A through B Commands

aaa accounting

Enable, disable, or view LOCAL, TACACS+, or RADIUS user accounting (on a server designated by the **aaa-server** command).

[**no**] **aaa accounting include | exclude** *service if_name local_ip local_mask foreign_ip foreign_mask server_tag*

[**no**] **aaa accounting include | exclude** *service if_name server_tag*

clear aaa [**accounting include | exclude** *service if_name server_tag*]

[**no**] **aaa accounting match** *acl_name if_name server_tag*

show aaa

Syntax Description

accounting	Enable or disable accounting services. Use of this command requires that you previously used the **aaa-server** command to designate a AAA server.
exclude	Create an exception to a previously stated rule by excluding the specified service from accounting. 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	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.
if_name	Interface name from which users require authentication. Use *if_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	Create 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.

match *acl_name*	Specify an **access-list** command statement name.
server_tag	The AAA server group tag defined by the **aaa-server** command. To use the local PIX Firewall user authentication database, enter **LOCAL** for this parameter.
service	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 *protocol*/*port*. Use **any** to provide accounting for all TCP services. To provide accounting for UDP services, use the *protocol*/*port* form. 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.

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.

Command Modes

Configuration mode.

Usage Guidelines

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.

Use the **aaa accounting** command with the **aaa authentication** and **aaa authorization** commands.

The **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.

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 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.

Note The **aaa accounting** command is only supported for TCP and UDP traffic. A warning message is displayed if you enter an **aaa accounting match** command referencing an access list that permits other protocols.

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.

Tip The **help aaa** command displays the syntax and usage for the **aaa authentication**, **aaa authorization**, **aaa accounting**, and **aaa proxy-limit** commands in summary form.

Examples

The default PIX Firewall configuration provides the following **aaa-server** protocols:

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

The following 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.

Related Commands

aaa authentication	Enables, disables, or displays LOCAL, TACACS+, or RADIUS user authentication on a server designated by the **aaa-server** command, or for PDM user authentication.
aaa authorization	Enables or disables LOCAL or TACACS+ user authorization services.
auth-prompt	Changes the AAA challenge text.
password	Sets the password for Telnet access to the PIX Firewall console.
service	Resets inbound connections.
ssh	Specifies a host for access through Secure Shell (SSH).
telnet	Specifies the host for access via Telnet.
virtual	Accesses the PIX Firewall virtual server.

aaa authentication

Enable, disable, or view LOCAL, TACACS+, or RADIUS user authentication, on a server designated by the **aaa-server** command, or PDM user authentication.

[**no**] **aaa authentication include** | **exclude** *authen_service if_name local_ip local_mask* [*foreign_ip foreign_mask*] *server_tag*

clear aaa [**authentication include** | **exclude** *authen_service if_name local_ip local_mask foreign_ip foreign_mask server_tag*]

[**no**] **aaa authentication match** *acl_name if_name server_tag*

[**no**] **aaa authentication secure-http-client**

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

show aaa

Syntax Description

authen_service	**Specifies the type of traffic to include or exclude from authentication based on the service option selected.** **access authentication** The access authentication service options are as follows: **enable**, **serial**, **ssh**, and **telnet**. Specify **serial** for serial console access, **telnet** for Telnet access, **ssh** for SSH access, and **enable** for enable-mode access. **cut-through 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. **Note** All traffic will reset the timer. This includes non-http traffic. 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 **ip** is specified, 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.
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.
console	Specify that access to the PIX Firewall console require authentication and optionally, log configuration changes to a syslog server. The maximum password length for accessing the console is 16 characters.

enable	Access verification for the PIX Firewall unit's privilege mode.
exclude	Create 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	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.
http	Access verification for the HTTP (Hypertext Transfer Protocol) access to the PIX Firewall (via PDM). The maximum username prompt for HTTP authentication is 30 characters. The maximum password length is 15 characters.
if_name	The interface name from which to authenticate users.
include	Create 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.
match *acl_name*	Specify an **access-list** command statement name. However, do not use an **access-list** command statement that uses the source port to identify matching traffic. Like the **aaa authentication include | exclude** command, the source port is not supported in the match criteria of the **aaa authentication match** *acl_name* command.
secure-http-client	Secures HTTP client authentication (through SSL) for HTTP cut-through proxy authentication.
serial	Access verification for the PIX Firewall unit's serial console.

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

ssh	Access verification for the SSH access to the PIX Firewall console.
telnet	Access verification for the Telnet access to the PIX Firewall console.

Defaults

If a **aaa authentication http console** *server_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** commands are 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.

The PIX Firewall supports authentication usernames up to 127 characters and passwords of up to 16 characters (some AAA servers accept passwords up to 32 characters). A password or username may not contain an "@" character as part of the password or username string, with a few exceptions.

Tip The **help aaa** command displays the syntax and usage for the **aaa authentication**, **aaa authorization**, **aaa accounting**, and **aaa proxy-limit** commands in summary form.

The authentication ports supported for AAA are fixed. We support port 21 for FTP, port 23 for Telnet, and port 80 for HTTP. For this reason, do not use Static PAT to reassign ports for services you wish to authenticate. In other words, when the port to authenticate is not one of the three known ports, the firewall rejects the connection instead of authenticating it.

Command Modes

Configuration mode.

Usage Guidelines

To use the **aaa authentication** command, you must first designate an authentication server with the **aaa-server** command. Also, for each IP address, one **aaa authentication** command is permitted for inbound connections and one for outbound connections.

Use the *if_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.

The **aaa authentication** command is not intended to mandate your security policy. 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 PIX Firewall interacts with FTP, HTTP , HTTPS, 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.

Note The PIX Firewall 501 platform supports a maximum of 15 authentication entries. If you try to create more than 15, the system displays the message "Unable to create a new auth range."

The **include** and **exclude** options are not backward compatible with previous PIX Firewall versions. If you downgrade to an earlier version, these **aaa authentication** command statements will be removed from your configuration.

Note When a cut-through proxy is configured, TCP sessions (TELNET, FTP, HTTP, or HTTPS) may have their sequence number 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.

aaa authentication console command

The **aaa authentication serial console** command enables 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.

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** server_tag **[LOCAL]** 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. The [**LOCAL**] keyword option specifies a second authentication method that can be local only.

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.

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.

Similar to the Telnet model, if a **aaa authentication ssh console** *server_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 timeouts, 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.

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

The **LOCAL** keyword is optional when specified as a RADIUS or TACACS+ server only. Any access to the module (**SSH, Telnet, enable**) requiring a username and password is prompted only three times.

If an **aaa authentication ssh console** *server_tag* command is not defined, you can gain access to the CLI with the username **pix** and with the PIX Telnet password (set with the **passwd** command). If the **aaa** command is defined but the SSH authentication requests timeouts, which implies that 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 (set with the **enable password** command).

The PIX Firewall supports authentication usernames up to 127 characters and passwords up to 16 characters (some AAA servers accept passwords up to 32 characters). A password or username may not contain an "@" character as part of the password or username string.

The command only accepts the second, optional **LOCAL** keyword when the *server_tag* refers to an existing, valid TACACS+ or RADIUS server group defined in a **aaa-server** command. You can configure **LOCAL** as the first and only *server_tag*.

The **no** form of the command removes the complete command and does not support removing single methods.

aaa authentication secure-http-client

The **aaa authentication secure-http-client** command enables SSL and secures username and password exchange between HTTP clients and the firewall. It offers a secure method for user authentication to the firewall prior to allowing the user's HTTP-based web requests to traverse the firewall.

The following example configures HTTP traffic to be authenticated securely:

```
aaa authentication secure-http-client
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 are limitations of the **aaa authentication secure-http-client** command:

- At runtime, a maximum of 16 HTTPS authentication processes are allowed. If all 16 HTTPS authentication processes are running, the 17th, new HTTPS connection requiring authentication is dropped.
- When **uauth timeout 0** is configured (the **uauth timeout** is set to 0), HTTPS authentication may 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 presented with an authentication page, continuously, even if the correct username and password are entered each time. You can workaround this by setting 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 may allow non-authenticated users to go through the firewall if they are comming 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
  ```

Enabling Authentication

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

- User authentication services provided by a TACACS+ or RADIUS server are first designated with the **aaa authorization** 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.
- 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.

The prompts users see requesting AAA credentials differ between the three services that can access the PIX Firewall for authentication: Telnet, FTP, HTTP, and HTTPS:

- 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.

- 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.

- 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 will load in the browser which is designed 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.

Authenticated access to the PIX Firewall console has different types of prompts depending on the option you choose with the **aaa authentication console** command:

- **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.
- **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.
- **ssh** option—Allows three tries before stopping with "Rejected by Server." The **ssh** option requests a username and password before the first command line prompt appears.
- **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.

You can specify an interface name with the **aaa authentication** command. 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
```

When a host is configured for authentication, all users on the host must 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.

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).

HTTP Authentication

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.

Note All traffic will reset the timer. This includes non-http traffic.

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.

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

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

Note To avoid interfering with these applications, do not enter blanket outgoing **aaa** command statements for all challenged ports such as using the **any** option. Be selective 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.

TACACS+ and RADIUS servers

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.

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.

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

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:

- The AAA server system is down.
- 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 between the two states and provided one timeout message.

aaa authentication match

The **aaa authentication match** *acl_name interface_name server_tag* command specifies to match an **access-list** command statement and then to provide authentication for that match. However, do not use an **access-list** command statement that uses the source port to identify matching traffic. Like the **aaa authentication include | exclude** command, the source port is not supported in the match criteria of the **aaa authentication match** *acl_name* command.

The following set of examples illustrates how to use this command, as 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
access-list yourlist permit tcp any any
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+
```

The 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** command format. Hybrid access control configurations (that is, old configurations combined with new **access-list** command-based configurations) are not recommended.

Examples

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

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

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 outbound 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
```

Related Commands

aaa authorization	Enable or disable LOCAL or TACACS+ user authorization services.
auth-prompt	Changes the AAA challenge text.
password	Sets the password for Telnet access to the PIX Firewall console.
service	Resets inbound connections.
ssh	Specifies a host for access through Secure Shell (SSH).

telnet	Specifies the host for access via Telnet.
virtual	Accesses the PIX Firewall virtual server.

aaa authorization

Enable or disable LOCAL or TACACS+ user authorization services.

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

[**no**] **aaa authorization include | exclude** *svc if_name local_ip local_mask foreign_ip foreign_mask*

clear aaa [**authorization** [**include | exclude** *svc if_name local_ip local_mask foreign_ip foreign_mask*]]

[**no**] **aaa authorization match** *acl_name if_name server_tag*

show aaa

Syntax Description

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.
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.
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.
if_name	Interface name from which users require authentication. Use *if_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	Create a new rule with the specified service to include.
LOCAL	Specifies use of the PIX Firewall local user database for local command authorization (using privilege levels). The command will only accept the second, optional LOCAL method when the <*server_tag*> refers to an existing, valid AAA TACACS+ or RADIUS server group defined in a **aaa-server** configuration command. Clearly, you can configure LOCAL as the first and only <*server_tag*>. The no form of the command will remove the complete command and will not support removing single methods.
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.
match *acl_name*	Specify an **access-list** command statement name.
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.
svc	The services which require authorization. Use **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. 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 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.
tacacs_server_tag	Specifies to use a TACACS user authentication server.

Defaults

An IP address of **0** means all hosts.

Command Modes

Configuration mode.

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.

Currently, the **aaa authorization** command is supported for use with LOCAL and TACACS+ servers but not with RADIUS servers.

Tip The **help aaa** command displays the syntax and usage for the **aaa authentication**, **aaa authorization**, **aaa accounting**, and **aaa proxy-limit** commands 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 PIX Firewall unit to verify the access permissions of the user with the designated AAA server.

The **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.

Note RADIUS authorization is supported for use with **access-list** command statements and for use in configuring a RADIUS server with 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.

Examples

The default PIX Firewall configuration provides the following **aaa-server** protocols:

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

The following 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.

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

```
aaa authorization include udp/53 inbound 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:

```
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.

The following 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 authentication	Enables, disables, or displays LOCAL, TACACS+, or RADIUS user authentication on a server designated by the **aaa-server** command, or for PDM user authentication.
auth-prompt	Changes the AAA challenge text.
password	Sets the password for Telnet access to the PIX Firewall console.
service	Resets inbound connections.
ssh	Specifies a host for access through Secure Shell (SSH).
telnet	Specifies the host for access via Telnet.
virtual	Accesses the PIX Firewall virtual server.

aaa mac-exempt

Exempts a list of MAC addresses from authentication and authorization.

[**no**] **aaa mac-exempt match** *id*

Syntax Description

id	A MAC access list number. (Configured with the **mac-list** command.)

Defaults

None.

Command Modes

The **aaa mac-exempt match** *id* command is available in configuration mode.

Usage Guidelines

The **aaa mac-exempt match** *id* command exempts a list of MAC addresses from authentication and authorization.

Note When configuring **mac-exempt**, it is recommended not to use the same IP address for both the MACs. However, in case the the hosts are getting their IP addresses from a DHCP Server, one can receive an IP address that another host in the same network used earlier. For example, if the **mac-exempt** command is configured for both the MACs, M1 and M2 when these two hosts are getting their IP addresses from the DHCP Server. Assume M1 with IP1 has gone through the PIX firewall earlier. At a later time, both hosts will get new IP addresses from the DHCP Server and this time M2 gets IP1. In this case the traffic from M1 is allowed to go through but the traffic from M2 would be dropped. However, If a **mac-exempt** is configured for one of them, then the traffic from both hosts would be allowed to pass in case they happend to send the traffic with the same IP address. A syslog alerting you to a possible spoof attack, is generated.

Examples

The following example shows how to configure MAC-based AAA:

```
pixfirewall(config)# show mac-list
mac-list adc permit 00a0.c95d.0282 ffff.ffff.ffff
mac-list adc deny 00a1.c95d.0282 ffff.ffff.ffff
mac-list ac permit 0050.54ff.0000 ffff.ffff.0000
mac-list ac deny 0061.54ff.b440 ffff.ffff.ffff
mac-list ac deny 0072.54ff.b440 ffff.ffff.ffff

pixfirewall(config)# aaa mac-exempt match ac

pixfirewall(config)# show aaa
aaa mac-exempt match ac

pixfirewall(config)# aaa ?
Usage: [no] aaa authentication|authorization|accounting include|exclude <svc>
       <if_name><l_ip> <l_mask> [<f_ip> <f_mask>] <server_tag>
       [no] aaa authentication serial|telnet|ssh|http|enable console <server_tag>
       [no] aaa authentication|authorization|accounting match <acl_name> <if_name>
       <server_tag>
       [no] aaa authorization command {LOCAL | tacacs_server_tag} aaa proxy-limit <proxy
       limit> | disable
       [no] aaa mac-exempt match <mcl-id>
```

Related Commands

aaa authentication	Enable, disable, or view LOCAL, TACACS+, or RADIUS user authentication, on a server designated by the **aaa-server** command, or PDM user authentication.
aaa authorization	Enable or disable LOCAL or TACACS+ user authorization services.
access-list	Create an access list, or use downloadable access lists. (Downloadable access lists are supported for RADIUS servers only.)
mac-list	Adds a list of MAC addresses using a first match search, and used by the firewall VPN client in performing MAC-based authentication.

aaa proxy-limit

Specifies the number of concurrent proxy connections allowed per user.

[**no**] **aaa proxy-limit** *proxy_limit* | **disable**

show aaa proxy-limit

Syntax Description

disable	Disables the proxy limit.
proxy_limit	Specifies the number of concurrent proxy connections allowed per user, from 1 to 128. (The default value is 16.)

Defaults

The default proxy limit value is 16.

Command Modes

Configuration mode.

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

The **show aaa proxy-limit** command displays the number of outstanding authentication requests allowed, or indicates that the proxy limit is disabled if disabled.

Examples

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

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

Related Commands

aaa authentication	Enable, disable, or view LOCAL, TACACS+, or RADIUS user authentication, on a server designated by the **aaa-server** command, or PDM user authentication
aaa authorization	Enable or disable LOCAL or TACACS+ user authorization services.
aaa-server	Specifies a AAA server.

aaa-server

Defines the AAA server group.

[no] aaa-server server_tag deadtime <*minutes*>

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

[no] aaa-server *server_tag* **max-failed-attempts** <*number*>

[**no**] **aaa-server** *server_tag* **protocol** *auth_protocol*

[**no**] **aaa-server radius-acctport** [*acct_port*]

[**no**] **aaa-server radius-authport** [*auth_port*]

clear aaa-server [*server_tag*]

show aaa-server

debug radius session

Syntax Description

aaa-server	Specifies a 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.
*acct*_port	RADIUS authentication port number. The default is 1645.

*auth_*port	RADIUS accounting port number. The default is 1646.
deadtime <*minutes*>	<*minutes*> identifies the minutes to declare the AAA server group as unresponsive.
debug radius session	Captures RADIUS session information and attributes for sent and received RADIUS packets.
host *server_ip*	The IP address of the TACACS+ or RADIUS server.
if_name	The interface name on which the server resides.
key	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 *key* must be the same on both the client and server systems. Spaces are not permitted in the key, but other special characters are.
max-failed-attempts <*number*>	<*number*> identifies the maximum number of AAA requests to attempt to each AAA server in a AAA server group.
no aaa-server	Unbinds a AAA server from and interface or host.
protocol *auth_protocol*	The type of AAA server, either **tacacs+** or **radius**.
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**.
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**.
server_tag	An alphanumeric string which is the name of the server group. Use the *server_tag* in the **aaa** command to associate **aaa authentication** and **aaa accounting** command statements to a AAA server. Up to 14 server groups are permitted. However, **LOCAL** cannot used with **aaa-server** command because **LOCAL** is predefined by the PIX Firewall.
timeout *seconds*	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.

Defaults

By default, the PIX Firewall listens for RADIUS on ports **1645** for authentication and **1646** for accounting. (The default ports 1645 for authentication and 1646 for accounting are as defined in RFC 2058.)

The default configuration provides the following **aaa-server** command protocols:

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

The default timeout value is 5 seconds.

Some AAA servers accept passwords up to 32 characters, but the PIX Firewall allows passwords up to 16 characters only.

Command Modes

Configuration mode.

Usage Guidelines

The **aaa-server** command lets you specify AAA server groups. 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.

Other **aaa** commands reference the server tag group defined by the **aaa-server** command *server_tag* parameter. This is a global setting that takes effect when the TACACS+ or RADIUS service is started.

Note When a cut-through proxy is configured, TCP sessions (TELNET, FTP, or HTTP) may have their sequence number 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.

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

The **show aaa-server** command displays AAA server configuration.

[no] aaa-server server_tag **deadtime** <minutes>

The *server_tag* identifies the AAA server group and is the same as the current **aaa-server** command.

<*minutes*> identifies the minutes to declare the AAA server group as unresponsive

Valid input rage: 0 - 1440
Units: minutes
Default:10

While the command may be configured even without having configured the LOCAL method on any of the three authentication and authorization commands described earlier, it only affects operations when a user has configured two methods. Obviously, at this time, the second method must and be *LOCAL*.

The command specifies the minutes a particular method should be marked unresponsive and skipped. When a AAA server group has been marked unresponsive, the firewall will immediately perform the authentication or authorization against the next method which will be the local firewall user database. Every server in a group must be marked unresponsive before the entire group will be declared unresponsive.

When you configure the deadtime to “0”, the AAA server group is never considered unresponsive and all authentication and authorization requests are always attempted against this AAA server group first before using the next method in the method list (for example, falling back to the local user database).

The **[no]** form of this command restores the **aaa-server** command to its default value of 10 minutes.

The *deadtime* begins as soon as the last server in the AAA server group has been marked DOWN. A server is marked down when maximum number of attempts defined in max-attempts has been reached and failed to receive a response. Upon expiration of the deadtime, the AAA server group becomes active and all requests will are submitted once again to the AAA servers in the AAA server group.

[no] aaa-server server_tag **max-failed-attempts** <number>

The *server_tag* identifies the AAA server group and is the same as existing **aaa-server** command today.

<*number*> identifies the maximum number of AAA requests to attempt to each AAA server in a AAA server group.

Valid input rage: 1 -5
Units: Counter
Default: 3 (same as current PIX/FWSM software)

The current PIX/FWSM software sends a AAA request 3 times to a AAA server before it declares the AAA server unresponsive and moves on to try the next server in the group. This command lets the user configure this number of attempts. Users should tune the *max-failed-attempts* and the timeout values to achieve the desired fall-back behavior when authenticating or authorizing commands in a fall-back configuration. That is, if you wish to declare an individual AAA server unresponsive more aggressively, you should reduce the *max-failed-attempts* counter to 1 or 2.

aaa-server radius-authport and aaa-server radius-acctport

You can change authorization and accounting port settings on the firewall with the **aaa-server radius-authport** and **aaa-server radius-acctport** commands. These commands specify the destination TCP/UDP port number of the remote RADIUS server host to which you wish to assign authentication or accounting functions.

By default, the PIX Firewall listens for RADIUS on ports 1645 and 1646. If your authentication server uses ports other than 1645 and 1646, then you must configure the firewall for the appropriate ports prior to starting the RADIUS service with the **aaa-server** command. For example, some RADIUS servers use the port numbers 1812 and 1813 as defined in RFC 2138 and RFC 2139. If your RADIUS server uses ports 1812 and 1813, you must use the **aaa-server radius-authport** and **aaa-server radius-acctport** commands to reconfigure the firewall to use ports 1812 and 1813.

The following port pairs are listed as assigned to authentication and accounting services on RADIUS servers:

- 1645 (authentication), 1646 (accounting) - default for PIX Firewall
- 1812 (authentication), 1813 (accounting) - alternate

You can view these and other commonly used port number assignments online at the following website:

http://www.iana.org/assignments/port-numbers

Or, alternately, refer to "Ports" in Chapter 2, "Using PIX Firewall Commands," for additional information.

Upgrading Your AAA Server Configuration and Backward Compatibility

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

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

Examples

The following 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
```

The following 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

aaa authentication	Enable, disable, or view LOCAL, TACACS+, or RADIUS user authentication, on a server designated by the **aaa-server** command, or PDM user authentication.
aaa authorization	Enable or disable LOCAL or TACACS+ user authorization services.

crypto ipsec	Creates, displays, or deletes IPSec security associations, security association global lifetime values, and global transform sets.
isakmp	Negotiates IPSec security associations and enables IPSec secure communications.

access-group

Binds the access list to an interface.

[**no**] **access-group** *access-list* **in interface** *interface_name* [*per-user-override*]

clear access-group [*access-list*]

show access-group [*access-list*]

Syntax Description

access-list	The access list *id*.
in interface	Filter inbound packets at the given interface.
interface_name	The name of the network interface.
[per-user-override]	Allow downloadable user access lists to override the access list applied to the interface.

Defaults

None.

Command Modes

Configuration mode.

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 id
```

PIX Firewall Version 6.3(2) adds support for the **per-user-override** option, which allows downloaded access lists to override the access list applied to the interface. If the **per-user-override** optional argument is not present, thePIX Firewall preserves the existing filtering behavior. When **per-user-override** is present, the PIX Firewall 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 overriden 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 109015 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.

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 *access-list* 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 *access-list*. If *access-list* 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.

Related Commands

access-list	Creates an access list, or uses a downloadable access list.

access-list

Create an access list, or use a downloadable access list. (Downloadable access lists are supported for RADIUS servers only).

access-list <acl_name> object-group-search

[**no**] **access-list deny-flow-max** *n*

[**no**] **access-list alert-interval** *secs*

[**no**] **access-list** [*id*] **compiled**

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

[**no**] **access-list** *id* [**line** *line-num*] {**deny** | **permit**}{*protocol* | **object-group** *protocol_obj_grp_id* {*source_addr source_mask*} | **object-group** *network_obj_grp_id* [*operator port* [*port*] | **interface** *if_name* | **object-group** *service_obj_grp_id*] {*destination_addr* | *remote_addr*} {*destination_mask* | *remote_mask*} | **object-group** *network_obj_grp_id* [*operator port* [*port*] | **object-group** *service_obj_grp_id*]} [**log** [[**disable** | **default**] | [*level*]]] [**interval** *secs*]]

[**no**] **access-list** *id* [**line** *line-num*] {**deny** | **permit**} **icmp** {*source_addr source_mask*} | **interface** *if_name* | **object-group** *network_obj_grp_id* {*destination_addr* | *remote_addr*} {*destination_mask* | *remote_mask*} | **interface** *if_name* | **object-group** *network_obj_grp_id* [*icmp_type* | **object-group** *icmp_type_obj_grp_id*] [**log** [[**disable** | **default**] | [*level*]]] [**interval** *secs*]]

[**no**] **debug access-list all | standard | turbo**

clear access-list {[*id*] | [*id* **counters**]}

show access-list [[*id*] *source_addr*]

Restricted for use with the **prefix-list** command:
[**no**] **access-list** *id* **deny | permit** {**any** | *prefix mask* | **host** *address*}

Syntax Description

alert-interval *secs*	Specifies the time interval, from 1 to 3600 seconds, for generating syslog message 106101, which alerts you that the firewall has reached a deny flow maximum. In other words, when the deny flow maximum is reached, another 106101 message is generated if has been at least *secs* seconds since the last 106101 message. If this option is not specified, the default interval is 300 seconds.
compiled	When used in conjunction with the **access-list** command, this turns on TurboACL unless the **no** qualifier is used, in which case the command **no access-list** *id* **compiled** turns off TurboACL for that access list. To use TurboACL globally, enter the **access-list compiled** command and to globally turn off TurboACL, enter the **no access-list compiled** command. After TurboACL has been globally configured, individual access lists or groups can have TurboACL enabled or disabled using individual **[no] access-list** *id* **compiled** commands. TurboACL is compiled only if the number of access list elements is greater than or equal to 19.

debug	Outputs access list debugging information to the console.
deny	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. 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.
deny-flow-max *n*	Specifies the maximum number of concurrent deny flows that can be created. (Syslog message 106101 is generated when the firewall has reached the maximum number, *n*, of ACL deny flows.) For a firewall with greater than 64 MB Flash memory, the value can be from 1 to 4096, with a default value of 4096. For a firewall with greater than 16 MB Flash memory, the value can be from 1 to 1024, with a default value of 1024. For a firewall with less than or equal to 16 MB Flash memory, the value can be from 1 to 256, with a default value of 256.
destination_addr	IP address of the network or host to which the packet is being sent. Specify a *destination_addr* 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, *destination_addr* is the address before NAT has been performed.
destination_mask	Netmask bits (mask) to be applied to *destination_addr*, if the destination address is a network mask.
disable	Disables ACL logging for the access control element (ACE), which is an access control list entry.
icmp_type	For 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. 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 *icmp_type* is ignored.
id	Name of an access list. You can use either a name or number.
interface *if_name*	The name of the firewall interface.
interval *secs*	The time interval in seconds, from 1 to 600, at which to generate an 106100 syslog message. The *secs* value is also used as the timeout value for deleting an inactive flow. If this option is not specified, the default interval is 300 seconds for a new access control element (ACE). If an ACE already exists, any interval previously associated with that ACE remains unchanged.
line-num	The line number at which to insert a remark or an access control element (ACE).

log disable | **default** | *level*	When the **log** option is specified, it generates syslog message 106100 for the access list element (ACE) to which it is applied. (Syslog message 106100 is generated for every matching permit or deny ACE flow passing through the firewall.) The first-match flow is cached. Subsequent matches increment the hit count displayed in the **show object-group** command (`hitcnt`) for the ACE, and new 106100 messages will be generated at the end of the interval defined by **interval** *secs* if the hit count for the flow is not zero. The default ACL logging behavior (the **log** keyword not specified) is that if a packet is denied, then message 106023 is generated, and if a packet is permitted, then no syslog message is generated. An optional syslog *level* (0 - 7) may be specified for the generated syslog messages (106100). If no *level* is specified, the default level is 6 (informational) for a new ACE. If the ACE already exists, then its existing log level remains unchanged. If the **log disable** option is specified, access list logging is completely disabled. No syslog message, including message 106023, will be generated. The **log default** option restores the default access list logging behavior.
mask	The netmask.
obj_grp_id	An existing object group.
object-group	Specifies an object group. Refer to the object-group command for information on how to configure object groups.
object-group-search	Use this keyword to specify that access list search is performed on object groups that are contained in access list instead of searching the entire expanded access list. – This mode overrides TurboACL mode (compiled). – When this mode is enabled, TurboACL on this access-list is not allowed. – When this mode is enabled on an access-list, the access-list cannot be used in the **nat** and **crypto** commands.

operator	The *operator* compares the source IP address (*sip*) or destination IP address (*dip*) ports. Possible operands include **lt** for less than, **gt** for greater than, **eq** for equal, **neq** for not equal, and **range** for an inclusive range. Use the **access-list** command the without an operator and port to indicate all ports by default.
	
	For example,
	
	`access-list acl_out permit tcp any host 209.165.201.1`
	
	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.
	
	`access-list acl_out deny tcp any host 209.165.201.1 eq ftp`
	
	Use **lt** and a port to permit or deny access to all ports less than the port you specify. For example, use **lt 1025** to permit or deny access to the well-known ports (1 to 1024).
	
	`access-list acl_dmz1 permit tcp any host 192.168.1.1 lt 1025`
	
	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.
	
	`access-list acl_dmz1 deny udp any host 192.168.1.2 gt 42`
	
	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.
	
	`access-list acl_dmz1 deny tcp any host 192.168.1.3 neq 10`
	
	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.

permit	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. 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.
prefix	The network number. For more information, refer to the **prefix-list** command.
port	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. You can view valid port numbers online at the following website: http://www.iana.org/assignments/port-numbers See "Ports" in Chapter 2, "Using PIX Firewall Commands" for a list of valid port literal names in port ranges; for example, **ftp h323**. You can also specify numbers.
protocol	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**.

remark *text*	The text of the remark to add before or after an **access-list** command statement, up to 100 characters in length.
remote_addr	IP address of the network or host remote to the PIX Firewall. Specify a *remote_addr* 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 **vpdn group split-tunnel** command statement.
remote_mask	Netmask bits (mask) to be applied to *remote_addr*, if the remote address is a network mask.
source_addr	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.
source_mask	Netmask bits (mask) to be applied to *source_addr*, if the source address is for a network mask.

Defaults

By default, PIX Firewall denies all inbound or outbound packets unless you specifically permit access.

TurboACL is used only if the number of access list elements is greater than or equal to 19.

The default time interval at which to generate syslog message 106100 is 300 seconds.

The default time interval for a deny flow maximum syslog message (106101) is 300 seconds.

The default ACL logging behavior is to generate syslog message 106023 for denied packets.

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

Command Modes

Configuration mode.

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-list** commands have an implicit **deny** unless you explicitly specify **permit**. In other words, by default, all access in an access list is denied unless you explicitly grant access using a **permit** statement.

Note Do not use the string "multicastACL" following the name of a PIX Firewall interface in an access-list name because this is a reserved keyword used by PIX Device Manager (PDM).

Additionally, you can use the **object-group** command to group access lists like any other network object.

Use the following guidelines for specifying a source 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 **access-list** command supports the **sunrpc** service.

The **show access-list** command lists the **access-list** command statements in the configuration and the hit count of the number of times each element has been matched during an **access-list** command search. Additionally, it displays the number of access list statements in the access list and indicates whether or not the list is configured for TurboACL. (If the list has less than eighteeen access control entries then it is marked to be turbo-configured but is not actually configured for TurboACL until there are 19 or more entries.)

The **show access-list** *source_addr* option filters the show output so that only those access-list elements that match the source IP address (or with **any** as source IP address) are displayed.

The **clear access-list** command removes all **access-list** command statements from the configuration or, if specified, access lists by their *id*. The **clear access-list** *id* **counters** command clears the hit count for the specified access list.

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, 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.

access-list line *line-num* commands

Use the **access-list** *id* **line** *line-num* command to insert an **access-list** command statement, and the **no access-list** *id* **line** *line-num* command to delete an **access-list** command statement.

Each access control element (ACE) and remark has an associated line number. Line numbers can be used to insert or delete elements at any position in an access list. These numbers are maintained internally in increasing order starting from 1. (For example, in sequence such as 1, 2, 3...) A user can insert a new entry between two consecutive ACEs by choosing the line number of the higher line number ACE.

The line numbers are always maintained in increasing order, with an individual line number for each ACE. However, all ACEs resulting from a single object group **access-list** command statement have a single line number. Consequently, you cannot insert an ACE in the middle of object-group ACEs.

Line numbers are displayed by the **show access-list** command. However, they are not shown in your configuration.

access-list logging commands

The following example shows what happens when an access list log option is enabled. There are some behavior differences among various types of IP traffic because the access check is only applied to those packets which do not have an existing "connection":

```
access-group outside-acl in interface outside
.
.
access-list outside-acl permit ip host 1.1.1.1 any log 7 interval 600
access-list outside-acl permit ip host 2.2.2.2 any
access-list outside-acl deny ip any any log 2
```

The following example illustrates the use of access list based logging in an ICMP context:

1. An inbound ICMP echo request (1.1.1.1 -> 192.168.1.1) arrives on the outside interface.
2. An ACL called **outside-acl** is applied for the access check.
3. The packet is permitted by the first ACE of **outside-acl** which has the **log** option enabled.
4. The log flow (ICMP, 1.1.1.1, 0, 192.168.1.1, 8) has not been cached, so the following syslog message is generated and the log flow is cached:

   ```
   106100: access-list outside-acl permitted icmp outside/1.1.1.1(0) ->
   inside/192.168.1.1(8) hit-cnt 1 (first hit)
   ```

5. Twenty such packets arrive on the outside interface within the next 10 minutes (600 seconds). Because the log flow has been cached, the log flow is located and the hit count of the log flow is incremented for each packet.
6. At the end of 10th minute, the following syslog message is generated and the hit count of the log flow is reset to 0:

   ```
   106100: access-list outside-acl permitted icmp outside/1.1.1.1(0) ->
   inside/192.168.1.1(8) hit-cnt 20 (300-second interval)
   ```

7. No such packets arrive on the outside interface within the next 10 minutes. So the hit count of the log flow remains 0.
8. At the end of 20th minute, the cached flow (ICMP, 1.1.1.1, 0, 192.168.1.1, 8) is deleted because of the 0 hit count.

To disable a log option without having to remove the ACE, use **access-list** *id* **log disable**.

When removing an access control element (ACE) with a log option enabled using a **no access-list** command, it is not necessary to specify all the log options. The ACE is removed as long as its permit or deny rule is used to uniquely identify it. However, the removal of an ACE (with a log option enabled) does not remove the associated cached flows. You must remove the entire access control list (ACL) to remove the cached flows. When a cached flow is flushed due to the removal of an ACL, a syslog message will be generated if the hit count of the flow is non-zero.

The **clear access-list** command removes all the cached flows.

access-list *id* remark command

The **access-list** *id* [**line** *line-num*] **remark** *text* command enables users to include comments (remarks) about entries in any access control list (ACL). You can use remarks to make the ACL easier to scan and interpret. Each remark line is limited to 100 characters.

The ACL remark can be placed before or after an **access-list** command statement, but it should be placed in a consistent position so that it is clear which remark describes which **access-list** command. For example, it would be confusing to have some remarks before the associated **access-list** commands and some remarks after the associated **access-list** commands.

The **no access-list** *id* **line** *line-num* **remark** *text* and **no access-list** *id* **line** *line-num* commands both remove the remark at that line number.

The following are samlpes of possible access list remarks:

```
access-list out-acl remark - ACL for the outside interface
access-list out-acl remark - Allow Joe Smith's group to login
access-list out-acl permit tcp 1.1.1.0 255.255.255.0 server
access-list out-acl remark - Allow Lee White's group to login
access-list out-acl permit tcp 1.1.3.0 255.255.255.0 server
access-list out-acl remark - Deny known hackers
access-list out-acl deny ip host 192.23.56.1 any
access-list out-acl deny ip host 197.1.1.125 any
```

RADIUS Authorization

PIX Firewall allows a RADIUS server to send user group attributes to the PIX Firewall in the RADIUS authentication response message. Additionally, the PIX Firewall allows downloadable access lists from the RADIUS server. For example, you can configure an access list on a Cisco Secure ACS server and download it to the PIX Firewall during RADIUS authorization.

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=***id* from CiscoSecure and extracts the ACL number from the attribute string, which it places 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.

Configure the access list specified in Attribute 11 to specify a per-user access list name. Otherwise, remove Attribute 11 from the AAA RADIUS server configuration if no access list is intended for user authentication. If the access list is not configured on the PIX Firewall when the user attempts to login, the login will fail.

For more information on how to use RADIUS server authorization, refer to the *Cisco PIX Firewall and VPN Configuration Guide*, Version 6.2 or higher.

TurboACL

On the PIX Firewall, TurboACL is turned on globally with the command **access-list compiled** (and turned off globally by the command **no access-list compiled**).

The PIX Firewall default mode is TurboACL off (**no access-list compiled**), and TurboACL is active only on access lists with 19 or more entries.

The minimum amount of Flash memory required to run TurboACL is 2.1 MB. If memory allocation fails, the TurboACL lookup tables will not be generated.

Note Use TurboACL only on PIX Firewall platforms that have 16 MB or more of Flash memory. Consequently, TurboACL is not supported on the PIX 501 because it has 8 MB of Flash memory.

If TurboACL is configured, some access control list or access control list group modifications can trigger regeneration of the TurboACL internal configuration. Depending on the extent of TurboACL configuration(s), this could noticeably consume CPU resources. Consequently, we recommend modifying turbo-complied access lists during non-peak system usage hours.

For more information on how to use TurboACL, refer to the *Cisco PIX Firewall and VPN Configuration Guide*, Version 6.2 or higher.

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. Access control lists that are dynamically updated on the PIX Firewall by a AAA server can only be shown using the **show access-list** command. The **write** command does not save or display these updated lists.
3. The **access-list** command operates on a first match basis.
4. 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.
5. 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.
6. You can view security levels for interfaces with the **show nameif** command.
7. The ICMP message type (*icmp_type*) option is ignored in IPSec applications because the message type cannot be negotiated with ISAKMP.
8. Only one access list can be bound to an interface using the **access-group** command.
9. 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 id
   ```

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 255.255.255.0 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 *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

For 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
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
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) *id* for this **access-list** command, then the **echo-repy** 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 referring to 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 20 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
```

The following example shows how access list entries (ACEs) are numbered by the firewall and how remarks are inserted:

```
pixfirewall(config)# show access-list ac
access-list ac; 2 elements
access-list ac line 1 permit ip any any
access-list ac line 2 permit tcp any any

pixfirewall(config)# access-list ac permit tcp object-group remote object-group locals
pixfirewall(config)# show access-list ac
access-list ac; 3 elements
```

```
access-list ac line 1 permit ip any any
access-list ac line 2 permit tcp any any (
access-list ac line 3 permit tcp object-group remote object-group locals
pixfirewall(config)# access-list ac remark This comment decribes the ACE line 3

pixfirewall(config)# show access-list ac
access-list ac; 3 elements
access-list ac line 1 permit ip any any
access-list ac line 2 permit tcp any any
access-list ac line 3 remark This comment decribes the ACE line 3
access-list ac line 4 permit tcp object-group remote object-group locals

pixfirewall(config)# access-list ac permit tcp 172.16.0.0 255.0.0.0 any
pixfirewall(config)# show access-list ac
access-list ac; 4 elements
access-list ac line 1 permit ip any any
access-list ac line 2 permit tcp any any
access-list ac line 3 remark This comment decribes the ACE line 3
access-list ac line 4 permit tcp object-group remote object-group locals
access-list ac line 5 permit tcp 172.16.0.0 255.0.0.0 any

pixfirewall(config)# no access-list ac permit tcp object-group remote object-group locals
pixfirewall(config)# show access-list ac
access-list ac; 3 elements
access-list ac line 1 permit ip any any
access-list ac line 2 permit tcp any any
access-list ac line 3 remark This comment decribes the ACE line 3
access-list ac line 4 permit tcp 172.16.0.0 255.0.0.0 any
```

The following shows how to remove an access list comment:

```
pixfirewall(config)# access-list ac remark This comment decribes the ACE line 5
pixfirewall(config)# sh access-list ac
access-list ac; 3 elements
access-list ac line 1 permit ip any any
access-list ac line 2 permit tcp any any
access-list ac line 3 remark This comment decribes the ACE line 3
access-list ac line 4 permit tcp 172.16.0.0 255.0.0.0 any
access-list ac line 5 remark This comment decribes the ACE line 5

pixfirewall(config)# no access-list ac remark This comment decribes the ACE line 5
pixfirewall(config)# show access-list ac
access-list ac; 3 elements
access-list ac line 1 permit ip any any line 1
access-list ac line 2 permit tcp any any line 2
access-list ac line 3 remark This comment decribes the ACE line 3
access-list ac line 4 permit tcp 172.16.0.0 255.0.0.0 any line 4
```

The following shows how to insert an access list statement at a specific line number:

```
pixfirewall(config)# show access-list ac
access-list ac; 3 elements
access-list ac line 1 permit ip any any
access-list ac line 2 permit tcp any any
access-list ac line 3 remark This comment decribes the ACE line 3
access-list ac line 4 permit tcp 172.16.0.0255.0.0.0 any

pixfirewall(config)# access-list ac line 4 permit ip 172.16.0.0 255.0.0.0 any
pixfirewall(config)# show access-list ac
access-list ac; 4 elements
access-list ac line 1 permit ip any any
access-list ac line 2 permit tcp any any
access-list ac line 3 remark This comment decribes the ACE line 3
access-list ac line 4 permit ip 172.16.0.0 255.0.0.0 any
```

```
access-list ac line 5 permit tcp 172.16.0.0 255.0.0.0 any
```

The **show access-list** command has the following line of output:

```
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
```

which shows the total number of cached ACL log flows (total), the number of cached deny-flows (denied), and the maximum number of allowed deny-flows.

Related Commands

access-group	Binds the access list to an interface.
conduit	(Deprecated command.) Add, delete, or show conduits through the PIX Firewall for incoming connections, superseded by the **access-list** command.
object-group	Defines object groups that you can use to optimize your configuration. Objects such as hosts, protocols, or services can be grouped, and then you can issue a single command using the group name to apply to every item in the group.
outbound/apply	Creates an access list for controlling Internet use.

activation-key

Updates the activation key on your PIX Firewall and checks the activation key running on your PIX Firewall against the activation key stored in the Flash memory of the PIX Firewall.

activation-key *activation-key-four-tuple*

show activation-key

Syntax Description

activation-key	Updates the PIX Firewall activation key unless there is a mismatch between the Flash memory and running PIX Firewall software versions.
activation-key-four-tuple	A four-element hexidecimal string with one space between each element. For example: `0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e` (The leading 0x specfier is optional; all values are assumed to be hexadecimal.)

Defaults

None.

Command Modes

Configuration mode.

Usage Guidelines

Use the **activation-key** *activation-key-four-tuple* command to change the activation key on your PIX Firewall.

Caution Use only an activation key valid for your PIX Firewall software version and platform or your system may not reload after rebooting.

The **activation-key** *activation-key-four-tuple* command output indicates the status of the activation key as follows:

- If the PIX Firewall Flash memory software image version is the same as the running PIX Firewall software version, and the PIX Firewall Flash memory activation key is the same as the running PIX Firewall software activation key, then the **activation-key** command output reads as follows:

```
The flash activation key has been modified.
The flash activation key is now the SAME as the running key.
```

- If the PIX Firewall Flash memory image version is the same as the running PIX Firewall software, and the PIX Firewall Flash memory activation key is different from the running PIX Firewall activation key, then the **activation-key** command output reads as follows:

```
The flash activation key has been modified.
The flash activation key is now DIFFERENT from the running key.
The flash activation key will be used when the unit is reloaded.
```

- If the PIX Firewall Flash memory image version is not the same as the running PIX Firewall software, then the **activation-key** command output reads as follows:

```
The flash image is DIFFERENT from the running image.
The two images must be the same in order to modify the flash activation key.
```

- If the PIX Firewall Flash memory image version is the same as the running PIX Firewall software, and the entered activation key is not valid, then the **activation-key** command output reads as follows:

```
ERROR: The requested key was not saved because it is not valid for this system.
```

- If the PIX Firewall Flash memory activation key is the same as the entered activation key, then the **activation-key** command output reads as follows:

```
The flash activation key has not been modified.
The requested key is the SAME as the flash activation key.
```

The **show activation-key** command output indicates the status of the activation key as follows:

- If the activation key in the PIX Firewall Flash memory is the same as the activation key running on the PIX Firewall, then the **show activation-key** output reads as follows:

```
The flash activation key is the SAME as the running key.
```

- If the activation key in the PIX Firewall Flash memory is the different from the activation key running on the PIX Firewall, then the **show activation-key** output reads as follows:

```
The flash activation key is DIFFERENT from the running key.
The flash activation key takes effect after the next reload.
```

- If the PIX Firewall Flash memory software image version is not the same as the running PIX Firewall software image, then the **show activation-key** output reads as follows:

```
The flash image is DIFFERENT from the running image.
The two images must be the same in order to examine the flash activation key.
```

Usage Notes

1. The PIX Firewall must be rebooted for a new activation key to be enabled.
2. If the PIX Firewall software image is being upgraded to a higher version and the activation key is being updated at the same time, we recommend that you first install the software image upgrade and reboot the PIX Firewall unit, and then update the activation key in the new image and reboot the unit again.
3. If you are downgrading to a lower PIX Firewall software version, we recommend that you ensure that the activation key running on your system is not intended for a higher version before installing the lower version software image. If this is the case, you must first change the activation key to one that is compatible with the the lower version before installing and rebooting. Otherwise, your system may refuse to reload after installation of the new software image.

Examples

The following example shows sample out from the **show activation-key** command:

```
pixfirewall(config)# show activation-key
Serial Number: 480221353 (0x1c9f98a9)

Running Activation Key: 0x36df4255 0x246dc5fc 0x39d2ec4d 0x09f6288f
Licensed Features:
Failover:           Enabled
VPN-DES:            Enabled
VPN-3DES:           Enabled
Maximum Interfaces: 6
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited

The flash activation key is the SAME as the running key.
```

Related Commands

show version	Displays the PIX Firewall operating information.

alias

Administer overlapping addresses with dual NAT.

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

clear alias

show alias

Syntax Description

dnat_ip	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.
foreign_ip	IP address on the external network that has the same address as a host on the internal network.

if_name	The internal network interface name in which the *foreign_ip* overlaps.
netmask	Network mask applied to both IP addresses. Use 255.255.255.255 for host masks.

Defaults

None.

Command Modes

Configuration mode.

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.

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

Use the **no alias** command to disable a previous **set alias** command statement. Use the **show alias** command to display **alias** command statements in the configuration. Use the **clear alias** command to remove all **alias** commands from the configuration. After changing or removing an **alias** command statement, use the **clear xlate** command.

The **alias** command changes the default behavior of the PIX Firewall in three ways:

- When receiving a packet coming in through the interface identified by *if_name*, destined for the address identified by *dnat_ip*, PIX Firewall sends it to the address identified by *foreign_ip*.
- When receiving a DNS A response, containing the address identified by *foreign_ip*, coming from a lower security interface, and destined for the host behind the inteface identified by *if_name*, PIX Firewall changes *foreign_ip* in the reply to *dnat_ip*. This can be turned off by using the command **sysopt nodnsalias inbound**.
- When receiving a DNS A response, containing the address identified by *dnat_ip*, coming from a DNS server behind the interface, *if_name*, and destined for a host behind the lower security interface, PIX Firewall changes *dnat_ip* address to *foreign_ip*. This can be turned off using the command **sysopt nodnsalias outbound**.

The **alias** command is applied on a per-interface basis, while the **sysopt nodnsalias** changes the behaviour for all interfaces. Also, note that addresses in the zone transfers made across the PIX Firewall, are not changed.

You can specify a net alias by using network addresses for the *foreign_ip* and *dnat_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.

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 the following 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=192.168.201.29. 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
```

Related Commands

access-list	Creates an access list, or uses a downloadable access list.
static	Configures a persistent one-to-one address translation rule by mapping a local IP address to a global IP address, also known as Static Port Address Translation (Static PAT).

arp

Configure the Address Resolution Protocol (ARP) cache timeout value, static ARP table entries, or static proxy ARP, and view the ARP cache, status, or timeout value.

[**no**] **arp** *if_name ip mac* [**alias**]

[**no**] **arp timeout** *seconds*

clear arp [**timeout** | **statistics**]

show arp [**timeout** | **statistics**]

Syntax Description

arp	Configure a static ARP mapping (IP-to-physical address binding) for the addresses specified. These entries are not cleared when the ARP persistence timer times out and are automatically stored in the configuration when you use the **write** command to store the configuration.
arp alias	Configure a static proxy ARP mapping (proxied IP-to-physical address binding) for the addresses specified. These entries are not cleared when the ARP persistence timer times out and are automatically stored in the configuration when you use the **write** command to store the configuration.
if_name	The interface name whose ARP table will be changed or viewed. (The interface name itself is specified by the **nameif** command.)
ip	IP address for an ARP table entry.
mac	Hardware MAC address for the ARP table entry; for example, 00e0.1e4e.3d8b.
seconds	Duration that a dynamic ARP entry can exist in the ARP table before being cleared. The permitted range of values is from 1 to 4294967. However, any value less than 60 seconds is not recommended and will result in an error message warning that ARP cache timeout values less than 60 seconds may cause packet loss.
statistics	The ARP statistics, including block usage.

Defaults

The default value for the ARP persistence timer is 14,400 seconds (4 hours).

Command Modes

Configuration mode.

Usage Guidelines

The Address Resolution Protocol (ARP) maps an IP address to a MAC address and is defined in RFC 826. Proxy Address Resolution Protocol (proxy ARP) is a variation of the ARP protocol in which an intermediate device (for example, the firewall) sends an ARP response on behalf of an end node to the requesting host. ARP mapping occurs automatically as the firewall processes traffic, however, you can configure the ARP cache timeout value, static ARP table entries, or proxy ARP.

Note Because ARP is a low-level TCP/IP protocol that resolves a node's MAC (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 firewall has network connectivity.

The **arp timeout** command specifies the duration to wait before the ARP table rebuilds itself, automatically updating new host information. This feature is also known as the ARP persistence timer. The **no arp timeout** command resets the ARP persistence timer to its default value. The **show arp timeout** command displays the current timeout value.

The **arp** *if_name ip mac* command adds a static (persistent) entry to the firewall ARP cache. (This matches the behavior of Cisco IOS). For example, you could use the **arp** *if_name ip mac* command to set up a static IP-to-MAC address mapping for hosts on your network. Use the **no arp** *if_name ip mac* command to remove the static ARP mapping.

The **arp** *if_name ip mac* **alias** command configures proxy ARP for the IP and MAC addresses specified. Enable proxy ARP when you want the firewall to respond to ARP requests for another host (determined by the IP address of the host) with the MAC address you specify in the **arp alias** command. Use the **no arp** *if_name ip mac* **alias** command to remove the static proxy ARP mapping.

The **clear arp** command clears all entries in the ARP cache table except for those you configure directly with the **arp** *if_name ip mac* command. Use the **no arp** *if_name ip mac* command to remove these entries. The **show arp** command lists the entries in the ARP table.

The **show arp statistics** command displays the following ARP information:

```
pixfirewall(config)# show arp statistics
        Dropped blocks in ARP: 6
        Maximum Queued blocks: 3
        Queued blocks: 1
        Interface collision ARPs Received: 5
        ARP-defense Gratuitous ARPS sent: 4
        Total ARP retries: 15
        Unresolved hosts: 1
        Maximum Unresolved hosts: 2
```

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
```

Related Commands

sysopt	Changes firewall system options.

auth-prompt

Change the AAA challenge text for through the firewall user sessions. (Configuration mode.)

Configure with the command...	Remove with the command...
auth-prompt [**accept** | **reject** | **prompt**] *string*	**no auth-prompt** [**accept** | **reject** | **prompt**] *string* **clear auth-prompt**

Show command options	Show command output
show auth-prompt	Displays the AAA challenge text.

Syntax Description

accept	If a user authentication via Telnet is accepted, display the prompt *string*.
prompt	The AAA challenge prompt string follows this keyword. This keyword is optional for backward compatibility.
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 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 through the firewall 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.

Following is the authentication sequence showing when each **auth-prompt** string is displayed:

1. A user initiates a telnet session from the **inside** interface through the firewall to the **outside** interface.
2. The user receives the **auth-prompt** challenge text, followed by the **username** prompt.
3. The user enters the AAA username/password username and password, or in the formats **aaa_user@outside_use**r and **aaa_pass@outside_pass**.
4. The firewall sends the **aaa_user/aaa_pass** to the TACACS or RADIUS AAA server.

5. If the AAA server authenticates the user, the firewall displays the **auth-prompt accept** text to the user, otherwise the **reject** challenge text is displayed. Authentication of http and ftp sessions displays only the challenge text at the prompt. The **accept** and **reject** text are not displayed.

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.

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 the following:

```
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!
```

Related Commands

aaa authentication	Enables, disables, or displays LOCAL, TACACS+, or RADIUS user authentication on a server designated by the **aaa-server** command, or for PDM user authentication.

auto-update

Specifies how often to poll an Auto Update Server.

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

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

clear auto-update

[**no**] **auto-update server** *url* [*verify_certificate*]

[**no**] **auto-update timeout** *period*

clear auto-update

show auto-update

Syntax Description

device-id	The device ID of the PIX Firewall.
hardware-serial	Specifies to use the hardware serial number of the PIX Firewall to uniquely identify the device.
hostname	Specifies to use the host name of the PIX Firewall to uniquely identify the device.
if_name	Specifies the interface to use (with its corresponding IP or MAC address) to uniquely identify the device.
ipaddress	Specifies to use the IP address of the specified PIX Firewall interface to uniquely identify the firewall.
mac-address	Specifies to use the MAC address of the specified PIX Firewall interface to uniquely identify the firewall.
period	Specifies how long to attempt to contact the Auto Update Server, after the last successful contact, before stopping all traffic passing through the firewall.
poll_period	Specifies how often, in minutes, to poll an Auto Update Server. 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. The default is 5 minutes and the valid range of values is from 1 to 35791.
text	Specifies the text string to uniquely identify the device to the Auto Update Server.
url	Specifies the location of the Auto Update Server using the following syntax: **http**[**s**]**:**[[*user:password*@] *location* [:*port*]] **/** *pathname* See the **copy** command for variable descriptions.
verify_certificate	Specifies to verify the certificate returned by the Auto Update Server.

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

Configuration mode.

Usage Guidelines

The **clear auto-update** command removes the entire auto-update configuration.

The **auto-update poll-period** command specifies how often to poll the Auto Update Server for configuration or software image updates. The **no auto-update poll-period** command resets the poll period to the default.

The **auto-update server** command specifies the URL of the Auto Update Server. Only one server can be configured. The **no auto-update server** command disables polling for auto-update updates (by terminating the auto-update daemon).

The **auto-update timeout** command is used to stop all new connections to the PIX Firewall if the Auto Update Server has not been contacted for *period* minutes. This can be used to ensure that the PIX Firewall has the most recent image and configuration.

The **show auto-update** command displays the Auto Update Server, poll time, and timeout period.

Examples

The **show auto-update** command displays the Auto Update Server, poll time, and timeout period. The following is sample output from the command:

```
show auto-update
Server: https://10.0.1.15/autoupdate/AutoUpdateServlet
Poll period: 1 minutes, retry count: 0, retry period: 5 minutes
Timeout: none
Device ID: string [device1]
Next poll in 0.13 minutes
Last poll: 23:43:33 UTC Fri Jun 7 2002
```

The format of the URL, `/autoupdate/AutoUpdateServlet`, is the standard URL format on the Auto Update Server. The port 443 (the default port for HTTPS) can be omitted because it is the default setting.

Related Commands

copy	Changes software images without requiring access to the TFTP monitor mode.

banner

Configures the session, login, or message-of-the-day banner.

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

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

show banner [{**exec | login | motd**}]

clear banner

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 firewall using telnet.
motd	Configures the system to display a message-of-the-day banner.
text	The line of message text to be displayed in the firewall CLI. Subsequent *text* entries are added to the end of an existing banner unless the banner is cleared first. The tokens $(domain) and $(hostname) are replaced with the host name and domain name of the firewall.

Defaults

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

Command Modes

The **banner** command is available in configuration mode.

The **show banner** command is available in privileged mode.

Usage Guidelines

The **banner** command configures a banner to display for the option specified. The *text* string consists of all characters following the first whitespace (space) until the end of the line (carriage return or LF). Spaces in the text are preserved. However, tabs cannot be entered through the CLI.

Multiple lines in a banner are handled by entering a new banner command for each line you wish to add. Each line is then appended to the end of the existing banner. If the text is empty, then a carriage return (CR) will be added to the banner. There is no limit on the length of a banner other than RAM and Flash memory limits.

When accessing the firewall 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 in attempting to display the banner messages.

To replace a banner, use the **no banner** command before adding the new lines. The **no banner** {**exec | login | motd**} command removes all the lines for the banner option specified. The **no banner** command does not selectively delete text strings, so any *text* entered at the end of the **no banner** command is ignored.

The **clear banner** command removes all the banners.

The **show banner** {**motd | exec | login**} command displays the specified banner option and all the lines configured for it. If a banner option is not specified, then all the banners are displayed.

Examples

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

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

login:
Enter your password to log in

motd:
Think on These Things
```

The following example shows how to add a second line to a banner:

```
pixfirewall(config)# banner motd and Enjoy Today
pixfirewall(config)# show banner motd
Think on These Things
and Enjoy Today
```

Related Commands

login	Specifies to log in as a particular user.
password	Sets the password for Telnet access to the PIX Firewall console.