

Examples

The following example shows how to specify the maximum number of concurrent deny flows that can be created:

```
hostname(config)# access-list deny-flow-max 256
```

Related Commands

Command	Description
access-list extended	Adds an access list to the configuration and used to configure policy for IP traffic through the FWSM.
clear access-group	Clears an access list counter.
clear configure access-list	Clears access lists from the running configuration.

Command	Description
show access-list	Displays the access list entries by number.
show running-config access-list	Displays the current running access-list configuration.

access-list ethertype

To configure an access list that controls traffic based on its EtherType, use the **access-list ethertype** command in global configuration mode. To remove the access list, use the **no** form of this command.

access-list *id* **ethertype** {**deny** | **permit**} {**ipx** | **bpdu** | **mpls-unicast** | **mpls-multicast** | **any** | *hex_number*}

no access-list *id* **ethertype** {**deny** | **permit**} {**ipx** | **bpdu** | **mpls-unicast** | **mpls-multicast** | **any** | *hex_number*}

Syntax Description

any	Specifies access to anyone.
bpdu	Specifies access to bridge protocol data units. By default, BPDUs are denied.
deny	Denies access if the conditions are matched.
hex_number	A 16-bit hexadecimal number greater than or equal to 0x600 by which an EtherType can be identified.
id	Name or number of an access list.
ipx	Specifies access to IPX.
mpls-multicast	Specifies access to MPLS multicast.
mpls-unicast	Specifies access to MPLS unicast.
permit	Permits access if the conditions are matched.

Defaults

The defaults are as follows:

- The FWSM denies all packets on the originating interface unless you specifically permit access.
- Access list logging generates syslog message 106027 for denied non-IP packets—Deny non-IP packets must be present to log denied non-IP packets.

Command Modes

The 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 can control any EtherType identified by a 16-bit hexadecimal number. EtherType access lists support Ethernet V2 frames. 802.3-formatted frames are not handled by the access list because they use a length field as opposed to a type field. Bridge protocol data units, which are handled by the access list, are the only exception; they are SNAP-encapsulated, and the FWSM is designed to specifically handle BPDUs.

Because EtherTypes are connectionless, you need to apply the access list to both interfaces if you want traffic to pass in both directions.

If you allow MPLS, ensure that LDP and TDP TCP connections are established through the FWSM by configuring both MPLS routers connected to the FWSM to use the IP address on the FWSM interface as the router-id for LDP or TDP sessions. (LDP and TDP allow MPLS routers to negotiate the labels (addresses) used to forward packets.)

You can apply only one access list of each type (extended and EtherType) to each direction of an interface. You can also apply the same access lists on multiple interfaces.

Note If an EtherType access list is configured to **deny all**, all ethernet frames are discarded. Only physical protocol traffic, such as auto-negotiation, for instance, is still allowed.

Examples

The following example shows how to add an EtherType access list:

```
hostname(config)# access-list ETHER ethertype permit ipx
hostname(config)# access-list ETHER ethertype permit bpdu
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

Related Commands

Command	Description
access-group	Binds the access list to an interface.
clear access-group	Clears access list counters.
clear configure access-list	Clears an access list from the running configuration.
show access-list	Displays the access list entries by number.
show running-config access-list	Displays the current running access-list configuration.

access-list extended

To add an Access Control Entry, use the **access-list extended** command in global configuration mode. An access list is made up of one or more ACEs with the same access list ID. Access lists are used to control network access or to specify traffic for many feature to act upon. To remove the ACE, use the **no** form of this command. To remove the entire access list, use the **clear configure access-list** command.

access-list *id* [**line** *line-number*] [**extended**] {**deny** | **permit**}
{*protocol* | **object-group** *protocol_obj_grp_id*}
{*src_ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id*}
[*operator port* | **object-group** *service_obj_grp_id*]
{*dest_ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id*}
[*operator port* | **object-group** *service_obj_grp_id* | **object-group** *icmp_type_obj_grp_id*]
[**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]
[**inactive** | **time-range** *time_range_name*]

no access-list *id* [**line** *line-number*] [**extended**] {**deny** | **permit**} {**tcp** | **udp**}
{*src_ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id*}
[*operator port*] | **object-group** *service_obj_grp_id*]
{*dest_ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id*}
[*operator port* | **object-group** *service_obj_grp_id* | **object-group** *icmp_type_obj_grp_id*]
[**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]
[**inactive** | **time-range** *time_range_name*]

Syntax Description

default	(Optional) Sets logging to the default method, which is to send system log message 106023 for each denied packet.
deny	Denies a packet if the conditions are matched. In the case of network access (the **access-group** command), this keyword prevents the packet from passing through the FWSM. In the case of applying application inspection to a class map (the **class-map** and **inspect** commands), this keyword exempts the traffic from inspection. Some features do not allow deny ACEs to be used, such as NAT. See the command documentation for each feature that uses an access list for more information.
dest_ip	Specifies the IP address of the network or host to which the packet is being sent. Enter the **host** keyword before the IP address to specify a single address. In this case, do not enter a mask. Enter the **any** keyword instead of the address and mask to specify any address.
disable	(Optional) Disables logging for this ACE.
icmp_type	(Optional) If the protocol is **icmp**, specifies the ICMP type.
id	Specifies the access list ID, as a string or integer up to 241 characters in length. The ID is case-sensitive. Tip: Use all capital letters so you can see the access list ID better in your configuration.
inactive	(Optional) Disables an ACE. To reenable it, enter the entire ACE without the **inactive** keyword. This feature lets you keep a record of an inactive ACE in your configuration to make reenabling easier.
interface *ifc_name*	Specifies the interface address as the source or destination address.
interval *secs*	(Optional) Specifies the log interval at which to generate a 106100 system log message. Valid values are from 1 to 600 seconds. The default is 300.

level	(Optional) Sets the 106100 system log message level from 0 to 7. The default level is 6.
line *line-num*	(Optional) Specifies the line number at which to insert the ACE. If you do not specify a line number, the ACE is added to the end of the access list. The line number is not saved in the configuration; it only specifies where to insert the ACE.
log	(Optional) Sets logging options when a deny ACE matches a packet for network access (an access list applied with the **access-group** command). If you enter the **log** keyword without any arguments, you enable system log message 106100 at the default level (6) and for the default interval (300 seconds). If you do not enter the log keyword, then the default logging occurs, using system log message 106023.
mask	The subnet mask for the IP address. When you specify a network mask, the method is different from the Cisco IOS software **access-list** command. The FWSM uses a network mask (for example, 255.255.255.0 for a Class C mask). The Cisco IOS mask uses wildcard bits (for example, 0.0.0.255).
object-group *icmp_type_obj_grp_id*	(Optional) If the protocol is **icmp**, specifies the identifier of an ICMP-type object group. See the **object-group icmp-type** command to add an object group.
object-group *network_obj_grp_id*	Specifies the identifier of an network object group. See the **object-group network** command to add an object group.
object-group *protocol_obj_grp_id*	Specifies the identifier of a protocol object group. See the **object-group protocol** command to add an object group.
object-group *service_obj_grp_id*	(Optional) If you set the protocol to **tcp** or **udp**, specifies the identifier of a service object group. See the **object-group service** command to add an object group.
operator	(Optional) Matches the port numbers used by the source or destination. The permitted operators are as follows: • **lt**—less than • **gt**—greater than • **eq**—equal to • **neq**—not equal to • **range**—an inclusive range of values. When you use this operator, specify two port numbers, for example: `range 100 200`
permit	Permits a packet if the conditions are matched. In the case of network access (the **access-group** command), this keyword lets the packet pass through the FWSM. In the case of applying application inspection to a class map (the **class-map** and **inspect** commands), this keyword applies inspection to the packet.
port	(Optional) If you set the protocol to **tcp** or **udp**, specifies the integer or name of a TCP or UDP port. DNS, Discard, Echo, Ident, NTP, RPC, SUNRPC, and Talk each require one definition for TCP and one for UDP. TACACS+ requires one definition for port 49 on TCP.
protocol	Specifies the IP protocol name or number. For example, UDP is 17, TCP is 6, and EGP is 47.

src_ip	Specifies the IP address of the network or host from which the packet is being sent. Enter the **host** keyword before the IP address to specify a single address. In this case, do not enter a mask. Enter the **any** keyword instead of the address and mask to specify any address.
time-range *time_range_name*	(Optional) Schedules each ACE to be activated at specific times of the day and week by applying a time range to the ACE. See the **time-range** command for information about defining a time range.

Defaults

The defaults are as follows:

- ACE logging generates syslog message 106023 for denied packets. A deny ACE must be present to log denied packets.
- When the **log** keyword is specified, the default level for syslog message 106100 is 6 (informational) and the default interval is 300 seconds.

Command Modes

The 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

Each ACE that you enter for a given access list name is appended to the end of the access list unless you specify the line number in the ACE.

The order of ACEs is important. When the FWSM decides whether to forward or drop a packet, the FWSM tests the packet against each ACE in the order in which the entries are listed. After a match is found, no more ACEs are checked. For example, if you create an ACE at the beginning of an access list that explicitly permits all traffic, no further statements are ever checked.

Access lists have an implicit deny at the end of the list, so unless you explicitly permit it, traffic cannot pass. For example, if you want to allow all users to access a network through the FWSM except for particular addresses, then you need to deny the particular addresses and then permit all others.

When you use NAT, the IP addresses you specify for an access list depend on the interface to which the access list is attached; you need to use addresses that are valid on the network connected to the interface. This guideline applies for both inbound and outbound access groups: the direction does not determine the address used, only the interface does.

For TCP and UDP connections, you do not need an access list to allow returning traffic, because the FWSM allows all returning traffic for established, bidirectional connections. For connectionless protocols such as ICMP, however, the FWSM establishes unidirectional sessions, so you either need

access lists to allow ICMP in both directions (by applying access lists to the source and destination interfaces), or you need to enable the ICMP inspection engine. The ICMP inspection engine treats ICMP sessions as bidirectional connections.

Because ICMP is a connectionless protocol, you either need access lists to allow ICMP in both directions (by applying access lists to the source and destination interfaces), or you need to enable the ICMP inspection engine. The ICMP inspection engine treats ICMP sessions as stateful connections. To control ping, specify **echo-reply** (**0**) (FWSM to host) or **echo** (**8**) (host to FWSM). See Table 1 for a list of ICMP types.

You can apply only one access list of each type (extended and EtherType) to each direction of an interface. You can apply the same access lists on multiple interfaces. See the **access-group** command for more information about applying an access list to an interface.

While the software allows you to enter the **inactive** option after the **time-range** option is specified for an ACE, the **inactive** option supersedes the **time-range** option, making the **time-range** option unavailable. Enter one or the other, as the syntax shows.

Note If you change the access list configuration, and you do not want to wait for existing connections to time out before the new access list information is used, you can clear the connections using the **clear local-host** command.

Table 1 lists the possible ICMP types values.

Table 2-1 ICMP Type Literals

ICMP Type	Literal
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
30	traceroute
31	conversion-error
32	mobile-redirect

Examples

The following access list allows all hosts (on the interface to which you apply the access list) to go through the FWSM:

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

The following sample access list prevents hosts on 192.168.1.0/24 from accessing the 209.165.201.0/27 network. All other addresses are permitted.

```
hostname(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
hostname(config)# access-list ACL_IN extended permit ip any any
```

If you want to restrict access to only some hosts, then enter a limited permit ACE. By default, all other traffic is denied unless explicitly permitted.

```
hostname(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```

The following access list restricts all hosts (on the interface to which you apply the access list) from accessing a website at address 209.165.201.29. All other traffic is allowed.

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
```

The following access list that uses object groups restricts several hosts on the inside network from accessing several web servers. All other traffic is allowed.

```
hostname(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

To temporarily disable an access list that permits traffic from one group of network objects (A) to another group of network objects (B):

```
hostname(config)# access-list 104 permit ip host object-group A object-group B inactive
```

To implement a time-based access list, use the **time-range** command to define specific times of the day and week. Then use the **access-list extended** command to bind the time range to an access list. The following example binds an access list named "Sales" to a time range named "New_York_Minute":

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
hostname(config)#
```

See the **time-range** command for more information about how to define a time range.

Related Commands

Command	Description
access-group	Binds the access list to an interface.
clear access-group	Clears an access list counter.
clear configure access-list	Clears an access list from the running configuration.
show access-list	Displays ACEs by number.
show running-config access-list	Displays the current running access-list configuration.

access-list mode

To switch the commitment mode for access lists between manual- and auto-commit, use the **access-list mode** command in global configuration mode.

access-list mode {**auto-commit** | **manual-commit**}

Syntax Description

auto-commit	Automatically commits an access list when you add an ACE.
manual-commit	Disables auto-commit. You must manually commit an access list using the **access-list commit** command.

Defaults

The default is **auto-commit**.

Command Modes

The 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 was introduced.

Usage Guidelines

When you add an ACE to an access list, the FWSM activates the access list by committing it to the network processors. In auto-commit mode, the FWSM waits a short period of time after you last entered an **access-list** command and then commits the access list. If you enter an ACE after the commitment starts, the FWSM aborts the commitment, and recommits the access list after a new short waiting period. The FWSM displays a message similar to the following after it commits the access list:

```
Access Rules Download Complete: Memory Utilization: < 1%
```

Large access lists of approximately 60 K ACEs can take 3 to 4 minutes to commit, depending on the size.

You can manually commit access lists if your management application or script needs to monitor the access list commitment for error messages. Some management applications cannot monitor errors that are the result of configuration commands, so if you add ACEs, and there is a commitment error, the management application might not receive the error. However, if the management application sets the mode to manual-commit, then it can monitor errors resulting from the **access-list commit** command, which is a run-time command. The management application typically sets this mode to manual-commit automatically.

Note Manual mode is a run-time configuration, so **access-list mode manual-commit** does not show up when you enter the **show run** command, and the configuration is not retained after a reboot.

If you enable manual commit, then you must remember to manually commit any changes you make to access lists, whether the change is an addition or a subtraction. Also, you must manually commit an access list before you assign it to an interface (**access-group** command); the FWSM cannot assign an access list to an interface if the access list does not exist yet.

If you delete an ACE, but have not yet committed your change, the **show running-config** command shows the ACE with the text "uncommitted deletion". Adding an ACE shows the ACE as "uncommitted addition".

Note Manual-commit mode only affects access lists that are not used or access lists that are used with the **access-group** command. Access lists used for other configuration commands are always committed automatically, except if the ACL mode is set to manual; then the uncommitted access lists cannot be used for the Commit feature, NAT, and AAA.

Note Manual-commit mode is a transitional state that should be used during access list configuration changes only and is not meant to be enabled at all times. Enabling the mode permanently leads to synchronization problems between the active and standby devices.

Examples

The following example shows how to modify an existing access list using the manual-commit mode without disrupting traffic:

```
fwsm(config)# access-list mode manual-commit
fwsm(config)# clear configure access-list CHANGEME
fwsm(config)# access-list CHANGEME ...
! New ACE 1
fwsm(config)# access-list CHANGEME ...
! New ACE 2
fwsm(config)# ...
fwsm(config)# access-list CHANGEME ...
! New ACE N
fwsm(config)# access-list commit
```

The following example shows how to delete the old access list and add a new one with a different name:

```
fwsm(config)# access-list mode manual-commit
fwsm(config)# clear config access-list old-acl
fwsm(config)# access-list new-acl …. : New ACE1
fwsm(config)# access-list new-acl …. : New ACE2
fwsm(config)# …….
fwsm(config)# access-list new-acl …. : New ACEn
fwsm(config)# access-list commit
fwsm(config)# access-group new-acl in interface old-interface
```

The previous example shows that there is a slight traffic disruption on the old interface, which is equal to the time taken for the commit to complete and the **access-group** command to be applied in the last two command lines.

The following example shows how to use the manual-commit mode:

```
fwsm(config)# show access-list mode
ERROR: access-list <mode> does not exists
fwsm(config)#
fwsm(config)# show access-list
access-list mode auto-commit
```

```
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
fwsm(config)#
fwsm(config)# access-list 1 permit ip any any
fwsm(config)# Access Rules Download Complete: Memory Utilization: < 1%
fwsm(config)#
fwsm(config)# show access-list
access-list mode auto-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
access-list 1; 1 elements
access-list 1 extended permit ip any any (hitcnt=0)
fwsm(config)#
fwsm(config)# access-list commit
ERROR: access-list mode set to auto-commit; command ignored
fwsm(config)#
fwsm(config)# Access Rules Download Complete: Memory Utilization: < 1%
fwsm(config)#
fwsm(config)# show access-list
access-list mode auto-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
fwsm(config)#
fwsm(config)# access-list mode manual-commit
fwsm(config)#
fwsm(config)# show access-list
access-list mode manual-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
fwsm(config)#
fwsm(config)# access-list 1 permit ip any any
fwsm(config)#
fwsm(config)# show access-list
access-list mode manual-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
access-list 1; 1 elements
access-list 1 extended permit ip any any (hitcnt=0) (uncommitted addition)
fwsm(config)#
fwsm(config)# access-group 1 in interface inside
ERROR: access-list not committed, ignoring command
fwsm(config)# access-list commit
Access Rules Download Complete: Memory Utilization: < 1%
fwsm(config)#
fwsm(config)# access-group 1 in interface inside
fwsm(config)# show access-list
access-list mode manual-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
access-list 1; 1 elements
access-list 1 extended permit ip any any (hitcnt=0)
fwsm(config)#
fwsm(config)# no access-list 1 permit ip any any
fwsm(config)#
fwsm(config)# show access-list
access-list mode manual-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
access-list 1; 1 elements
access-list 1 extended permit ip any any (hitcnt=0) (uncommitted deletion)
fwsm(config)#
fwsm(config)# access-list commit
Access Rules Download Complete: Memory Utilization: < 1%
fwsm(config)# #
```

```
fwsm(config)# show access-list
access-list mode manual-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
fwsm(config)#
```

Related Commands

Command	Description
access-list commit	Commits access lists when you are in manual-commit mode.
access-list extended	Adds an access list to the configuration and configures policy for IP traffic through the FWSM.
clear access-list	Clears an access list counter.
show access-list	Displays the counters for an access list.
show access-list mode	Displays the compilation mode for the system.

access-list optimization enable

To optimize an access list group, use the **access-list optimization enable** command in global configuration mode. To disable this feature, use the **no** form of this command.

access-list optimization enable

no access-list optimization enable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

When optimization is enabled, rules are optimized and downloaded to the NPs. The original non-optimized rules become inactive. Any addition/deletion of any rules must take place on the original non-optimized access lists. Whenever a new rule is added/deleted , the optimization process is repeated. During that processing time, some of the access lists information may not be accurate until the optimization process is complete.

Note Access list optimization is relevant to static extended access lists only. Dynamic access lists are not optimized. In addition, when an access list is bound to AAA, policy NAT, and fixup modules, two copies of the rules coexist in the system. An optimized copy that would be used in case the access list is attached to an access group, and the original non-optimized copy used for AAA, policy NAT and fixups.

Examples

The following example shows how to optimize access lists:

```
hostname(config)# access-list optimization enable
```

Related Commands

Command	Description
clear configure access-list	Clears an access list from the running configuration.
copy optimized-running-config	Copies the optimized running configuration to the designated location.
debug acl optimization	Debugs access list optimization.
show access-list	Displays the access list entries by number.
show running-config access-list	Displays the current running access-list configuration.

access-list remark

To specify the text of the remark to add before or after an **access-list extended** command, use the **access-list remark** command in global configuration mode. To delete the remark, use the **no** form of this command.

access-list *id* [**line** *line-num*] **remark** *text*

no access-list *id* [**line** *line-num*] **remark** *text*

Syntax Description

id	Name of an access list.
line *line-num*	(Optional) The line number at which to insert a remark or an access control element (ACE).
remark text	Text of the remark to add before or after an **access-list extended** command.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

The remark text can be up to 100 characters in length, including spaces and punctuation. The remark text must contain at least 1 non-space character; you cannot enter an empty remark.

You cannot use the **access-group** command on an ACL that includes a remark only.

When you attempt to delete a specific remark and specify the line number using the **no access-list** *id* **line** *line number* **remark** command, if the line number specified is not being used by an ACE in that ACL, then the entire access-list is searched until the first instance of the specified remark is identified. After the remark is identified, the first instance of the remark is deleted from the top, even if multiple occurrences of the same remark exist in the same access list.

Examples

The following example shows how to specify the text of the remark to add before or after an **access-list** command:

```
hostname(config)# access-list 77 remark checklist
```

Related Commands

Command	Description
access-list extended	Adds an access list to the configuration and used to configure policy for IP traffic through the FWSM.
clear access-group	Clears an access list counter.
clear configure access-list	Clears access lists from the running configuration.
show access-list	Displays the access list entries by number.
show running-config access-list	Displays the current running access-list configuration.

access-list standard

To add an access list to identify the destination IP addresses of OSPF routes, which can be used in a route map for OSPF redistribution, use the **access-list standard** command in global configuration mode. To remove the access list, use the **no** form of this command. Enter the command without the keyword **standard** to specify a line number.

access-list *id* **standard** {**deny** | **permit**} {**any** | **host** *ip_address* | *ip_address subnet_mask*}

no access-list *id* **standard** {**deny** | **permit**} {**any** | **host** *ip_address* | *ip_address subnet_mask*}

access-list *id* [**line** *line-num*] {**deny** | **permit**} {**any** | **host** *ip_address* | *ip_address subnet_mask*}

Syntax Description

any	Specifies access to anyone.
deny	Denies access if the conditions are matched. See the "Usage Guidelines" section for the description.
host *ip_address*	Specifies access to a host IP address.
id	Name or number of an access list.
ip_address ip_mask	Specifies access to a specific IP address and subnet mask.
line *line-num*	(Optional) The line number at which to insert an ACE.
permit	Permits access if the conditions are matched. See the "Usage Guidelines" section for the description.

Defaults

The defaults are as follows:

- The FWSM denies all packets on the originating interface unless you specifically permit access.
- ACL logging generates syslog message 106023 for denied packets—Deny packets must be present to log denied packets.

Command Modes

The 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

When used with the **access-group** command, the **deny** optional keyword does not allow a packet to traverse the FWSM. By default, the FWSM denies all packets on the originating interface unless you specifically permit access.

When you specify the *protocol* to match any Internet protocol, including TCP and UDP, use the **ip** keyword.

Refer to the **object-group** command for information on how to configure object groups.

You can use the **object-group** command to group access lists.

Use the following guidelines for specifying a source, local, or destination address:

- Use a 32-bit quantity in four-part, dotted-decimal format.
- Use the keyword **any** as an abbreviation for an address and mask of 0.0.0.0 0.0.0.0. We do not recommend that you use this keyword with IPSec.

Use **host** *address* as an abbreviation for a mask of 255.255.255.255.

Examples

The following example shows how to deny IP traffic through the firewall:

```
hostname(config)# access-list 77 standard deny
```

The following example shows how to permit IP traffic through the firewall if conditions are matched:

```
hostname(config)# access-list 77 standard permit
```

Related Commands

Command	Description
access-group	Defines object groups that you can use to optimize your configuration.
clear access-group	Clears an access list counter.
clear configure access-list	Clears access lists from the running configuration.
show access-list	Displays the access list entries by number.
show running-config access-list	Displays the current running access-list configuration.

accounting-mode

To indicate whether accounting messages are sent to a single server (single mode) or sent to all servers in the group (simultaneous mode), use the **accounting-mode** command in aaa-server group configuration mode. To remove the accounting mode specification, use the **no** form of this command.

accounting-mode simultaneous

accounting-mode single

no accounting-mode

Syntax Description

simultaneous	Sends accounting messages to all servers in the group.
single	Sends accounting messages to a single server.

Defaults

The default value is single mode.

Command Modes

The 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 configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Use the keyword **single** to send accounting messages to a single server. Use the keyword **simultaneous** to send accounting messages to all servers in the server group.

This command is meaningful only when the server group is used for accounting (RADIUS or TACACS+).

Examples

The following example shows the use of the **accounting-mode** command to send accounting messages to all servers in the group:

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# accounting-mode simultaneous
```

Related Commands

Command	Description
aaa accounting	Enables or disables accounting services.
aaa-server protocol	Enters AAA server group configuration mode, so that you can configure AAA server parameters that are group-specific and common to all hosts in the group.
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.

accounting-port

To specify the port number used for RADIUS accounting for this host, use the **accounting-port** command in aaa-server host configuration mode. To remove the authentication port specification, use the **no** form of this command. This command specifies the destination TCP/UDP port number of the remote RADIUS server hosts to which you want to send accounting records.

accounting-port *port*

no accounting-port

Syntax Description

port	A port number, in the range 1-65535, for RADIUS accounting.

Defaults

By default, the device listens for RADIUS on port 1646 for accounting (in compliance with RFC 2058). If the port is not specified, the RADIUS accounting default port number (1646) is used.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced, replacing the **aaa-server radius-acctport** command.

Usage Guidelines

If your RADIUS accounting server uses a port other than 1646, you must configure the FWSM for the appropriate port prior to starting the RADIUS service with the **aaa-server** command.

Tip RFC 2139 introduced a change to the standard port for RADIUS accounting, to port 1813.

This command is valid only for server groups that are configured for RADIUS.

Examples

The following example configures a RADIUS AAA server named “svrgrp1” on host “209.165.200.225”, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures accounting port 2222.

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 209.165.200.225
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# accounting-port 2222
```

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

Related Commands

Command	Description
aaa accounting	Keeps a record of which network services a user has accessed.
aaa-server host	Enters aaa server host configuration mode, so that you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa-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.

accounting-server-group

To specify the aaa-server group for sending accounting records, use the **accounting-server-group** command in tunnel-group general-attributes configuration mode. To return this command to the default, use the **no** form of this command.

[no] accounting-server-group *server-group*

Syntax Description

server-group	Specifies the name of the aaa-server group, which defaults to **NONE**.

Defaults

The default setting for this command is **NONE**.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Tunnel-group general-attributes configuration	•	•	•	•	•

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to all tunnel-group types.

Examples

The following example entered in config-general configuration mode, configures an accounting server group named aaa-server123 for an IPSec LAN-to-LAN tunnel group xyz:

```
hostname(config)# tunnel-group xyz type IPSec_L2L
hostname(config)# tunnel-group xyz general
hostname(config-general)# accounting-server-group aaa-server123
hostname(config-general)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group-map default-group	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.