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*] *tacacs+-server-tag*

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

Syntax Description

tacacs+-server-tag	Specifies the server or group of TACACS+ servers to which accounting records are sent, as specified by the **aaa-server protocol** command.
privilege *level*	If you customize the command privilege level using the **privilege** command, you can limit which commands the security appliance accounts for by specifying a minimum privilege level. The security appliance 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 security appliance 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.

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
7.0(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 aaa accounting for administrative access, use the **no** form of this command.

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

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

Syntax Description

enable	Enables the generation of accounting records to mark the entry to and exit from privileged EXEC mode.
serial	Enables the generation of accounting records to mark the establishment and termination of admin sessions that are established via the serial console interface.
server-tag	Specifies the server group to which accounting records are sent, defined by the **aaa-server protocol** command. Valid server group protocols are RADIUS and TACACS+.
ssh	Enables the generation of accounting records to mark the establishment and termination of admin sessions created over SSH.
telnet	Enables the generation of accounting records to mark the establishment and termination of admin sessions created over Telnet.

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
7.0(1)	This command was introduced.

Usage Guidelines

You must specify the name of the server group, previously specified in an **aaa-server** command.

Examples

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

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

Related Commands

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

aaa accounting include, exclude

To enable accounting for TCP or UDP connections through the security appliance, 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** • **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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The security appliance can send accounting information to a RADIUS or TACACS+ server about any TCP or UDP traffic that passes through the security appliance. 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 security appliance 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 security appliance, 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
Preexisting	This command was preexisting.

Usage Guidelines

The security appliance can send accounting information to a RADIUS or TACACS+ server about any TCP or UDP traffic that passes through the security appliance. 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 security appliance 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 include, exclude

To enable authentication for connections through the security appliance, 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* | **LOCAL**}

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** • **ssh** • **telnet** • **tcp/***port*[**-***port*] • **udp/***port*[**-***port*] • **icmp/***type* • *protocol*[**/***port*[**-***port*]] Although you can configure the security appliance 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 security appliance 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
Preexisting	This command was preexisting.

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.

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 security appliance 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 security appliance 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 security appliance allows other traffic requiring authentication.

The authentication ports that the security appliance supports for AAA are fixed:

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

Security Appliance Authentication Prompts

For Telnet and FTP, the security appliance generates an authentication prompt.

For HTTP, the security appliance uses basic HTTP authentication by default, and provides an authentication prompt. You can optionally configure the security appliance to redirect users to an internal web page where they can enter their username and password (configured with the **aaa authentication listener** command).

For HTTPS, the security appliance generates a custom login screen. You can optionally configure the security appliance to redirect users to an internal web page where they can enter their username and password (configured with the **aaa authentication listener** command).

Redirection is an improvement over the basic method because it provides an improved user experience when authenticating, and an identical user experience for HTTP and HTTPS in both Easy VPN and firewall modes. It also supports authenticating directly with the security appliance.

You might want to continue to use basic HTTP authentication if: you do not want the security appliance to open listening ports; if you use NAT on a router and you do not want to create a translation rule for the web page served by the security appliance; basic HTTP authentication might work better with your network. For example non-browser applications, like when a URL is embedded in email, might be more compatible with basic authentication.

After you authenticate correctly, the security appliance redirects you to your original destination. If the destination server also has its own authentication, the user enters another username and password. If you use basic HTTP authentication and need to enter another username and password for the destination server, then you need to configure the **virtual http** command.

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 security appliance 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 security appliance username followed by an at sign (@) and then the FTP username (name1@name2). For the password, the user enters the security appliance password followed by an at sign (@) and then the FTP password (password1@password2). For example, enter the following text.

```
name> jamiec@jchrichton
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 security appliance checks real ports when static PAT is configured. If it detects traffic destined for real port 80, regardless of the mapped port, the security appliance 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 security appliance intercepts the traffic and enforces HTTP authentication. Users see the HTTP authentication page in their web browsers before the security appliance 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 security appliance sends to the web browser an error message indicating that the user must be authenticated prior using the requested service.

Authenticating Directly with the Security Appliance

If you do not want to allow HTTP, HTTPS, Telnet, or FTP through the security appliance but want to authenticate other types of traffic, you can authenticate with the security appliance directly using HTTP or HTTPS by configuring the **aaa authentication listener** command.

You can authenticate directly with the security appliance at the following URLs when you enable AAA for the interface:

```
http://interface_ip[:port]/netaccess/connstatus.html
```

```
https://interface_ip[:port]/netaccess/connstatus.html
```

Alternatively, you can configure virtual Telnet (using the **virtual telnet** command). With virtual Telnet, the user Telnets to a given IP address configured on the security appliance, and the security appliance provides a Telnet prompt.

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 group named tacacs+. The second command line excludes Telnet traffic on the outside interface with an inside address of 192.168.38.0, with an outside IP address of all hosts:

```
hostname(config)# aaa authentication include tcp/0 outside 192.168.0.0 255.255.0.0 0 0
tacacs+
hostname(config)# aaa authentication exclude telnet outside 192.168.38.0 255.255.255.0 0 0
tacacs+
```

The following examples demonstrate ways to use the *interface-name* parameter. The security appliance 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/0 inside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

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

```
hostname(config)#aaa authentication include tcp/0 inside 192.168.1.0 255.255.255.0
209.165.202.128 255.255.255.224 tacacs+
```

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

```
hostname(config)# aaa authentication include tcp/0 outside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

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

```
hostname(config)# aaa authentication include tcp/0 outside 209.165.202.128 255.255.255.224
209.165.201.0 255.255.255.224 tacacs+
```

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

```
hostname(config)#aaa authentication include tcp/0 perimeter 209.165.202.128
255.255.255.224 209.165.201.0 255.255.255.224 tacacs+
```

Related Commands

Command	Description
aaa authentication console	Enables or disables authentication on entry to privileged mode or requires authentication verification to access the security appliance 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 security appliance prior to allowing HTTP requests to traverse the security appliance.
aaa-server protocol	Configures group-related server attributes.
aaa-server host	Configures host-related attributes.

aaa authentication console

To enable authentication service for access to the security appliance console over an SSH, HTTP, or Telnet connection or from the Console connector on the security appliance, use the **aaa authentication console** command in global configuration mode. This command also lets you enable access to privileged EXEC mode. To disable this authentication service, use the **no** form of this command.

aaa authentication {**serial** | **enable** | **telnet** | **ssh** | **http**} **console** {*server-tag* [**LOCAL**] | **LOCAL**}

no aaa authentication {**serial** | **enable** | **telnet** | **ssh** | **http**} **console** {*server-tag* [**LOCAL**] | **LOCAL**}

Syntax Description

enable	Enables authentication for entry to privileged EXEC mode using the **enable** command.
http	Enables authentication of ASDM sessions over HTTPS. The SDI server group protocol is not supported for HTTP management authentication.
LOCAL	The keyword **LOCAL** has two uses. It can designate the use of the local database, or it can specify fallback to the local database if the designated authentication server is unavailable.
serial	Enables authentication of admin sessions established on the serial console interface.
server-tag	Specifies the AAA server group tag defined by the **aaa-server protocol** command. You can also use the local user database by specifying the server group tag **LOCAL**.
ssh	Enables authentication of admin sessions over SSH.
telnet	Enables authentication of admin sessions over Telnet.

Defaults

By default, fallback to the local database 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
Preexisting	This command was preexisting.

Usage Guidelines

If you enable CLI authentication, the security appliance prompts you for your username and password to log in. After you enter your information, you have access to user EXEC mode.

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

If you configure enable authentication, the security appliance prompts you for your username and password. 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. This feature is particularly useful when you perform command authorization, where usernames are important to determine the commands a user can enter.

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

Before the security appliance can authenticate a Telnet, SSH, or HTTP user, you must first configure access to the security appliance using the **telnet**, **ssh**, and **http** commands. These commands identify the IP addresses that are allowed to communicate with the security appliance. Telnet access to the security appliance console is available from any internal interface, and from the outside interface with IPSec configured. SSH access to the security appliance console is available from any interface.

The **http** keyword authenticates the ASDM client that accesses the security appliance using HTTPS. You only need to configure HTTP authentication if you want to use a AAA server. By default, ASDM uses the local database for authentication even if you do not configure this command. HTTP management authentication does not support the SDI protocol for a AAA server group.

If you use a AAA server group for authentication, you can configure the security appliance to use the local database as a fallback method if the AAA server is unavailable. Specify the server group name followed by **LOCAL** (**LOCAL** is case sensitive). We recommend that you use the same username and password in the local database as the AAA server because the security appliance prompt does not give any indication which method is being used.

You can alternatively use the local database as your main method of authentication (with no fallback) by entering **LOCAL** alone.

The maximum username prompt for HTTP authentication is 30 characters. The maximum password length is 16 characters.

As the following table shows, the action of the prompts for authenticated access to the security appliance console differ, depending on the option you choose with this command.

Option	Number of Login Attempts Allowed
Enable	3 tries before access is denied
Serial	Continual until success
SSH	3 tries before access is denied
Telnet	Continual until success
HTTP	Continual until success

If the SSH authentication request times out (which implies the AAA servers may be down or not available), you can gain access to the security appliance using the username **pix** and the enable password (set with the **enable password** command). By default, the enable password is blank. This behavior differs from when you log into the security appliance without AAA configured; in that case, you use the login password (set by the **passwd** command).

If a **aaa authentication http console** command statement is not defined, you can gain access to the security appliance using ASDM with no username and the security appliance 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 security appliance using the default administrator username and the enable password. By default, the enable password is not set.

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 administrative 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 "srvgrp1" fail:

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config)# aaa authentication serial console srvgrp1 LOCAL
```

Related Commands

Command	Description
aaa authentication	Enables or disables user authentication.
aaa-server host	Specifies the AAA server to use for user authentication.
clear configure aaa	Remove/reset the configured AAA accounting values.
show running-config aaa	Display the AAA configuration.

aaa authentication listener

To enable HTTP(S) listening ports to authenticate network users, use the **aaa authentication listener** command in global configuration mode. When you enable a listening port, the security appliance serves an authentication page for direct connections and/or for through traffic. To disable the listeners, use the **no** form of this command.

aaa authentication listener http[**s**] *interface_name* [**port** *portnum*] [**redirect**]

no aaa authentication listener http[**s**] *interface_name* [**port** *portnum*] [**redirect**]

Syntax Description

http[s]	Specifies the protocol that you want to listen for, either HTTP or HTTPS. Enter this command separately for each protocol.
port *portnum*	Specifies the port number that the security appliance listens on; the defaults are 80 (HTTP) and 443 (HTTPS).
redirect	Redirects through traffic to an authentication web page served by the security appliance. Without this keyword, only traffic directed to the security appliance interface can access the authentication web pages.
interface_name	Specifies the interface on which you enable listeners.

Defaults

By default, no listener services are enabled, and HTTP connections use basic HTTP authentication. If you enable the listeners, the default ports are 80 (HTTP) and 443 (HTTPS).

If you are upgrading from 7.2(1), then the listeners are enabled on ports 1080 (HTTP) and 1443 (HTTPS). The **redirect** option is also enabled.

Command Modes

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

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

Command History

Release	Modification
7.2(2)	This command was introduced.

Usage Guidelines

Without the **aaa authentication listener** command, when HTTP(S) users need to authenticate with the security appliance after you configure the **aaa authentication match** or **aaa authentication include** command, the security appliance uses basic HTTP authentication. For HTTPS, the security appliance generates a custom login screen.

If you configure the **aaa authentication listener** command with the **redirect** keyword, the security appliance redirects all HTTP(S) authentication requests to web pages served by the security appliance.

Redirection is an improvement over the basic method because it provides an improved user experience when authenticating, and an identical user experience for HTTP and HTTPS in both Easy VPN and firewall modes. It also supports authenticating directly with the security appliance.

You might want to continue to use basic HTTP authentication if: you do not want the security appliance to open listening ports; if you use NAT on a router and you do not want to create a translation rule for the web page served by the security appliance; basic HTTP authentication might work better with your network. For example non-browser applications, like when a URL is embedded in email, might be more compatible with basic authentication.

If you enter the **aaa authentication listener** command *without* the **redirect** option, then you only enable direct authentication with the security appliance, while letting through traffic use basic HTTP authentication. The **redirect** option enables both direct and through-traffic authentication. Direct authentication is useful when you want to authenticate traffic types that do not support authentication challenges; you can have each user authenticate directly with the security appliance before using any other services.

Examples

The following example configures the security appliance to redirect HTTP and HTTPS connections to the default ports:

```
hostname(config)# aaa authentication http redirect
hostname(config)# aaa authentication https redirect
```

The following example allows authentication requests directly to the security appliance; through traffic uses basic HTTP authentication:

```
hostname(config)# aaa authentication http
hostname(config)# aaa authentication https
```

The following example configures the security appliance to redirect HTTP and HTTPS connections to non-default ports:

```
hostname(config)# aaa authentication http port 1100 redirect
hostname(config)# aaa authentication https port 1400 redirect
```

Related Commands

Command	Description
aaa authentication match	configures user authentication for through traffic.
aaa authentication secure-http-client	
clear configure aaa	Removes the configured AAA configuration.
show running-config aaa	Displays the AAA configuration.
virtual http	

aaa authentication match

To enable authentication for connections through the security appliance, 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
Preexisting	This command was preexisting.

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.

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 security appliance 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 security appliance 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 security appliance allows other traffic requiring authentication.

The authentication ports that the security appliance supports for AAA are fixed:

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

Security Appliance Authentication Prompts

For Telnet and FTP, the security appliance generates an authentication prompt.

For HTTP, the security appliance uses basic HTTP authentication by default, and provides an authentication prompt. You can optionally configure the security appliance to redirect users to an internal web page where they can enter their username and password (configured with the **aaa authentication listener** command).

For HTTPS, the security appliance generates a custom login screen. You can optionally configure the security appliance to redirect users to an internal web page where they can enter their username and password (configured with the **aaa authentication listener** command).

Redirection is an improvement over the basic method because it provides an improved user experience when authenticating, and an identical user experience for HTTP and HTTPS in both Easy VPN and firewall modes. It also supports authenticating directly with the security appliance.

You might want to continue to use basic HTTP authentication if: you do not want the security appliance to open listening ports; if you use NAT on a router and you do not want to create a translation rule for the web page served by the security appliance; basic HTTP authentication might work better with your network. For example non-browser applications, like when a URL is embedded in email, might be more compatible with basic authentication.

After you authenticate correctly, the security appliance redirects you to your original destination. If the destination server also has its own authentication, the user enters another username and password. If you use basic HTTP authentication and need to enter another username and password for the destination server, then you need to configure the **virtual http** command.

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 security appliance 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 security appliance username followed by an at sign (@) and then the FTP username (name1@name2). For the password, the user enters the security appliance password followed by an at sign (@) and then the FTP password (password1@password2). For example, enter the following text.

```
name> jamiec@jchrichton
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 security appliance checks real ports when static PAT is configured. If it detects traffic destined for real port 80, regardless of the mapped port, the security appliance 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 security appliance intercepts the traffic and enforces HTTP authentication. Users see the HTTP authentication page in their web browsers before the security appliance 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 security appliance sends to the web browser an error message indicating that the user must be authenticated prior using the requested service.

Authenticating Directly with the Security Appliance

If you do not want to allow HTTP, HTTPS, Telnet, or FTP through the security appliance but want to authenticate other types of traffic, you can authenticate with the security appliance directly using HTTP or HTTPS by configuring the **aaa authentication listener** command.

You can authenticate directly with the security appliance at the following URLs when you enable AAA for the interface:

```
http://interface_ip[:port]/netaccess/connstatus.html
https://interface_ip[:port]/netaccess/connstatus.html
```

Alternatively, you can configure virtual Telnet (using the **virtual telnet** command). With virtual Telnet, the user Telnets to a given IP address configured on the security appliance, and the security appliance provides a Telnet prompt.

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 security appliance 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	Remove/reset 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 security appliance, 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 security appliance prior to allowing user HTTP-based web requests to traverse the security appliance.

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
Preexisting	This command was preexisting.

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:

- At runtime, a maximum of 16 HTTPS authentication processes is allowed. If all 16 HTTPS authentication processes are running, the 17th, new HTTPS connection requiring authentication is 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
```

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 LOCAL, TACACS+, or RADIUS user authentication, on a server designated by the **aaa-server** command.
virtual telnet	Accesses the security appliance virtual server.

aaa authorization

To include or exclude user authorization for traffic through the security appliance using a TACACS+ server, use the **aaa authorization** command with the **include** or **exclude** keywords in global configuration mode. To disable user authorization, use the **no** form of this command.

aaa authorization {**include** | **exclude**} *authorization-service interface-name inside-ip inside-mask* [*outside-ip outside-mask*] *tacacs+-server-tag*

no aaa authorization {**include** | **exclude**} *authorization-service interface-name inside-ip inside-mask* [*outside-ip outside-mask*] *tacacs+-server-tag*

Syntax Description

authorization-service	The type of traffic to include or exclude from authorization, including: • **any**—Authorizes all traffic. • **telnet**—Authorizes Telnet traffic. • **ssh**—Authorizes SSH traffic. • **ftp**—Authorizes FTP traffic. • **http**—Authorizes HTTP traffic. • **https**—Authorizes HTTPS traffic. • **icmp/***type*—Authorizes ICMP traffic of the specified type. • *proto*—Authorizes an IP protocol, by value or name, for example, **ip** or **igmp**. • **tcp/***port*[**-***port*]—Authorizes TCP traffic of the specified port or port range. Specify **0** to authorize all TCP traffic. • **udp/***port*[**-***port*]—Authorizes UDP traffic of the specified port or port range. Specify **0** to authorize all UDP traffic. **Note** Specifying a port range might produce unexpected results at the authorization server. The security appliance 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.
exclude	Creates an exception to a previously stated rule by excluding the specified service from authorization.
include	Authorizes traffic that matches the rule.
inside-ip	Specifies the IP address of the inside (higher security level) host or network that is either the source or destination for connections requiring authorization. You can set this address to **0** to mean all hosts. Always specify the higher security IP addresses before the lower security IP addresses in this command, regardless of the interface to which you apply authorization.
inside-mask	Specifies the network mask of *inside-ip*.
interface-name	Specifies the interface where connections originate.

outside-ip	(Optional) Specifies the outside (lower security level) IP address for traffic you want to authorize. Specify **0** to indicate all hosts. Always specify the higher security IP addresses before the lower security IP addresses in this command, regardless of the interface to which you apply authorization.
outside-mask	(Optional) The network mask of *outside-ip*.
tacacs+-server-tag	Specifies a TACACS+ server group tag defined by the **aaa-server protocol** 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
7.0(1)	The **exclude** parameter now allows the user to specify a port to exclude to a specific host or hosts.

Usage Guidelines

You can configure the security appliance to perform network access authorization with TACACS+.

We recommend using the **aaa authorization match** command instead of the **aaa authorization include** or **exclude** command. You cannot use the **aaa authorization include** or **exclude** command and the **aaa authorization match** command in the same configuration. The **aaa authorization match** command uses an access list to match traffic, and is a more robust command for this feature.

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

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 security appliance. A specific authorization rule does not require the equivalent authentication. Authentication is required only with FTP, HTTP, or Telnet to provide an interactive way for the user to enter the authorization credentials. 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 security appliance checks the authorization rules for matching traffic. If the traffic matches the authorization statement, the security appliance sends the username to the TACACS+ server. The TACACS+ server responds to the security appliance with a permit or a deny for that traffic, based on the user profile. The security appliance enforces the authorization rule in the response.

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
```

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 serial 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 access to the security appliance serial 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	Remove/reset the configured AAA accounting values.
show running-config aaa	Display the AAA configuration.

aaa authorization command

To configure command authorization for management access, 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** | *tacacs+-server-tag* [**LOCAL**]}

no **aaa authorization command** {**LOCAL** | *tacacs+-server-tag* [**LOCAL**]}

Syntax Description

LOCAL	Specifies the use of the 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.
tacacs+-server-tag	Specifies a predefined server group tag for the TACACS+ authorization server. The AAA server group tag as defined by the **aaa-server protocol** 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
7.0(1)(1)	This command was modified to allow configuring administrative authorization to support fallback to the local user database if all servers in the specified group are disabled.

Usage Guidelines

By default when you log in, you can access user EXEC mode, which offers only minimal commands. When you enter the **enable** command (or the **login** command when you use the local database), you can access privileged EXEC mode and advanced commands, including configuration commands. If you want to control the access to commands, the security appliance lets you configure command authorization, where you can determine which commands that are available to a user.

You can use one of two command authorization methods:

- Local database—Configure the command privilege levels on the security appliance using the **privilege** command. When a local user authenticates with the **enable** command (enabled with the **aaa authenticate enable console** command) or logs in with the **login** command, the security appliance places that user in the privilege level that is defined by the local database. The user can then access commands at the user's privilege level and below. Local command authorization places each user at a privilege level, and each user can enter any command at their privilege level or below. The security appliance lets you assign commands to one of 16 privilege levels (0 to 15). By default, each command is assigned either to privilege level 0 or 15.

Note You can use local command authorization without any users in the local database and without CLI or enable authentication. Instead, when you enter the **enable** command, you enter the system enable password, and the security appliance places you in level 15. You can then create enable passwords for every level, so that when you enter **enable** *n* (2 to 15), the security appliance 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. If you enable TACACS+ command authorization, and a user enters a command at the CLI, the security appliance sends the command and username to the TACACS+ server to determine if the command is authorized.

  Before you enable TACACS+ command authorization, be sure that you are logged into the security appliance as a user that is defined on the TACACS+ server, and that you have the necessary command authorization to continue configuring the security appliance. For example, you should log in as an admin user with all commands authorized. Otherwise, you could become unintentionally locked out.

  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 security appliance.

  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 security appliance. 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.

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	Enable or disable user authorization for a LOCAL or a TACACS+ server designated by the **aaa-server** command, or for ASDM user authentication.
aaa-server host	Configure host-related attributes.
aaa-server protocol	Configure group-related server attributes.

Command	Description
clear configure aaa	Remove/reset the configured AAA accounting values.
show running-config aaa	Display the AAA configuration.

aaa authorization match

To enable user authorization for traffic through the security appliance using a TACACS+ server, use the **aaa authorization match** command in global configuration mode. To disableauthorization, 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 the name of an access list to identify the traffic you want to authorize. See the **access-list** command. The **permit** ACEs mark matching traffic for authorization, while **deny** entries exclude matching traffic from authorization.
interface-name	Specifies the interface where connections originate.
server-tag	Specifies the TACACS+ server group tag defined by the **aaa-server protocol** 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
Preexisting	This command was preexisting.

Usage Guidelines

You can configure the security appliance to perform network access authorization with TACACS+.

We recommend using the **aaa authorization match** command instead of the **aaa authorization include** or **exclude** command. You cannot use the **aaa authorization include** or **exclude** command and the **aaa authorization match** command in the same configuration. The **aaa authorization match** command uses an access list to match traffic, and is a more robust command for this feature.

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 security appliance. A specific authorization rule does not require the equivalent authentication. Authentication is required only with FTP, HTTP, or Telnet to provide an interactive way for the user to enter the authorization credentials. 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 security appliance checks the authorization rules for matching traffic. If the traffic matches the authorization statement, the security appliance sends the username to the TACACS+ server. The TACACS+ server responds to the security appliance with a permit or a deny for that traffic, based on the user profile. The security appliance enforces the authorization rule in the response.

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
```

Examples

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

```
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 authen1 inside tplus1
hostname(config)#aaa accounting match acct1 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 two command statements specify that any connections traversing the inside interface to any foreign host are authenticated using the tplus1 server group, and that all these connections are logged in the accounting database. The last command statement specifies that any connections that match the ACEs in myacl are authorized by the AAA servers in the tplus1 server group.

Related Commands

Command	Description
aaa authorization	Enable or disable user authorization for a LOCAL or a TACACS+ server designated by the **aaa-server** command, or for ASDM user authentication.
clear configure aaa	Reset all aaa configuration parameters to the default values.
clear uauth	Delete one user or all users' AAA authorization and authentication caches, which forces the user to reauthenticate the next time that he or she creates a connection.
show running-config aaa	Display the AAA configuration.
show uauth	Display 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 security appliance 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
7.0(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.

After a user makes the configured number of attempts with the wrong password, the user is locked out and cannot log in successfully until the 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 security appliance 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 user's locked-out status.
show aaa local user	Shows the list of usernames that are currently locked.

aaa mac-exempt

To specify the use of a predefined list of MAC addresses to exempt from authentication and authorization, use the **aaa mac-exempt** command in global configuration mode. You can only add one **aaa mac-exempt** command. To disable the use of a list of MAC addresses, 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
Preexisting	This command was preexisting.

Usage Guidelines

Configure the MAC list number 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 manually configure the uauth session limit by setting 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 (16), 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
Preexisting	This command was preexisting.

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	Enable, disable, or view LOCAL, TACACS+, or RADIUS user authentication, on a server designated by the **aaa-server** command, or ASDM user authentication
aaa authorization	Enable or disable LOCAL or TACACS+ user authorization services.
aaa-server host	Specifies a AAA server.
clear configure aaa	Remove/reset the configured AAA accounting values.
show running-config aaa	Display the AAA configuration.

aaa-server host

To configure a AAA server as part of a AAA server group and 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 the 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* | *name*} [*key*] [**timeout** *seconds*]

no aaa-server *server-tag* [(*interface-name*)] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*]

Syntax Description

(*interface-name*)	(Optional) Specifies the network interface where the authentication server resides. The parentheses are required in this parameter. If you do not specify an interface, the default is **inside**, if available.
key	(Optional) Specifies a case-sensitive, alphanumeric keyword of up to 127 characters that is the same value as the key on the RADIUS or TACACS+ server. Any characters entered past 127 are ignored. The key is used between the security appliance and the server for encrypting data between them. the key must be the same on both the security appliance 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 host mode.
name	Specifies the name of the server using either a name assigned locally using the **name** command or a DNS name. Maximum characters is 128 for DNS names and 63 characters for names assigned using the **name** command.
server-ip	Specifies the IP address of the AAA server.
server-tag	Specifies a symbolic name of the server group, which is matched by the name specified by the **aaa-server protocol** command.
timeout *seconds*	(Optional) The timeout interval for the request. This is the time after which the security appliance gives up on the request to the primary AAA server. If there is a standby AAA server, the security appliance 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.

The default interface is inside.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	Support for DNS names was added.

Usage Guidelines

You control AAA server configuration by defining a AAA server group protocol with the **aaa-server protocol** command, and then you add servers to the group using the **aaa-server host** command.

You can have up to 15 server groups in single mode or 4 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.

After you enter the **aaa-server host** command, you can configure host-specific parameters.

Examples

The following example configures a Kerberos AAA server group named “watchdogs”, adds a AAA server to the group, and defines the Kerberos realm for the server.

Note Kerberos realm names use numbers and upper-case letters only. Although the security appliance accepts lower-case letters for a realm name, it does not translate lower-case letters to upper-case letters. Be sure to use upper-case letters only.

```
hostname(config)# aaa-server watchdogs protocol kerberos
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server watchdogs host 192.168.3.4
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
```

The following example configures an SDI AAA server group named “svrgrp1”, and then adds a AAA server to the group, 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)# exit
hostname(config)# aaa-server svrgrp1 host 192.168.3.4
hostname(config-aaa-server-host)# timeout 6
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# sdi-version sdi-5
```

Related Commands

Command	Description
aaa-server protocol	Creates and modifies AAA server groups.
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 protocol

To create a AAA server group and configure AAA server parameters that are group-specific and common to all group hosts, use the **aaa-server protocol** command in global configuration mode to enter the AAA-server group mode, from which you can configure these group parameters. To remove the designated group, use the **no** form of this command.

aaa-server *server-tag* **protocol** *server-protocol*

no aaa-server *server-tag* **protocol** *server-protocol*

Syntax Description

server-tag	Specifies the server group name, which is matched by the name specified by the **aaa-server host** commands. Other AAA commands make reference to the AAA server group name.
server-protocol	The AAA protocol that the servers in the group support: **kerberos**, **ldap**, **nt**, **radius, sdi,** or **tacacs+**.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You control AAA server configuration by defining a AAA server group protocol with the **aaa-server protocol** command, and then you add servers to the group using the **aaa-server host** command.

You can have up to 15 server groups in single mode or 4 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.

After you enter the **aaa-server protocol** command, you can configure host-specific parameters. For example, if AAA accounting is in effect, the accounting information goes only to the active server unless you have configured simultaneous accounting using the **accounting-mode** command.

Examples

The following example shows the use of the **aaa-server protocol** command to modify details of a TACACS+ server group configuration:

```
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
```

Related Commands

Command	Description
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

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
7.0(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 security appliance.
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 security appliance based on time.

accept-subordinates

To configure the security appliance 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 the 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
7.0(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 security appliance. 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 security appliance to accept subordinate certificates for trustpoint central:

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

Related Commands

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

access-group

To bind an access list to an interface, use the **access-group** command in global configuration mode. To unbind an 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*

Syntax Description

access-list	Access list *id.*
in	Filters the inbound packets at the specified interface.
interface *interface-name*	Name of the network interface.
out	Filters the outbound packets at the specified interface.
per-user-override	(Optional) Allows downloadable user access lists to override the access list applied to the interface.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **access-group** command binds an access list to an interface. The access list is applied to traffic inbound to an interface. If you enter the **permit** option in an **access-list** command statement, the security appliance continues to process the packet. If you enter the **deny** option in an **access-list** command statement, the security appliance discards the packet and generates the following syslog message.

```
%hostname-4-106019: IP packet from source_addr to destination_addr, protocol
protocol received from interface interface_name deny by access-group id
```

The *per-user-override* option allows downloaded access lists to override the access list applied to the interface. If the *per-user-override* optional argument is not present, the security appliance preserves the existing filtering behavior. When *per-user-override* is present, the security appliance allows the **permit** or **deny** status from the per-user access-list (if one is downloaded) associated to a user to override the permit or deny status from the **access-group** command associated access list. 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.

Always use the **access-list** command with the **access-group** command.

The **access-group** command binds an access list to an interface. The **in** keyword applies the access list to the traffic on the specified interface. The **out** keyword applies the access list to the outbound traffic.

Note If all of the functional entries (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.

The **no access-group** command unbinds the access list from the interface *interface_name*.

The **show running config access-group** command displays the current access list bound to the interfaces.

The **clear configure access-group** command removes all the access lists from the interfaces.

Examples

The following example shows how to use the **access-group** command:

```
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
```

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.

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
Preexisting	This command was preexisting.

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 security appliance 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 security appliance.
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 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
Preexisting	This command was preexisting.

Usage Guidelines

Syslog message 106101 is generated when the security appliance 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 security appliance.
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 security appliance 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.

When the **log** optional keyword is specified, the default level for syslog message 106100 is 6 (informational).

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Because EtherTypes are connectionless, you need to apply the ACL 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 security appliance by configuring both MPLS routers connected to the security appliance to use the IP address on the security appliance 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 ACL of each type (extended and EtherType) to each direction of an interface. You can also apply the same ACLs 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 security appliance. 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.
extended	(Optional) Adds an 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. **Note** You must specify the interface keyword instead of specifying the actual IP address in the access list when the traffic destination is device interface.
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 security appliance 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 security appliance. 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 system log 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 system log 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
Preexisting	This command was preexisting.

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 security appliance decides whether to forward or drop a packet, the security appliance 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 security appliance 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 security appliance 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**) (security appliance to host) or **echo** (**8**) (host to security appliance). 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.

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

Table 2-1 ICMP Type Literals (continued)

ICMP Type	Literal
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 security appliance:

```
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 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
Preexisting	This command was preexisting.

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.

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 security appliance.
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.

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

no access-list *id* **standard** [**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 (optional).
id	Name or number of an access list.
ip_address ip_mask	Specifies access to a specific IP address (optional) 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 security appliance 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
7.0(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 security appliance. By default, the security appliance denies all packets on the originating interface unless you specifically permit access.

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.
- Use the **host** *ip_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
```

The following example shows how to specify a destination address:

```
hostname(config)# access-list 77 standard permit host 10.1.10.123
```

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.

access-list webtype

To add an access list to the configuration that supports filtering for WebVPN, use the **access-list webtype** command in global configuration mode. To remove the access list, use the **no** form of this command.

access-list *id* **webtype** {**deny** | **permit**} **url** [*url_string* | **any**] [**log** [[**disable** | **default**] | *level*] [**interval** *secs*] [**time_range** *name*]]

no access-list *id* **webtype** {**deny** | **permit**} **url** [*url_string* | **any**] [**log** [[**disable** | **default**] | *level*] [**interval** *secs*] [**time_range** *name*]]

access-list *id* **webtype** {**deny** | **permit**} **tcp** [**host** *ip_address* | *ip_address subnet_mask* | **any**] [*oper port* [*port*]] [**log** [[**disable** | **default**] | *level*] [**interval** *secs*] [**time_range** *name*]]

no **access-list** *id* **webtype** {**deny** | **permit**} **tcp** [**host** *ip_address* | *ip_address subnet_mask* | **any**] [*oper port* [*port*]] [**log** [[**disable** | **default**] | *level*] [**interval** *secs*] [**time_range** *name*]]

Syntax Description

any	Specifies all IP addresses.
any	(Optional) Specifies all urls.
deny	Denies access if the conditions are matched.
host *ip_address*	Specifies a host IP address.
id	Name or number of an access list.
interval *secs*	(Optional) Specifies the time interval at which to generate an 106100 syslog message; valid values are from 1 to 600 seconds.
ip_address ip_mask	Specifies a specific IP address and subnet mask.
log [[**disable** | **default**] | *level*]	(Optional) Specifies that a syslog message 106100 is generated for the ACE. See the **log** command for information.
oper	Compares *ip_address* ports. Possible operands include lt (less than), gt (greater than), eq (equal), neq (not equal), and range (inclusive range).
permit	Permits access if the conditions are matched.
port	Specifies the decimal number or name of a TCP or UDP port.
time_range *name*	(Optional) Specifies a keyword for attaching the time-range option to this access list element.
url	Specifies that a url be used for filtering.
url_string	(Optional) Specifies the url to be filtered.

Defaults

The defaults are as follows:

- The security appliance 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.
- When the **log** optional keyword is specified, the default level for syslog message 106100 is 6 (informational).

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **access-list webtype** command is used to configure WebVPN filtering. The url specified may be full or partial (no file specified), may include wildcards for the server, or may specify a port.

Valid protocol identifiers are: http, https, cifs, imap4, pop3, and smtp. The url may also contain the keyword **any** to refer to any url. An asterisk may be used to refer to a subcomponent of a DNS name.

Examples

The following example shows how to deny access to a specific company url:

```
hostname(config)# access-list acl_company webtype deny url http://*.company.com
```

The following example shows how to deny access to a specific file:

```
hostname(config)# access-list acl_file webtype deny url
https://www.company.com/dir/file.html
```

The following example shows how to deny http access to anywhere through port 8080:

```
hostname(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

Related Commands

Command	Description
access-group	Defines object groups that you can use to optimize your configuration.
access-list ethertype	Configures an access list that controls traffic based on its EtherType.
access-list extended	Adds an access list to the configuration and configures policy for IP traffic through the firewall.
clear access-group	Clears an access list counter.
show running-config access-list	Displays the access list configuration running on the security appliance.

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 mode. To remove the accounting mode specification, use the **no** form of this command:

accounting-mode {**simultaneous** | **single**}

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	•	•	•	•	—

Command History

Release	Modification
7.0(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
hostname(config-aaa-server-group)# exit
hostname(config)#
```

Related Commands

Command	Description
aaa accounting	Enables or disables accounting services.

aaa-server protocol	Enters AAA server group configuration mode, so 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 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	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

Examples

The following example configures a RADIUS AAA server named "srvgrp1" on host "1.2.3.4", 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 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# accountinq-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 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.

accounting-server-group *server-group*

no accounting-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
7.0(1)	This command was introduced.
7.1(1)	Moved this command to the tunnel-group general-attributes configuration mode from the webvpn configuration mode.

Usage Guidelines

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

Examples

The following example entered in tunnel-group-general attributes 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-attributes
hostname(config-tunnel-general)# accounting-server-group aaa-server123
hostname(config-tunnel-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 general-attributes	Specifies the general attributes for the named tunnel-group.

accounting-server-group (webvpn)

To specify the set of accounting servers to use with WebVPN or e-mail proxy, use the **accounting-server-group** command. For WebVPN, use this command in webvpn mode. For e-mail proxies (IMAP4S. POP3S, SMTPS), use this command in the applicable e-mail proxy mode. To remove accounting servers from the configuration, use the **no** form of this command.

The security appliance uses accounting to keep track of the network resources that users access.

accounting-server-group *group tag*

no accounting-server-group

Syntax Description

group tag	Identifies the previously configured accounting server or group of servers. Use the **aaa-server** command to configure accounting servers. Maximum length of the group tag is 16 characters.

Defaults

No accounting servers are configured by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	This command was deprecated. The accounting-server-group command is now available in tunnel-group general-attributes configuration mode.

Usage Guidelines

In Release 7.1(1), if you enter this command in webvpn configuration mode, it is transformed to the same command in tunnel-group general-attributes mode.

Examples

The following example shows how to configure WebVPN services to use the set of accounting servers named WEBVPNACCT:

```
hostname(config)# webvpn
hostname(config-webvpn)# accounting-server-group WEBVPNACCT
```

The following example shows how to configure POP3S e-mail proxy to use the set of accounting servers named POP3SSVRS:

```
hostname(config)# pop3s
hostname(config-pop3s)# accounting-server-group POP3SSVRS
```

Related Commands

Command	Description
aaa-server host	Configures authentication, authorization, and accounting servers.