



## T through Z Commands

### telnet

Specify the host for PIX Firewall console access via Telnet.

```
telnet ip_address [netmask] [if_name]  
clear telnet [ip_address [netmask] [if_name]]  
no telnet [ip_address [netmask] [if_name]]  
telnet timeout minutes  
show telnet  
show telnet timeout
```

Syntax Description	
<i>if_name</i>	If IPsec is operating, PIX Firewall lets you specify an unsecure interface name, typically, the outside interface. At a minimum, the <b>crypto map</b> command must be configured to specify an interface name with the <b>telnet</b> command.
<i>ip_address</i>	An IP address of a host or network that can access a PIX Firewall Telnet management session. If an interface name is not specified, the address is assumed to be on an internal interface. PIX Firewall automatically verifies the IP address against the IP addresses specified by the <b>ip address</b> commands to ensure that the address you specify is on an internal interface. If an interface name is specified, PIX Firewall only checks the host against the interface you specify.
<i>netmask</i>	Bit mask of <i>ip_address</i> . To limit access to a single IP address, use 255 in each octet; for example, 255.255.255.255. If you do not specify <i>netmask</i> , it defaults to 255.255.255.255 regardless of the class of <i>local_ip</i> . Do not use the subnetwork mask of the internal network. The <i>netmask</i> is only a bit mask for the IP address in <i>ip_address</i> .
<b>timeout</b> <i>minutes</i>	The number of minutes that a Telnet session can be idle before being closed by PIX Firewall. The default is 5 minutes. The range is <b>1</b> to <b>60</b> minutes.

**Command Modes** Configuration mode.

## Usage Guidelines

The **telnet** command lets you specify which hosts can access the PIX Firewall console with Telnet. You can enable Telnet to the PIX Firewall on all interfaces. However, the PIX Firewall enforces that all Telnet traffic to the outside interface be IPSec protected. Therefore, to enable Telnet session to the outside interface, configure IPSec on the outside interface to include IP traffic generated by the PIX Firewall and enable Telnet on the outside interface.

A maximum of five (5) active Telnet management sessions to the PIX Firewall are allowed at the same time. The **show telnet** command displays the current list of IP addresses authorized to Telnet to the PIX Firewall. Use the **no telnet** or **clear telnet** command to remove Telnet access from a previously set IP address. Use the **telnet timeout** feature to set the maximum time a console Telnet session can be idle before being logged off by PIX Firewall. The **clear telnet** command does not affect the **telnet timeout** command duration. The **no telnet** command cannot be used with the **telnet timeout** command.

Use the **passwd** command to set a password for Telnet access to the console. The default is **cisco**. Use the **who** command to view which IP addresses are currently accessing the PIX Firewall console. Use the **kill** command to terminate an active Telnet management session.

If the **aaa** command is used with the **console** option, Telnet management access must be authenticated with an authentication server.



### Note

If you have configured the **aaa** command to require authentication for PIX Firewall Telnet management access and the console login request times out, you can gain access to the PIX Firewall from the serial console by entering the **pix** username and the password that was set with the **enable password** command.

## Usage Notes

1. If you do not specify the interface name, the **telnet** command adds command statements to the configuration to let the host or network access the Telnet management session from all internal interfaces.

When you use the **show telnet** command, this assumption may not seem to make sense. For example, if you enter the following command without a netmask or interface name.

```
telnet 192.168.1.1
```

If you then use the **show telnet** command, you see that not just one command statement is specified, but all internal interfaces are represented with a command statement:

```
show telnet
192.168.1.1 255.255.255.255 inside
192.168.1.1 255.255.255.255 intf2
192.168.1.1 255.255.255.255 intf3
```

The purpose of the **show telnet** command is that, were it possible, the 192.168.1.1 host could access the Telnet management session from any of these internal interfaces. An additional facet of this behavior is that you must delete each of these command statements individually with the following commands.

```
no telnet 192.168.1.1 255.255.255.255 inside
no telnet 192.168.1.1 255.255.255.255 intf2
no telnet 192.168.1.1 255.255.255.255 intf3
```

2. To access the PIX Firewall with Telnet from the intf2 perimeter interface, use the following command:

```
telnet 192.168.1.1 255.255.255.255 intf2
```

3. The default password to access the PIX Firewall console via Telnet is **cisco**.

4. Some Telnet applications such as the Windows 95 or Windows NT Telnet sessions may not support access to the PIX Firewall unit's command history feature via the arrow keys. However, you can access the last entered command by pressing Ctrl-P.
5. The **telnet timeout** command affects the next session started but not the current session.
6. If you connect a computer directly to the inside interface of the PIX Firewall with Ethernet to test Telnet access, you must use a cross-over cable and the computer must have an IP address on the same subnet as the inside interface. The computer must also have its default route set to be the inside interface of the PIX Firewall.
7. If you need to access the PIX Firewall console from outside the PIX Firewall, you can use a **static** and **access-list** command pair to permit a Telnet session to a Telnet server on the inside interface, and then from the server to the PIX Firewall. In addition, you can attach the console port to a modem but this may add a security problem of its own. You can use the same terminal settings as for HyperTerminal, which is described in the *Cisco PIX Firewall and VPN Configuration Guide*.  
If you have IPSec configured, you can access the PIX Firewall console with Telnet from outside the PIX Firewall. Once an IPSec tunnel is created from an outside host to the PIX Firewall, you can access the console from the outside host.
8. Output from the **debug crypto ipsec**, **debug crypto isakmp**, and **debug ssh** commands do not display in a Telnet or SSH console session. For information about the **debug crypto ipsec** and **debug crypto isakmp** commands, refer to the [debug](#) command page.

## Examples

The following examples permit hosts 192.168.1.3 and 192.168.1.4 to access the PIX Firewall console via Telnet. In addition, all the hosts on the 192.168.2.0 network are given access:

```
telnet 192.168.1.3 255.255.255.255 inside
telnet 192.168.1.4 255.255.255.255 inside
telnet 192.168.2.0 255.255.255.0 inside
show telnet
      192.168.1.3 255.255.255.255 inside
      192.168.1.4 255.255.255.255 inside
      192.168.2.0 255.255.255.0 inside
```

You can remove individual entries with the **no telnet** command or all **telnet** command statements with the **clear telnet** command:

```
no telnet 192.168.1.3 255.255.255.255 inside
show telnet
      192.168.1.4 255.255.255.255 inside
      192.168.2.0 255.255.255.0 inside
clear telnet
show telnet
```

You can change the maximum session idle duration as follows:

```
telnet timeout 10
show telnet timeout
telnet timeout 10 minutes
```

An example Telnet login session appears as follows (the password does not display when entered):

```
PIX passwd: cisco

Welcome to the PIX Firewall
...
Type help or '?' for a list of available commands.
pixfirewall>
```

**Related Commands**

- [aaa accounting](#)
- [kill](#)
- [password](#)
- [who](#)

# terminal

Change console terminal settings.

**terminal monitor**

**terminal no monitor**

**terminal width** *characters*

**Syntax Description**

<i>characters</i>	Permissible values are 0, which means 511 characters, or a value in the range of 40 to 511.
<b>monitor</b>	Enable or disable syslog message displays on the console.
<b>width</b>	Set the width for displaying information during console sessions.

**Command Modes**

Configuration mode.

**Usage Guidelines**

The **terminal monitor** command lets you enable or disable the display of syslog messages in the current session for Telnet access to the PIXFirewall console. Use the **logging monitor** command to enable or disable various levels of syslog messages to the Telnet console; use the **terminal no monitor** command to disable the messages on a per session basis. Use the **terminal monitor** command to restart the syslog messages for the current session.

The **terminal width** command sets the width for displaying command output. The terminal width is controlled by the command: **terminal width** *nn*, where *nn* is the width in characters. If you enter a line break, it is not possible to backspace to the previous line.

**Examples**

The following example shows enabling logging and then disabling logging only in the current session with the **terminal no monitor** command:

```
logging monitor
...
terminal no monitor
```

# tftp-server

Specify the IP address of the TFTP configuration server.

**[no] tftp-server** [*if\_name*] *ip\_address path*

**clear tftp-server** [[*if\_name*] *ip\_address path*]

**show tftp-server**

## Syntax Description

<i>if_name</i>	Interface name on which the TFTP server resides. If not specified, an internal interface is assumed. If you specify the outside interface, a warning message informs you that the outside interface is insecure.
<i>ip_address</i>	The IP address or network of the TFTP server.
<i>path</i>	The path and filename of the configuration file. The format for path differs by the type of operating system on the server. The contents of path are passed directly to the server without interpretation or checking. The configuration file must exist on the TFTP server. Many TFTP servers require the configuration file to be world-writable to write to it and world-readable to read from it.

## Command Modes

Configuration mode.

## Usage Guidelines

The **tftp-server** command lets you specify the IP address of the server that you use to propagate PIX Firewall configuration files to your firewalls. Use the **tftp-server** command with the **configure net** command to read from the configuration or with the **write net** command to store the configuration in the file you specify. The **clear tftp-server** command removes the **tftp-server** command from your configuration.

PIX Firewall supports only one TFTP server.

The *path* name you specify in the **tftp-server** is appended to the end of the IP address you specify in the **configure net** and **write net** commands. The more you specify of a file and path name with the **tftp-server** command, the less you need to specify with the **configure net** and **write net** commands. If you specify the full path and filename in the **tftp-server** command, the IP address in the **configure net** and **write net** commands can be represented with a colon (:).

The **no tftp server** command disables access to the server. The **show tftp-server** command lists the **tftp-server** command statements in the current configuration.



### Note

If the TFTP server to which the firewall is trying to connect is not running the TFTP service, the firewall hangs and does not timeout. Press "ESC" key on the firewall console to abort the TFTP session and return to the firewall command line prompt.

## Examples

The following example specifies a TFTP server and then reads the configuration from /pixfirewall/config/test\_config:

```
tftp-server 10.1.1.42 /pixfirewall/config/test_config
...
```

```
configure net :
```

## timeout

Set the maximum idle time duration.


```
timeout [xlate hh[:mm[:ss]]] [conn hh[:mm[:ss]]] [half-closed hh[:mm[:ss]]] [udp hh[:mm[:ss]]]
[rpc hh[:mm[:ss]]] [h225 hh[:mm[:ss]]] [h323 hh[:mm[:ss]]] [mgcp hh[:mm[:ss]]]
[sip hh[:mm[:ss]]] [sip_media hh[:mm[:ss]]] [uauth hh[:mm[:ss]]] [absolute | inactivity]
```

```
clear timeout
```

```
show timeout
```

### Syntax Description

<b>absolute</b>	Run <b>uauth</b> timer continuously, but after timer elapses, wait to reprompt the user until the user starts a new connection, such as clicking a link in a web browser. The default <b>uauth</b> timer is <b>absolute</b> . To disable <b>absolute</b> , set the uauth timer to <b>0</b> (zero).
<b>conn</b> hh[:mm[:ss]]	Idle time after which a connection closes. Use <b>0:0:0</b> for the time value to never time out a connection. This duration must be at least 5 minutes. The default is 1 hour.
<b>h225</b> hh[:mm[:ss]]	The idle time after which H.225 signalling closes, where <i>hh</i> is hours, <i>mm</i> is minutes, and <i>ss</i> is seconds. The default is 1 hour. A timeout value of <b>h225 00:00:00</b> means never tear down H.225 signalling. A timeout value of <b>h225 00:00:01</b> disables the timer and closes the TCP connection immediately after all calls are cleared.
<b>h323</b> hh[:mm[:ss]]	The idle time after which an H.323 media connection closes. The default is 5 minutes. (This is the H.323 UDP inactivity timer.)
<b>half-closed</b> hh[:mm[:ss]]	Idle time until a TCP half-close connection is freed. The default is 10 minutes. Use <b>0:0:0</b> to never time out a half-closed connection. The minimum is 5 minutes.
<b>inactivity</b>	Start <b>uauth</b> timer after a connection becomes idle.
<b>mgcp</b> hh[:mm[:ss]]	Sets the duration for the Media Gateway Control Protocol (MGCP) inactivity timer. The default is 5 minutes.
<b>rpc</b> hh[:mm[:ss]]	Idle time until an RPC slot is freed. This duration must be at least 1 minute. The default is 10 minutes.
<b>sip</b> hh[:mm[:ss]]	Modifies the SIP timer which is used for UDP signalling connections identified by the value T in the output from the <b>show conn detail</b> command. The default timeout value is 30 minutes.
<b>sip_media</b> hh[:mm[:ss]]	Modifies the media timer, which is used for SIP RTP/RTCP with SIP UDP media packets, instead of the UDP inactivity timeout. SIP media port is set to 2 minutes in the list of protocol timers.

<b>uauth</b> <i>hh[:mm[:ss]]</i>	Duration before authentication and authorization cache times out and user has to re authenticate next connection. This duration must be shorter than the <b>xlate</b> values. Set to <b>0</b> to disable caching. Do not set to zero if passive FTP is used on the connections.
	
<b>Note</b>	All traffic will reset the timer. This includes non-http traffic.
<b>udp</b> <i>hh[:mm[:ss]]</i>	Idle time until a UDP slot is freed. This duration must be at least 1 minute. The default is 2 minutes.
<b>xlate</b> <i>hh[:mm[:ss]]</i>	Idle time until a translation slot is freed. This duration must be at least 1 minute. The default is 3 hours.
<b>Note</b>	PIX Firewall clears UDP PAT connections 30 seconds after the connection is closed, regardless of the setting of the <b>timeout xlate</b> command.

**Command Modes**

Configuration mode.

**Usage Guidelines**

The **timeout** command sets the idle time for connection, translation UDP, RPC, and H.323 slots. If the slot has not been used for the idle time specified, the resource is returned to the free pool. TCP connection slots are freed approximately 60 seconds after a normal connection close sequence.

The **clear timeout** command sets the durations to their default values.

This command is used in conjunction with the **show** and **clear uauth** commands.

**Note**

Do not use the **timeout uauth 0:0:0** command if passive FTP is used for the connection, or if the **virtual** command is used for Web authentication.

The connection timer takes precedence over the translation timer, such that the translation timer only works after all connections have timed out.

**timeout mgcp**

The **timeout mgcp** *hh:mm:ss* command sets the duration for the MGCP inactivity timer. If this time elapses before new activity occurs, the MGCP media ports close. The default is five minutes. For example, to set the MGCP timeout to five minutes, enter the following:

```
pixfirewall(config)# timeout mgcp 00:05:00
```

**Uauth Inactivity and Absolute Qualifiers**

The **uauth inactivity** and **absolute** qualifiers cause users to have to reauthenticate after either a period of inactivity or an absolute duration.

If you set the inactivity timer to a duration, but the absolute timer to zero, then users are only reauthenticated after the inactivity timer elapses. If you set both timers to zero, then users have to reauthenticate on every new connection.

The inactivity timer starts after a connection becomes idle. If a user establishes a new connection before the duration of the inactivity timer, the user is not required to reauthenticate. If a user establishes a new connection after the inactivity timer expires, the user must reauthenticate. The default durations are zero for the inactivity timer and 5 minutes for the absolute timer; that is, the default behavior is to cause the user to reauthenticate every 5 minutes.

The absolute timer runs continuously, but waits to reprompt the user when the user starts a new connection, such as clicking a link and the absolute timer has elapsed, then the user is prompted to reauthenticate. The absolute timer must be shorter than the **xlite** timer; otherwise, a user could be reprompted after their session already ended.

Inactivity timers give users the best Web access because they are not prompted to regularly reauthenticate. Absolute timers provide security and manage the PIX Firewall connections better. By being prompted to reauthenticate regularly, users manage their use of the resources more efficiently. Also by being reprompted, you minimize the risk that someone will attempt to use another user's access after they leave their workstation, such as in a college computer lab. You may want to set an absolute timer during peak hours and an inactivity timer thereafter.

Both an inactivity timer and an absolute timer can operate at the same time, but you should set the absolute timer duration longer than the inactivity timer. If the absolute timer is less than the inactivity timer, the inactivity timer never occurs. For example, if you set the absolute timer to 10 minutes and the inactivity timer to an hour, the absolute timer reprompts the user every 10 minutes; therefore, the inactivity timer will never be started.

**Note**


---

RPC and NFS are very insecure protocols and should be used with caution.

---

**Examples**

The following is sample output from the **show timeout** command:

```
show timeout
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
```

The following is sample output from the **timeout** command in which variables are changed and then displayed with the **show timeout** command:

```
timeout uauth 0:5:00 absolute uauth 0:4:00 inactivity
show timeout
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute uauth 0:04:00 inactivity
```

**Related Commands**

- [show xlate/clear xlate](#)
- [show uauth/clear uauth](#)



# url-block

For Websense filtering servers, the **url-block url-size** command allows filtering of long URLs, up to 4 KB. For both Websense and N2H2 filtering servers, the **url-block block** command causes the PIX Firewall to buffer packets received from a web server in response to a web client request while waiting for a response from the URL filtering server. This improves performance for the web client compared to the default PIX Firewall behavior, which is to drop the packets and to require the web server to retransmit the packets if the connection is permitted.

If you use the **url-block block** command and the filtering server permits the connection, the PIX Firewall sends the blocks to the web client from the HTTP response buffer and removes the blocks from the buffer. If the filtering server denies the connection, the PIX Firewall sends a deny message to the web client and removes the blocks from the HTTP response buffer.

[no] **url-block block** *block\_buffer\_limit*

**clear url-block block stat**

**show url-block block stat**

## Websense only:

[no] **url-block url-mempool** *memory\_pool\_size*

[no] **url-block url-size** *long\_url\_size*

## Syntax Description

<b>block</b> <i>block_buffer_limit</i>	Creates an HTTP response buffer to store web server responses while waiting for a filtering decision from the filtering server. The permitted values are from 0 to 128, which specifies the number of 1550-byte blocks.
<b>stat</b>	Displays block buffer usage statistics.
<b>url-mempool</b> <i>memory_pool_size</i>	For Websense URL filtering only. The size of the URL buffer memory pool in Kilobytes (KB). The permitted values are from 2 to 10240, which specifies a URL buffer memory pool from 2 KB to 10240 KB.
<b>url-size</b> <i>long_url_size</i>	For Websense URL filtering only. The maximum allowed URL size in KB. The permitted values are 2, 3, or 4, which specifies a maximum URL size of 2 KB, 3 KB, or 4KB.

## Command Modes

Configuration mode.

## Usage Guidelines

Use the **url-block block** command to specify the number of blocks to use for buffering web server responses while waiting for a filtering decision from the filtering server.

Use the **url-block url-size** command with the **url-block url-mempool** command to specify the maximum length of a URL to be filtered by a Websense filtering server and the maximum memory to assign to the URL buffer. Use these commands to pass URLs longer than 1159 bytes, up to a maximum of 4096 bytes, to the Websense server. The **url-block url-size** command stores URLs longer than 1159 bytes in a buffer and then passes the URL to the Websense server (through a TCP packet stream) so that the Websense server can grant or deny access to that URL.

The **clear url-block block stat** command clears the block buffer usage counters, except for the **Current number of packets held (global) counter**.

The **show url-block block stat** command displays the number of packets held in the url-block buffer and the number (if any) dropped due to exceeding the buffer limit or retransmission.

### Examples

The following example illustrates the use of the **show url-block block stat** and **clear url-block block stat** commands:

```
pixfirewall(config)# sh url-block block stat

URL Pending Packet Buffer Stats with max block 128
-----
Cumulative number of packets held:          896
Maximum number of packets held (per URL):    3
Current number of packets held (global):     38
Packets dropped due to
    exceeding url-block buffer limit:        7546
    HTTP server retransmission:              10
Number of packets released back to client:    0

pixfirewall(config)# sh url-block
url-block url-mempool 128
url-block url-size 4
url-block block 128

pixfirewall(config)# clear url-block block stat
pixdocipsecl(config)# show url-block block stat

URL Pending Packet Buffer Stats with max block 0
-----
Cumulative number of packets held:          0
Maximum number of packets held (per URL):    0
Current number of packets held (global):     38
Packets dropped due to
    exceeding url-block buffer limit:        0
    HTTP server retransmission:              0
Number of packets released back to client:    0
```

## url-cache

Caches URL access privileges that were previously retrieved from a Websense or N2H2 server.

**[no] url-cache {dst | src\_dst} size *kbytes***

**clear url-cache**

**show url-cache stats**

### Syntax Description

<b>dst</b>	Cache entries based on the URL destination address. Select this mode if all users share the same URL filtering policy on the N2H2 or Websense server.
<b>size <i>kbytes</i></b>	Specifies a value for the cache size within the range 1 to 128 KB.

<b>src_dst</b>	Cache entries based on the both the source address initiating the URL request as well as the URL destination address. Select this mode if users do not share the same URL filtering policy on the N2H2 or Websense server.
<b>stat</b>	Use the <b>stat</b> option to display additional URL cache statistics, including the number of cache lookups and hit rate.

### Command Modes

Configuration mode.

### Usage Guidelines

The **url-cache** command provides a configuration option to allow the PIX to cache previously retrieved URL access privileges from a Websense or N2H2 server.

Use the **url-cache** command to enable URL caching, set the size of the cache, and display cache statistics.

Caching stores URL access privileges in memory on the PIX Firewall. When a host requests a connection, the PIX Firewall first looks in the URL cache for matching access privileges instead of forwarding the request to the N2H2 or Websense server. Disable caching with the **no url-cache** command.

The **clear url-cache** command removes **url-cache** command statements from the configuration.

Using the URL cache does not update the Websense accounting logs for Websense protocol Version 1. If you are using Websense protocol Version 1, let Websense run to accumulate logs so you can view the Websense accounting information. After you get a usage profile that meets your security needs, enable **url-cache** to increase throughput. Accounting logs are updated for Websense protocol Version 4 and for N2H2 URL filtering while using the **url-cache** command.



#### Note

If you change settings on the N2H2 or Websense server, disable the cache with the **no url-cache** command and then reenable the cache with the **url-cache** command.

The **show url-cache** command with the **stats** option displays the following entries:

- Size—The size of the cache in kilobytes, set with the **url-cache size** option.
- Entries—The maximum number of cache entries based on the cache size.
- In Use—The current number of entries in the cache.
- Lookups—The number of times the PIX Firewall has looked for a cache entry.
- Hits—The number of times the PIX Firewall has found an entry in the cache.

You can view additional information about N2H2 or Websense filtering activity with the **show perfmon** command.

### Examples

The following example caches all outbound HTTP connections based on the source and destination addresses:

```
url-cache src_dst 128
```

The following is sample output from the **show url-cache stat** command:

```
show url-cache stat
```

```
URL Filter Cache Stats
```

```

-----
Size :      1KB
Entries :    36
In Use :     30
Lookups :   300
Hits :      290

```

## url-server

Designate a server running either N2H2 or Websense for use with the **filter** command; you cannot run both of these URL filtering services simultaneously.

### N2H2

**[no] url-server** [(if\_name)] **vendor n2h2** **host** local\_ip [port number] [timeout seconds] [protocol {TCP | UDP}]

### Websense

**[no] url-server** [(if\_name)] **vendor websense** **host** local\_ip [timeout seconds] [protocol {TCP | UDP} version]

**show url-server**

**show url-server stats**

### Syntax Description

#### N2H2

<b>host</b> local_ip	The server that runs the URL filtering application.
<i>if_name</i>	The network interface where the authentication server resides. If not specified, the default is inside.
<b>port</b> number	The N2H2 server port. The PIX Firewall also listens for UDP replies on this port. The default port number is 4005.
<b>protocol</b>	The protocol can be configured using <b>TCP</b> or <b>UDP</b> keywords. The default is TCP.
<b>timeout</b> seconds	The maximum idle time permitted before PIX Firewall switches to the next server you specified. The default is 5 seconds.
<b>vendor n2h2</b>	Indicates URL filtering service vendor is N2H2.

#### Websense

<i>if_name</i>	The network interface where the authentication server resides. If not specified, the default is inside.
<b>host</b> local_ip	The server that runs the URL filtering application.
<b>timeout</b> seconds	The maximum idle time permitted before PIX Firewall switches to the next server you specified. The default is 5 seconds.
<b>protocol</b>	The protocol can be configured using <b>TCP</b> or <b>UDP</b> keywords. The default is TCP protocol, Version 1.

<b>vendor</b> <b>websense</b>	Indicates URL filtering service vendor is Websense.
<b>version</b>	Specifies protocol Version <b>1</b> or <b>4</b> . The default is TCP protocol Version 1. TCP can be configured using Version 1 or Version 4. UDP can be configured using Version 4 only.

**Command Modes**

Configuration mode.

**Usage Guidelines**

The **url-server** command designates the server running the N2H2 or Websense URL filtering application. The limit is 16 URL servers; however, and you can use only one application at a time, either N2H2 or Websense. Additionally, changing your configuration on the PIX Firewall does not update the configuration on the application server; this must be done separately, according to the individual vendor's instructions.

Once you designate the server, enable the URL filtering service with the **filter** command.

Follow these steps to filter URLs:

- 
- Step 1** Designate the URL filtering application server with the appropriate form of the vendor-specific **url-server** command.
  - Step 2** Enable URL filtering with the **filter** command.
  - Step 3** (Optional) Use the **url-cache** command to enable URL caching to improve perceived response time.
  - Step 4** (Optional) Enable long URL and HTTP buffering support using the **url-block** commands.
  - Step 5** Use the **show url-block block stats**, **show url-cache stats**, **show url-server stats**, and the **show pdm** commands to view run information.

For more information about Filtering by N2H2, visit N2H2's website at:

<http://www.n2h2.com>

For more information on Websense filtering services, visit the following website:

<http://www.websense.com/>

---

The **url-server** command must be configured before issuing the **filter** command for HTTPS and FTP. If all URL servers are removed from the server list, then all **filter** commands related to URL filtering are also removed.

**show url-server commands**

The **show url-server stats** command displays the URL server vendor; number of URLs total, allowed, and denied; number of HTTPS connections total, allowed, and denied; number of TCP connections total, allowed, and denied; and the URL server status.

The **show url-server** command displays the following information:

- For N2H2, **url-server (if\_name) vendor n2h2 host local\_ip port number timeout seconds protocol [{TCP | UDP}] {version 1 | 4}**
- For Websense, **url-server (if\_name) vendor websense host local\_ip timeout seconds protocol [{TCP | UDP}]**

**Examples**

Using N2H2, the following example filters all outbound HTTP connections except those from the 10.0.2.54 host:

```
url-server (perimeter) vendor n2h2 host 10.0.1.1
filter url http 0 0 0 0
filter url except 10.0.2.54 255.255.255.255 0 0
```

Using Websense, the following example filters all outbound HTTP connections except those from the 10.0.2.54 host:

```
url-server (perimeter) vendor websense host 10.0.1.1
filter url http 0 0 0 0
filter url except 10.0.2.54 255.255.255.255 0 0
```

The following is sample output from the **show url-server stats** command:

```
pixfirewall# show url-server stats

URL Server Statistics:
-----
Vendor websense
HTTPs total/allowed/denied 0/0/0
HTTPSS total/allowed/denied 0/0/0
FTPs total/allowed/denied 0/0/0

URL Server Status:
-----
172.23.58.103 UP

URL Packets Send and Recieve Stats:
-----
Message Send Recieve
STATUS_REQUEST 200 200
LOOKUP_REQUEST 10 10
LOG_REQUEST 20 NA
```

**Related Commands**

- [aaa authorization](#)
- [filter](#)
- [show](#)

**username**

Sets the username for the specified privilege level.

**username** *username* {[**nopassword** | **password** *password*] [**encrypted**]} [**privilege level**]

**no username** *username*

**clear username**

**show username** *username*

<b>Syntax Description</b>	<i>username</i> Specifies the name of a specific user in the local PIX Firewall authentication database.
<b>Command Modes</b>	Configuration mode.
<b>Usage Guidelines</b>	<p>The local PIX Firewall user authentication database consists of the users entered with the <b>username</b> command. The PIX Firewall <b>login</b> command uses this database for authentication.</p> <p>The <b>show username <i>username</i></b> command displays users entered in the local PIX Firewall user authentication database.</p>
<b>Related Commands</b>	<ul style="list-style-type: none"> <li><a href="#">login</a></li> <li><a href="#">privilege</a></li> </ul>

## virtual

Access the PIX Firewall virtual server.

**virtual http *ip\_address* [warn]**

**virtual telnet *ip\_address***

<b>Syntax Description</b>	<p><i>ip_address</i> For outbound use, <i>ip_address</i> must be an address routed to the PIX Firewall. Use an RFC 1918 address that is not in use on any interface.</p> <p>For inbound use, <i>ip_address</i> must be an unused global address. An <b>access-list</b> and <b>static</b> command pair must provide access to <i>ip_address</i>, as well as an <b>aaa accounting authentication</b> command statement. See the “<a href="#">Examples</a>” section for more information.</p> <p>For example, if an inside client at 192.168.0.100 has a default gateway set to the inside interface of the PIX Firewall at 192.168.0.1, the <i>ip_address</i> can be any IP address not in use on that segment (such as 10.2.3.4). As another example, if the inside client at 192.168.0.100 has a default gateway other than the PIX Firewall (such as a router at 192.168.0.254), then the <i>ip_address</i> would need to be set to a value that would get statically routed to the PIX Firewall. This might be accomplished by using a value of 10.0.0.1 for the <i>ip_address</i>, then on the client, setting the PIX Firewall at 192.168.0.1 as the route to host 10.0.0.1.</p>
<b>warn</b>	Let <b>virtual http</b> command users know that the command was redirected. This option is only applicable for text-based browsers where the redirect cannot happen automatically.

<b>Command Modes</b>	Configuration mode.
----------------------	---------------------

### Usage Guidelines

The **virtual http** command lets web browsers work correctly with the PIX Firewall **aaa** command. The **aaa** command assumes that the AAA server database is shared with a web server. PIX Firewall automatically provides the AAA server and web server with the same information. The **virtual http** command works with the **aaa** command to authenticate the user, separate the AAA server information from the web client's URL request, and direct the web client to the web server. Use the **show virtual http** command to list commands in the configuration. Use the **no virtual http** command to disable its use.

The **virtual http** command works by redirecting the web browser's initial connection to the *ip\_address*, which resides in the PIX Firewall, authenticating the user, then redirecting the browser back to the URL which the user originally requested. This mechanism comprises the PIX Firewall unit's new virtual server feature. The reason this command is named as it is, is because the **virtual http** command accesses the virtual server for use with HTTP, another name for the Web. This command is especially useful for PIX Firewall interoperability with Microsoft IIS, but is useful for other authentication servers.

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

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

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

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

If you want double authentication through the authentication and web browser, configure the authentication server to not accept anonymous connections.



#### Note

Do not set the **timeout uauth** duration to 0 seconds when using the **virtual** command because this will prevent HTTP connections to the real web server.

For both the **virtual http** and **virtual telnet** commands, if the connection is started on either an outside or perimeter interface, a **static** and **access-list** command pair is required for the fictitious IP address.

The **virtual telnet** command allows the Virtual Telnet server to provide a way to pre-authenticate users who require connections through the PIX Firewall using services or protocols that do not support authentication.

The **virtual telnet** command can be used both to log in and log out of the PIX Firewall. When an unauthenticated user Telnets to the virtual IP address, they are challenged for their username and password, and then authenticated with the TACACS+ or RADIUS server. Once authenticated, they see the message "Authentication Successful" and their authentication credentials are cached in the PIX Firewall for the duration of the *uauth* timeout.

If a user wishes to log out and clear their entry in the PIX Firewall *uauth* cache, the user can again Telnet to the virtual address. The user is prompted for their username and password, the PIX Firewall removes the associated credentials from the *uauth* cache, and the user will receive a "Logout Successful" message.



If inbound users on either the perimeter or outside interfaces need access to the Virtual Telnet server, a **static** and **access-list** command pair must accompany use of the **virtual telnet** command.

The Virtual Telnet server provides a way to pre-authenticate users who require connections through the PIX Firewall using services or protocols that do not support authentication. Users first connect to the Virtual Telnet server IP address, where the user is prompted for a username and password.

## Examples

- **virtual http**—The following example shows the commands required to use the **virtual http** command for an inbound connection:

```
static (inside, outside) 209.165.201.1 209.165.201.1 netmask 255.255.255.255
access-list acl_out permit tcp any host 209.165.201.1 eq 80
access-group acl_out in interface outside
aaa authentication include any inbound 209.165.201.1 255.255.255.255 0 0 tacacs+
virtual http 209.165.201.1
```

This configuration uses an identity static, where both the global IP address and the local address in the static command is the IP address of the virtual server.

The next example is sample output from the **show virtual** command:

```
show virtual http
virtual http 209.165.201.1
```

- **virtual telnet**—After adding the **virtual telnet** command to the configuration and writing the configuration to Flash memory, users wanting to start PPTP sessions through PIX Firewall use Telnet to access the *ip\_address* as shown in the following example:

On the PIX Firewall:

```
virtual telnet 209.165.201.25
static (inside, outside) 209.165.201.25 209.165.201.25 netmask 255.255.255.255
access-list acl_out permit tcp any host 209.165.201.25 eq telnet
access-group acl_out in interface outside
write memory
```

This configuration uses an identity static, where both the global IP address and the local address in the static command is the IP address of the virtual server.

On an inside host:

```
/unix/host%telnet 209.165.201.30
Trying 209.165.201.25...
Connected to 209.165.201.25.
Escape character is '^]'.

username: username

TACACS+ Password: password

Authentication Successful

Connection closed by foreign host.
/unix/host%
```

The *username* and *password* are those for the user on the TACACS+ server.

# vpdn

Configure Virtual Private Dial-up Networking using the L2TP, PPTP, or PPPoE.

```
vpdn group group_name [[accept dialin pptp | l2tp] | request dialout pppoe] | [ppp authentication pap|chap|mschap] | [ppp encryption mppe 40 | 128| auto [required]] | [client configuration address local address_pool_name ] | [client configuration dns dns_ip1 [dns_ip2]] | [client configuration wins wins_ip1 [wins_ip2]] | [client authentication local | aaa auth_aaa_group] | [client accounting acct_aaa_group] | [pptp echo echo_time] | [l2tp tunnel hello hello_time]
```

```
vpdn username name password passwd [store-local]
```

```
vpdn enable if_name
```

```
show vpdn tunnel [l2tp|pptp|pppoe] [id tnl_id | packets | state | summary | transport]
```

```
show vpdn session [l2tp|pptp|pppoe] [id sess_id | packets | state | window]
```

```
show vpdn pppinterface [id dev_id]
```

```
show vpdn group [group_name]
```

```
show vpdn username [user_name]
```

```
clear vpdn [group | interface | tunnel tnl_id | username]
```

## Syntax Description

<b>accept dialin pptp l2tp pptp</b>	Accept a dial-in request using PPTP or L2TP.
<b>all</b>	[ <b>clear</b> command only]—Removes all L2TP or PPTP tunnels from the configuration.
<b>client accounting aaa-server-group</b>	Specifies the AAA server group for accounting. The accounting AAA server group can be different from the AAA server group for user authentication.
<b>client authentication aaa aaa_server_group</b>	Specifies the AAA server group for user authentication.
<b>client authentication local</b>	Authenticate using the local username and password entries you specify in the PIX Firewall configuration.
<b>client configuration address local address_pool_name</b>	Specifies the local address pool used to allocate an IP address to a client. Use the <b>ip local pool</b> command to specify the IP addresses for use by the clients.
<b>client configuration dns dns_server_ip1 [dns_server_ip2]</b>	Specifies up to two DNS server IP addresses. If set, the PIX Firewall sends this information to the Windows client during the IPCP phase of PPP negotiation.
<b>client configuration wins wins_server_ip1 [wins_server_ip2]</b>	Specifies up to two WINS server IP addresses.
<b>enable if_name</b>	Enable the VPDN function on a PIX Firewall interface. Specifies the interface in <i>if_name</i> where L2TP or PPTP traffic is received. Only inbound connections are supported.

<b>group</b>	[ <b>clear</b> command only]—Removes all <b>vpdn group</b> commands from the configuration.
<b>group</b> <i>group_name</i>	Specifies the VPDN group name. The VPDN <i>group_name</i> is an ASCII string to denote a VPDN group. You can make up the name. The maximum length is 63 characters.
<b>id</b>	Identify tunnel or session.
<b>id</b> <i>session_id</i>	Unique session identifier.
<b>id</b> <i>tnl_id</i>	Unique tunnel identifier.
<i>l2tp</i>   <i>pptp</i>   <b>pppoe</b>	Select either <i>l2tp</i> , <i>pptp</i> , or <b>pppoe</b> to display information for only that tunnel type.
<i>l2tp</i> tunnel hello <i>hello_timeout</i>	Specifies L2TP tunnel keep-alive hello timeout value in seconds. Default is 60 seconds if not specified. The value can be between 10 to 300 seconds.
<b>localname</b> <i>username</i>	Assigns a name to the group for PPPoE use. This is also the <i>name</i> in the <b>vpdn username</b> command.
<b>packets</b>	Packet and byte count.
<i>passwd</i>	Specifies the password for the local group used for PPPoE.
<b>password</b>	Specifies local user password.
<b>ppp authentication PAP   CHAP   MSCHAP</b>	Specifies the Point-to-Point Protocol (PPP) authentication protocol. The Windows client dial-up networking settings lets you specify what authentication protocol to use (PAP, CHAP, or MS-CHAP). Whatever you specify on the client must match the setting you use on the PIX Firewall. Password Authentication Protocol (PAP) lets PPP peers authenticate each other. PAP passes the host name or username in clear text. Challenge Handshake Authentication Protocol (CHAP) lets PPP peers prevent unauthorized access through interaction with an access server. MS-CHAP is a Microsoft derivation of CHAP. PIX Firewall supports MS-CHAP Version 1 only (not Version 2.0).  If an authentication protocol is not specified on the host, do not specify the <b>ppp authentication</b> option in your configuration.
<b>ppp encryption mppe 40   128   auto [required]</b>	Specifies the number of session key bits used for MPPE (Microsoft Point-to-Point Encryption) negotiation. The domestic version of the Windows client can support 40- and 128-bit session keys, but international version of the Windows client only supports 40-bit session keys. On the PIX Firewall, use <b>auto</b> to accommodate both. Use <b>required</b> to indicate that MPPE must be negotiated or the connection will be terminated.
<b>pppinterface id</b> <i>intf_id</i>	A PPP virtual interface is created for each PPTP or PPPoE tunnel.
<b>pptp echo</b> <i>echo_timeout</i>	Specifies the PPTP keep-alive echo timeout value in seconds. PIX Firewall terminates a tunnel if an echo reply is not received within the timeout period you specify.
request <b>dialout pppoe</b>	Specifies to allow dialout PPPoE requests.
<b>state</b>	Session state.
<b>store-local</b>	Store in local Flash memory instead of using external configuration.
<b>summary</b>	Tunnel summary information.
<b>transport</b>	Tunnel transport information.
<b>tunnel</b>	[ <b>clear</b> command only]—Removes one or more L2TP or PPTP tunnels from the configuration.

<b>tunnel</b> <i>tnl_id</i>	[ <b>clear</b> command only]—Removes PPTP tunnels from the configuration that match <i>tnl_id</i> . You can view the tunnel IDs with the <b>show vpng tunnel</b> command.
<b>username</b> <i>name</i>	Enter or display local username. However, when used as a <b>clear</b> command option, <b>username</b> removes all <b>vpng username</b> commands from the configuration.
<b>window</b>	Window information.

### Command Modes

Configuration mode.

### Usage Guidelines

Virtual Private Dial-up Networking (VPDN) is used to provide long distance, point-to-point connections between remote dial-in users and a private network. VPDN uses Layer 2 tunnelling technologies (L2TP, PPTP, and PPPOE) to establish dial-up networking connections from the remote user to the private network across a public network.

Point-to-Point Tunneling Protocol (PPTP) is a Layer 2 protocol that tunnels the IP protocol. (For more details on PPTP, see RFC 2637, which describes the PPTP protocol.)

L2TP supports PPP by managing communications transactions. (There is a one-to-one relationship between a PPP connection and L2TP session.)

PPPOE is the Point-to-Point Protocol (PPP) over Ethernet. PPP is designed to work with network layer protocols such as IP, IPX, and ARA. PPP also has CHAP and PAP as built-in security mechanisms.

The **vpng** command implements the L2TP, PPTP, and PPPoE features for the inbound connections. Refer to the *Cisco PIX Firewall and VPN Configuration Guide* for L2TP, PPTP, and PPPOE configuration examples.



#### Note

The PIX Firewall is a PPTP and L2TP Server and a PPPoE client.

The **show vpng tunnel** and **show vpng session** commands display tunnel and session information (respectively) for L2TP (*l2tp*), PPTP (*pptp*), and PPPOE (**pppoe**). If you want to display information for only one protocol, use the option for that protocol. For example, the **show vpng session pppoe** command displays session information for PPPOE sessions only.

The **clear vpng** command removes all **vpng** commands from the configuration and stops all the active PPTP, L2TP, and PPPoE tunnels. The **clear vpng all** command lets you remove all tunnels, and the **clear vpng id tnl\_id** command lets you remove tunnels associated with *tnl\_id*. (You can view the *tnl\_id* with the **show vpng** command.) The **clear vpng group** command removes all the **vpng group** commands from the configuration. The **clear vpng username** command removes all the **vpng username** commands from the configuration.

### PPPoE

Because PPPoE encapsulates PPP, PPPoE relies on PPP to perform authentication and ECP and CCP functions for client sessions operating within the VPN tunnel. Additionally, PPPoE is not supported in conjunction with DHCP because PPP assigns the IP address for PPPoE.

The following are PPPoE restrictions on the PIX Firewall:

- The PIX Firewall acts as a PPPoE client only.
- The PPPoE client is only supported on the outside interface of the PIX Firewall in PIX Firewall software Version 6.2.

**Note**

Unless the VPDN group for PPPoE is configured, PPPoE will not be able to establish a connection.

To define a VPDN group to be used for PPPoE, use the **vpdn group** *group\_name* **request dialout pppoe** command.

If your ISP requires authentication, use the **vpdn group** *group\_name* **ppp authentication PAP | CHAP | MSCHAP** command to select the authentication protocol used by your ISP.

Use the **vpdn group** *group\_name* **localname** *username* command to associate the username assigned by your ISP with the VPDN group.

Use the **vpdn username** *username* **password** *pass* command to create a username and password pair for the PPPoE connection. The username must be a username that is already associated with the VPDN group specified for PPPoE.

**Note**

If your ISP is using CHAP or MS-CHAP, the username may be called the remote system name and the password may be called the CHAP secret.

The PPPoE client functionality is turned off by default, so after VPDN configuration, enable PPPoE with the **ip address** *if\_name* **pppoe** [**setroute**] command. The **setroute** option causes a default route to be created if no default route exists.

As soon as PPPoE is configured, the PIX Firewall attempts to find a PPPoE access concentrator with which to communicate. When a PPPoE connection is terminated, either normally or abnormally, the PIX Firewall attempts to find a new access concentrator with which to communicate.

The following **ip address** commands should not be used after a PPPoE session is initiated because they will terminate the PPPoE session:

- **ip address outside pppoe**, because it attempts to initiate a new PPPoE session.
- **ip address outside dhcp**, because it disables the interface until the interface gets its DHCP configuration.
- **ip address outside** *address netmask*, because it brings up the interface as a normally initialized interface.

**PPTP**

Use the **vpdn** command with the **sysopt connection permit-pptp** to allow PPTP traffic to bypass checking of **conduit** or **access-list** command statements.

You can troubleshoot PPTP traffic with the **debug ppp** and **debug vpdn** commands.

PPTP is an alternative to IPsec handling for VPN clients or Easy VPN Remote devices. While PPTP is less secure than IPsec, PPTP is easier to implement and maintain. Only inbound PPTP connections are supported and only one PIX Firewall interface can have the **vpdn** command enabled.

Supported authentication protocols include: PAP, CHAP, and MS-CHAP using external AAA (RADIUS or TACACS+) servers or the PIX Firewall local username and password database. Through the PPP IPCP protocol negotiation, PIX Firewall assigns a dynamic internal IP address to the PPTP client allocated from a locally defined IP address pool.

PIX Firewall PPTP VPN supports standard PPP CCP negotiations with Microsoft Point-To-Point Encryption (MPPE) extensions using RSA/RC4 algorithm. MPPE currently supports 40-bit and 128-bit session keys. MPPE generates an initial key during user authentication and refreshes the key regularly. In this release, compression is not supported.

When you specify MPPE, you must use the MS-CHAP PPP authentication protocol. If you are using an external AAA server, the protocol must be RADIUS and the external RADIUS server must be able to return the Microsoft MSCHAP\_MPPE\_KEY attribute to the PIX Firewall in the RADIUS Authentication Accept packet. See RFC 2548, "Microsoft Vendor Specific RADIUS Attributes," for more information on the MSCHAP\_MPPE\_KEY attribute.

Cisco Secure ACS 2.5 and higher versions support the MSCHAP/MPPE encryption.

PIX Firewall PPTP VPN has been tested with the following Microsoft Windows products: Windows 95 with DUN 1.3, Windows 98, Windows NT 4.0 with Service Pack (SP) 6, and Windows 2000.



#### Note

If you configure PIX Firewall for 128-bit encryption and if a Windows 95 or Windows 98 client does not support 128-bit or greater encryption, then the connection to the PIX Firewall is refused. When this occurs, the Windows client moves the dial-up connection menu down to the screen corner while the PPP negotiation is in progress. This gives the appearance that the connection is accepted when it is not. When the PPP negotiation completes, the tunnel terminates and PIX Firewall ends the connection. The Windows client eventually times out and disconnects.

## Examples

The following is a sample PPPoE configuration:

```
vpdn group pppoegroup request dialout pppoe
vpdn group pppoegroup localname myusername
vpdn group pppoegroup ppp authentication pap
vpdn username myusername password mypassword
```

```
ip address outside pppoe setroute
```

The VPDN commands configure a VPDN group for PPPoE, and the **ip address outside pppoe setroute** command enables the PPPoE session.

The following is sample output from the **show vpdn tunnel l2tp** command:

```
pix# show vpdn tunnel l2tp

L2TP Tunnel Information (Total tunnels=1 sessions=1)

Tunnel id 1 is up, remote id is 7, 1 active sessions
Tunnel state is established, time since change 12 secs
Remote Internet Address 172.122.16.8, port 1701
Local Internet Address 172.23.58.48, port 1701
15 packets sent, 48 received, 377 bytes sent, 4368 received
Control Ns 3, Nr 4
Local RWS 16, Remote RWS 8
Retransmission time 1, max 1 seconds
Unsent queuesize 0, max 0
Resend queuesize 0, max 1
Total resends 0, ZLB ACKs 2
Retransmit time distribution: 0 0 0 0 0 0 0 0 0
pix#
```

The following is sample output from the **show vpdn tunnel** command:

```

pix# show vpdn tunnel

L2TP Tunnel Information (Total tunnels=1 sessions=1)

Tunnel id 1 is up, remote id is 7, 1 active sessions
  Tunnel state is established, time since change 12 secs
  Remote Internet Address 172.122.16.8, port 1701
  Local Internet Address 172.23.58.48, port 1701
  15 packets sent, 48 received, 377 bytes sent, 4368 received
  Control Ns 3, Nr 4
  Local RWS 16, Remote RWS 8
  Retransmission time 1, max 1 seconds
  Unsent queue size 0, max 0
  Resend queue size 0, max 1
  Total resends 0, ZLB ACKs 2
  Retransmit time distribution: 0 0 0 0 0 0 0 0 0
% No active PPTP tunnels
pix#

```

The following is sample output from the **show vpdn tunnel packet** command:

```

show vpdn tunnel packet
PPTP Tunnel Information (Total tunnels=1 sessions=1)

LocID   Pkts-In  Pkts-Out  Bytes-In  Bytes-Out
  1      1196      13      113910      420

```

The following is sample output from the **show vpdn tunnel state** command:

```

show vpdn tunnel state
PPTP Tunnel Information (Total tunnels=1 sessions=1)

LocID RemID   State   Time-Since-Event-Chg
  1     1   estab   6 secs

```

The following is sample output from the **show vpdn tunnel summary** command:

```

show vpdn tunnel summary
PPTP Tunnel Information (Total tunnels=1 sessions=1)

LocID RemID   State   Remote Address   Port   Sessions
  1     1   estab   172.16.38.194   1723     1

```

The following is sample output from the **show vpdn tunnel transport** command:

```

show vpdn tunnel transport
PPTP Tunnel Information (Total tunnels=1 sessions=1)

LocID Type Local Address   Port Remote Address   Port
  1   IP   172.16.1.209   1723 172.16.38.194   1723

```

The following is sample output from the **show vpdn session** command:

```

pix# show vpdn session
L2TP Session Information (Total tunnels=1 sessions=1)

Call id 1 is up on tunnel id 1
Remote tunnel name is abc-win2ke2
  Internet Address is 172.122.16.8
  Session username is guest, state is established
  Time since change 158 secs, interface outside
  Remote call id is 1
  PPP interface id is 1
  15 packets sent, 83 received, 377 bytes sent, 8412 received
  Sequencing is off

% No active PPTP tunnels

```

The following is sample output of a simple configuration that allows Windows PPTP clients to dial in without any authentication (not recommended). The Windows client can Telnet to internal host 192.168.0.2 through the static global address 209.165.201.2.

```

ip local pool my-addr-pool 10.1.1.1-10.1.1.254
vpdn group 1 accept dialin pptp
vpdn group 1 client configuration address local my-addr-pool
vpdn enable outside
static (inside, outside) 209.165.201.2 192.168.0.2
access-list acl_out permit tcp 10.1.1.0 255.255.255.0 host 209.165.201.2 eq telnet
access-group acl_out in interface outside

```

In the next example, PPTP clients authenticate using MS-CHAP and negotiate MPPE encryption with the PIX Firewall. The PPTP client can Telnet to host 192.168.0.2 through the static global 209.165.201.2. The Telnet session will be encrypted.

```

ip local pool my-addr-pool 10.1.1.1-10.1.1.254
aaa-server my-aaa-server-group (inside) host 192.168.0.10 key 12345678
aaa-server my-aaa-server-group protocol radius
vpdn group 1 accept dialin pptp
vpdn group 1 ppp authentication mschap
vpdn group 1 client authentication aaa my-aaa-server-group
vpdn group 1 ppp encryption mppe auto required
vpdn group 1 client configuration address local my-addr-pool
vpdn enable outside
static (inside, outside) 209.165.201.2 192.168.0.2
access-list acl_out permit tcp 10.1.1.0 255.255.255.0 host 209.165.201.2 eq telnet
access-group acl_out in interface outside

```



In the next example, PPTP clients authenticate using MS-CHAP, negotiate MPPE encryption, receive the DNS and WINS server addresses, and can Telnet to the host 192.168.0.2 directly through the **nat 0** command statement.

```
ip local pool my-addr-pool 10.1.1.1-10.1.1.254
aaa-server my-aaa-server-group (inside) host 192.168.0.10 key 12345678
aaa-server my-aaa-server-group protocol radius
vpdn group 1 accept dialin pptp
vpdn group 1 ppp authentication mschap
vpdn group 1 ppp encryption mppe auto required
vpdn group 1 client configuration address local my-addr-pool
vpdn group 1 client authentication aaa my-aaa-server-group
vpdn group 1 client configuration dns 10.2.2.99
vpdn group 1 client configuration wins 10.2.2.100
vpdn enable outside
access-list nonat permit ip host 192.168.0.2 10.1.1.0 255.255.255.0
access-list nonat permit ip host 10.2.2.99 10.1.1.0 255.255.255.0
access-list nonat permit ip host 10.2.2.100 10.1.1.0 255.255.255.0
nat (inside) 0 access-list nonat
access-list acl_out permit tcp 10.1.1.0 255.255.255.0 host 192.168.0.2 eq telnet
access-list acl_out permit udp 10.1.1.0 255.255.255.0 host 10.2.2.99 eq domain
access-list acl_out permit udp 10.1.1.0 255.255.255.0 host 10.2.2.100 eq netbios-ns
access-group acl_out in interface outside
```

In the next example, PPTP clients authenticate using MS-CHAP, negotiate MPPE encryption, receive the DNS and WINS server addresses, and can Telnet to the host 192.168.0.2 directly through the **nat 0** command statement. An **access-group** command statement is not present because the **sysopt connection permit-pptp** command statement allows all the PPTP traffic through the tunnel.

```
ip local pool my-addr-pool 10.1.1.1-10.1.1.254
aaa-server my-aaa-server-group (inside) host 192.168.0.10 key 12345678
aaa-server my-aaa-server-group protocol radius
vpdn group 1 accept dialin pptp
vpdn group 1 ppp authentication mschap
vpdn group 1 ppp encryption mppe auto required
vpdn group 1 client configuration address local my-addr-pool
vpdn group 1 client authentication aaa my-aaa-server-group
vpdn group 1 client configuration dns 10.2.2.99
vpdn group 1 client configuration wins 10.2.2.100
vpdn enable outside
access-list nonat permit ip host 192.168.0.2 10.1.1.0 255.255.255.0
access-list nonat permit ip host 10.2.2.99 10.1.1.0 255.255.255.0
access-list nonat permit ip host 10.2.2.100 10.1.1.0 255.255.255.0
nat (inside) 0 access-list nonat
sysopt connection permit-pptp
```

In the next example, PPTP clients authenticate using MS-CHAP, negotiate MPPE encryption, receive the DNS and WINS server addresses, and can Telnet to the host 192.168.0.2 directly through the **nat 0** command. The PPTP authenticates using the PIX Firewall local username and password database you create with the **vpdn username** command. Users are reauthenticated again by the **aaa** command when they start a Telnet session. An **access-group** command statement is not present because the **sysopt connection permit-pptp** command statement allows all the PPTP traffic through the tunnel.

```
ip local pool my-addr-pool 10.1.1.1-10.1.1.254
aaa-server my-aaa-server-group (inside) host 192.168.0.10 key 12345678
aaa-server my-aaa-server-group protocol radius
vpdn username usrname1 password password1
vpdn group 1 accept dialin pptp
vpdn group 1 ppp authentication mschap
vpdn group 1 ppp encryption mppe auto required
vpdn group 1 client configuration address local my-addr-pool
vpdn group 1 client authentication local
vpdn group 1 client configuration dns 10.2.2.99
vpdn group 1 client configuration wins 10.2.2.100
vpdn enable outside
access-list nonat permit ip host 192.168.0.2 10.1.1.0 255.255.255.0
access-list nonat permit ip host 10.2.2.99 10.1.1.0 255.255.255.0
access-list nonat permit ip host 10.2.2.100 10.1.1.0 255.255.255.0
nat (inside) 0 access-list nonat
sysopt connection permit-pptp
aaa authentication include telnet inbound 192.168.0.2 255.255.255.255 10.1.1.0
255.255.255.0
```

## vpnclient

Configures Easy VPN Remote.

**vpnclient vpngroup** *group\_name* **password** *presared\_key*

**vpnclient username** *xauth\_username* **password** *xauth\_password*

**vpnclient server** *ip\_primary* [*ip\_secondary\_1 ip\_secondary\_2 ... ip\_secondary\_10*]

**vpnclient mac-exempt** *mac\_addr\_1 mac\_mask\_1* [*mac\_addr\_2 mac\_mask\_2*]

**vpnclient mode** *client-mode* | *network-extension-mode*

**vpnclient management** [{**tunnel** {*ip\_addr\_1 ip\_mask\_1*} [{*ip\_addr\_2 ip\_mask\_1*}...]} | [**clear**}]

**no vpnclient management**

[**no**] **vpnclient connect**

**vpnclient disconnect**

[**no**] **vpnclient nem-st-autoconnect**

**vpnclient enable**

**no vpnclient** {*server* | *mode* | *vpngroup* | *username* | *mac-exempt* | *management* | *enable*}

**clear vpnclient**

**show vpnclient [detail]**

Syntax	Description
<i>group_name</i>	The name of the VPN group configured on the VPN headend. The maximum length is 63 characters and no spaces are permitted.
<i>ip_addr_1, ip_addr_2, ...</i>	The IP address of the remote network managing the client through the VPN tunnel.
<i>ip_mask_1, ip_mask_2, ...</i>	The IP mask of the remote network managing the client through the VPN tunnel.
<i>ip_primary</i>	The IP address of the primary Cisco Easy VPN Server.
<i>ip_secondary_1, ip_secondary_2, ... , ip_secondary_10</i>	The IP address of a secondary Cisco Easy VPN Server. There can be from 1 to 10 secondary Cisco Easy VPN Servers (backup VPN headends) configured. However, check your platform-specific documentation for applicable peer limits on your PIX Firewall platform.
<i>mac_addr_n</i>	The MAC address for user authentication exemption.
<i>mac_mask_n</i>	The MAC mask for user authentication exemption.
<b>management clear</b>	Specifies to use clear network traffic for management access to an Easy VPN Remote device.
<b>management tunnel</b> { <i>ip_addr_1 ip_mask_1</i> } [ { <i>ip_addr_2 ip_mask_2</i> } ... ]	Specifies to use a VPN tunnel for management access to an Easy VPN Remote device.
<b>nem-st-autoconnect</b>	Specifies to automatically initiate IPSec data tunnels when split tunneling is configured. Note that IPSec data tunnels are automatically initiated and sustained when in network extension mode, except when split tunneling is configured.
<b>password</b>	Specifies to set the password.
<i>preshared_key</i>	The IKE pre-shared key used for authentication by the Easy VPN Server. The maximum length is 127 characters.
<i>xauth_password</i>	The user password to be used for XAUTH. The maximum length is 127 characters.
<i>xauth_username</i>	The username to be used for XAUTH. The maximum length is 127 characters.

**Defaults** Easy VPN management is through the network by default.

**Command Modes** Configuration mode.

**Usage Guidelines** The **vpnclient** command stores non-transitory Easy VPN Remote device configuration information in the Flash memory of the PIX Firewall so that it is preserved whether or not the PIX Firewall reboots.

**Note**

The PIX 501 and PIX 506/506E are both Easy VPN Remote and Easy VPN Server devices. The PIX 515/515E, PIX 525, and PIX 535 act as Easy VPN Servers only.

The PIX 501 and PIX 506/506E can act as Easy VPN Remote devices or Easy VPN Servers so that they can be used either as a client device or VPN headend in a remote office installation. The PIX 515/515E, PIX 525, and PIX 535 act as Easy VPN Servers only because the capacity of these devices makes them appropriate VPN headends for higher traffic environments.

Easy VPN management is through clear network traffic by default (**vpnclient management clear**). However, if Easy VPN management through a VPN tunnel is desired, use the **vpnclient management tunnel** {ip\_addr\_1 ip\_mask\_1} [{ip\_addr\_2 ip\_mask\_1}...] command.

You must specify all variables for the **vpnclient** configuration prior to enabling a Easy VPN Remote connection, except for the *xauth\_username* and *xauth\_password*. Also, you must configure NAT, IKE (using the **isakmp** and **isakmp policy** commands), the **crypto ipsec** transform set, **crypto map**, and an access control list (to trigger building the VPN tunnel) to enable Easy VPN Remote.

The **no vpnclient enable** command closes all established VPN tunnels and prevents new VPN tunnels from initiating until you enter a **vpnclient enable** command. The **no vpnclient connect** and **vpnclient disconnect** commands disconnect the existing VPN sessions but do not prevent new VPN tunnels from initiating.

The **clear vpnclient** command clears the Easy VPN Remote configuration and security policy stored in Flash memory.

The **show vpnclient [detail]** command displays VPN client or Easy VPN Remote device configuration information. The **show vpnclient [detail]** option displays dynamically generated configuration information.

**vpnclient server**

The **vpnclient server** ip\_primary ip\_secondary\_1[ip\_secondary\_2 ... ip\_secondary\_10] command enables you to create a backup VPN server list on the VPN client.

If a backup server list is already configured locally on the VPN client, then it ignores any backup server configuration downloaded from the VPN headend.

If the VPN client has already downloaded a backup server configuration from the VPN headend and saved it to Flash memory, then you cannot configure a new backup server list locally until the headend deletes the downloaded list or you enter a **clear vpnclient** command on the VPN client.

**Examples**

The following is an example Easy VPN Remote configuration:

```
vpnclient vpngroup group_a password pre_share_a
vpnclient username user_1 password pass_1
vpnclient server 1.1.1.1
vpnclient mode client-mode
```

The following example sets up management access to an Easy VPN Remote device through a VPN tunnel:

```
vpnclient management tunnel 10.0.0.0 255.255.255.0
```

The following example sets up management access to an Easy VPN Remote device through clear network traffic:

```
vpnclient management clear
```

# vpngroup

Supports Cisco VPN Client Version 3.x (Cisco Unified VPN Client Framework) and Easy VPN Remote devices.

```

vpngroup group_name address-pool pool_name

vpngroup group_name authentication-server server_tag

vpngroup group_name backup-server {{ ip1 [ip2 ... ip10]} | clear-client-cfg}

vpngroup group_name default-domain domain_name

vpngroup group_name device-pass-through

vpngroup group_name dns-server dns_ip_prim [dns_ip_sec]

vpngroup group_name idle-time idle_seconds

vpngroup group_name max-time max_seconds

vpngroup group_name password preshared_key

vpngroup group_name pfs

vpngroup group_name secure-unit-authentication

vpngroup group_name split-dns domain_name1 [domain_name2 ... domain_8]

vpngroup group_name split-tunnel access_list

vpngroup group_name user-authentication

vpngroup group_name user-idle-timeout user_idle_seconds

vpngroup group_name wins-server wins_ip_prim [wins_ip_sec]

show vpngroup [group_name]

```

Syntax	Description
<i>access_list</i>	The name of the access list for the split-tunnel configuration.
<b>authentication-server</b> <i>server_tag</i>	Specifies the IUA AAA server on the firewall headend.
<b>backup-server</b>	Configures a backup server list to be used for access by VPN clients if the primary server is not available.
<b>clear-client-cfg</b>	Clears backup servers from the client configuration.
<b>device-pass-through</b>	Specifies to exempt devices based on their MAC address from authentication. This may be used for devices such as Cisco IP Phones that cannot use IUA for authentication. Use with the <b>vpnclient mac-exempt</b> command.
<i>dns_ip_prim</i>	The IP address of the primary DNS server.
<i>dns_ip_sec</i>	The IP address of the secondary DNS server.
<i>domain_name</i>	The default domain name, up to 127 characters.

<i>domain_name1</i> [ <i>domain_name2</i> , <i>domain_name3</i> , ... , <i>domain_name8</i> ]	The domains to configure for split DNS. The maximum length for a domain name is 127 characters.
<i>group_name</i>	Specifies the VPN policy group name and is an ASCII string with a maximum length of 63 characters. (You choose the name.)
<i>idle_seconds</i>	The idle timeout in seconds, from 60 to 86400. The default is 1800 seconds (30 minutes).
<i>max_seconds</i>	The maximum connection time in seconds that the VPN group is allowed, from 60 to 31536000. The default maximum connection time is set to unlimited.
<b>pfs</b>	Specifies to require that the VPN client or Easy VPN Remote device to perform PFS.
<i>pool_name</i>	The IP address pool name, up to 63 characters.
<i>preshared_key</i>	The VPN group pre-shared key. The maximum is 127 characters.
<i>server_tag</i>	AAA server tag to authenticate remote users of a hardware client.
split-dns	Specifies to use split DNS.
<i>user_idle_seconds</i>	Idle timeout for user authentication, in seconds.
<b>vpngroup</b>	Identifies the VPN dial-up group. The maximum identifier length is 63 characters.
<i>wins_ip_prim</i>	The IP address of the primary WINS server.
<i>wins_ip_sec</i>	The IP address of the secondary WINS server.

**Command Modes**

Configuration mode.

**Usage Guidelines**

Be sure to configure the IKE Mode Config prior to configuring support for the Cisco VPN 3000 Client. In configuring IKE Mode Config, specify that the PIX Firewall initiates the IKE Mode Config.

For additional information about configuring interoperability with the Cisco VPN 3000 Client using the **vpngroup** commands, see the *Cisco PIX Firewall and VPN Configuration Guide*.

The Cisco VPN 3000 Client supports Windows 2000.

The **vpngroup** command set lets you configure Cisco VPN 3000 Client policy attributes to be associated with a VPN group name and downloaded to the Cisco VPN 3000 Client(s) that are part of the given group. The same VPN group name is configured in the Cisco VPN 3000 Client to ensure the matching of VPN client or Easy VPN Remote policy.

Configure a VPN group name of “default” to create a VPN group policy that matches any group name. The PIX Firewall selects the VPN group name “default,” if there is no other policy match.

The **vpngroup address-pool** command lets you define a pool of local addresses to be assigned to a VPN group.

**Note**

Both the **vpngroup address-pool** command and the **ip local pool** command enable you to specify a pool of local addresses to be used for assigning dynamic IP addresses to VPN clients and Easy VPN Remote devices. In the case of the Cisco VPN 3000 Client, the specified pool of addresses is associated with a given group, which consists of Cisco VPN 3000 Client users. We recommend using the **vpngroup address-pool** command only if you will configure more than one pool of addresses to be used by more than one VPN user group. The **vpngroup address-pool** command gives the PIX Firewall added flexibility to configure different pools of local addresses for different user groups.

Individual User Authentication (IUA) is a centrally managed feature that cannot be configured locally, but it must be enabled locally. The **vpngroup group\_name user-authentication** command enables IUA on the firewall.

The **vpngroup group\_name secure-unit-authentication** command enables Secure Unit Authentication (SUA) for the vpngroup. SUA is a centrally managed feature and cannot be directly configured on Easy VPN Remote devices. If SUA is enabled, a downloaded VPN policy activates SUA on the Easy VPN Remote device. SUA can be disabled by a corresponding VPN policy. SUA status reverts to UNSPECIFIED if a **clear vpnclient** command is entered on the firewall.

The **vpngroup group\_name user-idle-timeout user\_idle\_seconds** command sets the IUA idle timeout.

The **vpngroup dns-server** command enables the PIX Firewall to download an IP address of a DNS server to a Cisco VPN 3000 Client as part of an IKE negotiation.

The **vpngroup wins-server** command lets the PIX Firewall download an IP address of a WINS server to a Cisco VPN 3000 Client as part of an IKE negotiation.

To enable the PIX Firewall to download a default domain name to a Cisco VPN 3000 Client as part of IKE negotiation, use the **vpngroup default-domain** command.

Use the **vpngroup split-tunnel** command to enable split tunneling on the PIX Firewall. Split tunneling allows a remote VPN client or Easy VPN Remote device simultaneous encrypted access to the corporate network and clear access to the Internet. Using the **vpngroup split-tunnel** command, specify the access list name to which to associate the split tunnelling of traffic. With split tunnelling enabled, the PIX Firewall downloads its local network IP address and netmask specified within the associated access list to the VPN client or Easy VPN Remote device as part of the policy push to the client. In turn, the VPN client or Easy VPN Remote device sends the traffic destined to the specified local PIX Firewall network via an IPSec tunnel and all other traffic in the clear. The PIX Firewall receives the IPSec-protected packet on its outside interface, decrypts it, and then sends it to its specified local network.

If you do not enable split tunneling, all traffic between the VPN client or Easy VPN Remote device and the PIX Firewall is sent through an IPSec tunnel. All traffic originating from the VPN client or Easy VPN Remote device is sent to the PIX Firewall's outside interface through a tunnel, and the client's access to the Internet from its remote site is denied.

Regardless of whether split tunneling is enabled, VPN clients and Easy VPN Remote devices negotiate an IPSec tunnel to the PIX Firewall unit's IP address with a netmask of 255.255.255.255.

Networks defined in **access-list deny** command statements are not pushed to VPN clients or Easy VPN Remote devices.

The **vpngroup idle-time** command sets the inactivity timeout for a Cisco VPN 3000 Client. When the inactivity timeout for all IPSec SAs have expired for a given VPN client or Easy VPN Remote device, the tunnel is terminated. The default inactivity timeout is 30 minutes.

The **vpngroup max-time** command sets the maximum connection time for a Cisco VPN 3000 Client. When the maximum connection time is reached for a given VPN client or Easy VPN Remote device, the tunnel is terminated. This means the connection between the Cisco VPN 3000 Client and the PIX Firewall will have to be reestablished. The default maximum connection time is set to an unlimited amount of time.

**Note**

The inactivity timeout specified with the **vpngroup idle-time** command and maximum connection time specified with the **vpngroup max-time** command for a given Cisco VPN 3000 Client take precedence over the commands used to set global lifetime timeouts. These commands are the **isakmp policy lifetime** and **crypto map set security-association lifetime seconds** commands.

Configure the VPN group's pre-shared key employing the **vpngroup password** command to be used during IKE authentication. This pre-shared key is equivalent to the password that you enter within the **Group Password** box of the Cisco VPN 3000 Client while configuring your group access information for a connection entry.

The PIX Firewall configured password displays in asterisks within the file configuration.

**Note**

Both the **vpngroup password** command and the **isakmp key address** command let you specify a pre-shared key to be used for IKE authentication. We recommend that you use the **vpngroup password** command only if you plan to configure more than one VPN user group. The **vpngroup password** command gives the PIX Firewall added flexibility to configure different VPN user groups.

**Examples**

The following example show use of the **vpngroup** commands. The VPN client(s) or Easy VPN Remote device(s) within the VPN group named as "myVpnGroup" will be dynamically assigned one of the IP addresses from the pool of addresses ranging from 10.140.40.0 to 10.140.40.7. The policy attributes for the group "myVpnGroup" will be downloaded to the given VPN client or Easy VPN Remote device during the policy push to the client. Split tunnelling is enabled. In the example, all traffic destined for the 10.130.38.0 255.255.255.0 PIX Firewall network from the VPN client or Easy VPN Remote device will be IPSec protected.

```
access-list 90 permit ip 10.130.38.0 255.255.255.0 10.140.40.0 255.255.255.248
```

```
ip local pool vpnpool 10.140.40.1-10.140.40.7
```

```
crypto ipsec transform-set esp-sha esp-null esp-sha-hmac
crypto dynamic-map dynmap 50 set transform-set esp-sha
crypto map mapName 10 ipsec-isakmp dynamic dynmap
crypto map mapName client configuration address initiate
crypto map mapName interface outside
```

```
isakmp enable outside
isakmp identity hostname
isakmp policy 7 authentication pre-share
isakmp policy 7 encryption 3des
isakmp policy 7 hash md5
isakmp policy 7 group 1
```

```
vpngroup myVpnGroup address-pool vpnpool
vpngroup myVpnGroup dns-server 10.131.31.11
vpngroup myVpnGroup wins-server 10.131.31.11
vpngroup myVpnGroup default-domain example.com
vpngroup myVpnGroup split-tunnel 90
vpngroup myVpnGroup idle-time 1800
```



```
vpngroup myVpnGroup max-time 86400
vpngroup myVpnGroup password *****
```

## who

Show active Telnet administration sessions on the PIX Firewall.

**who** [*local\_ip*]

**show who** [*local\_ip*]

### Syntax Description

<i>local_ip</i>	An optional internal IP address to limit the listing to one IP address or to a network IP address.
-----------------	--

### Command Modes

Unprivileged mode.

### Usage Guidelines

The **who** command shows the PIX Firewall TTY\_ID and IP address of each Telnet client currently logged into the PIX Firewall. This command is the same as the **show who** command.

### Examples

The following example shows how to display the current Telnet sessions:

```
pixfirewall# who
0: From 192.168.1.3
1: From 192.168.2.2
```

### Related Commands

- [kill](#)
- [telnet](#)

## write

Store, view, or erase the current configuration.

**write net** [[*server\_ip*]:*filename*]

**write erase**

**write floppy**

**write memory | floppy** [*uncompressed*]

**write standby**

**write terminal**

**Note**

The PIX 506/506E does not support use of the **write standby** command. Also, the PIX 506/506E, PIX 515/515E, and the PIX 525 do not support use of the **write floppy** command.

**Syntax Description**

<b>erase</b>	Clear the Flash memory configuration.
<i>filename</i>	A filename you specify to qualify the location of the configuration file on the TFTP server named in <i>server_ip</i> . If you set a filename with the <b>tftp-server</b> command, do not specify it in the <b>write</b> command; instead just use a colon (:) without a filename.  Many TFTP servers require the configuration file to be world-writable to write to it.
<b>floppy</b>	Stores the current configuration on diskette.
<b>memory</b>	Stores the current configuration in Flash memory, along with the activation key value and timestamp for when the configuration was last modified.
<i>server_ip</i>	Specifies the IP address of the TFTP server. If you specify the full path and filename in the <b>tftp-server</b> command, then use a ":" in the <b>write</b> command.
<b>standby</b>	Stores the configuration to the failover standby unit from RAM-to-RAM.
<b>terminal</b>	Display current configuration on the terminal.
<b>uncompressed</b>	Writes the configuration to memory without storing it in compressed format.

**Command Modes**

Privileged mode.

**Usage Guidelines**

The **write net** command stores the current configuration into a file on a TFTP server elsewhere in the network. Additionally, the **write net** command uses the TFTP server IP address specified in the **tftp-server** command. If you specify both the IP address and path name in the **tftp-server** command, you can specify the **write net :filename** command as simply a colon (:) as follows:

```
write net :
```

Use the **configure net** command to get the configuration from the file.

The **write erase** command clears the Flash memory configuration.

The **write floppy** command stores the current configuration on diskette. The diskette must be DOS formatted or a PIX Firewall boot disk. If you are formatting the diskette from Windows, choose the Full format type, not the Quick (erase) selection. You can tell that information is stored on the diskette by observing that the light next to the diskette drive glows while information transfers.

The diskette you create can only be read or written by the PIX Firewall. If you use the **write floppy** command with a diskette that is not a PIX Firewall boot disk, do not leave the floppy in the floppy drive because it will prevent the firewall from rebooting in the event of a power failure or system reload. Only one copy of the configuration can be stored on a single diskette.

The **write memory** command saves the current running configuration to Flash memory. Use the **configure memory** command to merge the current configuration with the image you saved in Flash memory.

PIX Firewall lets processing continue during the **write memory** command.

If another PIX Firewall console user tries to change the configuration while you are executing the **write memory** command, the user receives the following messages:

```
Another session is busy writing configuration to memory
Please wait a moment for it to finish
```

After the **write memory** command completes, PIX Firewall lets the other command complete.

**Note**

Only use the **write memory** command if a configuration has been created with IP addresses for both network interfaces.

The **write standby** command writes the configuration stored in RAM on the active failover unit to the RAM on the standby unit. When the primary unit boots it automatically writes the configuration to the secondary unit. Use the **write standby** command if the primary and secondary units' configurations have different information.

The **write terminal** command displays the current configuration in the PIX Firewall unit's RAM memory.

You can also display the configuration stored in Flash memory using the **show configure** command.

**Defaults**

The default on the PIX Firewall is to store all configurations in compressed format. However, whether a configuration is stored compressed or uncompressed is transparent when executing configuration commands.

**Examples**

The following example specifies the TFTP server and creates a file named **new\_config** in which to store the configuration:

```
tftp-server 10.1.1.2 /pixfirewall/config/new_config
write net :
```

The following example erases the contents of Flash memory and reloads the PIX Firewall:

```
write erase
Erase PIX configuration in Flash memory? [confirm] y
reload
Proceed with reload? [confirm] y
```

The following example saves the configuration on diskette:

```
write floppy
Building configuration...
[OK]
```

The following example saves the current configuration to Flash memory:

```
write memory
Building configuration...
[OK]
```

The following example displays the configuration:

```
write terminal
Building configuration...
: Saved
...
```

---

**Related Commands**

- [configure](#)

## Y and Z Commands

There are no “y” or “z” PIX Firewall commands.



