



A Commands

aaa

Enable, disable, or view TACACS+ or RADIUS user authentication, authorization, and accounting for the server previously designated with the **aaa-server** command. (Configuration mode.)

aaa accounting include | exclude *acctg_service inbound | outbound | if_name local_ip local_mask foreign_ip foreign_mask group_tag*

no aaa accounting include | exclude *authn_service inbound | outbound | if_name group_tag*

aaa accounting match *acl_name inbound | outbound | if_name group_tag*

no aaa accounting match *acl_name inbound | outbound | if_name group_tag*

aaa authentication include | exclude *authn_service inbound | outbound | if_name local_ip local_mask foreign_ip foreign_mask group_tag*

no aaa authentication [**include | exclude** *authn_service inbound | outbound | if_name local_ip local_mask foreign_ip foreign_mask group_tag*]

aaa authentication match *acl_name inbound | outbound | if_name group_tag*

no aaa authentication match *acl_name inbound | outbound | if_name group_tag*

aaa authentication [**serial | enable | telnet | ssh | http**] *console group_tag*

[no] aaa authentication [**serial | enable | telnet | ssh | http**] *console group_tag*

aaa authorization include | exclude *author_service inbound | outbound | if_name local_ip local_mask foreign_ip foreign_mask*

no aaa authorization [**include | exclude** *author_service inbound | outbound | if_name local_ip local_mask foreign_ip foreign_mask*]

aaa authorization match *acl_name inbound | outbound | if_name group_tag*

no aaa authorization match *acl_name inbound | outbound | if_name group_tag*

clear aaa [**accounting include** | **exclude** *authen_service* **inbound** | **outbound** | *if_name group_tag*]

clear aaa [**authentication include** | **exclude** *authen_service* **inbound** | **outbound** | *if_name local_ip local_mask foreign_ip foreign_mask group_tag*]

clear aaa [**authorization** [**include** | **exclude** *author_service* **inbound** | **outbound** | *if_name local_ip local_mask foreign_ip foreign_mask*]]

show aaa

Syntax Description

accounting	Enable or disable accounting services with authentication server. Use of this command requires that you previously used the aaa-server command to designate an authentication server.
include	Create a new rule with the specified service to include.
exclude	Create an exception to a previously stated rule by excluding the specified service from authentication, authorization, or accounting to the specified host. The exclude parameter improves the former except option by allowing the user to specify a port to exclude to a specific host or hosts.
<i>acctg_service</i>	The accounting service. Accounting is provided for all services or you can limit it to one or more services. Possible values are any , ftp , http , telnet , or <i>protocolport</i> . Use any to provide accounting for all TCP services. To provide accounting for UDP services, use the <i>protocolport</i> form. For <i>protocolport</i> , the TCP <i>protocol</i> 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 <i>port</i> is not applicable and should not be used.
match <i>acl_name</i>	Specify an access-list command statement name.
authentication	Enable or disable user authentication, prompt user for username and password, and verify information with authentication server. When used with the console option, enables or disables authentication service for access to the PIX Firewall console over Telnet or from the Console connector on the PIX Firewall unit. Use of the aaa authentication command requires that you previously used the aaa-server command to designate an authentication server. The aaa authentication command supports HTTP authentication. The PIX Firewall requires authentication verification of the HTTP server through the aaa authentication http console command before PDM can access the PIX Firewall.

authen_service The application with which a user is accessing a network. Use **any**, **ftp**, **http**, or **telnet**. The **any** value enables accounting or authentication for all TCP services. To have users prompted for authentication credentials, they must use FTP, HTTP, or Telnet. (HTTP is the Web and only applies to web browsers that can prompt for a username and password.)

If the authentication or authorization server is authenticating services other than FTP, HTTP, or Telnet, using **any** will not permit those services to authenticate in the firewall. The firewall only knows how to communicate with FTP, HTTP, and Telnet for authentication and authorization.

Only set this parameter to a service other than **any** if the authentication or authorization server is set the same way. Unless you want to temporarily restrict access to a specific service, setting a service in this command can increase system administration work and may cause all connections to fail if the authentication or authorization server is authenticating one service and you set this command to another.

authorization Enable or disable TACACS+ user authorization for services (PIX Firewall does not support RADIUS authorization). The authentication server determines what services the user is authorized to access.

author_service The services which require authorization. Use **any**, **ftp**, **http**, **telnet**, or *protocol/port*. Services not specified are authorized implicitly. Services specified in the **aaa authentication** command do not affect the services which 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 only applies to the TCP and UDP protocols, not to ICMP. For protocols other than TCP, UDP, and ICMP the *port* is not applicable and should not be used. An example port specification follows.

```
aaa authorization include udp/53-1024 inside 0 0 0 0
```

This example enables 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.



Note Specifying a port range may produce unexpected results at the authorization server. PIX Firewall 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 may want users to be authorized on specific services, which will not occur if a range is accepted.

inbound	Authenticate or authorize inbound connections. Inbound means the connection originates on the outside interface and is being directed to the inside interface.
outbound	Authenticate or authorize outbound connections. Outbound means the connection originates on the inside and is being directed to the outside interface.
<i>if_name</i>	Interface name from which users require authentication. Use <i>if_name</i> in combination with the <i>local_ip</i> address and the <i>foreign_ip</i> address to determine where access is sought and from whom. The <i>local_ip</i> address is always on the highest security level interface and <i>foreign_ip</i> is always on the lowest. See the Examples section for how the <i>if_name</i> affects the use of this command.
<i>local_ip</i>	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.
<i>local_mask</i>	Network mask of <i>local_ip</i> . Always specify a specific mask value. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
<i>foreign_ip</i>	The IP address of the hosts you want to access the <i>local_ip</i> address. Use 0 to mean all hosts.
<i>foreign_mask</i>	Network mask of <i>foreign_ip</i> . Always specify a specific mask value. Use 0 if the IP address is 0. Use 255.255.255.255 for a host.
serial	Access verification for the PIX Firewall unit's serial console.
enable	Access verification for the PIX Firewall unit's privilege mode.
telnet	Access verification for the Telnet access to the PIX Firewall console.
ssh	Access verification for the SSH access to the PIX Firewall console.
http	Access verification for the HTTP (Hypertext Transfer Protocol) access to the PIX Firewall (via PDM).
console	Specifies that access to the PIX Firewall console requires authentication.
<i>group_tag</i>	The AAA server group tag defined by the aaa-server command.

console	<p>Specify that access to the PIX Firewall console require authentication and optionally, log configuration changes to a syslog server.</p> <p>The aaa authentication serial console command allows you to require authentication verification to access the PIX Firewall unit's serial console. The serial console options also logs to a syslog server changes made to the configuration from the serial console.</p> <p>Authenticated access to the PIX Firewall console has different types of prompts depending on the option you choose with the aaa authentication [serial enable telnet ssh] console command. While the enable and ssh options allow three tries before stopping with an access denied message, both the serial and telnet options cause the user to be prompted continually until successfully logging in. The serial option requests a username and password before the first command line prompt on the serial console connection. The telnet option forces you to specify a username and password before the first command line prompt of a Telnet console connection. The enable option requests a username and password before accessing privileged mode for serial, Telnet, or SSH connections. The ssh option requests a username and password before the first command line prompt on the SSH console connection. The ssh option allows a maximum of three authentication attempts.</p> <p>Telnet access to the PIX Firewall console is available from any internal interface, and from the outside interface with IPsec configured, and requires previous use of the telnet command. SSH access to the PIX Firewall console is also available from any interface without IPsec configured, and requires previous use of the ssh command.</p> <p>The new ssh option specifies the group of AAA servers to be used for SSH user authentication. The authentication protocol and AAA server IP addresses are defined with the aaa-server command statement.</p> <p>Similar to the Telnet model, if an aaa authentication ssh console group_tag command statement is not defined, you can gain access to the PIX Firewall console with the username pix and with the PIX Firewall Telnet password (set with the passwd command). If the aaa command is defined but the SSH authentication requests a timeout, which implies the AAA servers may be down or not available, you can gain access to the PIX Firewall using username pix and the enable password (set with the enable password command). By default, the Telnet password is cisco and the enable password is not set.</p> <p>If the console login request times out, you can gain access to the PIX Firewall from the serial console by entering the pix username and the enable password.</p> <p>The maximum password length for accessing the console is 16 characters.</p>
<i>group_tag</i>	The group tag set with the aaa-server command.

Usage Guidelines

The **aaa** command enables or disables the following AAA (Authentication, Authorization, and Accounting) features:

- User authentication services provided by a TACACS+ or RADIUS server are first designated with the **aaa-server** command. A user starting a connection via FTP, Telnet, or over the World Wide Web is prompted for their username and password. If the username and password are verified by the designated TACACS+ or RADIUS authentication server, the PIX Firewall unit will allow further traffic between the authentication server and the connection to interact independently through the PIX Firewall unit's "cut-through proxy" feature.

- User authorization services which control which network services a user can access. After a user is authenticated, attempts to access restricted services cause the PIX Firewall unit to verify the access permissions of the user with the designated AAA server.
- User accounting services keep a record of which network services a user has accessed. These records are also kept on the designated AAA server. Accounting information is only sent to the active server in a server group.
- Administrative authentication services providing access to the PIX Firewall unit's console via Telnet, SSH, or the serial console. Telnet access requires previous use of the `telnet` command. SSH access requires previous use of the `ssh` command.

For additional information, see Usage Note 17.



Note

RADIUS authorization is supported with the use of `access-list` command statement and configuring a RADIUS server to send an `acl=acl_name` vendor-specific identifier. Refer to the `access-list` command page for more information. Also see the `aaa-server radius-authport` commands.

If the AAA console login request times out, you can gain access to the PIX Firewall from the serial console by entering the `pix` username and the enable password

match *acl_name* Option Usage

The syntax for this command is as follows:

```
aaa authentication | authorization | accounting match acl_name inbound | outbound |
interface_name group_tag
```

An example follows:

```
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)
show aaa
aaa authentication match mylist outbound TACACS+
```

Similar to IPSec, the keyword `permit` means “yes” and `deny` means “no.” Therefore, the following command.

```
aaa authentication match yourlist outbound tacacs
```

is equal to this command:

```
aaa authentication include any 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 the following command is entered.

```
aaa authentication match yourlist outbound tacacs
```

after this command:

```
aaa authentication match mylist outbound TACACS+
```

PIX Firewall 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.

Old **aaa** command configuration and functionality stays the same and is not converted to the **access_list** format. Hybrid configurations; that is, old configurations combined with the new **access_list** configuration are not recommended.

Usage Notes

1. The maximum username prompt for HTTP authentication is 30 characters. The maximum password length is 15 characters.
2. The **aaa** command is not intended to mandate your security policy. The authentication and authorization 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 PIX Firewall interacts with FTP, HTTP (Web access), and Telnet to display the credentials prompts for logging in to the network or logging in to exit the network. You can specify that only a single service be authenticated, but this must agree with the authentication server to ensure that both the firewall and server agree.
3. Accounting information is only sent to the active server in a server group.
4. The new **include** and **exclude** options are not backward compatible with previous PIX Firewall versions. If you downgrade to an earlier version, the **aaa** command statements will be removed from your configuration.
5. The prompts users see requesting AAA credentials differ between the three services that can access the PIX Firewall for authentication: Telnet, FTP, and HTTP (Web):
 - a. Telnet users see a prompt generated by the PIX Firewall that you can change with the **auth-prompt** command. The PIX Firewall permits a user up to four chances to log in and then if the username or password still fails, the PIX Firewall drops the connection.
 - b. FTP users receive a prompt from the FTP program. If a user enters an incorrect password, the connection is dropped immediately. If the username or password on the authentication database differs from the username or password on the remote host to which you are using FTP to access, enter the username and password in these formats:

```
authentication_user_name@remote_system_user_name
authentication_password@remote_system_password
```

If you daisy-chain PIX Firewall units, Telnet authentication works in the same way as a single unit, but FTP and HTTP authentication have additional complexity for users because they have to enter each password and username with an additional at (@) character and password or username for each daisy-chained system. Users can exceed the 63-character password limit depending on how many units are daisy-chained and password length.
Some FTP graphical user interfaces (GUIs) do not display challenge values.
 - c. HTTP users see a pop-up window generated by the browser itself. 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.
6. Use of the **aaa authorization** command requires previous use of the **aaa authentication** command; however, use of the **aaa authentication** command does not require use of an **aaa authorization** command.
7. 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.

8. Authenticated access to the PIX Firewall console has different types of prompts depending on the option you choose with the **aaa authentication ... console** command:
 - a. **enable** option—Allows three tries before stopping with “Access denied.” The **enable** option requests a username and password before accessing privileged mode for serial or Telnet connections.
 - b. **serial** option—Causes the user to be prompted continually until successfully logging in. The **serial** option requests a username and password before the first command line prompt on the serial console connection.
 - c. **telnet** option—Causes the user to be prompted continually until successfully logging in. The **telnet** option forces you to specify a username and password before the first command line prompt of a Telnet console connection.

9. You can specify an interface name with **aaa authentication**. In previous versions, if you specified **aaa authentication include any outbound 0 0 server**, PIX Firewall only authenticated outbound connections and not those to the perimeter interface. PIX Firewall now authenticates any outbound connection to the outside as well as to hosts on the perimeter interface. To preserve the behavior of previous versions, use these commands to enable authentication and to disable authentication from the inside to the perimeter interface:

```
aaa authentication include any outbound 0 0 server
aaa authentication exclude outbound perim_net perim_mask server
```

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

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

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

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

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

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

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

12. For outbound connections, first use the **nat** command to determine which IP addresses can access the PIX Firewall. For inbound connections, first use the **static** and **access-list** command statements to determine which inside IP addresses can be accessed through the PIX Firewall from the outside network.
13. When a host is configured for authentication, all users on the host have to use a web browser or Telnet first before performing any other networking activity, such as accessing mail or a news reader. The reason for this is that users must first establish their authentication credentials and programs such as mail agents and newsreaders do not have authentication challenge prompts.
14. The PIX Firewall only accepts 7-bit characters during authentication. After authentication, the client and server can negotiate for 8 bits if required. During authentication, the PIX Firewall only negotiates Go-Ahead, Echo, and NVT (network virtual terminal).
15. Up to 196 TACACS+ or RADIUS servers are permitted (up to 14 servers in each of the up to 14 server groups—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.
16. For each IP address, one **aaa authentication** command is permitted for inbound connections and one for outbound connections. Also, for an 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.
17. The PIX Firewall permits only one authentication type per network. For example, if one network connects through the PIX Firewall using TACACS+ for authentication, another network connecting through the PIX Firewall can authenticate with RADIUS, but one network cannot authenticate with both TACACS+ and RADIUS.
18. For the TACACS+ server, if you do not specify a key to the **aaa-server** command, no encryption occurs.
19. Network browsers such as Netscape Navigator do not present a challenge value during authentication; therefore, only password authentication can be used from a network browser.
20. PIX Firewall supports authentication usernames up to 127 characters and passwords of up to 63 characters. A password or username may not contain an at (@) character as part of the password or username string, except as shown in Note 5.
21. The PIX Firewall displays the same timeout message for both RADIUS and TACACS+. The message “aaa server host machine not responding” displays when either of the following occurs:
 - a. The AAA server system is down.
 - b. The AAA server system is up, but the service is not running.

Previously, TACACS+ differentiated between the two preceding states and provided two different timeout messages, while RADIUS did not differentiate the two states and provided one timeout message.

22. If the first attempt at authorization fails and a second attempt causes a timeout, use the **service resetinbound** command to reset the client that failed the authorization so that it will not retransmit any connections. An example authorization timeout message in Telnet follows.

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

Examples

The following example lists the new include and exclude options:

```
aaa authentication include any outbound 172.31.0.0 255.255.0.0 0.0.0.0 0.0.0.0 tacacs+
aaa authentication exclude telnet outbound 172.31.38.0 255.255.255.0 0.0.0.0 0.0.0.0
tacacs+
```

The following examples demonstrate ways to use the *if_name* parameter. The PIX Firewall 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:

```
aaa authentication include any outbound 192.168.1.0 255.255.255.0 209.165.201.0
255.255.255.224 tacacs+
```

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

```
aaa authentication include any outbound 192.168.1.0 255.255.255.0 209.165.202.128
255.255.255.224 tacacs+
```

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

```
aaa authentication include any inbound 192.168.1.0 255.255.255.0 209.165.201.0
255.255.255.224 tacacs+
```

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

```
aaa authentication include any inbound 209.165.201.0 255.255.255.224 209.165.202.128
255.255.255.224 tacacs+
```

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

```
aaa authentication include any perimeter 209.165.202.128 255.255.255.224 209.165.201.0
255.255.255.224 tacacs+
```

This example specifies that IP addresses 10.0.0.1 through 10.0.0.254 can originate outbound connections and then enables user authentication so that those addresses must enter user credentials to exit the PIX Firewall. In this example, the first **aaa authentication** command permits authentication on FTP, HTTP, or Telnet depending on what the authentication server handles. The second **aaa authentication** command lets host 10.0.0.42 start outbound connections without being authenticated. This example uses the default authentication group **tacacs+**.

```
nat (inside) 1 10.0.0.0 255.255.255.0
aaa authentication include any outbound 0 0 tacacs+
aaa authentication exclude outbound 10.0.0.42 255.255.255.255 tacacs+ any
```

This example permits inbound access to any 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 permits authentication on FTP, HTTP, or Telnet depending on what the authentication server handles. The authentication server is at IP address 10.16.1.20 on the inside interface.

```
aaa-server AuthIn protocol tacacs+
aaa-server AuthIn (inside) host 10.16.1.20 thisisakey timeout 20
static (inside,outside) 209.165.201.0 10.16.1.0 netmask 255.255.255.224
access-list acl_out permit tcp 10.16.1.0 255.255.255.0 209.165.201.0 255.255.255.224
access-group acl_out in interface outside
aaa authentication include any inbound 0 0 AuthIn
```

This example enables authorization for DNS lookups from the outside interface:

```
aaa authorization include udp/53 inbound 0.0.0.0 0.0.0.0
```

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

```
aaa authorization include 1/0 outbound 0.0.0.0 0.0.0.0
```

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

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

```
aaa authorization include 1/8 outbound 0.0.0.0 0.0.0.0
```

Related Commands

- [aaa-server](#)
- [auth-prompt](#)
- [service](#)
- [ssh](#)
- [telnet](#)
- [virtual](#).

aaa authentication

The **aaa authentication** command has been modified to support PDM authentication. The PIX Firewall requires authentication verification of the HTTP server through the **aaa authentication http console** command before PDM can access the PIX Firewall. (Configuration mode.)

```
[no] aaa authentication [serial | enable | telnet | ssh | http] console group_tag
```

Syntax Description

authentication	Enable or disable user authentication, prompt user for username and password, and verify information with the authentication server.
serial	Access verification for the PIX Firewall unit's serial console.
enable	Access verification for the PIX Firewall unit's privilege mode.
telnet	Access verification for the Telnet access to the PIX Firewall console.
ssh	Access verification for the SSH access to the PIX Firewall console.
http	Access verification for the HTTP (Hypertext Transfer Protocol) access to the PIX Firewall (via PDM).
console	Specifies that access to the PIX Firewall console requires authentication.
<i>group_tag</i>	The AAA server group tag defined by the aaa-server command.

Defaults

If an **aaa authentication http console** *group_tag* command statement is not defined, you can gain access to the PIX Firewall (via PDM) with no username and the PIX Firewall enable password (set with the **password** command). If the **aaa** command is defined but the HTTP authentication requests a time out, which implies the AAA servers may be down or not available, you can gain access to the PIX Firewall using the username **pix** and the enable password. By default, the enable password is not set.

Usage Guidelines

Use of the **aaa authentication** command requires that you previously used the **aaa-server** command to designate an authentication server.

The web browser prompts for the username and password with a pop-up window.

Examples

The following example shows use of the **aaa authentication** command:

```
pixfirewall(config) aaa authentication telnet console radius
```

Related Commands

- [aaa-server](#)
- [http](#)
- [setup](#)

aaa proxy-limit

Specifies the number of concurrent proxy connections allowed per user. (Configuration mode.)

Configure with the command...	Remove with the command...
aaa proxy-limit <i>proxy_limit</i> disable	no aaa-server <i>group_tag</i> (<i>if_name</i>) host <i>server_ip</i> key timeout <i>seconds</i> clear aaa-server [<i>group_tag</i>]

Show command options	Show command output
show aaa proxy-limit	Displays the number of outstanding authentication requests allowed, or indicates that the proxy limit is disabled if disabled.

Syntax Description

disable	Disables the proxy limit.
<i>group_tag</i>	Specifies the AAA server. Enter LOCAL for the group tag value for local AAA services such as local command authorization using privilege levels, or use the AAA server group tag as defined by the aaa-server command.
<i>proxy_limit</i>	Specifies the number of concurrent proxy connections allowed per user, from 1 to 128. (The default value is 3.)

Usage Guidelines

The **aaa proxy-limit** command enables you to manually configure the uauth session limit by setting the maximum number of concurrent proxy connections allowed per user. By default, this value is set to 3. 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 and display the maximum number of outstanding authentication requests allowed:

```
pixdoc515(config)# aaa proxy-limit 6
pixdoc515(config)# show aaa proxy-limit
aaa proxy-limit 6
```

aaa-server

Specify an AAA server. (Configuration mode.)

aaa-server *group_tag* (*if_name*) **host** *server_ip* **key** **timeout** *seconds*

no aaa-server *group_tag* (*if_name*) **host** *server_ip* **key** **timeout** *seconds*

aaa-server *group_tag* **protocol** *auth_protocol*

aaa-server radius-acctport *port*

aaa-server radius-authport *port*

clear aaa-server [*group_tag*]

show aaa-server

Syntax Description

aaa-server	Specifies an AAA server or up to 14 groups of servers with a maximum of 14 servers each. Certain types of AAA services can be directed to different servers. Services can also be set up to fail over to multiple servers.
<i>group_tag</i>	An alphanumeric string which is the name of the server group. Use the <i>group_tag</i> in the aaa command to associate aaa authentication and aaa accounting command statements to an AAA server. Up to 14 server groups are permitted.
<i>if_name</i>	The interface name on which the server resides.
host <i>server_ip</i>	The IP address of the TACACS+ or RADIUS server.
<i>key</i>	A case-sensitive, alphanumeric keyword of up to 127 characters that is the same value as the key on the TACACS+ server. Any characters entered past 127 are ignored. The key is used between the client and server for encrypting data between them. The <i>key</i> must be the same on both the client and server systems. Spaces are not permitted in the key, but other special characters are.

timeout <i>seconds</i>	The timeout interval for the request. This is the time after which the PIX Firewall gives up on the request to the primary AAA server. If there is a standby AAA server, the PIX Firewall will send the request to the backup server. The retransmit timeout is currently set to 10 seconds and is not user configurable.
protocol <i>auth_protocol</i>	The type of AAA server, either tacacs+ or radius .
aaa-server radius-acctport	Sets the port number of the RADIUS server which the PIX Firewall unit will use for accounting functions. The default port number used for RADIUS accounting is 1646 .
aaa-server radius-authport	Sets the port number of the RADIUS server which the PIX Firewall will use for authentication functions. The default port number used for RADIUS authentication is 1645 .
<i>port</i>	<p>Specifies the destination TCP/UDP port number of the remote RADIUS server host to which you wish to assign authentication or accounting functions for the PIX Firewall.</p> <p>These port pairs are listed as assigned to authentication and accounting services on RADIUS servers:</p> <ul style="list-style-type: none"> • 1645 (authentication), 1646 (accounting) - default for PIX Firewall • 1812 (authentication), 1813 (accounting) - alternate <p>You can view these and other commonly used port number assignments online at the following website:</p> <p style="text-align: center;">http://www.iana.org/assignments/port-numbers</p> <p>See “Ports” in Chapter 1, “Using PIX Firewall Commands” for additional information.</p>
no aaa-server	Unbinds an AAA server from an interface or host.
show aaa-server	Displays configuration information of an AAA server in the configuration.
clear aaa-server	Removes an AAA server from the configuration.

Defaults

By default, the PIX Firewall listens for RADIUS on ports **1645** for authentication and **1646** for accounting.

Usage Guidelines

The **aaa-server** command allows you to specify an AAA server group. PIX Firewall lets you define separate groups of TACACS+ or RADIUS servers for specifying different types of traffic; such as, a TACACS+ server for inbound traffic and another for outbound traffic. Another use is where all outbound HTTP traffic will be authenticated by a TACACS+ server, and all inbound traffic will use RADIUS.

AAA server groups are defined by a tag name that directs different types of traffic to each authentication server. If the first authentication server in the list fails, the AAA subsystem fails over to the next server in the tag group. You can have up to 14 tag groups and each group can have up to 14 AAA servers for a total of up to 196 AAA servers.

If your RADIUS server uses ports 1812 for authentication and 1813 for accounting, you are required to reconfigure the PIX Firewall to use ports 1812 and 1813.

**Note**

This is a global setting that takes effect when RADIUS service is started. The default ports are 1645 for authentication and 1646 for accounting as defined in RFC 2058. Newer RADIUS servers may use the port numbers 1812 and 1813 as defined in RFC 2138 and 2139. If your server uses ports other than 1645 and 1646, then you should define ports using the **aaa-server radius-authport** and **aaa-server radius-acctport** commands prior to starting the RADIUS service with the **aaa-server** command.

The **aaa** command references the tag group.

**Note**

The previous server type option at the end of the **aaa authentication** and **aaa accounting** commands has been replaced with the **aaa-server** group tag. Backward compatibility with previous versions is maintained by the inclusion of two default protocols for TACACS+ and RADIUS.

If accounting is in effect, the accounting information goes only to the active server.

The default configuration provides these two **aaa-server** protocols:

```
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
```

**Note**

Changing authorization and accounting port settings is possible. By default, PIX Firewall listens for RADIUS on ports 1645 and 1646. If your RADIUS server uses ports 1812 and 1813, you may also reconfigure it to use ports 1812 and 1813 with the **aaa-server radius-authport** and **aaa-server radius-acctport** commands.

If you are upgrading from a previous version of PIX Firewall and have **aaa** command statements in your configuration, using the default server groups allows you to maintain backward compatibility with the **aaa** command statements in your configuration.

Examples

1. This example uses the default protocol TACACS+ with the **aaa** commands:

```
aaa-server TACACS+ (inside) host 10.1.1.10 thekey timeout 20
aaa authentication include any outbound 0 0 0 0 TACACS+
aaa authorization include any outbound 0 0 0 0
aaa accounting include any outbound 0 0 0 0 TACACS+
aaa authentication serial console TACACS+
```

This example specifies that the authentication server with the IP address 10.1.1.10 resides on the inside interface and is in the default 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 PIX Firewall unit's serial console requires authentication from the TACACS+ server.

- This example creates the AuthOut and AuthIn server groups for RADIUS authentication and specifies that servers 10.0.1.40, 10.0.1.41, and 10.1.1.2 on the inside interface provide authentication. The servers in the AuthIn group authenticate inbound connections, the AuthOut group authenticates outbound connections.

```

aaa-server AuthIn protocol radius
aaa-server AuthIn (inside) host 10.0.1.40 ab timeout 20
aaa-server AuthIn (inside) host 10.0.1.41 abc timeout 4
aaa-server AuthOut protocol radius
aaa-server AuthOut (inside) host 10.1.1.2 abc123 timeout 15
aaa authentication include any inbound 0 0 0 0 AuthIn
aaa authentication include any outbound 0 0 0 0 AuthOut

```

- This example lists the commands that can be used to establish an Xauth crypto map:

```

ip address inside 10.0.0.1 255.255.255.0
ip address outside 168.20.1.5 255.255.255.0
ip local pool dealer 10.1.2.1-10.1.2.254
nat (inside) 0 access-list 80
aaa-server TACACS+ host 10.0.0.2 secret123
crypto ipsec transform-set pc esp-des esp-md5-hmac
crypto dynamic-map cisco 4 set transform-set pc
crypto map partner-map 20 ipsec-isakmp dynamic cisco
crypto map partner-map client configuration address initiate
crypto map partner-map client authentication TACACS+
crypto map partner-map interface outside
isakmp key cisco1234 address 0.0.0.0 netmask 0.0.0.0
isakmp client configuration address-pool local dealer outside
isakmp policy 8 authentication pre-share
isakmp policy 8 encryption des
isakmp policy 8 hash md5
isakmp policy 8 group 1
isakmp policy 8 lifetime 86400

```

The **aaa-server** command is used with the **crypto map** command to establish an authentication association so that VPN clients are authenticated when they access the PIX Firewall.

Related Commands

- [crypto ipsec](#)
- [isakmp](#)

access-group

Binds the access list to an interface. (Configuration mode.)

```
access-group acl_ID in interface interface_name
```

```
clear access-group [acl_ID]
```

```
no access-group acl_ID in interface interface_name
```

```
show access-group [acl_ID]
```

Syntax Description

<i>acl_ID</i>	The name associated with a given access list.
---------------	---

in interface	Filter on inbound packets at the given interface.
<i>interface_name</i>	The name of the network interface.

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 PIX Firewall continues to process the packet. If you enter the **deny** option in an **access-list** command statement, PIX Firewall discards the packet and generates the following syslog message.

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

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



Note

The use of **access-group** command overrides the **conduit** and **outbound** command statements for the specified *interface_name*.

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

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

The **clear access-group** command removes all entries from an access list indexed by *acl_ID*. If *acl_ID* is not specified, all **access-list** command statements are removed from the configuration.

Examples

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

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

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

access-list

Create an access list. (Configuration mode.)

```
access-list acl_ID [deny | permit] protocol {source_addr | local_addr} {source_mask |
local_mask} operator port {destination_addr | remote_addr} {destination_mask |
remote_mask} operator port
```

```
access-list acl_ID [deny | permit] icmp {source_addr | local_addr} {source_mask | local_mask}
operator port {destination_addr | remote_addr} {destination_mask | remote_mask} operator
port icmp_type
```

```
no access-list acl_ID [[deny | permit] protocol {source_addr | local_addr} {source_mask |
local_mask} operator port {destination_addr | remote_addr} {destination_mask |
remote_mask} operator port]
```

```
clear access-list [acl_ID [deny | permit] icmp {source_addr | local_addr} {source_mask |
local_mask} operator port {destination_addr | remote_addr} {destination_mask |
remote_mask} operator port icmp_type]
```

```
show access-list
```

Syntax Description	
<i>acl_ID</i>	Name of an access list. You can use either a name or number.
deny	<p>When used with the access-group command, the deny option does not allow a packet to traverse the PIX Firewall. By default, PIX Firewall denies all inbound or outbound packets unless you specifically permit access.</p> <p>When used with a crypto map command statement, deny does not select a packet for IPsec protection. The deny option prevents traffic from being protected by IPsec in the context of that particular crypto map entry. In other words, it does not allow the policy as specified in the crypto map command statements to be applied to this traffic.</p>
permit	<p>When used with the access-group command, the permit option selects a packet to traverse the PIX Firewall. By default, PIX Firewall denies all inbound or outbound packets unless you specifically permit access.</p> <p>When used with a crypto map command statement, permit selects a packet for IPsec protection. The permit option causes all IP traffic that matches the specified conditions to be protected by IPsec using the policy described by the corresponding crypto map command statements.</p>
<i>protocol</i>	Name or number of an IP protocol. It can be one of the keywords icmp , ip , tcp , or udp , or an integer in the range 1 to 254 representing an IP protocol number. To match any Internet protocol, including ICMP, TCP, and UDP, use the keyword ip .
<i>source_addr</i>	Address of the network or host from which the packet is being sent. Use this field when an access-list command statement is used in conjunction with an access-group command statement, or with the aaa match access-list command and the aaa authorization command.
<i>source_mask</i>	Netmask bits (mask) to be applied to <i>source_addr</i> , if the source address is for a network mask.
<i>local_addr</i>	Address of the network or host local to the PIX Firewall. Specify a <i>local_addr</i> when the access-list command statement is used in conjunction with a crypto access-list command statement, a nat 0 access-list command statement, or a vpngroup split-tunnel command statement. The <i>local_addr</i> is the address after NAT has been performed.
<i>local_mask</i>	Netmask bits (mask) to be applied to <i>local_addr</i> , if the local address is a network mask.
<i>destination_addr</i>	IP address of the network or host to which the packet is being sent. Specify a <i>destination_addr</i> when the access-list command statement is used in conjunction with an access-group command statement, or with the aaa match access-list command and the aaa authorization command. For inbound and outbound connections, <i>destination_addr</i> is the address before NAT has been performed.
<i>destination_mask</i>	Netmask bits (mask) to be applied to <i>destination_addr</i> , if the destination address is a network mask.

<i>remote_addr</i>	IP address of the network or host remote to the PIX Firewall. specify a <i>remote_addr</i> when the access-list command statement is used in conjunction with a crypto access-list command statement, a nat 0 access-list command statement, or a vpngroup split-tunnel command statement.
<i>remote_mask</i>	Netmask bits (mask) to be applied to <i>remote_addr</i> , if the remote address is a network mask.
<i>operator</i>	<p>A comparison operand that allows you to specify a port or a port range. Use without an operator and port to indicate all ports; for example.</p> <pre>access-list acl_out permit tcp any host 209.165.201.1</pre> <p>Use eq and a port to permit or deny access to just that port. For example, use eq ftp to permit or deny access only to FTP.</p> <pre>access-list acl_out deny tcp any host 209.165.201.1 eq ftp</pre> <p>Use lt and a port to permit or deny access to all ports less than the port you specify. For example, use lt 2025 to permit or deny access to the well known ports (1 to 1024).</p> <pre>access-list acl_dmz1 permit tcp any host 192.168.1.1 lt 1025</pre> <p>Use gt and a port to permit or deny access to all ports greater than the port you specify. For example, use gt 42 to permit or deny ports 43 to 65535.</p> <pre>access-list acl_dmz1 deny udp any host 192.168.1.2 gt 42</pre> <p>Use neq and a port to permit or deny access to every port except the ports that you specify. For example, use neq 10 to permit or deny ports 1-9 and 11 to 65535.</p> <pre>access-list acl_dmz1 deny tcp any host 192.168.1.3 neq 10</pre> <p>Use range and a port range to permit or deny access to only those ports named in the range. For example, use range 10 1024 to permit or deny access only to ports 10 through 1024. All other ports are unaffected. The use of port ranges can dramatically increase the number of IPSec tunnels. For example, if a port range of 5000 to 65535 is specified for a highly dynamic protocol, up to 60,535 tunnels can be created.</p>
<i>port</i>	<p>Services you permit or deny access to. Specify services by the port that handles it, such as smtp for port 25, www for port 80, and so on. You can specify ports by either a literal name or a number in the range of 0 to 65535.</p> <p>You can view valid port numbers online at the following website:</p> <p>http://www.isi.edu/in-notes/iana/assignments/port-numbers</p> <p>See “Ports” in Chapter 1, “Using PIX Firewall Commands” for a list of valid port literal names in port ranges; for example, ftp h323. You can also specify numbers.</p>
<i>icmp_type</i>	<p>[Non-IPSec use only]—Permit or deny access to ICMP message types. Refer to Table 3-1 for a list of message types. Omit this option to mean all ICMP types.</p> <p>ICMP message types are not supported for use with IPSec; that is when the access-list command is used in conjunction with the crypto map command, the <i>icmp_type</i> is ignored.</p>

Usage Guidelines

The **access-list** command lets you specify if an IP address is permitted or denied access to a port or protocol. In this document, one or more **access-list** command statements with the same access list name are referred to as an “access list.” Access lists associated with IPsec are known as “crypto access lists.” By default, all access in an access list is denied. You must explicitly permit it.

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. This keyword is normally not recommended for use with IPsec.
- Use **host address** as an abbreviation for a mask of 255.255.255.255.

Use the following guidelines for specifying a network mask:

- Do not specify a mask if the address is for a host; if the destination address is for a host, use the **host** parameter before the address; for example:

```
access-list acl_grp permit tcp any host 192.168.1.1
```

- If the address is a network address, specify the mask as a 32-bit quantity in four-part, dotted-decimal format. Place zeros in the bit positions you want to ignore.
- Remember that you specify a network mask differently than with the Cisco IOS software **access-list** command. With PIX Firewall, use 255.0.0.0 for a Class A address, 255.255.0.0 for a Class B address, and 255.255.255.0 for a Class C address. If you are using a subnetted network address, use the appropriate network mask; for example.

```
access-list acl_grp permit tcp any 209.165.201.0 255.255.255.224
```

If appropriate, after you have defined an access list, bind it to an interface using the **access-group** command. For IPsec use, bind it with a **crypto ipsec** command statement. In addition, you can bind an access list with the RADIUS authorization feature (described in the next section).

The **show access-list** command lists the **access-list** command statements in the configuration. The **show access-list** command also lists a hit count that indicates the number of times an element has been matched during an **access-list** command search. The **clear access-list** command removes all **access-list** command statements from the configuration.

The **no access-list** command removes an **access-list** command from the configuration. If you remove all the **access-list** command statements in an access list group, the **no access-list** command also removes the corresponding **access-group** command from the configuration.

**Note**

The **aaa**, **crypto map**, and **icmp** commands make use of the **access-list** command statements.

RADIUS Authorization Feature

PIX Firewall allows a RADIUS server to send user group attributes to the PIX Firewall in the RADIUS authentication response message.

The administrator first defines access lists on the PIX Firewall for each user group. For example, there could be access lists for each department in an organization, sales, marketing, engineering, and so on. The administrator then defines each access list in the group profile in CiscoSecure.

After the PIX Firewall authenticates a user, it can then use the CiscoSecure **acl** attribute returned by the authentication server to identify an access list for a given user group. To maintain consistency, PIX Firewall also provides the same functionality for TACACS+.

To restrict users in a department to three servers and deny everything else, the **access-list** command statements are as follows:

```
access-list eng permit ip any server1 255.255.255.255
access-list eng permit ip any server2 255.255.255.255
access-list eng permit ip any server3 255.255.255.255
access-list eng deny ip any any
```

In this example, the vendor specific attribute string in the CiscoSecure configuration has been set to **acl=eng**. Use this field in the CiscoSecure configuration to identify the **access-list** identification name. The PIX Firewall gets the **acl=acl_ID** from CiscoSecure and extracts the ACL number from the attribute string, which it puts in a user's uauth entry. When a user tries to open a connection, PIX Firewall checks the access list in the user's uauth entry, and depending on the permit or deny status of the access list match, permits or denies the connection. When a connection is denied, PIX Firewall generates a corresponding syslog message. If there is no match, then the implicit rule is to deny.

Because the source IP of a given user can vary depending on where they are logging in from, set the source address in the **access-list** command statement to **any**, and the destination address to identify which network services the user is permitted or denied access to. If you want to specify that only users logging in from a given subnet may use the specified services, specify the subnet instead of using **any**.

**Note**

An access list used for RADIUS authorization does not require an **access-group** command to bind the statements to an interface.

There is *not* a **radius** option to the **aaa authorization** command.

Follow these steps to enable RADIUS authorization:

-
- Step 1** Enable RADIUS authentication with the **aaa authentication** command.
 - Step 2** Create the **access-list** command statements to specify what services hosts are authorized to use with RADIUS.
 - Step 3** Configure the authentication server with the vendor-specific **acl=acl_ID** identifier to specify the **access-list ID**.

When the PIX Firewall sends a request to the authentication server, it returns the **acl=acl_ID** string, which tells PIX Firewall to use the **access-list** command statements to determine how RADIUS users are authorized.

Usage Notes

1. The **clear access-list** command automatically unbinds an access list from a **crypto map** command or interface. The unbinding of an access list from a **crypto map** command can lead to a condition that discards all packets because the **crypto map** command statements referencing the access list are incomplete. To correct the condition, either define other **access-list** command statements to complete the **crypto map** command statements or remove the **crypto map** command statements that pertain to the **access-list** command statement. Refer to the [crypto map](#) command for more information.
2. The **access-list** command operates on a first match basis.

3. If you specify an **access-list** command statement and bind it to an interface with the **access-group** command statement, by default, all traffic inbound to that interface is denied. You must explicitly permit traffic. Note that “inbound” in this context means traffic passing through the interface, rather than the more typical PIX Firewall usage of inbound meaning traffic passing from a lower security level interface to a higher security level interface.
4. Always permit access first and then deny access afterward. If the host entries match, then use a **permit** statement, otherwise use the default **deny** statement. You only need to specify additional **deny** statements if you need to deny specific hosts and permit everyone else.
5. You can view security levels for interfaces with the **show nameif** command.
6. The ICMP message type (*icmp_type*) option is ignored in IPSec applications because the message type cannot be negotiated with ISAKMP.
7. Only one access list can be bound to an interface using the **access-group** command.
8. If you specify the **permit** option in the access list, the PIX Firewall continues to process the packet. If you specify the **deny** option in the access list, PIX Firewall discards the packet and generates the following syslog message.


```
%PIX-4-106019: IP packet from source_addr to destination_addr, protocol protocol
received from interface interface_name deny by access-group acl_ID
```
9. The **access-list** command uses the same syntax as the Cisco IOS software **access-list** command *except* that PIX Firewall uses a subnet mask, whereas Cisco IOS software uses a wildcard mask. (In Cisco IOS software, the mask in this example would be specified with the **0.0.0.255** value.) For example, in the Cisco IOS software **access-list** command, a subnet mask of 0.0.0.255 would be specified as 255.0.0.0 in the PIX Firewall **access-list** command.
10. We recommend that you do not use the **access-list** command with the **conduit** and **outbound** commands. While using these commands together will work, the way in which these commands operate may cause debugging issues because the **conduit** and **outbound** commands operate from one interface to another whereas the **access-list** command used with the **access-group** command applies only to a single interface. If these commands must be used together, PIX Firewall evaluates the **access-list** command before checking the **conduit** and **outbound** commands.
11. Refer to the Chapter 3, "Managing Network Access and Use" in the *Cisco PIX Firewall and VPN Configuration Guide* for a detailed description about using the **access-list** command to provide server access and to restrict outbound user access.
12. Refer to the **aaa-server radius-acctport** and **aaa-server radius-authport** commands to verify or change port settings.

ICMP Message Types

[Non-IPSec use only]—If you prefer more selective ICMP access, you can specify a single ICMP message type as the last option in this command. [Table 3-1](#) lists possible ICMP types values.

Table 3-1 ICMP Type Literals

ICMP Type	Literal
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address

Table 3-1 ICMP Type Literals (continued)

ICMP Type	Literal
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-reply
14	timestamp-request
15	information-request
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect

If you specify an ICMP message type for use with IPsec, PIX Firewall ignores it.

For example:

```
access-list 10 permit icmp any any echo-reply
```

IPsec is enabled such that a **crypto map** command references the *acl_name* for this **access-list** command, then the **echo-reply** ICMP message type is ignored.

Using the access-list Command with IPsec

If an access list is bound to an interface with the **access-group** command, the access list selects which traffic can traverse the PIX Firewall. When bound to a **crypto map** command statement, the access list selects which IP traffic IPsec protects and which traffic IPsec does not protect. For example, access lists can be created to protect all IP traffic between Subnet X and Subnet Y or traffic between Host A and Host B. More information is available in the **crypto map** command section of this guide.

The access lists themselves are not specific to IPsec. It is the **crypto map** command statement referencing the specific access list that defines whether IPsec processing is applied to the traffic matching a permit in the access list.

Crypto access lists associated with the IPsec **crypto map** command statement have these primary functions:

- Select outbound traffic to be protected by IPsec (permit = protect).
- Indicate the data flow to be protected by the new security associations (specified by a single permit entry) when initiating negotiations for IPsec security associations.
- Process inbound traffic to filter out and discard traffic that IPsec protects.
- Determine whether or not to accept requests for IPsec security associations on behalf of the requested data flows when processing IKE negotiation from the IPsec peer. (Negotiation is only done for **crypto map** command statements with the **ipsec-isakmp** option.) For a peer's initiated IPsec negotiation to be accepted, it must specify a data flow that is permitted by a crypto access list associated with an **ipsec-isakmp** crypto map entry.

You can associate a crypto access list with an interface by defining the corresponding **crypto map** command statement and applying the crypto map set to an interface. Different access lists must be used in different entries of the same crypto map set. However, both inbound and outbound traffic will be evaluated against the same "outbound" IPsec access list. Therefore, the access list's criteria are applied in the forward direction to traffic exiting your PIX Firewall and the reverse direction to traffic entering your PIX Firewall.

If you want certain traffic to receive one combination of IPsec protection (for example, authentication only) and other traffic to receive a different combination of IPsec protection (for example, both authentication and encryption), you need to create two different crypto access lists to define the two different types of traffic. These different access lists are then used in different crypto map entries that specify different IPsec policies.

We recommend that you configure "mirror image" crypto access lists for use by IPsec and that you avoid using the **any** keyword. See the *Cisco PIX Firewall and VPN Configuration Guide* for more information.

If you configure multiple statements for a given crypto access list, in general, the first **permit** statement matched, will be the statement used to determine the scope of the IPsec security association. That is, the IPsec security association will be set up to protect traffic that meets the criteria of the matched statement only. Later, if traffic matches a different **permit** statement of the crypto access list, a new, separate IPsec security association will be negotiated to protect traffic matching the newly matched **access list** command statement.

Some services such as FTP require two **access-list** command statements, one for port 10 and another for port 21, to properly encrypt FTP traffic.

Examples

The following example creates a numbered access list that specifies a Class C subnet for the source and a Class C subnet for the destination of IP packets. Because the **access-list** command is referenced in the **crypto map** command statement, PIX Firewall encrypts all IP traffic that is exchanged between the source and destination subnets.

```
access-list 101 permit ip 172.21.3.0 255.255.0.0 172.22.2.0 255.255.0.0
access-group 101 in interface outside
crypto map mymap 10 match address 101
```

The next example only lets an ICMP message type of echo-reply be permitted into the outside interface:

```
access-list acl_out permit icmp any any echo-reply
access-group acl_out interface outside
```

alias

Administer overlapping addresses with dual NAT. (Configuration mode.)

alias [(if_name)] dnat_ip foreign_ip [netmask]

no alias [(if_name)] dnat_ip foreign_ip [netmask]

show alias

clear alias

Syntax Description

<i>if_name</i>	The internal network interface name in which the <i>foreign_ip</i> overlaps.
<i>dnat_ip</i>	An IP address on the internal network that provides an alternate IP address for the external address that is the same as an address on the internal network.
<i>foreign_ip</i>	IP address on the external network that has the same address as a host on the internal network.
<i>netmask</i>	Network mask applied to both IP addresses. Use 255.255.255.255 for host masks.

Usage Guidelines

The **alias** command translates one address into another. Use this command to prevent conflicts when you have IP addresses on a network that are the same as those on the Internet or another intranet. You can also use this command to do 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

For DNS **fixup** to work properly, **proxy-arp** has to be disabled. If you are using the **alias** command for DNS **fixup**, disable **proxy-arp** with the following command after the **alias** command has been executed:

```
sysopt noproxyarp internal_interface
```

If the **alias** command is used with the **sysopt ipsec pl-compatible** command, a static **route** command statement must be added for each IP address specified in the **alias** command statement.

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

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

The **alias** command has two uses which can be summarized in the following ways of reading an **alias** command statement:

- If the PIX Firewall gets a packet destined for the *dnat_IP_address*, send it to the *foreign_IP_address*.
- If the PIX Firewall gets a DNS packet returned to the PIX Firewall destined for *foreign_network_address*, alter the DNS packet to change the foreign network address to *dnat_network_address*.

The **no alias** command disables a previously set **alias** command statement. The **show alias** command displays **alias** command statements in the configuration. The **clear alias** command removes all **alias** commands from the configuration.

The **alias** command automatically interacts with 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 *foreign_ip* and *dnat_ip* IP addresses. For example, **alias 192.168.201.0 209.165.201.0 255.255.255.224** creates aliases for each IP address between 209.165.201.1 and 209.165.201.30.

**Note**

ActiveX blocking does not occur when users access an IP address referenced by the **alias** command. ActiveX blocking is set with the **filter activex** command.

Usage Notes

- To access an **alias** *dnat_ip* address with **static** and **access-list** command statements, specify the *dnat_ip* address in the **access-list** command statement as the address from which traffic is permitted from. The following example illustrates this note.

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

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

- You can use the **sysopt nodnsalias** command to disable inbound embedded DNS A record fixups according to aliases that apply to the A record address and outbound replies.

Examples

In this example, 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 PIX Firewall because the client assumes 209.165.201.29 is on the local inside network. To correct this, use the **alias** command as follows:

```
alias (inside) 192.168.201.0 209.165.201.0 255.255.255.224
```

```
show alias
```

```
alias 192.168.201.0 209.165.201.0 255.255.255.224
```

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 PIX Firewall to be 192.168.201.29. If the PIX Firewall uses 209.165.200.225 through 209.165.200.254 as the global pool IP addresses, the packet goes to the PIX Firewall with SRC=209.165.201.2 and DST=209.165.201.29. The PIX Firewall translates the address to SRC=209.165.200.254 and DST=209.165.201.29 on the outside.

In the next example, a web server is on the inside at 10.1.1.11 and a **static** command statement was created for it 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.

```
www.example.com.      IN      A      209.165.201.11
```

The period at the end of the www.example.com. domain name must be included.

The **alias** command follows:

```
alias 10.1.1.11 209.165.201.11 255.255.255.255
```

PIX Firewall doctors the nameserver replies to 10.1.1.11 for inside clients to directly connect to the web server.

The **static** command statement is as follows:

```
static (inside,outside) 209.165.201.11 10.1.1.11
```

The **access-list** command statement you would expect to use follows:

```
access-list acl_grp permit tcp host 209.165.201.7 host 209.165.201.11 eq telnet
```

But with the **alias** command, use this command:

```
access-list acl_grp permit tcp host 209.165.201.11 eq telnet host 209.165.201.7
```

You can test the DNS entry for the host with the following UNIX **nslookup** command:

```
nslookup -type=any www.example.com
```

arp

Change or view the ARP cache, and set the timeout value. (Configuration mode.)

```
arp if_name ip_address mac_address [alias]
```

```
clear arp
```

```
no arp if_name ip_address
```

```
show arp [if_name] [ip_address mac_address alias]
```

```
arp timeout seconds
```

```
no arp timeout
```

```
show arp timeout
```

Syntax Description

<i>if_name</i>	The internal or external interface name specified by the nameif command.
<i>ip_address</i>	Host IP address for the ARP table entry.
<i>mac_address</i>	Hardware MAC address for the ARP table entry; for example, 00e0.1e4e.3d8b.
alias	Make this entry permanent. Alias entries do not time out and are automatically stored in the configuration when you use the write command to store the configuration.
<i>seconds</i>	Duration that an ARP entry can exist in the ARP table before being cleared.

Usage Guidelines

The **arp** command adds an entry to the PIX Firewall ARP cache. ARP is a low-level TCP/IP protocol that resolves a node's physical address from its IP address through an ARP request asking the node with a particular IP address to send back its physical address. The presence of entries in the ARP cache indicates that the PIX Firewall has network connectivity. The **clear arp** command clears the ARP table but not the **alias** (permanent) entries. Use the **no arp** command to remove these entries. The **show arp** command lists the entries in the ARP table.

**Note**

You can use the **sysopt noproxyarp** command to disable proxy-arp on an interface.

Use the **arp** command to add an entry for new hosts you add on your network or when you swap an existing host for another. Alternatively, you can wait for the duration specified with the **arp timeout** command to expire and the ARP table rebuilds itself automatically with the new host information.

The **arp timeout** command sets the duration that an ARP entry can stay in the PIX Firewall ARP table before expiring. The timer is known as the ARP persistence timer. The default value is 14,400 seconds (4 hours).

The **no arp timeout** command sets the timer to its default value. The **show arp timeout** command displays its current value.

Examples

The following examples illustrate use of the **arp** and **arp timeout** commands:

```
arp inside 192.168.0.42 00e0.1e4e.2a7c
arp outside 192.168.0.43 00e0.1e4e.3d8b alias
show arp
    outside 192.168.0.43 00e0.1e4e.3d8b alias
    inside 192.168.0.42 00e0.1e4e.2a7c
```

```
clear arp inside 192.168.0.42
```

```
arp timeout 42
show arp timeout
arp timeout 42 seconds
```

```
no arp timeout
show arp timeout
arp timeout 14400 seconds
```

auth-prompt

Change the AAA challenge text. (Configuration mode.)

```
auth-prompt [accept | reject | prompt] string
no auth-prompt [accept | reject | prompt] string
clear auth-prompt
show auth-prompt
```

Syntax Description

accept	If a user authentication via Telnet is accepted, display the prompt <i>string</i> .
reject	If a user authentication via Telnet is rejected, display the prompt <i>string</i> .
prompt	The AAA challenge prompt string follows this keyword. This keyword is optional for backward compatibility.
<i>string</i>	A string of up to 235 alphanumeric characters. Special characters should not be used; however, 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.)

Usage Guidelines

The **auth-prompt** command lets you change the AAA challenge text for HTTP, FTP, and Telnet access. This text displays above the username and password prompts that users view when logging in. If you do not use this command, FTP users view `FTP authentication`, HTTP users view `HTTP Authentication`, and challenge text does not appear for Telnet access.

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

**Note**

Microsoft Internet Explorer only 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 shows how to set the authentication prompt and how users view the prompt:

```
auth-prompt XYZ Company Firewall Access
```

After this string is added to the configuration, users view:

```
Example.com Company Firewall Access  
User Name:  
Password:
```

The **prompt** keyword can be included or omitted. For example:

```
auth-prompt prompt Hello There!
```

This command statement is the same as the following:

```
auth-prompt Hello There!
```

