aaa accounting through accounting-server-group Commands

aaa accounting

To enable, disable, or view TACACS+, or RADIUS user accounting (on a server designated by the **aaa-server host** command), use the **aaa accounting** command in global configuration mode. To disable these functions use the **no** form of this command.

aaa accounting {**include** | **exclude**} *service interface-name local-ip local-mask foreign-ip foreign-mask server-tag*

no aaa accounting {**include** | **exclude**} *service interface-name local-ip local-mask foreign-ip foreign-mask server-tag*

aaa accounting {**include** | **exclude**} *service interface-name server-tag*

no aaa accounting {**include** | **exclude**} *service interface-name server-tag*

Syntax Description

exclude	Create an exception to a previously stated rule by excluding the specified service from accounting. The **exclude** parameter allows the user to specify a service or protocol/port to exclude to a specific host or hosts.
foreign-ip	Specify the IP address of the hosts you want to access the *local-ip* address. Use 0 to mean all hosts. the *foreign-ip address* is always on the lowest security-level interface.
foreign-mask	Specify the network mask of *foreign-ip*. Always specify a specific mask value. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
interface-name	Specify the interface name from which users require authentication. Use *interface-name* in combination with the *local-ip* address and the *foreign-ip* address to determine where access is sought and from whom.
include	Create a new rule with the specified service to include.
local-ip	Specify the IP address of the host or network of hosts that you want to be authenticated or authorized. Set this address to 0 to mean all hosts and to let the authentication server decide which hosts are allowed access. The *local-ip* address is always on the highest security-level interface.
local-mask	Specify the network mask of *local-ip*. Always specify a specific mask value. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
server-tag	Specify the AAA server group tag defined by the **aaa-server host** command.
service	The services/access method that should be accounted for. Accounting is provided for all services, or you can limit it to one or more services. Possible values are **enable**, **http**, **serial**, **ssh**, **telnet**, or *protocol/port*. Use **enable** to provide accounting for all TCP services. To provide accounting for UDP services, use the *protocol/port* form.

Defaults

For *protocol/port*, the TCP protocol appears as 6, the UDP protocol appears as 17, and so on, and port is the TCP or UDP destination port. A port value of 0 (zero) means all ports. For protocols other than TCP and UDP, the *port* is not applicable and should not be used.

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
Preexisting	This command was preexisting.

Usage Guidelines

User accounting services keep a record of which network services a user has accessed. These records are kept on the designated AAA server or servers. Accounting information is sent only to the active server in a server group unless you enable simultaneous accounting.

Before you can use this command, you must first designate an 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.

Note Traffic that is not specified by an **include** statement is not processed.

For outbound connections, first use the **nat** command to determine which IP addresses can access the security appliance. For inbound connections, first use the **static** and **access-list extended** command statements to determine which inside IP addresses can be accessed through the security appliance from the outside network.

If you want to allow connections to come from any host, code the local IP address and netmask as **0.0.0.0 0.0.0.0**, or **0 0**. The same convention applies to the foreign host IP address and netmask; **0.0.0.0 0.0.0.0** means any foreign host.

Examples

The following example enables accounting on all 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 authentication include any inside 0 0 0 0 mygroup
hostname(config)# aaa authorization include any inside 0 0 0 0 mygroup
hostname(config)# aaa accounting include any inside 0 0 0 0 mygroup
hostname(config)# aaa authentication serial console mygroup
```

This example specifies that the authentication server with the IP address 192.168.10.10 resides on the inside interface and is in the TACACS+ server group. The next three command statements specify that any users starting outbound connections to any foreign host will be authenticated using TACACS+, 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 TACACS+ server.

Related Commands

Command	Description
aaa accounting match	Enable or disable the use of a specified access list that must be matched to enable user accounting (on a server designated by the **aaa-server** command).
aaa accounting command	Enable support for AAA accounting administrative access.
aaa-server host	Configure host-related attributes.
clear configure aaa	Remove/reset the configured AAA accounting values.
show running-config aaa	Display the AAA configuration.

aaa accounting command

To configure command accounting so that the security appliance sends to the accounting server each command entered by an administrator, use the **aaa accounting command** command in global configuration mode. To disable support for AAA command privilege accounting, use the **no** form of this command. The **aaa accounting command** command indicates the minimum level that must be associated with a command for an accounting record to be generated.

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

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

Syntax Description

server-tag	The server or group of TACACS+ servers to which accounting records are sent.
privilege *level*	The minimum level that must be associated with a command for an accounting record to be generated. The default privilege level is 0.

Defaults

The default privilege level is 0. By default, AAA command-privilege 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 modified to include the administrative option.

Usage Guidelines

When you configure the **aaa accounting command** command, each command entered by an administrator/user is recorded and sent to the accounting server or servers. The optional **privilege** specification indicates the minimum privilege level that must be associated with a command for an accounting record to be generated.

This command applies only to TACACS+ servers.

You must specify the name of the server or group, previously specified in an **aaa-server** command, to which this command applies.

Examples

The following example specifies that accounting records will be generated for any command at privilege level 6 or higher, and that these records are sent to the server from the group named adminserver.

```
hostname(config)# aaa accounting command privilege 6 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 {**http | serial| telnet | ssh | enable**} **console** *server-tag*

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

Syntax Description

enable	Enables or disables the generation of accounting records to mark the entry to and exit from privileged EXEC mode.
http	Enables or disables the generation of accounting records to mark the establishment and termination of admin sessions created over HTTP.
serial	Enables or disables 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 or group of servers to which accounting records are sent. Valid server group protocols are RADIUS and TACACS+.
ssh	Enables or disables the generation of accounting records to mark the establishment and termination of admin sessions created over SSH.
telnet	Enables or disables 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 HTTP transactions, and that these records are sent to the server named adminserver.

```
hostname(config)# aaa accounting http 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 match

To enable accounting for traffic that is identified by an access list, use the **aaa accounting match** command in global configuration mode. To disable accounting for traffic that is identified by an access list, use the **no** form of this command. The **aaa accounting match** command specifies an access list name that must be matched, as well as an interface name and a server tag.

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 name of an ACL that matches the traffic that you want the security appliance to perform accounting for. The *acl-name* argument must be the name of an ACL created with the **access-list** command.
interface-name	Specify the interface name from which users require accounting.
server-tag	Specify the AAA 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

The **aaa accounting match** command requires that you specify an ACL that permits the traffic for which you want the security appliance to send accounting data to AAA servers. The security appliance performs accounting for traffic permitted by the ACL and does not perform accounting for traffic denied by the ACL.

Before you can use this command, you must first create the AAA-server group tag by using the **aaa-server protocol** command.

User accounting services keep a record of which network services a user has accessed. These records are kept on the designated AAA servers. Accounting information is sent only to the active server in a server group unless simultaneous accounting is enabled. See the **accounting-mode** command for more information.

Examples

The following example enables accounting for traffic matching an ACL, acl2, followed by the output of the **show access-list** command that displays the ACL:

```
hostname(config) # aaa accounting match acl2 outside radserver1
hostname(config) # show access-list acl12
access-list acl12; 1 elements
access-list acl12 line 1 extended permit tcp any any (hitcnt=54021)
```

Related Commands

Command	Description
aaa accounting	Enable, disable, or view TACACS+ or RADIUS user accounting (on a server designated by the **aaa-server** command).
access-list extended	Create 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

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

Authentication lets you control access by requiring a valid username and password. You can configure the security appliance to authenticate the following items:

- All administrative connections to the security appliance including the following sessions:
  - Telnet
  - SSH
  - ASDM (using HTTPS)
  - VPN management access
- The **enable** command
- Network access through the security appliance

Each authentication server has a single pool of users. If you use the same server for multiple authentication rules and types, then a user needs to authenticate only one time for all rules and types, until the session expires. For example, if you configure the security appliance to authenticate Telnet and FTP, and a user successfully authenticates for Telnet, then as long as the session exists, the user does not also have to authenticate for FTP.

aaa authentication include | exclude *authentication-service interface-name local-ip local-mask* [*foreign-ip foreign-mask*] *server-tag*

no aaa authentication include | exclude *authentication-service interface-name local-ip local-mask* [*foreign-ip foreign-mask*] *server-tag*

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

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

Syntax Description

authentication-service	The type of traffic to include or exclude from authentication, based on the service option selected.
exclude	Creates an exception to a previously stated rule by excluding the specified service from authentication. The **exclude** parameter improves the former **except** option by allowing the user to specify a port to exclude to a specific host or hosts.
foreign-ip	(Optional) IP address of the foreign host that is either the source or destination for connections requiring authentication; **0** indicates all hosts.
foreign-mask	(Optional) The network mask of *foreign-ip*.
ftp	Specifies FTP for enabling or disabling authentication challenge for traffic of this protocol type.
include	Creates a new rule with the specified service to include.
interface-name	The interface name from which users require authentication.
http	Specifies HTTP for enabling or disabling authentication challenge for traffic of this protocol type.

https	Specifies HTTPS for enabling or disabling authentication challenge for traffic of this protocol type.
local-ip	The IP address of the local/internal host or network of hosts that is either the source or destination for connections requiring authentication. You can set this address to **0** to mean all hosts and to let the authentication server decide which hosts are authenticated.
local-mask	The network mask of *local-ip*.
server-tag	The AAA server group tag defined by the **aaa-server** command.
telnet	Specifies Telnet for enabling or disabling authentication challenge for traffic of this protocol type.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

To include or exclude traffic for authentication, you must designate an authentication server with the **aaa-server** command before using the **aaa authentication** command. Each combination of local and foreign IP addresses can have one **aaa authentication** command for inbound connections and one for outbound connections. A session whose IP address is identified by the **aaa-server authentication** command starts a connection through FTP, Telnet, HTTP, or HTTPS and is prompted for a username and password. If the username and password are verified by the designated authentication server, the security appliance allows further traffic between the authenticating host and the client address.

Use the *interface-name*, *local-ip*, and *foreign-ip* variables to define where access is sought and from whom. The address for *local-ip* is always on the highest security level interface and *foreign-ip* is always on the lowest.

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

For the local and foreign IP address masks, you can use **0** as a shorthand representation if the IP address is 0.0.0.0. Use **255.255.255.255** for a host.

The authentication servers determine whether a user can or cannot access the system, what services can be accessed, and what IP addresses the user can access. The security appliance proxies FTP, HTTP, HTTPS, and Telnet to display the credentials prompts.

Note When a cut-through proxy is configured, TCP sessions (TELNET, FTP, HTTP, or HTTPS) might have their sequence numbers randomized even if the **norandomseq** option is used in the **nat** or **static** command. This occurs when a AAA server proxies the TCP session to authenticate the user before permitting access.

local access authentication

To configure a AAA server (TACACS+, RADIUS, or LOCAL) to authenticate administrators, choose one of the following access authentication service options: **serial** for serial console access, **telnet** for Telnet access, **ssh** for SSH access, **http** for HTTP access, and **enable** for enable-mode access.

cut-through authentication

For cut-through proxy and "to the box" authentication, you can also use the local security appliance user authentication database by specifying the server group tag **LOCAL**. If **LOCAL** is specified for *server-tag* and the local user credential database is empty, the following warning message appears:

```
Warning:local database is empty! Use 'username' command to define local users.
```

Conversely, if the local database becomes empty when **LOCAL** is still present in the command, the following warning message appears:

```
Warning:Local user database is empty and there are still commands using 'LOCAL' for
authentication.
```

The cut-through authentication service options are as follows: **telnet**, **ftp**, **http**, **https**, **icmp/***type*, *proto*, **tcp/***port*, and **udp/***port*. The variable *proto* can be any supported IP protocol value or name: for example, **ip** or **igmp**. Only Telnet, FTP, HTTP, or HTTPS traffic triggers interactive user 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

For this reason, do not use Static PAT to reassign ports for services you want to authenticate. In other words, when the port to authenticate is not one of the three known ports, the security appliance rejects the connection instead of authenticating it.

You can enter an ICMP message type number for *type* to include or exclude that specific ICMP message type from authentication. For example, **icmp/8** includes or excludes type 8 (echo request) ICMP messages.

The **tcp/0** option enables authentication for all TCP traffic, which includes FTP, HTTP, HTTPS, and Telnet. When a specific *port* is specified, only the traffic with a matching destination port is included or excluded for authentication. Note that FTP, Telnet, HTTP, and HTTPS are equivalent to **tcp/21**, **tcp/23**, **tcp/80**, and **tcp/443**, respectively.

If you specify **ip**, all IP traffic is included or excluded for authentication, depending on whether **include** or **exclude** is specified. When all IP traffic is included for authentication, following are the expected behaviors:

- Before a user (source IP-based) is authenticated, an FTP, Telnet, HTTP, or HTTPS request triggers authentication, and all other IP requests are denied.
- After a user is authenticated through FTP, Telnet, HTTP, HTTPS, or virtual Telnet authentication (see the **virtual** command), all traffic is free from authentication until the uauth timeout.

Enabling Authentication

The **aaa authentication** command enables or disables the following features:

- User authentication services provided by a LOCAL, TACACS+, or RADIUS server are first designated with the **aaa-server** command. A user starting a connection via FTP, Telnet, HTTP, or HTTPS is prompted for the username and password. If the username and password are verified by the designated authentication server, the security appliance cut-through proxy feature allows further FTP, Telnet, HTTP, or HTTPS traffic between the source and destination.
- Administrative authentication services providing access to the security appliance console via Telnet, SSH, HTTP, or the serial console. Telnet access requires previous use of the **telnet** command. SSH access requires previous use of the **ssh** command.

The prompts users see requesting AAA credentials differ among the services that can access the security appliance for authentication: Telnet, FTP, HTTP, and HTTPS:

Option	Number of Login Attempts Allowed	Notes
ftp	Incorrect password causes the connection to be dropped immediately.	FTP users receive a prompt from the FTP program. Some FTP graphical user interfaces do not display challenge values
http	Continual reprompting until successful login.	HTTP users see a pop-up window generated by the browser itself if **aaa aauthentication secure-http-client** is *not* configured. If **aaa aauthentication secure-http-client** is configured,a form loads in the browser to collect username and password.
telnet	4 tries before dropping the connection.	Before the first command line prompt of a Telnet console connection

Note For HTTP or HTTPS, when the web server and the authentication server are on different hosts, use the **virtual** command to get the correct authentication behavior.

You can specify an interface name with the **aaa authentication** command. For example, if you specified **aaa authentication include tcp outside 0 0** *server-tag*, the security appliance authenticates a tcp connection originating on the outside interface.

Note For HTTP or HTTPS authentication, once authenticated, a user never has to reauthenticate, no matter how low the security appliance uauth timer 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 Netscape Navigator or Internet Explorer and restarts. Flushing the cache is of no use.

Disabling Challenge Authentication

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

```
hostname/contexta(config)# aaa authentication protocol challenge disable
```

For example, to disable the username and password challenge for new connections using FTP, enter the following command:

```
hostname/contexta(config)# aaa authentication ftp challenge disable
```

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

TACACS+ and RADIUS servers

You can have up to 15 single-mode server groups or 4 multi-mode server groups. Each group can have up to 16 servers in single mode or 4 servers in multi-mode. The servers can be either TACACS+ or RADIUS servers—set with the **aaa-server** command. 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.

The security appliance permits only one authentication type per network. For example, if one network connects through the security appliance using TACACS+ for authentication, another network connecting through the security appliance can authenticate with RADIUS, but one network cannot authenticate with both TACACS+ and RADIUS.

Note The security appliance does not enforce VPN attributes enforced by a RADIUS authentication server, if VPN attributes are enforced by the authorization server, since authorization takes place after authentication. For example, if the attribute-value pair "tunnel-group=VPN" is defined for RADIUS authentication and LDAP authorization, then all the VPN remote-access attributes configured on the LDAP server are enforced on the VPN remote-access tunnel. Those attributes defined by the RADIUS authentication server are ignored. This behavior affects the authentication/authorization parameters for tunnel-group, webvpn, pop, imap, and smtps.

Examples

The following examples show some uses of the **aaa authentication** command:

Example 1:

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

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

Example 2:

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

Example 3:

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

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

Example 4:

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

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

Example 5:

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

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

Example 6:

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

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

Example 7:

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

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

Example 8:

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

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

Related Commands

Command	Description
aaa authentication console	Enables or disables authentication on entry to privileged mode or requires authentication verification to access the 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 do any of the following, use the **aaa authentication console** command in global configuration mode:

- 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.
- Enable access to privileged mode, use the **aaa authentication console** command in global configuration mode.
- Configure administrative authentication to support fallback to a list of specified server groups or to the local database.

To disable this authentication service, use the **no** form of this command.

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

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

Syntax Description

console	Specifies that access to the console requires authentication.
enable	Enables or disables authentication on entry to privileged mode. Valid server group protocols are LOCAL, RADIUS, and TACACS+.
http	Enables or disables authentication of admin sessions over HTTP. Valid server group protocols are LOCAL, RADIUS, and TACACS+.
LOCAL	The keyword **LOCAL** has two uses. It can designate the use of a local authentication server, or it can specify fallback to the local database if the designated authentication server is unavailable.
serial	Enables or disables authentication of admin sessions established on the serial interface to the console. Valid server group protocols are LOCAL, RADIUS, and TACACS+.

server-tag	The AAA server group tag defined by the **aaa-server** command.
	For cut-through proxy and "to the box" authentication, you can also use the local security appliance user authentication database by specifying the server group tag **LOCAL**. If **LOCAL** is specified for *server-tag* and the local user credential database is empty, the following warning message appears:
	`Warning:local database is empty! Use 'username' command to define local users.`
	Conversely, if the local database becomes empty when **LOCAL** is still present in the command, the following warning message appears:
	`Warning:Local user database is empty and there are still commands using 'LOCAL' for authentication.`

ssh	Enables or disables authentication of admin sessions over SSH. Valid server group protocols are LOCAL, RADIUS, and TACACS+.
telnet	Enables or disables authentication of admin sessions over Telnet. Valid server group protocols are LOCAL, RADIUS, and TACACS+.

Defaults

By default, fallback to the local database is disabled.

If a **aaa authentication http console** *server-tag* command statement is not defined, you can gain access to the security appliance (via ASDM) with no username and the security appliance enable password (set with the **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.

The **help aaa** command displays the syntax and usage for the **aaa authentication** commands in summary form.

Command Modes

The 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)	Pre-existing command, enhanced for security appliance.

Usage Guidelines

The **aaa authentication console** command enables or disables authentication on entry to privileged mode, lets you require authentication verification to access the security appliance via the specified type of connection, or supports administrative authentication fallback.

Telnet access requires previous use of the **telnet** command. SSH access requires previous use of the **ssh** command.

The **serial** keyword also causes the security appliance to log to a syslog server any changes made to the configuration from the serial console.

Using the **aaa authentication console** command requires that you have previously used the **aaa-server** command to designate an authentication server, unless you have specified LOCAL as the server-group protocol. The **aaa authentication console** command supports RADIUS and TACACS+ groups.

Except as noted in "Defaults," if you are using HTTP authentication, the security appliance requires authentication verification of the HTTP server through the **aaa authentication http console** command.

When an administrator requests an action that requires authentication, the security appliance initiates an authentication session with servers from the server group specified. If the system is unable to communicate with any server from this group.

To configure administrative authentication to support fallback to the local user database if all servers in the specified server group are unavailable, use the **aaa authentication** command with the **LOCAL** option specified. This feature is disabled by default.

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 the **aaa authentication** {**serial** | **enable** | **telnet** | **ssh** | **http**} **console** *server-tag* 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

Telnet access to the security appliance console is available from any internal interface, and from the outside interface with IPSec configured, and requires previous use of the **telnet** command. SSH access to the security appliance console is also available from any interface without IPSec configured, and requires previous use of the **ssh** command.

The **ssh** option specifies the group of AAA servers to be used for SSH user authentication. The authentication protocol and AAA server IP addresses are defined with the **aaa-server** command statement.

Similar to the Telnet model, if a **aaa authentication ssh console** *server-tag* command statement is not defined, you can gain access to the security appliance console with the username **pix** and with the security appliance Telnet password (set with the **passwd** command). If the **aaa** command is defined, but the SSH authentication requests timeouts (which implies the AAA servers may be down or not available), you can gain access to the security appliance using administrator username and the enable password (set with the **enable password** command). By default, the Telnet password is **cisco** and the enable password is not set.

The prompts users see requesting AAA credentials differ among the services that can access the security appliance for authentication: Telnet, FTP, HTTP, and HTTPS:

- Telnet users see a prompt, generated by the security appliance, that you can change with the **auth-prompt** command. The security appliance permits a user up to four chances to log in. Then, if the username or password still fails, the security appliance drops the connection.
- FTP users receive a prompt from the FTP program. If a user enters an incorrect password, the connection is dropped immediately. If the username or password on the authentication database differs from the username or password on the remote host that you are using FTP to access, enter the username and password in these formats:

  ```
  authentication-user-name@remote-system-user-name
  authentication-password@remote-system-password
  ```

  If you daisy-chain security appliances, Telnet authentication works in the same way as a single unit, but FTP and HTTP users must enter each password and username with an additional “at” (@) character and password or username for each daisy-chained system. Users can exceed the 63-character password limit, depending on how many units are daisy-chained and password length.

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

The security appliance accepts only 7-bit characters during authentication. After authentication, the client and server can negotiate for 8 bits, if required. During authentication, the security appliance negotiates only Go-Ahead, Echo, and NVT (network virtual terminal).

HTTP Authentication

When using HTTP authentication to a site running Microsoft IIS that has "Basic text authentication" or "NT Challenge" enabled, users might be denied access from the Microsoft IIS server. This occurs because the browser appends the string: "Authorization: Basic=Uuhjksdkfhk==" to the HTTP GET commands. This string contains the security appliance authentication credentials.

Windows NT Microsoft IIS servers respond to the credentials and assume that a Windows NT user is trying to access privileged pages on the server. Unless the security appliance username-password combination is exactly the same as a valid Windows NT username and password combination on the Microsoft IIS server, the HTTP GET command is denied.

To solve this problem, the security appliance provides the **virtual http** command, which redirects the browser's initial connection to another IP address, authenticates the user, then redirects the browser back to the URL that the user originally requested.

Once authenticated, a user never has to reauthenticate, no matter how low the security appliance uauth timeout is set, because the browser caches the "Authorization: Basic=Uuhjksdkfhk==" string in every subsequent connection to that particular site. This can be cleared *only* when the user exits *all* instances of Netscape Navigator or Internet Explorer and restarts. Flushing the cache is of no use.

As long as the user repeatedly browses the Internet, the browser resends the "Authorization: Basic=Uuhjksdkfhk==" string to transparently reauthenticate the user.

Multimedia applications such as CU-SeeMe, Intel Internet Phone, MeetingPoint, and MS NetMeeting silently start the HTTP service before an H.323 session is established from the inside to the outside.

Network browsers such as Netscape Navigator do not present a challenge value during authentication; therefore, only password authentication can be used from a network browser.

Note To avoid interfering with these applications, do not enter blanket outgoing **aaa** command statements for all challenged ports, such as using the **any** option. Be selective about which ports and addresses you use to challenge HTTP and when to set user authentication timeouts to a higher timeout value. If interfered with, the multimedia programs might fail on the PC and might even cause the PC to fail after establishing outgoing sessions from the inside.

TACACS+ and RADIUS servers

You can have up to 15 single-mode groups or 4 multi-mode groups. Each group can have up to 16 servers in single mode or 4 servers in multi-mode. The servers can be either TACACS+ or RADIUS servers. 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.

For the TACACS+ server, if you do not specify a key to the **aaa-server** command, no encryption occurs.

The security appliance displays the same timeout message for both RADIUS and TACACS+. The message "aaa server host machine not responding" displays when either of the following occurs:

- The AAA server system is down.
- The AAA server system is up, but the service is not running.

Examples

The following examples show the use of the **aaa authentication console** command.

Example 1:

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
```

Example 2:

The following example identifies the server group "AuthIn" for administrative authentication.

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

Example 3:

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 match

To enable the use of a specified access list that must be matched to enable LOCAL, TACACS+, or RADIUS user authentication on a server designated by the **aaa-server** command or ASDM user authentication, use the **aaa authentication match** command in global configuration mode. To disable the requirement to match a specified access list, use the **no** form of this command. The **aaa authentication match** *c*ommand 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 match *acl-name interface-name server-tag*

no aaa authentication match *acl-name interface-name server-tag*

Syntax Description

acl-name	An **access-list** command statement name.
interface-name	The interface name from which to authenticate users.
server-tag	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

Using the **aaa authentication match** command requires that you have previously used the **aaa-server** command to designate an authentication server—unless you specify **LOCAL**, and that you have previously used the **access-list** command to define a named access list. Do not use an **access-list** command statement that uses the source port to identify matching traffic. The source port is not supported in the match criteria of the **aaa authentication match** command.

Use the *interface-name* variable to define where access is sought.

For cut-through proxy, you can also use the local user authentication database by specifying the server group tag **LOCAL**. If **LOCAL** is specified for server-tag and the local user credential database is empty, the following warning message appears:

```
Warning: local database is empty! Use 'username' command to define localisms.
```

Conversely, if the local database becomes empty when **LOCAL** is still present in the command, the following warning message appears:

```
Warning: local database is empty and there are still commands using 'LOCAL' for
authentication.
```

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 10.0.0.0 255.255.255.0 172.23.2.0 255.255.255.0 (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
```

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

Tip The **help aaa** command displays the syntax and usage for the **aaa authentication** commands in summary form.

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 enable or disable user authorization for services on the specified host, use the **aaa authorization** command in global configuration mode. To disable user authorization services for a specified host, use the **no** form of this command. The authentication server determines what services the user is authorized to access.

aaa authorization { **include** | **exclude** } *service interface-name local-ip local-mask foreign-ip foreign-mask server-tag*

no aaa authorization { **include** | **exclude** } *service interface-name local-ip local-mask foreign-ip foreign-mask server-tag*

Syntax Description

exclude	Creates an exception to a previously stated rule by excluding the specified service from authorization to the specified host.
foreign-ip	The IP address of the hosts you want to access the *local-ip* address. Use 0 to mean all hosts.
foreign-mask	Network mask of *foreign-ip*. Always specify a specific mask value. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
interface-name	Interface name from which users require authentication. Use *interface-name* in combination with the *local-ip* address and the *foreign-ip* address to determine where access is sought and from whom. The *local-ip* address is always on the highest security level interface and *foreign-ip* is always on the lowest.
include	Creates a new rule with the specified service to include.
local-ip	The IP address of the host or network of hosts that you want to be authenticated or authorized. You can set this address to **0** to mean all hosts and to let the authentication server decide which hosts are authenticated.
local-mask	Network mask of *local-ip*. Always specify a specific mask value. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
server-tag	The AAA server group tag as defined by the **aaa-server** command. You can also enter **LOCAL** for the group tag value and use the local firewall database AAA services such as local command authorization privilege levels.
service	The services that require authorization. Valid values are **any**, **ftp**, **http**, **telnet**, or *protocol/port*. Use **any** to provide authorization for all TCP services. To provide authorization for UDP services, use the *protocol/port* form. See the section “Usage Guidelines” for more information.

Defaults

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

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

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was modified for this release. The **exclude** parameter now allows the user to specify a port to exclude to a specific host or hosts.

Usage Guidelines

Except for its use with command authorization, the **aaa authorization** command requires previous configuration with the **aaa authentication** command; however, use of the **aaa authentication** command does not require use of a **aaa authorization** command.

The security appliance supports RADIUS authorization with the **aaa authorization** command only when authentication is performed with a different protocol. RADIUS servers return authorization information along with replies to authentication requests. See the description of the **aaa authentication** command. The **aaa authorization** command is permitted with LOCAL servers, only for command authorization, and with RADIUS or TACACS+ servers. You can set a dynamic ACL at the RADIUS server to provide authorization (even if it is not configured on the security appliance).

When VPN authorization is defined as LOCAL, the attributes configured in the default group policy DfltGrpPolicy are enforced. This affects the settings in the **tunnel-group** `and` **webvpn** commands.

Tip The **help aaa** command displays the syntax and usage for the **aaa authentication** command in summary form.

For each IP address, one **aaa authorization** command is permitted. If you want to authorize more than one service with **aaa authorization**, use the **any** parameter for the service type.

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
```

User authorization services control which network services a user can access. After a user is authenticated, attempts to access restricted services cause the security appliance to verify the access permissions of the user with the designated AAA server.

Note RADIUS authorization is supported for use with **access-list deny-flow-max** command statements and for use in configuring a RADIUS server with an **acl=***acl-name* vendor-specific identifier. For more information, refer to the **access-list deny-flow-port** command page and the **authentication-port** command page.

When specifying the foreign (destination) IP address, use **0** to indicate all hosts. For the destination and local masks, always specify a specific mask value. Use a mask of **0** if the IP address is **0**, and use a mask of **255.255.255.255** for a host.

Service Parameter

Services not specified are authorized implicitly. Services specified in the **aaa authentication** command do not affect the services that require authorization.

For *protocol/port*:

- *protocol*—the protocol (6 for TCP, 17 for UDP, 1 for ICMP, and so on).
- *port*—the TCP or UDP destination port, or port range. The *port* can also be the ICMP type; that is, 8 for ICMP echo or ping. A port value of 0 (zero) means all ports. Port ranges apply only to the TCP and UDP protocols, not to ICMP. For protocols other than TCP, UDP, and ICMP, do not use the *port* parameter. The following is a sample port specification.

  ```
  hostname(config)# aaa authorization include udp/53-1024 outside 0 0 0 0
  ```

  This example shows how to enable authorization for DNS lookups to the inside interface for all clients and authorizes access to any other services that have ports in the range of 53 to 1024.

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.

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.

The valid values for the *service* option are **telnet**, **ftp**, **http**, **https**, **tcp** or **0**, **tcp** or *port*, **udp** or *port*, **icmp** or *port*, or *protocol* [/*port*]. Only the Telnet, FTP, HTTP, and HTTPS traffic triggers user interactive authentication.

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

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

aaa authorization command {LOCAL | *server-tag*}

no aaa authorization command {LOCAL | *server-tag*}

The following syntax configures administrative authorization to support fallback to the local user database if all servers in the specified server group are disabled. This option is disabled by default.

aaa authorization command *server-tag* [**LOCAL**]

no aaa authorization command *server-tag* [**LOCAL**]

Syntax Description

LOCAL	Specify the use of the security appliance local user database for local command authorization (using privilege levels). If **LOCAL** is specified after a TACACS+ server group tag, the local user database is used for command authorization only as a fallback when the TACACS+ server group is unavailable.
server-tag	Specify a predefined server group tag for the TACACS+ authorization server. The AAA server group tag as defined by the **aaa-server** command. You can also enter **LOCAL** for the group tag value and use the local command authorization privilege levels.

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

When used for command authorization, the **aaa authorization command** command does not require previous configuration with the **aaa authentication** command.

The **aaa authorization** command is supported for use with TACACS+ servers and with LOCAL servers (only for command authorization), but not with RADIUS servers.

Tip The **help aaa** command displays the syntax and usage for the **aaa authorization** command in summary form.

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

aaa authorization match

To enable the use of a specified access list that must be matched to enable or disable user authorization services, use the **aaa authorization match** command in global configuration mode. To disable the use of a specified access list for user authorization services, use the **no** form of this command. The authentication server determines what services the user is authorized to access.

aaa authorization match *acl-name interface-name server-tag*

no aaa authorization match *acl-name interface-name server-tag*

Syntax Description

acl-name	Specify an **access-list** command statement name.
interface-name	Interface name from which users require authentication.
server-tag	The AAA server group tag as defined by the **aaa-server protocol** command. You can also enter **LOCAL** for the group tag value and use the local security appliance database AAA services such as local command authorization privilege levels.

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 authorization match** command requires previous configuration with the **aaa authentication** command; however, use of the **aaa authentication** command does not require use of any **aaa authorization** command.

The security appliance supports RADIUS authorization with the **aaa authorization** command only when authentication is performed with a different protocol. RADIUS servers return authorization information along with replies to authentication requests. See the description of the **aaa authentication** command. The **aaa authorization** command is permitted with LOCAL servers, only for command authorization, and with RADIUS or TACACS+ servers. You can set a dynamic ACL at the RADIUS server to provide authorization (even if it is not configured on the security appliance).

Tip The **help aaa** command displays the syntax and usage for the **aaa authorization match** command in summary form.

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
```

User authorization services control which network services a user can access. After a user is authenticated, attempts to access restricted services cause the security appliance to verify the access permissions of the user with the designated AAA server.

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 include any inside 0 0 0 0 tplus1
hostname(config)#aaa accounting include any inside 0 0 0 0 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. To disable the use of a list of MAC addresses, use the **no** form of this command. The **aaa mac-exempt** command exempts a list of MAC addresses from authentication and authorization.

aaa mac-exempt match *id*

no aaa mac-exempt match *id*

Syntax Description

id	A MAC access 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 access list number using the **mac-list** command before using the **aaa mac-exempt** command. Authorization is automatically exempted for MAC addresses for which authentication is exempted.

Examples

The following example shows how to specify the mac-exempt list:

```
hostname(config)# aaa mac-exempt mac-list-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.
mac-list	Add a list of MAC addresses using a first-match search; used by the security appliance in performing MAC-based authentication.

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

aaa-server *server-tag* [(*interface-name*)] **host** *server-ip* [*key*] [**timeout** *seconds*]

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

Syntax Description

(*interface-name*)	(Optional) The network interface where the authentication server resides. The parentheses are required in this parameter.
key	(Optional) 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.
server-ip	The IP address of the AAA server.
server-tag	Symbolic name of the server group. Other aaa commands make reference to the *server-tag* group defined by the **aaa-server** command *server-tag* parameter.
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.

Command Modes

The 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 have up to 15 single-mode groups or 4 multi-mode groups. Each group can have up to 16 servers in single mode or 4 servers in multi-mode. When a user logs in, the servers are accessed one at a time starting with the first server you specify in the configuration, until a server responds.

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

Since the security appliance version of the **aaa-server** command supports the specification of server ports on a per-host basis, the following command forms that were available on earlier PIX Firewall systems have been phased out (deprecated), with their semantics changing as indicated. This applies only to server groups that contain RADIUS servers. These commands will be accepted but will no longer be written to the configuration.

- **aaa-server radius-authport** [*auth-port*]—This command controls the *default* authentication port for all RADIUS servers. This means that if a host specific authentication port has not been specified, the value specified by this command is used. If a value has not been specified by this command, the default radius authentication port (1645) is used.
- **aaa-server radius-acctport** [*acct-port*]—This command applies the behavior described above to the RADIUS accounting port (default 1646).

The following are all the host mode commands. Only the ones that apply to the AAA server type for the server group you selected will be available. See the individual command descriptions for details.

Command	Applicable AAA Server Types	Default Value
accounting-port	RADIUS	1646
acl-netmask-convert	RADIUS	standard
authentication-port	RADIUS	1645
kerberos-realm	Kerberos	—
key*	RADIUS	—
	TACACS+	—
ldap-attribute-map	LDAP	—
ldap-base-dn	LDAP	—
ldap-login-dn	LDAP	—
ldap-login-password	LDAP	—
ldap-naming-attribute	LDAP	—
ldap-over-ssl	LDAP	—
ldap-scope	LDAP	—
nt-auth-domain-controller	NT	—
radius-common-pw	RADIUS	—
retry-interval	Kerberos	10 seconds
	RADIUS	10 seconds
	SDI	10 seconds
sasl-mechanism	LDAP	—
sdi-pre-5-slave	SDI	—
sdi-version	SDI	sdi-5

Command	Applicable AAA Server Types	Default Value
server-type	LDAP	auto-detection determines server type
server-port	Kerberos	88
	LDAP	389
	NT	139
	SDI	5500
	TACACS+	49
timeout**	All	10 seconds

* If you specify the *key* parameter with the **aaa-server** command, that parameter has the same effect as using the **key** command in host mode.

** If you specify the **timeout** parameter with the **aaa-server** command, that parameter has the same effect as using the **timeout** command in host mode.

The **aaa-server** command was modified for this release. It is now two separate commands, **aaa-server** *group-tag* **protocol** to enter group mode and **aaa-server host** to enter host mode.

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

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

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 configure AAA server parameters that are group-specific and common to all 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	Symbolic name of the server group.Other AAA commands make reference to the *server-tag* group defined by the **aaa-server** command *server-tag* parameter.
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
7.0(1)	This command was introduced.

Usage Guidelines

You can have up to 15 single-mode groups or 4 multi-mode groups. Each group can have up to 16 servers in single mode or 4 servers in multi-mode. When a user logs in, the servers are accessed one at a time starting with the first server you specify in the configuration, until a server responds.

If AAA accounting is in effect, the accounting information goes only to the active server unless you have configured simultaneous accounting.

You control AAA server configuration with two commands: **aaa-server protocol** to enter AAA-server group mode and **aaa-server host** to enter AAA-server host mode. In addition, group mode, which you enter by specifying the **aaa-server protocol** command, supports accounting mode and server reactivation features through the **accounting-mode** and **reactivation-mode** commands.

The supported commands in AAA-server group mode are as follows:

- **accounting-mode**
- **reactivation-mode**

- **max-failed-attempts**

See the individual command descriptions for details about these commands.

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

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.
icmp_type	(Optional) If the protocol is **icmp**, specifies the ICMP type.
id	Specifies the access list ID, as a string or integer up to 241 characters in length. The ID is case-sensitive. Tip: Use all capital letters so you can see the access list ID better in your configuration.
inactive	(Optional) Disables an ACE. To reenable it, enter the entire ACE without the **inactive** keyword. This feature lets you keep a record of an inactive ACE in your configuration to make reenabling easier.
interface *ifc_name*	Specifies the interface address as the source or destination address.
interval *secs*	(Optional) Specifies the log interval at which to generate a 106100 system log message. Valid values are from 1 to 600 seconds. The default is 300.

level	(Optional) Sets the 106100 system log message level from 0 to 7. The default level is 6.
line *line-num*	(Optional) Specifies the line number at which to insert the ACE. If you do not specify a line number, the ACE is added to the end of the access list. The line number is not saved in the configuration; it only specifies where to insert the ACE.
log	(Optional) Sets logging options when a deny ACE matches a packet for network access (an access list applied with the **access-group** command). If you enter the **log** keyword without any arguments, you enable system log message 106100 at the default level (6) and for the default interval (300 seconds). If you do not enter the log keyword, then the default logging occurs, using ystem 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 syslog message 106023 for denied packets. A deny ACE must be present to log denied packets.
- When the **log** keyword is specified, the default level for syslog message 106100 is 6 (informational) and the default interval is 300 seconds.

Command Modes

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

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

Command History

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

Defaults

The defaults are as follows:

- The 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.

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

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

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

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

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

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

Examples

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

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

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

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

Related Commands

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

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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple 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

accounting-mode single

no accounting-mode

Syntax Description

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

Defaults

The default value is single mode

Command Modes

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

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

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)# accounting-port 2222
hostname(config-aaa-server-host)# exit
hostname(config)#
```

Related Commands

Command	Description
aaa accounting	Keeps a record of which network services a user has accessed.
aaa-server host	Enters AAA server host configuration mode, so 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.