A through B 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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple 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 console

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

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

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

Syntax Description

enable	Enables or disables the generation of accounting records to mark the entry to and exit from privileged EXEC mode.
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 Telnet transactions, and that these records are sent to the server named adminserver.

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

Related Commands

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

aaa accounting 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. **Note** If you enter a deprecated command and enabled the **privilege** keyword, then the security appliance does not send accounting information for the deprecated command. If you want to account for deprecated commands, be sure to disable the **privilege** keyword. Many deprecated commands are still accepted at the CLI, and are often converted into the currently-accepted command at the CLI; they are not included in CLI help or this guide.

Defaults

The default privilege level is 0. 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	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 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*.
include	Creates a new rule with the specified service to include.
interface-name	The interface name from which users require authentication.
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.

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.

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

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

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

Syntax Description

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

Defaults

By default, fallback to the local database is disabled.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

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

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

If you configure enable authentication, the security appliance prompts you for your username and password. If you do not configure enable authentication, enter the system enable password when you enter the **enable** command (set by the **enable password** command). However, if you do not use enable authentication, after you enter the **enable** command, you are no longer logged in as a particular user. To maintain your username, use enable authentication. This feature is particularly useful when you perform command authorization, where usernames are important to determine the commands a user can enter.

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

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

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

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

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

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

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

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

If the SSH authentication request times out (which implies the AAA servers may be down or not available), you can gain access to the security appliance using the username **pix** and the login password (set with the **password** command). By default, the login password is **cisco**.

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

Examples

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

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

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

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

The following example shows use of the **aaa authentication console** command with fallback to the LOCAL user database if all the servers in the group "srvgrp1" fail:

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

Related Commands

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

aaa authentication 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:

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

Command History

Release	Modification
7.0	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	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	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[1]	RADIUS	—
	TACACS+	—
ldap-base-dn	LDAP	—
ldap-login-dn	LDAP	—
ldap-login-password	LDAP	—
ldap-naming-attribute	LDAP	—
ldap-scope	LDAP	—
nt-auth-domain-controller	NT	—
radius-common-pw	RADIUS	—
retry-interval	Kerberos	10 seconds
	RADIUS	10 seconds
sdi-pre-5-slave	SDI	—
sdi-version	SDI	sdi-5

Command	Applicable AAA Server Types	Default Value
server-port	Kerberos	88
	LDAP	389
	NT	139
	SDI	5500
	TACACS+	49
timeout[2]	All	10 seconds

1. 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.
2. 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 an SDI AAA server group named "svrgrp1" on host "192.168.3.4", 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 7
hostname(config-aaa-server-host)# sdi-version sdi-5
hostname(config-aaa-server-host)# exit
hostname(config)#
```

Related Commands

Command	Description
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	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	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	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-list	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-list	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	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-list	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-list	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	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-list	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		
				Multiple	
	Routed	Transparent	Single	Context	System
Global Configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

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

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

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

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

Related Commands

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

accounting-mode

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

accounting-mode simultaneous

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	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	This command was introduced.

Usage Guidelines

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

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

Examples

The following example configures a RADIUS AAA server named “srvgrp1” on host “1.2.3.4”, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures accounting port 2222.

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# accountinq-port 2222
hostname(config-aaa-server-host)# exit
hostname(config)#
```

Related Commands

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

accounting-server-group

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

accounting-server-group *server-group*

no accounting-server-group

Syntax Description

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

Defaults

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

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.

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

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	This command was introduced.

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.

acl-netmask-convert

To specify how the security appliance treats netmasks received in a downloadable ACL from a RADIUS server, use the **acl-netmask-convert** command in AAA-server host mode, which is accessed by using the **aaa-server host** command. Use the **no** form of this command to remove the command.

acl-netmask-convert {**auto-detect** | **standard** | **wildcard**}

no acl-netmask-convert

Syntax Description

auto-detect	Specifies that the security appliance should attempt to determine the type of netmask expression used. If it detects a wildcard netmask expression, it converts it to a standard netmask expression. See "Usage Guidelines" for more information about this keyword.
standard	Specifies that the security appliance assumes downloadable ACLs received from the RADIUS server contain only standard netmask expressions. No translation from wildcard netmask expressions is performed.
wildcard	Specifies that the security appliance assumes downloadable ACLs received from the RADIUS server contain only wildcard netmask expressions and it converts them all to standard netmask expressions when the ACLs are downloaded.

Defaults

By default, no conversion from wildcard netmask expressions is performed.

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(4)	This command was introduced.

Usage Guidelines

Use the **acl-netmask-convert** command with the wildcard or auto-detect keywords when a RADIUS server provides downloadable ACLs that contain netmasks in wildcard format. The security appliance expects downloadable ACLs to contain standard netmask expressions whereas Cisco Secure VPN 3000 Series Concentrators expect downloadable ACLs to contain wildcard netmask expressions, which are the reverse of a standard netmas expression. A wildcard mask has ones in bit positions to ignore, zeros in bit positions to match.The **acl-netmask-convert** command helps minimize the effects of these differences upon how you configure downloadable ACLs on your RADIUS servers.

The **auto-detect** keyword is helpful when you are uncertain how the RADIUS server is configured; however, wildcard netmask expressions with "holes" in them cannot be unambiguously detected and converted. For example, the wildcard netmask 0.0.255.0 permits anything in the third octet and can be used validly on Cisco VPN 3000 Series Concentrators, but the security appliance may not detect this expression as a wildcard netmask.

Examples

The following example configures a RADIUS AAA server named "srvgrp1" on host "192.168.3.4", enables conversion of downloadable ACL netmasks, sets a timeout of 9 seconds, sets a retry-interval of 7 seconds, and configures authentication port 1650.

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
hostname(config-aaa-server-host)# acl-netmask-convert wildcard
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# authentication-port 1650
hostname(config-aaa-server-host)# exit
hostname(config)#
```

Related Commands

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

activation-key

To change the activation key on the security appliance and check the activation key running on the security appliance against the activation key that is stored as a hidden file in the Flash partition of the security appliance, use the **activation-key** command in global configuration mode.

activation-key [*activation-key-four-tuple*| *activation-key-five-tuple*]

Syntax Description

activation-key-four-tuple	Activation key; see the "Usage Guidelines" section for formatting guidelines.
activation-key-five-tuple	Activation key; see the "Usage Guidelines" section for formatting guidelines.

Defaults

This command has no default settings.

Command Modes

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

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

Command History

Release	Modification
7.0	Support for this command was introduced on the security appliance.

Usage Guidelines

Enter the *activation-key-four-tuple* as a four-element hexadecimal string with one space between each element, or *activation-key-five-tuple* as a five-element hexidecimal string withe one space between each element as follows:

```
0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

The leading 0x specifier is optional; all values are assumed to be hexadecimal.

The key is not stored in the configuration file. The key is tied to the serial number.

Examples

This example shows how to change the activation key on the security appliance:

```
hostname(config)# activation-key 0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

Related Commands

Command	Description
show activation-key	Displays the activation key.

address-pool

To specify a list of address pools for allocating addresses to remote clients, use the **address-pool** command in tunnel-group general-attributes configuration mode. To eliminate address pools, use the **no** form of this command.

address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

no address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

Syntax Description

address_pool	Specifies the name of the address pool configured with the **ip local pool** command. You can specify up to 6 local address pools.
interface name	(Optional) Specifies the interface to be used for the address pool.

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
Tunnel-group general attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You can enter multiples of each of these commands, one per interface. If an interface is not specified, then the command specifies the default for all interfaces that are not explicitly referenced.

Examples

The following example entered in config-general configuration mode, specifies a list of address pools for allocating addresses to remote clients for an IPSec remote-access tunnel group xyz:

```
hostname(config)# tunnel-group xyz
hostname(config)# tunnel-group xyz general
hostname(config-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
hostname(config-general)#
```

Related Commands

Command	Description
ip local pool	Configures IP address pools to be used for VPN remote-access tunnels.
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group-map default-group	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

admin-context

To set the admin context for the system configuration, use the **admin-context** command in global configuration mode. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the security appliance software or allowing remote management for an administrator), it uses one of the contexts that is designated as the admin context.

admin-context *name*

Syntax Description

name	Sets the name as a string up to 32 characters long. If you have not defined any contexts yet, then first specify the admin context name with this command. Then, the first context you add using the **context** command must be the specified admin context name. This name is case sensitive, so you can have two contexts named "customerA" and "CustomerA," for example. You can use letters, digits, or hyphens, but you cannot start or end the name with a hyphen. "System" or "Null" (in upper or lower case letters) are reserved names, and cannot be used.

Defaults

For a new security appliance in multiple context mode, the admin context is called "admin."

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	This command was introduced.

Usage Guidelines

You can set any context to be the admin context, as long as the context configuration resides on the internal Flash memory.

You cannot remove the current admin context, unless you remove all contexts using the **clear configure context** command.

Examples

The following example sets the admin context to be "administrator":

```
hostname(config)# admin-context administrator
```

Related Commands

Command	Description
clear configure context	Removes all contexts from the system configuration.
context	Configures a context in the system configuration and enters context configuration mode.
show admin-context	shows the current admin context name.

alias

To manually translate an address and perform DNS reply modification, use the **alias** command in global configuration mode. To remove an **alias** command, use the **no** form of this command. This command functionality has been replaced by outside NAT commands, including the **nat** and **static** commands with the **dns** keyword. We recommend that you use outside NAT instead of the **alias** command.

alias (*interface_name***)** *real_ip mapped_ip* [*netmask*]

no alias (*interface_name***)** *real_ip mapped_ip* [*netmask*]

Syntax Description

(*interface_name*)	Specifies the ingress interface name for traffic destined for the mapped IP address (or the egress interface name for traffic from the mapped IP address). Be sure to include the parentheses in the command.
mapped_ip	Specifies the IP address to which you want to translate the real IP address.
netmask	(Optional) Specifies the subnet mask for both IP addresses. Enter **255.255.255.255** for a host mask.
real_ip	Specifies the real IP address.

Defaults

This command has no default settings.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

You can also use this command to perform address translation on a destination address. For example, if a host sends a packet to 209.165.201.1, you can use the **alias** command to redirect traffic to another address, such as 209.165.201.30.

Note If the **alias** command is used for DNS rewrite and not for other address translation, disable **proxy-arp** on the alias-enabled interface. Use the **sysopt noproxyarp** command to prevent the security appliance from pulling traffic toward itself via **proxy-arp** for generic NAT processing.

After changing or removing an **alias** command, use the **clear xlate** command.

You must have an A (address) record in the DNS zone file for the “dnat” address in the **alias** command.

The **alias** command has two uses that can be summarized in the following ways:

- If the security appliance gets a packet that is destined for the *mapped_ip*, you can configure the **alias** command to send it to the *real_ip*.
- If the security appliance gets a DNS packet that is returned to the security appliance destined for *real_ip*, you can configure the **alias** command to alter the DNS packet to change the destination network address to *mapped_ip*.

The **alias** command automatically interacts with the DNS servers on your network to ensure that domain name access to the aliased IP address is handled transparently.

You can specify a net alias by using network addresses for the *real_ip* and *mapped_ip* IP addresses. For example, the **alias 192.168.201.0 209.165.201.0 255.255.255.224** command creates aliases for each IP address between 209.165.201.1 and 209.165.201.30.

To access an **alias** *mapped_ip* address with **static** and **access-list** commands, specify the *mapped_ip* address in the **access-list** command as the address from which traffic is permitted as follows:

```
hostname(config)# alias (inside) 192.168.201.1 209.165.201.1 255.255.255.255
hostname(config)# static (inside,outside) 209.165.201.1 192.168.201.1 netmask
255.255.255.255
hostname(config)# access-list acl_out permit tcp host 192.168.201.1 host 209.165.201.1 eq
ftp-data
hostname(config)# access-group acl_out in interface outside
```

An alias is specified with the inside address 192.168.201.1 mapping to the destination address 209.165.201.1.

When the inside network client 209.165.201.2 connects to example.com, the DNS response from an external DNS server to the internal client's query would be altered by the security appliance to be 192.168.201.29. If the security appliance uses 209.165.200.225 through 209.165.200.254 as the global pool IP addresses, the packet goes to the security appliance with SRC=209.165.201.2 and DST=192.168.201.29. The security appliance translates the address to SRC=209.165.200.254 and DST=209.165.201.29 on the outside.

Examples

This example shows that the inside network contains the IP address 209.165.201.29, which on the Internet belongs to example.com. When inside clients try to access example.com, the packets do not go to the security appliance because the client assumes that the 209.165.201.29 is on the local inside network.

To correct this, use the **alias** command as follows:

```
hostname(config)# alias (inside) 192.168.201.0 209.165.201.0 255.255.255.224

hostname(config)# show running-config alias
alias 192.168.201.0 209.165.201.0 255.255.255.224
```

This example shows a web server that is on the inside at 10.1.1.11 and the **static** command that was created at 209.165.201.11. The source host is on the outside with address 209.165.201.7. A DNS server on the outside has a record for www.example.com as follows:

```
dns-server# www.example.com. IN A 209.165.201.11
```

You must include the period at the end of the www.example.com. domain name.

This example shows how to use the **alias** command:

```
hostname(config)# alias 10.1.1.11 209.165.201.11 255.255.255.255
```

The security appliance changes the name server replies to 10.1.1.11 for inside clients to directly connect to the web server.

To provide access you also need the following commands:

```
hostname(config)# static (inside,outside) 209.165.201.11 10.1.1.11

hostname(config)# access-list acl_grp permit tcp host 209.165.201.7 host 209.165.201.11 eq
telnet
hostname(config)# access-list acl_grp permit tcp host 209.165.201.11 eq telnet host
209.165.201.7
```

Related Commands

Command	Description
access-list extended	Creates an access list.
clear configure alias	Removes all **alias** commands from the configuration.
show running-config alias	Displays the overlapping addresses with dual NAT commands in the configuration.
static	Configures a one-to-one address translation rule by mapping a local IP address to a global IP address, or a local port to a global port.

allocate-interface

To allocate interfaces to a security context, use the **allocate-interface** command in context configuration mode. To remove an interface from a context, use the **no** form of this command.

allocate-interface *physical_interface* [*map_name*] [**visible** | **invisible**]

no allocate-interface *physical_interface*

allocate-interface *physical_interface*.*subinterface*[-*physical_interface*.*subinterface*] [*map_name*[-*map_name*]] [**visible** | **invisible**]

no allocate-interface *physical_interface*.*subinterface*[-*physical_interface*.*subinterface*]

Syntax Description

invisible	(Default) Allows context users to only see the mapped name (if configured) in the **show interface** command.

map_name	(Optional) Sets a mapped name.
	
	The *map_name* is an alphanumeric alias for the interface that can be used within the context instead of the interface ID. If you do not specify a mapped name, the interface ID is used within the context. For security purposes, you might not want the context administrator to know which interfaces are being used by the context.
	
	A mapped name must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, or an underscore. For example, you can use the following names:
	
	`int0`
	
	`inta`
	
	`int_0`
	
	For subinterfaces, you can specify a range of mapped names.
	
	See the "Usage Guidelines" section for more information about ranges.

physical_interface	Sets the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	Sets the subinterface number. You can identify a range of subinterfaces.
visible	(Optional) Allows context users to see physical interface properties in the **show interface** command even if you set a mapped name.

Defaults

The interface ID is invisible in the **show interface** command output by default if you set a mapped name.

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
Context configuration	•	•	—	—	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You can enter this command multiple times to specify different ranges. To change the mapped name or visible setting, reenter the command for a given interface ID, and set the new values; you do not need to enter the **no allocate-interface** command and start over. If you remove the **allocate-interface** command, the security appliance removes any interface-related configuration in the context.

Transparent firewall mode allows only two interfaces to pass through traffic; however, on the ASA adaptive security appliance, you can use the dedicated management interface, Management 0/0, (either the physical interface or a subinterface) as a third interface for management traffic.

Note The management interface for transparent mode does not flood a packet out the interface when that packet is not in the MAC address table.

You can assign the same interfaces to multiple contexts in routed mode, if desired. Transparent mode does not allow shared interfaces.

If you specify a range of subinterfaces, you can specify a matching range of mapped names. Follow these guidelines for ranges:

- The mapped name must consist of an alphabetic portion followed by a numeric portion. The alphabetic portion of the mapped name must match for both ends of the range. For example, enter the following range:

  ```
  int0-int10
  ```

  If you enter **gigabitethernet0/1.1-gigabitethernet0/1.5 happy1-sad5**, for example, the command fails.

- The numeric portion of the mapped name must include the same quantity of numbers as the subinterface range. For example, both ranges include 100 interfaces:

  ```
  gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100
  ```

  If you enter **gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int15**, for example, the command fails.

Examples

The following example shows gigabitethernet0/1.100, gigabitethernet0/1.200, and gigabitethernet0/2.300 through gigabitethernet0/1.305 assigned to the context. The mapped names are int1 through int8.

```
hostname(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
```

```
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

Related Commands

Command	Description
context	Creates a security context in the system configuration and enters context configuration mode.
interface	Configures an interface and enters interface configuration mode.
show context	Shows a list of contexts (system execution space) or information about the current context.
show interface	Displays the runtime status and statistics of interfaces.
vlan	Assigns a VLAN ID to a subinterface.

area

To create an OSPF area, use the **area** command in router configuration mode. To remove the area, use the **no** form of this command.

area *area_id*

no area *area_id*

Syntax Description

area_id	The ID of the area being created. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.

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
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The area that you create does not have any parameters set. Use the related area commands to set the area parameters.

Examples

The following example shows how to create an OSPF area with an area ID of 1:

```
hostname(config-router)# area 1
hostname(config-router)#
```

Related Commands

Command	Description
area authentication	Enables authentication for the OSPF area.
area nssa	Defines the area as a not-so-stubby area.
area stub	Defines the area as a stub area.

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area authentication

To enable authentication for an OSPF area, use the **area authentication** command in router configuration mode. To disable area authentication, use the **no** form of this command.

area *area_id* **authentication** [**message-digest**]

no area *area_id* **authentication** [**message-digest**]

Syntax Description

area_id	The identifier of the area on which authentication is to be enabled. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
message-digest	(Optional) Enables Message Digest 5 (MD5) authentication on the area specified by the *area_id*.

Defaults

Area authentication is disabled.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If the specified OSPF area does not exist, it is created when this command is entered. Entering the **area authentication** command without the **message-digest** keyword enables simple password authentication. Including the **message-digest** keyword enables MD5 authentication.

Examples

The following example shows how to enable MD5 authentication for area 1:

```
hostname(config-router)# area 1 authentication message-digest
hostname(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area default-cost

To specify a cost for the default summary route sent into a stub or NSSA, use the **area default-cost** command in router configuration mode. To restore the default cost value, use the **no** form of this command.

area *area_id* **default-cost** *cost*

no area *area_id* **default-cost**

Syntax Description

area_id	The identifier of the stub or NSSA whose default cost is being changed. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
cost	Specifies the cost for the default summary route that is used for a stub or NSSA. Valid values range from 0 to 65535

Defaults

The default value of *cost* is 1.

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
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

Examples

The following example show how to specify a default cost for summary route sent into a stub or NSSA:

```
hostname(config-router)# area 1 default-cost 5
hostname(config-router)#
```

Related Commands

Command	Description
area nssa	Defines the area as a not-so-stubby area.
area stub	Defines the area as a stub area.

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area filter-list prefix

To filter prefixes advertised in type 3 LSAs between OSPF areas of an ABR, use the **area filter-list prefix** command in router configuration mode. To change or cancel the filter, use the **no** form of this command.

area *area_id* **filter-list prefix** *list_name* {**in** | **out**}

no area *area_id* **filter-list prefix** *list_name* {**in** | **out**}

Syntax Description

area_id	Identifier of the area for which filtering is configured. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
in	Applies the configured prefix list to prefixes advertised inbound to the specified area.
list_name	Specifies the name of a prefix list.
out	Applies the configured prefix list to prefixes advertised outbound from the specified area.

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
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

Only type 3 LSAs can be filtered. If an ASBR is configured in the private network, then it will send type 5 LSAs (describing private networks) which are flooded to the entire AS including the public areas.

Examples

The following example filters prefixes that are sent from all other areas to area 1:

```
hostname(config-router)# area 1 filter-list prefix-list AREA_1 in
hostname(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area nssa

To configure an area as an NSSA, use the **area nssa** command in router configuration mode. To remove the NSSA designation from the area, use the **no** form of this command.

area *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type** {**1** | **2**}] [**metric** *value*]] [**no-summary**]

no area *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type** {**1** | **2**}] [**metric** *value*]] [**no-summary**]

Syntax Description

area_id	Identifier of the area being designated as an NSSA. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
default-information-originate	Used to generate a Type 7 default into the NSSA area. This keyword only takes effect on an NSSA ABR or an NSSA ASBR.
metric *metric_value*	(Optional) Specifies the OSPF default metric value. Valid values range from 0 to 16777214.
metric-type {**1** | **2**}	(Optional) the OSPF metric type for default routes. Valid values are the following: • **1**—type 1 • **2**—type 2. The default value is 2.
no-redistribution	(Optional) Used when the router is an NSSA ABR and you want the **redistribute** command to import routes only into the normal areas, but not into the NSSA area.
no-summary	(Optional) Allows an area to be a not-so-stubby area but not have summary routes injected into it.

Defaults

The defaults are as follows:

- No NSSA area is defined.
- The **metric-type** is 2.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

If you configure one option for an area, and later specify another option, both options are set. For example, entering the following two command separately results in a single command with both options set in the configuration:

```
area 1 nssa no-redistribution
area area_id nssa default-information-originate
```

Examples

The following example shows how setting two options separately results in a single command in the configuration:

```
hostname(config-router)# area 1 nssa no-redistribution
hostname(config-router)# area 1 nssa default-information-originate
hostname(config-router)# exit
hostname(config-router)# show running-config router ospf 1
router ospf 1
 area 1 nssa no-redistribution default-information-originate
```

Related Commands

Command	Description
area stub	Defines the area as a stub area.
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area range

To consolidate and summarize routes at an area boundary, use the **area range** command in router configuration mode. To disable this function, use the **no** form of this command.

area *area_id* **range** *address mask* [**advertise | not-advertise**]

no area *area_id* **range** *address mask* [**advertise | not-advertise**]

Syntax Description

address	IP address of the subnet range.
advertise	(Optional) Sets the address range status to advertise and generates type 3 summary link-state advertisements (LSAs).
area_id	Identifier of the area for which the range is configured. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
mask	IP address subnet mask.
not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.

Defaults

The address range status is set to advertise.

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
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

If the specified area has not been previously defined using the **area** command, this command creates the area with the specified parameters.

The **area range** command is used only with ABRs. It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range. This behavior is called *route summarization*. You can configure multiple **area range** commands for an area. Thus, OSPF can summarize addresses for many different sets of address ranges.

The **no area** *area_id* **range** *ip_address netmask* **not-advertise** command removes only the **not-advertise** optional keyword.

Examples

The following example specifies one summary route to be advertised by the ABR to other areas for all subnets on network 10.0.0.0 and for all hosts on network 192.168.110.0:

```
hostname(config-router)# area 10.0.0.0 range 10.0.0.0 255.0.0.0
hostname(config-router)# area 0 range 192.168.110.0 255.255.255.0
hostname(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area stub

To define an area as a stub area, use the **area stub** command in router configuration mode. To remove the stub area function, use the **no** form of this command.

area *area_id* [**no-summary**]

no area *area_id* [**no-summary**]

Syntax Description

area_id	Identifier for the stub area. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
no-summary	Prevents an ABR from sending summary link advertisements into the stub area.

Defaults

The default behaviors are as follows:

- No stub areas are defined.
- Summary link advertisements are sent into the stub area.

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
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The command is used only on an ABR attached to a stub or NSSA.

There are two stub area router configuration commands: the **area stub** and **area default-cost** commands. In all routers and access servers attached to the stub area, the area should be configured as a stub area using the **area stub** command. Use the **area default-cost** command only on an ABR attached to the stub area. The **area default-cost** command provides the metric for the summary default route generated by the ABR into the stub area.

Examples

The following example configures the specified area as a stub area:

```
hostname(config-router)# area 1 stub
hostname(config-router)#
```

Related Commands

Command	Description
area default-cost	Specifies a cost for the default summary route sent into a stub or NSSA
area nssa	Defines the area as a not-so-stubby area.
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

area virtual-link

To define an OSPF virtual link, use the **area virtual-link** command in router configuration mode. To reset the options or remove the virtual link, use the **no** form of this command.

area *area_id* **virtual-link** *router_id* [**authentication** [**message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** seconds] [**transmit-delay** *seconds*] [**dead-interval** *seconds* [[**authentication-key** *key*] | [**message-digest-key** *key_id* **md5** *key*]]

no area *area_id* **virtual-link** *router_id* [**authentication** [**message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** seconds] [**transmit-delay** *seconds*] [**dead-interval** *seconds* [[**authentication-key** *key*] | [**message-digest-key** *key_id* **md5** *key*]]

Syntax Description

area_id	Area ID of the transit area for the virtual link. You can specify the identifier as either a decimal number or an IP address. Valid decimal values range from 0 to 4294967295.
authentication	(Optional) Specifies the authentication type.
authentication-key *key*	(Optional) Specifies an OSPF authentication password for use by neighboring routing devices.
dead-interval *seconds*	(Optional) Specifies the interval before declaring a neighboring routing device is down if no hello packets are received; valid values are from 1 to 65535 seconds.
hello-interval *seconds*	(Optional) Specifies the interval between hello packets sent on the interface; valid values are from 1 to 65535 seconds.
md5 *key*	(Optional) Specifies an alphanumeric key up to 16 bytes.
message-digest	(Optional) Specifies that message digest authentication is used.
message-digest-key *key_id*	(Optional) Enables the Message Digest 5 (MD5) authentication and specifies the numerical authentication key ID number; valid values are from 1 to 255.
null	(Optional) Specifies that no authentication is used. Overrides password or message digest authentication if configured for the OSPF area.
retransmit-interval *seconds*	(Optional) Specifies the time between LSA retransmissions for adjacent routers belonging to the interface; valid values are from 1 to 65535 seconds.
router_id	The router ID associated with the virtual link neighbor. The router ID is internally derived by each router from the interface IP addresses. This value must be entered in the format of an IP address. There is no default.
transmit-delay *seconds*	(Optional) Specifies the delay time between when OSPF receives a topology change and when it starts a shortest path first (SPF) calculation in seconds from 0 to 65535. The default is 5 seconds.

Defaults

The defaults are as follows:

- *area_id*: No area ID is predefined.
- *router_id*: No router ID is predefined.
- **hello-interval** *seconds*: 10 seconds.
- **retransmit-interval** *seconds*: 5 seconds.

- **transmit-delay** *seconds*: 1 second.
- **dead-interval** *seconds*: 40 seconds.
- **authentication-key** *key*: No key is predefined.
- **message-digest-key** *key_id* **md5** *key*: No key is predefined.

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
Router configuration	•	—	•	—	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

In OSPF, all areas must be connected to a backbone area. If the connection to the backbone is lost, it can be repaired by establishing a virtual link.

The smaller the hello interval, the faster topological changes are detected, but more routing traffic ensues.

The setting of the retransmit interval should be conservative, or needless retransmissions occur. The value should be larger for serial lines and virtual links.

The transmit delay value should take into account the transmission and propagation delays for the interface.

The specified authentication key is used only when authentication is enabled for the backbone with the **area** *area_id* **authentication** command.

The two authentication schemes, simple text and MD5 authentication, are mutually exclusive. You can specify one or the other or neither. Any keywords and arguments you specify after **authentication-key** *key* or **message-digest-key** *key_id* **md5** *key* are ignored. Therefore, specify any optional arguments before such a keyword-argument combination.

If the authentication type is not specified for an interface, the interface uses the authentication type specified for the area. If no authentication type has been specified for the area, the area default is null authentication.

Note Each virtual link neighbor must include the transit area ID and the corresponding virtual link neighbor router ID for a virtual link to be properly configured. Use the **show ospf** command to see the router ID.

To remove an option from a virtual link, use the **no** form of the command with the option that you want removed. To remove the virtual link, use the **no area** *area_id* **virtual-link** command.

Examples

The following example establishes a virtual link with MD5 authentication:

```
hostname(config-router)# area 10.0.0.0 virtual-link 10.3.4.5 message-digest-key 3 md5
sa5721bk47
```

Related Commands

Command	Description
area authentication	Enables authentication for an OSPF area.
router ospf	Enters router configuration mode.
show ospf	Displays general information about the OSPF routing processes.
show running-config router	Displays the commands in the global router configuration.

arp

To add a static ARP entry to the ARP table, use the **arp** command in global configuration mode. To remove the static entry, use the **no** form of this command. A static ARP entry maps a MAC address to an IP address and identifies the interface through which the host is reached. Static ARP entries do not time out, and might help you solve a networking problem. In transparent firewall mode, the static ARP table is used with ARP inspection (see the **arp-inspection** command).

arp *interface_name ip_address mac_address* [**alias**]

no arp *interface_name ip_address mac_address*

Syntax Description

alias	(Optional) Enables proxy ARP for this mapping. If the security appliance receives an ARP request for the specified IP address, then it responds with the security appliance MAC address. When the security appliance receives traffic destined for the host belonging to the IP address, the security appliance forwards the traffic to the host MAC address that you specify in this command. This keyword is useful if you have devices that do not perform ARP, for example. In transparent firewall mode, this keyword is ignored; the security appliance does not perform proxy ARP.
interface_name	The interface attached to the host network.
ip_address	The host IP address.
mac_address	The host MAC address.

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

Although hosts identify a packet destination by an IP address, the actual delivery of the packet on Ethernet relies on the Ethernet MAC address. When a router or host wants to deliver a packet on a directly connected network, it sends an ARP request asking for the MAC address associated with the IP address, and then delivers the packet to the MAC address according to the ARP response. The host or router keeps an ARP table so it does not have to send ARP requests for every packet it needs to deliver.

The ARP table is dynamically updated whenever ARP responses are sent on the network, and if an entry is not used for a period of time, it times out. If an entry is incorrect (for example, the MAC address changes for a given IP address), the entry times out before it can be updated.

Note In transparent firewall mode, dynamic ARP entries are used for traffic to and from the security appliance, such as management traffic.

Examples

The following example creates a static ARP entry for 10.1.1.1 with the MAC address 0009.7cbe.2100 on the outside interface:

```
hostname(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

Related Commands

Command	Description
arp timeout	Sets the time before the security appliance rebuilds the ARP table.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show arp	Shows the ARP table.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

arp timeout

To set the time before the security appliance rebuilds the ARP table, use the **arp timeout** command in global configuration mode. To restore the default timeout, use the **no** form of this command. Rebuilding the ARP table automatically updates new host information and removes old host information. You might want to reduce the timeout because the host information changes frequently.

arp timeout *seconds*

no arp timeout *seconds*

Syntax Description

seconds	The number of seconds between ARP table rebuilds, from 60 to 4294967.

Defaults

The default value is 14,400 seconds (4 hours).

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.

Examples

The following example changes the ARP timeout to 5,000 seconds:

```
hostname(config)# arp timeout 5000
```

Related Commands

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

arp-inspection

To enable ARP inspection for transparent firewall mode, use the **arp-inspection** command in global configuration mode. To disable ARP inspection, use the **no** form of this command. ARP inspection checks all ARP packets against static ARP entries (see the **arp** command) and blocks mismatched packets. This feature prevents ARP spoofing.

arp-inspection *interface_name* **enable** [**flood** | **no-flood**]

no arp-inspection *interface_name* **enable**

Syntax Description

enable	Enables ARP inspection.
flood	(Default) Specifies that packets that do not match any element of a static ARP entry are flooded out all interfaces except the originating interface. If there is a mismatch between the MAC address, the IP address, or the interface, then the security appliance drops the packet. **Note** The management-specific interface, if present, never floods packets even if this parameter is set to flood.
interface_name	The interface on which you want to enable ARP inspection.
no-flood	(Optional) Specifies that packets that do not exactly match a static ARP entry are dropped.

Defaults

By default, ARP inspection is disabled on all interfaces; all ARP packets are allowed through the security appliance. When you enable ARP inspection, the default is to flood non-matching ARP 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	This command was introduced.

Usage Guidelines

Configure static ARP entries using the **arp** command before you enable ARP inspection.

When you enable ARP inspection, the security appliance compares the MAC address, IP address, and source interface in all ARP packets to static entries in the ARP table, and takes the following actions:

- If the IP address, MAC address, and source interface match an ARP entry, the packet is passed through.

- If there is a mismatch between the MAC address, the IP address, or the interface, then the security appliance drops the packet.
- If the ARP packet does not match any entries in the static ARP table, then you can set the security appliance to either forward the packet out all interfaces (flood), or to drop the packet.

Note The dedicated management interface, if present, never floods packets even if this parameter is set to flood.

ARP inspection prevents malicious users from impersonating other hosts or routers (known as ARP spoofing). ARP spoofing can enable a "man-in-the-middle" attack. For example, a host sends an ARP request to the gateway router; the gateway router responds with the gateway router MAC address. The attacker, however, sends another ARP response to the host with the attacker MAC address instead of the router MAC address. The attacker can now intercept all the host traffic before forwarding it on to the router.

ARP inspection ensures that an attacker cannot send an ARP response with the attacker MAC address, so long as the correct MAC address and the associated IP address are in the static ARP table.

Note In transparent firewall mode, dynamic ARP entries are used for traffic to and from the security appliance, such as management traffic.

Examples

The following example enables ARP inspection on the outside interface and sets the security appliance to drop any ARP packets that do not match the static ARP entry:

```
hostname(config)# arp outside 209.165.200.225 0009.7cbe.2100
hostname(config)# arp-inspection outside enable no-flood
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
clear configure arp-inspection	Clears the ARP inspection configuration.
firewall transparent	Sets the firewall mode to transparent.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

asdm disconnect

To terminate an active ASDM session, use the **asdm disconnect** command in privileged EXEC mode.

asdm disconnect *session*

Syntax Description

session	The session ID of the active ASDM session to be terminated. You can display the session IDs of all active ASDM sessions using the **show asdm sessions** 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
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0	This command was changed from the **pdm disconnect** command to the **asdm disconnect** command.

Usage Guidelines

Use the **show asdm sessions** command to display a list of active ASDM sessions and their associated session IDs. Use the **asdm disconnect** command to terminate a specific session.

When you terminate an ASDM session, any remaining active ASDM sessions keep their associated session ID. For example, if there are three active ASDM sessions with the session IDs of 0, 1, and 2, and you terminate session 1, the remaining active ASDM sessions keep the session IDs 0 and 2. The next new ASDM session in this example would be assigned a session ID of 1, and any new sessions after that would begin with the session ID 3.

Examples

The following example terminates an ASDM session with a session ID of 0. The **show asdm sessions** commands display the active ASDM sessions before and after the **asdm disconnect** command is entered.

```
hostname# show asdm sessions

0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# show asdm sessions

1 192.168.1.2
```

Related Commands

Command	Description
show asdm sessions	Displays a list of active ASDM sessions and their associated session ID.

asdm disconnect log_session

To terminate an active ASDM logging session, use the **asdm disconnect log_session** command in privileged EXEC mode.

asdm disconnect log_session *session*

Syntax Description

session	The session ID of the active ASDM logging session to be terminated. You can display the session IDs of all active ASDM sessions using the **show asdm log_sessions** 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
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use the **show asdm log_sessions** command to display a list of active ASDM logging sessions and their associated session IDs. Use the **asdm disconnect log_session** command to terminate a specific logging session.

Each active ASDM session has one or more associated ASDM logging sessions. ASDM uses the logging session to retrieve syslog messages from the security appliance. Terminating a log session may have an adverse effect on the active ASDM session. To terminate an unwanted ASDM session, use the **asdm disconnect** command.

Note Because each ASDM session has at least one ASDM logging session, the output for the **show asdm sessions** and **show asdm log_sessions** may appear to be the same.

When you terminate an ASDM logging session, any remaining active ASDM logging sessions keep their associated session ID. For example, if there are three active ASDM logging sessions with the session IDs of 0, 1, and 2, and you terminate session 1, the remaining active ASDM logging sessions keep the session IDs 0 and 2. The next new ASDM logging session in this example would be assigned a session ID of 1, and any new logging sessions after that would begin with the session ID 3.

Examples

The following example terminates an ASDM session with a session ID of 0. The **show asdm log_sessions** commands display the active ASDM sessions before and after the **asdm disconnect log_sessions** command is entered.

```
hostname# show asdm log_sessions

0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# show asdm log_sessions

1 192.168.1.2
```

Related Commands

Command	Description
show asdm log_sessions	Displays a list of active ASDM logging sessions and their associated session ID.

asdm group

Caution Do not manually configure this command. ASDM adds **asdm group** commands to the running configuration and uses them for internal purposes. This command is included in the documentation for informational purposes only.

asdm group *real_grp_name real_if_name*

asdm group *ref_grp_name ref_if_name* **reference** *real_grp_name*

Syntax Description

real_grp_name	The name of an ASDM object group.
real_if_name	The name of the interface to which the specified object group is associated.
ref_grp_name	The name of an object group that contains translated IP addresses of the object group specified by the *real_grp_name* argument.
ref_if_name	The name of the interface from which the destination IP address of inbound traffic is translated.

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	This command was changed from the **pdm group** command to the **asdm group** command.

Usage Guidelines

Do not manually configure or remove this command.

asdm history enable

To enable ASDM history tracking, use the **asdm history enable** command in global configuration mode. To disable ASDM history tracking, use the **no** form of this command.

asdm history enable

no asdm history enable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was changed from the **pdm history enable** command to the **asdm history enable** command.

Usage Guidelines

The information obtained by enabling ASDM history tracking is stored in the ASDM history buffer. You can view this information using the **show asdm history** command. The history information is used by ASDM for device monitoring.

Examples

The following example enables ASDM history tracking:

```
hostname(config)# asdm history enable
hostname(config)#
```

Related Commands

Command	Description
show asdm history	Displays the contents of the ASDM history buffer.

asdm image

To specify the ASDM software image, use the **asdm image** command in global configuration mode. To remove the image specification, use the **no** form of this command.

asdm image *image_path*

no asdm image [*image_path*]

Syntax Description

image_path	The path to the ASDM image file on the security appliance, for example, `flash:/asdm`.

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	This command changed from the **pdm image** command to the **asdm image** command.

Usage Guidelines

The **asdm image** command specifies the ASDM software image used when ASDM sessions are initiated. If this command does not appear in the configuration, ASDM sessions cannot be started.

You can store more than one ASDM software image in Flash memory. Using the **asdm image** command to specify a new ASDM software image while there are active ASDM sessions does not disrupt the active sessions; active ASDM sessions will continue to use the ASDM software image they started with. New ASDM sessions will use the new software image.

Use the **no** form of this command to disable ASDM.

Examples

The following example sets the ASDM image to asdm.bin:

```
hostname(config)# asdm image flash:/asdm.bin
hostname(config)#
```

Related Commands

Command	Description
show asdm image	Displays the current ASDM image file.

asdm location

Caution Do not manually configure this command. ASDM adds **asdm location** commands to the running configuration and uses them for internal communication. This command is included in the documentation for informational purposes only.

asdm location *ip_addr netmask if_name*

asdm location *ipv6_addr/prefix if_name*

Syntax Description

ip_addr	IP address used internally by ASDM to define the network topology.
netmask	The subnet mask for *ip_addr.*
if_name	The name of the interface through which ASDM is accessed.
ipv6_addr/prefix	The IPv6 address and prefix used internally by ASDM to define the network topology.

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	This command was changed from the **pdm location** command to the **asdm location** command.

Usage Guidelines

Do not manually configure or remove this command.

asr-group

To specify an asymmetrical routing interface group ID, use the **asr-group** command in interface configuration mode. To remove the ID, use the **no** form of this command.

asr-group *group_id*

no asr-group *group_id*

Syntax Description

group_id	The asymmetric routing group ID. Valid values are from 1 to 32.

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
Interface configuration	•	•	—	•	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

When Active/Active failover is enabled, you may encounter situations where load balancing causes the return traffic for outbound connections to be routed through an active context on the peer unit, where the context for the outbound connection is in the standby group.

The **asr-group** command causes incoming packets to be re-classified with the interface of the same asr-group if a flow with the incoming interface cannot be found. If re-classification finds a flow with another interface, and the associated context is in standby state, then the packet is forwarded to the active unit for processing.

Stateful Failover must be enabled for this command to take effect.

You can view ASR statistics using the **show interface detail** command. These statistics include the number of ASR packets sent, received, and dropped on an interface.

Examples

The following example assigns the selected interfaces to the asymmetric routing group 1.

Context ctx1 configuration:

```
hostname/ctx1(config)# interface e2
hostname/ctx1(config-if)# nameif outside
hostname/ctx1(config-if)# ip address 192.168.1.11 255.255.255.0 standby 192.168.1.21
hostname/ctx1(config-if)# asr-group 1
```

Context ctx2 configuration:

```
hostname/ctx2(config)# interface e3
hostname/ctx2(config-if)# nameif outside
hostname/ctx2(config-if)# ip address 192.168.1.31 255.255.255.0 standby 192.168.1.41
hostname/ctx2(config-if)# asr-group 1
```

Related Commands

Command	Description
interface	Enters interface configuration mode.
show interface	Displays interface statistics.

authentication

To configure authentication methods for WebVPN or e-mail proxy, use the **authentication** 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 restore the default, AAA, use the **no** form of this command.

The security appliance authenticates users to verify their identity.

authentication {**aaa** | **certificate** | **mailhost** | **piggyback**}

no authentication

Syntax Description

aaa	Provides a username and password that the security appliance checks against a previously configured AAA server.
certificate	Provides a certificate during SSL negotiation.
mailhost	Authenticates via the remote mail server. You can configure mailhost for SMTPS only. For the IMAP4S and POP3S, mailhost authentication is mandatory, and not displayed as a configurable option.
piggyback	Requires that an HTTPS WebVPN session already exists. Piggyback authentication is available for e-mail proxies only.

Defaults

The following table shows the default authentication method for WebVPN and e-mail proxies:

Protocol	Default Authentication Method
WebVPN	AAA
IMAP4S	Mailhost (required)
POP3S	Mailhost (required)
SMTPS	AAA

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	This command was introduced.

Usage Guidelines

For WebVPN, you can require both AAA and certificate authentication, in which case users must provide both a certificate *and* a username and password.

For e-mail proxy authentication, you can require more than one authentication method.

Specifying the command again overwrites the current configuration.

Examples

The following example shows how to require that WebVPN users provide certificates for authentication:

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication certificate
```

authentication chap

For L2TP connections, to permit CHAP authentication for PPP, use the **authentication chap** command in tunnel-group ppp-attributes configuration mode. In response to the server challenge, the client returns the encrypted [challenge plus password], with a cleartext username. This protocol is more secure than the PAP, but it does not encrypt data.

To return the command to its default setting (permit CHAP and MS-CHAP), use the **no** form of this command.

authentication chap

no authentication chap

Syntax Description

This command has no arguments or keywords.

Defaults

By default, CHAP is a permitted authentication protocol.

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 ppp attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

You can apply this attribute only to the L2TP/IPSec tunnel-group type.

Examples

The following example entered in config-ppp configuration mode, permits CHAP for PPP connections for the tunnel group. The name of the tunnel group in this example is pppremotegrp:

```
hostname(config)# tunnel-group pppremotegrp
hostname(config)# tunnel-group pppremotegrp ppp-attributes
hostname(config-ppp)# authentication chap
hostname(config-ppp)#
```

Related Commands

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

authentication-port

To specify the port number used for RADIUS authentication for this host, use the **authentication-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 assign authentication functions:

authentication-port *port*

no authentication-port

Syntax Description

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

Defaults

By default, the device listens for RADIUS on port 1645 (in compliance with RFC 2058). If the port is not specified, the RADIUS authentication default port number (1645) 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	Semantic change to the command to support the specification of server ports on a per-host basis for server groups that contain RADIUS servers.

Usage Guidelines

If your RADIUS authentication server uses a port other than 1645, 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 authentication port 1650.

```
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)# authentication-port 1650
hostname(config-aaa-server-host)# exit
hostname(config)#
```

Related Commands

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

authentication-server-group

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

authentication-server-group [(*interface name*)] *server group* [**LOCAL** | **NONE**]

no authentication-server-group [(*interface name*)] *server group*

Syntax Description

interface name	(Optional) Specifies the interface where the IPSec tunnel terminates.
LOCAL	(Optional) Specifies authentication to be performed against the local user database if all of the servers in the server group have been deactivated due to communication failures. If the server group name is either **LOCAL** or **NONE,** do not use the **LOCAL** keyword here.
NONE	(Optional) Specifies the server group name as none. To indicate that authentication is not required, use the **NONE** keyword as the server group name.
server group	Specifies the name of the aaa-server group, which defaults to **LOCAL**.

Defaults

The default setting for this command is **LOCAL**.

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	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You can apply this attribute to the IPSec remote access tunnel-group type only:

Examples

The following example entered in config-general configuration mode, configures an authentication server group named aaa-server456 for an IPSec remote-access tunnel group named remotegrp:

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-general)# authentication-server-group aaa-server456
hostname(config-general)#
```

Related Commands

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

authentication-server-group (webvpn)

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

The security appliance authenticates users to verify their identity.

authentication-server-group *group tag*

no authentication-server-group

Syntax Description

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

Defaults

No authentication 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.

Usage Guidelines

If you configure AAA authentication, you must configure this attribute as well. Otherwise, authentication always fails.

Examples

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

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication-server-group WEBVPNAUTH
```

The next example shows how to configure IMAP4S e-mail proxy to use the set of authentication servers named IMAP4SSVRS:

```
hostname(config)# imap4s
hostname(config-imap4s)# authentication-server-group IMAP4SSVRS
```

Related Commands

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

authorization-dn-attributes

To specify what part of the subject DN field to use as the username for authorization, use the **authorization-dn-attributes** command in tunnel-group ipsec-attributes configuration mode. To return this command to the default, use the **no** form of this command.

authorization-dn-attributes {*primary-attr* [*secondary-attr*] | **use-entire-name**}

no authorization-dn-attributes

Syntax Description

primary-attr	Specifies the attribute to use in deriving a name for an authorization query from a certificate.
secondary-attr	(Optional) Specifies an additional attribute to use in deriving a name for an authorization query from a certificate, if the primary attribute does not exist.
use-entire-name	Specifies that the security appliance should use the entire subject DN (RFC1779) to derive the name.

Defaults

The default value for the primary attribute is CN (Common Name).

The default value for the secondary attribute is OU (Organization Unit).

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 ipsec attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You can apply this attribute to IPSec remote access tunnel type only.

Primary and secondary attributes include the following:

Attribute	Definition
CN	Common Name: the name of a person, system, or other entity
OU	Organizational Unit: the subgroup within the organization (O)
O	Organization: the name of the company, institution, agency, association or other entity
L	Locality: the city or town where the organization is located

Attribute	Definition
SP	State/Province: the state or province where the organization is located
C	Country: the two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
EA	E-mail address
T	Title
N	Name
GN	Given Name
SN	Surname
I	Initials
GENQ	Generational Qualifier
DNQ	Domain Name Qualifier
UID	User Identifier

Examples

The following example entered in config-ipsec configuration mode, creates a remote access tunnel group (ipsec_ra) named remotegrp, specifies IPSec group attributes and defines the Common Name to be used as the username for authorization:

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-ipsec)# authorization-dn-attributes CN
hostname(config-ipsec)#
```

Related Commands

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

authorization-dn-attributes (webvpn)

To specify the primary and secondary subject DN fields to use as the username for authorization, use the **authorization-dn-attributes** command.

For WebVPN, use this command in webvpn mode. For e-mail proxies (IMAP4S. POP3S, or SMTPS), use this command in the applicable e-mail proxy mode. To remove the attribute from the configuration and restore default values, use the **no** form of this command.

authorization-dn-attributes {*primary-attr***} [***secondary-attr***] | use-entire-name}**

no authorization-dn-attributes

Syntax Description

primary-attr	Specifies the attribute to use to derive a name for an authorization query from a digital certificate.
secondary-attr	(Optional) Specifies an additional attribute to use with the primary attribute to derive a name for an authorization query from a digital certificate.
use-entire-name	Specifies that the security appliance should use the entire subject DN to derive a name for an authorization query from a digital certificate.

Defaults

The default value for the primary attribute is CN (Common Name).

The default value for the secondary attribute is OU (Organization Unit).

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 ipsec-attributes	•	—	•	—	—
Webvpn	•	—	•	—	—
Imap4s	•	—	•	—	—
Pop3s	•	—	•	—	—
SMTPS	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The following table explains the DN fields.

DN Field	Explanation
C	Country
CN	Common Name
DNQ	DN Qualifier
EA	E-mail Address
GENQ	Generational Qualifier
GN	Given Name
I	Initials
L	Locality
N	Name
O	Organization
OU	Organizational Unit
SER	Serial Number
SN	Surname
SP	State/Province
T	Title
UID	User ID
user-entire-name	Use entire DN name

Examples

The following example shows how to specify that WebVPN users must authorize according to their e-mail address (primary attribute) and organization unit (secondary attribute):

```
hostname(config)# webvpn
hostname(config-webvpn)# authorization-dn-attributes EA OU
```

Related Commands

Command	Description
authorization-required	Requires users to authorize successfully prior to connecting.

authorization-required

To require users to authorize successfully to connect, use the **authorization-required** command in tunnel-group ipsec-attributes configuration mode. To return this command to the default, use the **no** form of this command.

authorization-required

no authorization-required

Defaults

The default setting of this command is disabled.

Syntax Description

This command has no arguments or keywords.

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 ipsec attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You can apply this attribute to IPSec remote-access tunnel-group type only.

Examples

The following example entered in config-ipsec configuration mode, requires authorization based on the complete DN for users connecting through a remote-access tunnel group named remotegrp. The first command configures the tunnel-group type as ipsec_ra (IPSec remote access) for the remote group named remotegrp. The second command enters ipsec-attributes mode for the specified tunnel group, and the last command specifies authorization required for the named tunnel group:

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-ipsec)# authorization-required
hostname(config-ipsec)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.

Command	Description
show running-config tunnel-group	Shows the indicated certificate map entry.
tunnel-group-map default-group	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

authorization-required (webvpn)

To require WebVPN users or e-mail proxy users to authorize successfully prior to connecting, use the **authorization-required** command. For WebVPN, use this command in webvpn mode. For e-mail proxies (IMAP4S. POP3S, or SMTPS), use this command in the applicable e-mail proxy mode. To remove the attribute from the configuration, use the **no** version of this command.

authorization-required

no authorization-required

Syntax Description

This command has no arguments or keywords.

Defaults

Authorization-required 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
Webvpn	•	—	•	—	—
Imap4s	•	—	•	—	—
Pop3s	•	—	•	—	—
SMTPS	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to require authorization for WebVPN users:

```
hostname(config)# webvpn
hostname(config-webvpn)# authorization-required
```

Related Commands

Command	Description
authorization-dn-attributes (webvpn)	Specifies the primary and secondary subject DN fields to use as the username for authorization

authorization-server-group

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

authorization-server-group *server group*

no authorization-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 **no authorization-server-group**.

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	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You can apply this attribute only to IPSec remote access tunnel-group types.

When VPN Authorization is defined as LOCAL, the attributes configured in the default group policy DfltGrpPolicy are enforced.

Examples

The following example entered in config-general configuration mode, configures an authorization server group named “aaa-server78” for an IPSec remote-access tunnel group named “remotegrp”:

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp general
hostname(config-general)# authorization-server-group aaa-server78
hostname(config-general)#
```

Related Commands

Command	Description
aaa-server host	Configures AAA-server parameters.
clear configure tunnel-group	Clears all configured tunnel groups.

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

authorization-server-group (webvpn)

To specify the set of authorization servers to use with WebVPN or one of the e-mail proxies, use the **authorization-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 authorization servers from the configuration, use the **no** form of this command.

The security appliance uses authorization to verify the level of access to network resources that users are permitted.

authorization-server-group *group tag*

no authorization-server-group

Syntax Description

group tag	Identifies the previously configured authorization server or group of servers. Use the **aaa-server** command to configure authorization servers.

Defaults

No authorization 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	This command was introduced.

Examples

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

```
hostname(config)# webvpn
hostname(config-webvpn)# authorization-server-group WebVPNpermit
```

The following example shows how to configure POP3S e-mail proxy to use the set of authorization servers namedPOP3Spermit:

```
hostname(config)# pop3s
hostname(config-pop3s)# authorization-server-group POP3Spermit
```

Related Commands

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

auth-prompt

To specify or change the AAA challenge text for through-the-security appliance user sessions, use the **auth-prompt** command in global configuration mode. To remove the authentication challenge text, use the **no** form of this command.

auth-prompt prompt [**prompt** | **accept** | **reject**] *string*

no auth-prompt prompt [**prompt** | **accept** | **reject**]

Syntax Description

accept	If a user authentication via Telnet is accepted, display the prompt *string*.
prompt	The AAA challenge prompt string follows this keyword.
reject	If a user authentication via Telnet is rejected, display the prompt *string*.
string	A string of up to 235 alphanumeric characters or 31 words, limited by whichever maximum is first reached. Special characters, spaces, and punctuation characters are permitted. Entering a question mark or pressing the **Enter** key ends the string. (The question mark appears in the string.)

Defaults

If you do not specify an authentication prompt:

- FTP users see `FTP authentication`,
- HTTP users see `HTTP Authentication`
- Telnet users see no challenge text.

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	Minor semantic changes.

Usage Guidelines

The **auth-prompt** command lets you specify the AAA challenge text for HTTP, FTP, and Telnet access through the security appliance when requiring user authentication from TACACS+ or RADIUS servers. This text is primarily for cosmetic purposes and displays above the username and password prompts that users view when logging in.

If the user authentication occurs from Telnet, you can use the **accept** and **reject** options to display different status prompts to indicate that the authentication attempt is accepted or rejected by the AAA server.

If the AAA server authenticates the user, the security appliance displays the **auth-prompt accept** text, if specified, to the user; otherwise it displays the **reject** text, if specified. Authentication of HTTP and FTP sessions displays only the challenge text at the prompt. The **accept** and **reject** text are not displayed.

Note Microsoft Internet Explorer displays up to 37 characters in an authentication prompt. Netscape Navigator displays up to 120 characters, and Telnet and FTP display up to 235 characters in an authentication prompt.

Examples

The following example sets the authentication prompt to the string "Please enter your username and password.":

```
hostname(config)# auth-prompt prompt Please enter your username and password
```

After this string is added to the configuration, users see the following:

```
Please enter your username and password
User Name:
Password:
```

For Telnet users, you can also provide separate messages to display when the security appliance accepts or rejects the authentication attempt; for example:

```
hostname(config)# auth-prompt reject Authentication failed. Try again.
hostname(config)# auth-prompt accept Authentication succeeded.
```

The following example sets the authentication prompt for a successful authentication to the string, "You're OK."

hostname(config)# auth**-prompt accept You're OK.**

After successfully authenticating, the user sees the following message:

```
You're OK.
```

Related Commands

Command	Description
clear configure auth-prompt	Removes the previously specified authentication prompt challenge text and reverts to the default value, if any.
show running-config auth-prompt	Displays the current authentication prompt challenge text.

auto-update device-id

To configure the security appliance device ID for use with an Auto Update Server, use the **auto-update device-id** command in global configuration mode. To remove the device ID, use the **no** form of this command.

auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

no auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

Syntax Description

hardware-serial	Uses the hardware serial number of the security appliance to uniquely identify the device.
hostname	Uses the hostname of the security appliance to uniquely identify the device.
ipaddress [*if_name*]	Uses the IP address of the security appliance to uniquely identify the security appliance. By default, the security appliance uses the interface used to communicate with the Auto Update Server. If you want to use a different IP address, specify the *if_name*.
mac-address [*if_name*]	Uses the MAC address of the security appliance to uniquely identify the security appliance. By default, the security appliance uses the MAC address of the interface used to communicate with the Auto Update Server. If you want to use a different MAC address, specify the *if_name*.
string *text*	Specifies the text string to uniquely identify the device to the Auto Update Server.

Command History

Release	Modification
7.0	This command was introduced.

Defaults

The default ID is the hostname.

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	•	•	•	—	—

Examples

The following example sets the device ID to the serial number:

```
hostname(config)# auto-update device-id hardware-serial
```

Related Commands

auto-update poll-period	Sets how often the security appliance checks for updates from an Auto Update Server.
auto-update server	Identifies the Auto Update Server.
auto-update timeout	Stops traffic from passing through the security appliance if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update poll-period

To configure how often the security appliance checks for updates from an Auto Update Server, use the **auto-update poll-period** command in global configuration mode. To reset the parameters to the defaults, use the **no** form of this command.

auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

no auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

Syntax Description

poll_period	Specifies how often, in minutes, to poll an Auto Update Server, between 1 and 35791. The default is 720 minutes (12 hours).
retry_count	Specifies how many times to try reconnecting to the Auto Update Server if the first attempt fails. The default is 0.
retry_period	Specifies how long to wait, in minutes, between connection attempts, between 1 and 35791. The default is 5 minutes.

Defaults

The default poll period is 720 minutes (12 hours).

The default number of times to try reconnecting to the Auto Update Server if the first attempt fails is 0.

The default period to wait between connection attempts is 5 minutes.

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	This command was introduced.

Examples

The following example sets the poll period to 360 minutes, the retries to 1, and the retry period to 3 minutes:

```
hostname(config)# auto-update poll-period 360 1 3
```

Related Commands

auto-update device-id	Sets the security appliance device ID for use with an Auto Update Server.
auto-update server	Identifies the Auto Update Server.

auto-update timeout	Stops traffic from passing through the security appliance if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update server

To identify the Auto Update Server, use the **auto-update server** command in global configuration mode. To remove the server, use the **no** form of this command. The security appliance periodically contacts the Auto Update Server for any configuration, operating system, and ASDM updates.

auto-update server *url* [**source** *interface*] [*verify-certificate*]

no auto-update server *url* [**source** *interface*] [*verify-certificate*]

Syntax Description

url	Specifies the location of the Auto Update Server using the following syntax: **http**[**s**]**:**[[*user:password*@]*location* [:*port*]] **/** *pathname*
interface	Specifies which interface to use when sending requests to the auto-update server.
verify_certificate	Verifies the certificate returned by the Auto Update Server.

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	This command was introduced.

Usage Guidelines

Only one server can be configured.

For auto update functionality to work properly, you must use the **boot system configuration** command and ensure it specifies a valid boot image.

If the interface specified in the **source** *interface* argument is the same interface specified with the **management-access** command, requests to the auto-update server will be sent over the VPN tunnel.

Examples

The following example sets the Auto Update Server URL and specifies the interface outside:

```
hostname(config)# auto-update server http://10.1.1.1:1741/ source outside
```

Related Commands

auto-update device-id	Sets the security appliance device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the security appliance checks for updates from an Auto Update Server.
auto-update timeout	Stops traffic from passing through the security appliance if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration.
management-access	Enables access to an internal management interface on the security appliance.
show running-config auto-update	Shows the Auto Update Server configuration.

auto-update timeout

To set a timeout period in which to contact the Auto Update Server, use the **auto-update timeout** command in global configuration mode. If the Auto Update Server has not been contacted for the timeout period, the security appliance stops all traffic through the security appliance. Set a timeout to ensure that the security appliance has the most recent image and configuration. To remove the timeout, use the **no** form of this command.

auto-update timeout *period*

no auto-update timeout [*period*]

Syntax Description

period	Specifies the timeout period in minutes between 1 and 35791. The default is 0, which means there is no timeout. You cannot set the timeout to 0; use the **no** form of the command to reset it to 0.

Defaults

The default timeout is 0, which sets the security appliance to never time out.

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	This command was introduced.

Usage Guidelines

A timeout condition is reported with system log message 201008.

Examples

The following example sets the timeout to 24 hours:

```
hostname(config)# auto-update timeout 1440
```

Related Commands

auto-update device-id	Sets the security appliance device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the security appliance checks for updates from an Auto Update Server.
auto-update server	Identifies the Auto Update Server.

clear configure auto-update	Clears the Auto Update Server configuration
show running-config auto-update	Shows the Auto Update Server configuration.

backup-servers

To configure backup servers, use the **backup-servers** command in group-policy configuration mode. To remove a backup server, use the **no** form of this command. To remove the backup-servers attribute from the running configuration, use the **no** form of this command without arguments. This enables inheritance of a value for backup-servers from another group policy.

IPSec backup servers let a VPN client connect to the central site when the primary security appliance is unavailable. When you configure backup servers, the security appliance pushes the server list to the client as the IPSec tunnel is established.

backup-servers {server1 server2. . . . server10 | clear-client-config | keep-client-config}

no backup-servers [server1 server2. . . . server10 | clear-client-config | keep-client-config]

Syntax Description

clear-client-config	Specifies that the client uses no backup servers. The security appliance pushes a null server list.
keep-client-config	Specifies that the security appliance sends no backup server information to the client. The client uses its own backup server list, if configured.
server1 server 2.... server10	Provides a space delimited, priority-ordered list of servers for the VPN client to use when the primary security appliance is unavailable. Identifies servers by IP address or hostname. The list can be 500 characters long, but can contain only 10 entries.

Defaults

Backup servers do not exist until you configure them, either on the client or on the primary security appliance.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Group-policy	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Configure backup servers either on the client or on the primary security appliance. If you configure backup servers on the security appliance, it pushes the backup server policy to the clients in the group, replacing the backup server list on the client if one is configured.

Note If you are using hostnames, it is wise to have backup DNS and WINS servers on a separate network from that of the primary DNS and WINS servers. Otherwise, if clients behind a hardware client obtain DNS and WINS information from the hardware client via DHCP, and the connection to the primary server is lost, and the backup servers have different DNS and WINS information, clients cannot be updated until the DHCP lease expires. Further, if you use hostnames and the DNS server is unavailable, significant delays can occur.

Examples

The following example shows how to configure backup servers with IP addresses 10.10.10.1 and 192.168.10.14, for the group policy named "FirstGroup":

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```

banner

To configure the session, login, or message-of-the-day banner, use the **banner** command in global configuration mode. The **no banner** command removes all lines from the banner keyword specified (**exec**, **login**, or **motd**).

banner {**exec | login | motd** *text*}

[no] banner {**exec | login | motd** [*text*]}

Syntax Description

exec	Configures the system to display a banner before displaying the enable prompt.
login	Configures the system to display a banner before the password login prompt when accessing the security appliance using Telnet.
motd	Configures the system to display a message-of-the-day banner when you first connect.
text	Line of message text to display.

Defaults

The default is no login, session, or message-of-the-day banner.

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 **banner** command configures a banner to display for the keyword specified. The *text* string consists of all characters following the first white space (space) until the end of the line (carriage return or line feed [LF]). Spaces in the text are preserved. However, you cannot enter tabs through the CLI.

Subsequent *text* entries are added to the end of an existing banner unless the banner is cleared first.

Note The tokens $(domain) and $(hostname) are replaced with the hostname and domain name of the security appliance. When you enter a $(system) token in a context configuration, the context uses the banner configured in the system configuration.

Multiple lines in a banner are handled by entering a new banner command for each line that you wish to add. Each line is then appended to the end of the existing banner. There is no limit on the length of a banner other than RAM and Flash limits.

When accessing the security appliance through Telnet or SSH, the session closes if there is not enough system memory available to process the banner messages or if a TCP write error occurs. Only the exec and motd banners support access to the security appliance through SSH. The login banner does not support SSH.

To replace a banner, use the **no banner** command before adding the new lines.

Use the **no banner** {**exec | login | motd**} command to remove all the lines for the banner keyword specified.

The **no banner** command does not selectively delete text strings, so any *text* that you enter at the end of the **no banner** command is ignored.

Examples

This example shows how to configure the **exec**, **login**, and **motd** banners:

```
hostname(config)# banner motd Think on These Things
hostname(config)# banner exec Enter your password carefully
hostname(config)# banner login Enter your password to log in
hostname(config)# show running-config banner
exec:
Enter your password carefully

login:
Enter your password to log in

motd:
Think on These Things
```

This example shows how to add a second line to the **motd** banner:

```
hostname(config)# banner motd and Enjoy Today
hostname(config)# show running-config banner motd
Think on These Things and Enjoy Today
```

Related Commands

Command	Description
clear configure banner	Removes all banners.
show running-config banner	Displays all banners.

banner (group-policy)

To display a banner, or welcome text, on remote clients when they connect, use the **banner** command in group-policy configuration mode. To delete a banner, use the **no** form of this command. This option allows inheritance of a banner from another group policy. To prevent inheriting a banner, use the **banner none** command.

banner {**value** *banner_string* | **none**}

no banner

Note If you configure multiple banners under a VPN group-policy, and you delete any one of the banners, all banners will be deleted.

Syntax Description

none	Sets a banner with a null value, thereby disallowing a banner. Prevents inheriting a banner from a default or specified group policy.
value *banner_string*	Constitutes the banner text. Maximum string size is 500 characters. Use the "\n" sequence to insert a carriage return.

Defaults

There is no default banner.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy	•	—	•	—	—

Command History

Release	Modification
7.0	This command was introduced.

Examples

The following example shows how to create a banner for the group policy named "FirstGroup":

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# banner value Welcome to Cisco Systems 7.0.
```

blocks

To allocate additional memory to block diagnostics (displayed by the **show blocks** command), use the **blocks** command in privileged EXEC mode. To set the value back to the default, use the **no** form of this command. The amount of memory allocated will be at most 150 KB but never more than 50% of free memory. Optionally, you can specify the memory size manually.

blocks queue history enable [*memory_size*]

no blocks queue history enable [*memory_size*]

Syntax Description

memory_size	(Optional) Sets the memory size for block diagnostics in Bytes, instead of applying the dynamic value. If this value is greater than free memory, an error message displays and the value is not accepted. If this value is greater than 50% of free memory, a warning message displays, but the value is accepted.

Defaults

The default memory assigned to track block diagnostics is 2136 Bytes.

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	This command was introduced.

Usage Guidelines

To view the currently allocated memory, enter the **show blocks queue history** command.

If you reload the security appliance, the memory allocation returns to the default.

Examples

The following example increases the memory size for block diagnostics:

```
hostname# blocks queue history enable
```

The following example increases the memory size to 3000 Bytes:

```
hostname# blocks queue history enable 3000
```

The following example attempts to increase the memory size to 3000 Bytes, but the value is more than free memory:

```
hostname# blocks queue history enable 3000
```

```
ERROR: memory size exceeds current free memory
```

The following example increases the memory size to 3000 Bytes, but the value is more than 50% of free memory:

```
hostname# blocks queue history enable 3000
WARNING: memory size exceeds 50% of current free memory
```

Related Commands

Command	Description
clear blocks	Clears the system buffer statistics.
show blocks	Shows the system buffer utilization.

boot

To specify which system image the system will use at next reload and which configuration file the system will use at startup, use the **boot** command in privileged EXEC mode. Use the **no** form of this command to restore the default value.

boot {**config** | **system**} *url*

no boot {**config** | **system**} *url*

Syntax Description

config	Specifies which configuration file to use when the system is loaded.
system	Specifies which system image file to use when the system is loaded.
url	Sets the context configuration URL. All remote URLs must be accessible from the admin context. See the following URL syntax: • **disk0:/**[*path*/]*filename* This option is only available for the ASA platform, and indicates the internal Flash card. You can also use **flash** instead of **disk0**; they are aliased. • **disk1:/**[*path*/]*filename* This option is only available for the ASA platform, and indicates the external Flash card. • **flash:/**[*path*/]*filename* • **tftp://**[*user*[**:***password*]@]*server*[:*port*]**/**[*path*/]*filename*

Defaults

If the **boot config** command is not specified, the startup-config will be saved to a hidden location, and used only with commands that utilize it, such as the **show startup-config** command and the **copy startup-config** command.

For the **boot system** command, there are no defaults. If the BOOT environment variable is not configured, the system searches only the internal Flash for the first valid image to boot. If no valid image is found no system image will be loaded, and the system will boot loop until ROMMON or Monitor mode is broken into.

You can enter up to four **boot system** command entries, to specify different images to boot from in order, and the security appliance will boot the first valid image it finds.

Note The PIX platform **boot system** command does not support loading an image using a TFTP location.

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

You set the CONFIG_FILE environment variable in the current running memory when you use the **boot config** command. This variable specifies which configuration file to load when the system boots.

Note Only one **boot system tftp:** command may be configured, and it must be the first one configured. Subsequent multiple **boot system tftp:** commands will fail unless a **no boot system** command is issued.

When you use this global configuration command, you affect only the running configuration. Use the **write memory** or **copy** command to save the environment variable from your running configuration to your startup configuration. Note that saving the running configuration to the startup configuration will also overwrite the configured file with the running configuration, so change this variable and execute the **write memory** command before copying the new configuration file to the configured name.

The system stores and executes the boot system commands in the order in which you enter them in the configuration file. To execute the configuration when the reloads use the **write memory** command or **copy** command to save the environment variable from your running configuration to your startup configuration.

Tip The ASDM image file is specified by the **asdm image** command.

Examples

The following example specifies that at startup the security appliance should load a configuration file called configuration.txt:

```
hostname(config)# boot config configuration.txt
```

Related Commands

Command	Description
asdm image	Specifies the ASDM software image.
show bootvar	Displays boot file and configuration properties.