

Command Summary

This appendix provides an abbreviated listing of the PIX Firewall command set. Refer to Chapter 4, “Command Reference” for more information and examples on each command. Only unique variable information is defined for each command.

Parameters that appear frequently in commands are as follows:

- *ip_address*—The IP address of a host consisting of four sets of numbers called octets. An example is 192.168.42.1. Use 0.0.0.0 to indicate all hosts (0.0.0.0 can be abbreviated as 0). IP addresses can be specified singly or in a range; for example, 10.0.01-10.0.0-254.

IP addresses consist of a network ID and the host ID:

- For a Class A IP address, which ranges from 0.0.0.0 to 127.255.255.255, the network address is in the first octet and the host ID is in the last three. This permits over a million hosts to be represented by a single Class A IP address.
- For a Class B address, which ranges from 128.0.0.0 to 191.255.255.255, the network address is in the first two octets and the host ID is in the last two. This permits 65,536 hosts to be represented by a single Class B IP address.
- For a Class C address, which ranges from 192.0.0.0 to 223.255.255.255, the network address is in the first three octets and the host ID is in the last octet. This permits 256 hosts to be represented by a single Class C IP address.
- *netmask*—The network mask associated with *ip_address*. If *ip_address* is a network address (the host ID has a zero in each octet), then the network mask determines which hosts in the network are accessible. If the IP address is 0.0.0.0, use the same value for the network mask. To specify a range of hosts, specify the maximum host number in the host ID. For example, in a Class C address, if you want hosts 1 through 167 to be accessible, the subnet mask would be 255.255.255.167.
- **inside**—Applies to the inside network interface that connects the firewall to the local network. This interface handles outbound connections.
- **outside**—Applies to the outside network interface that connects the firewall to the Internet side of the network. This interface handles inbound connections.
- *port*—Connection port for a service. You can specify a numeric value or the following reserve words: **ftp**, **h323**, **http**, **rpc**, and **telnet**. **0** means match any port. The port values are defined in RFC 1700. If an invalid port range is specified, such as 32-25, the command fails, but an error message is not returned. Reserve words can be used in a range; such as, **ftp-telnet**.

Command Summary

Note Of the commands that follow, the majority are only available in configuration mode. The exceptions are the unprivileged **show**, **enable**, **quit**, and **who** commands, and the privileged **configure**, **disable**, **http**, **kill**, **passwd**, **ping**, **radius-server**, **reload**, **tacacs-server**, **telnet**, and **write** commands.

aaa authentication *service* **inbound|outbound** *ip_address netmask* **tacacs+|radius**

service The service to be authenticated. Use **any**, **ftp**, **http**, or **telnet**.

aaa authorization *service* **inside|outside** *ip_address netmask*

service The service to be authenticated. Use **any**, **ftp**, **http**, or **telnet**.

age *minutes*

minutes Duration in minutes that a Private Link key is used to encrypt information on the connection. The maximum duration is 130,000,000 minutes (247 years).

alias *inside_net outside_net* [*netmask*]

inside_net IP address on the inside network that is an alias for the *outside_net* address. This is a NIC-registered IP address assigned to a network on the inside of the firewall. Use a network address to create a net alias.

outside_net IP address on the outside network. This is a NIC-registered address assigned to a site on the Internet. Use a network address to create a net alias.

apply *number* **outgoing_src|outgoing_dest**

number An outbound access list identification number previously created with the **outbound** command.

outgoing_src Applies the access list to the source address(es) of packets received on the inside interface. This allows security policies regarding access to outside services from specific inside systems to be implemented. For example, specify **outgoing_src** if you want to prevent an inside system using the web.

outgoing_dest Applies the access list to the destination address(es) of packets received on the inside interface. This allows security policies regarding access to specific outside services and systems from the inside network to be implemented. For example, specify **outgoing_dest** to prevent inside systems from accessing a specific web site.

arp inside|outside *ip_address mac_address* [*alias*]

mac_address Hardware MAC address for the ARP table entry.

alias Make this entry permanent. Alias entries do not time out and are automatically stored in the configuration when you use the **write** command to store the configuration.

arp timeout *seconds*

seconds Duration that an ARP entry can exist in the ARP table before being cleared.

auth inside|outside

Obsolete

auth-server *type server_ip* [-*server_ip*] *key*

Obsolete

type Authentication type: **radius** or **tacacs+**.

server_ip The IP address of the authentication server.

key An alphanumeric keyword of up to 127 characters defined by what the authentication server accepts. This is a public key between the client and server for encrypting data between them. The *key* value must be the same on both the client and server systems.

auth-user inside|outside *type host_ip netmask*

Obsolete

type Authentication type: **radius** or **tacacs+**.

host_ip The IP address from which or to which access is authenticated.

clear [*command*]

The **clear** commands are:

clear apply

clear arp [*inside|outside ip_address*]

clear http *ip_address* [*netmask*]

clear lnkopath

clear mailhost

clear names

clear outbound *num* [*permit|deny ip_address netmask port*]

clear radius-server [*address key*]

clear route inside|outside

clear snmp-server contact|location|host *value*

clear static

clear syslog console

clear syslog host *ip_address*

clear syslog output *facility.level*

clear tacacs-server [*address key*]

clear telnet *ip_address netmask*

clear uauth

conduit *global_ip* *port*[-*port*] **udp|tcp** *ip_address* [*netmask*]

global_ip Registered IP address. Use a network address when mapping a net static.

udp Add conduit for incoming UDP connections.

tcp Add conduit for incoming TCP connections.

configure floppy

configure memory

configure terminal

disable

enable

enable password *password*

password A password of up to 16 alphanumeric characters, which is not case sensitive. PIX Firewall converts the password to all lowercase.

established **udp|tcp**

udp Allow return UDP connections.

tcp Allow return TCP connections.

failover [**active**]

active Make a PIX Firewall the active unit. Use this command when you need to force control of the connection back to the unit you are accessing, such as when you want to switch control back from a unit after you have fixed a problem and want to restore service to the primary unit. Either enter **no failover active** on the secondary unit to switch service to the primary or **failover active** on the primary unit.

global *global_id* *ip_address*

global_id You can specify up to 256 unique ID values. The valid ID numbers can be any positive number up to 2,147,483,647. If there is a single network on the inside of the PIX Firewall, the *global_id* has no meaning and you use **1**.

ip_address One or more IP addresses that the PIX Firewall shares among its connections.
NOTE: If you specify a single IP address, port address translation occurs on that address.

groom

help

hostname *newname*

newname New host name for the PIX Firewall prompt. This name can be up to 17 alphanumeric characters and is not case sensitive. PIX Firewall converts the host name to all lowercase.

http *ip_address netmask*

interface ethernet inside|outside 10baseT|100baseTX|auto|auilbnc

10baseT	Sets 10 Mbit Ethernet and half duplex communications.
100baseTX	Sets 100 Mbit Ethernet and half duplex communications.
auto	Automatically determines networking speed and sets full duplex communications.
auil	Sets 10 Mbit Ethernet half duplex communications for an AUI cable interface.
bnc	Sets 10 Mbit Ethernet half duplex communications for a BNC cable interface.

interface token inside|outside [4mbps|16mbps]

4mbps	4 megabytes per second data transfer speed. Can be abbreviated as 4.
16mbps	(default) 16 megabytes per second data transfer speed. Can be abbreviated as 16.

ip address inside|outside *ip_address* [*netmask*]

kill *telnet_id*

telnet_id Telnet session ID. Use **show who** to display Telnet session IDs.

link *remote_ip_address key-id key*

remote_ip_addresses IP address of a PIX Firewall running Private Link.

key-id The key number. Version 4 PIX Firewall supports up to seven Private Link encryption keys. The *key_id* value can be from 1 to 7.

key The 56-bit key (up to 14 hexadecimal digits) used to seed the encryption chip. This key must be the same on each host end of an encrypted link. The key consists of hexadecimal numbers; for example, **fadebac7733669**. Select a unique key that is difficult to guess and do not use those shown in this document.

linkpath *dest_net netmask remote_ip*

<i>dest_net</i>	The IP address of the destination network on the inside interface of the remote PIX Firewall of a Private Link.
<i>netmask</i>	Specifies a subnet mask to apply to <i>dest_net</i> .
<i>remote_ip</i>	IP address of the remote PIX Firewall's outside network interface.

Inko *remote_global key*

<i>remote_global</i>	IP address from the global address pool.
<i>key</i>	The encryption key. Version 2 PIX Firewall supports one Private Link encryption key. The encryption key can be up to 56 bits in length (14 hexadecimal digits); for example, fadebacbaabaaa .

Inkopath *dest_net netmask remote_global*

<i>dest_net</i>	The IP address of the destination network on the inside interface of the remote PIX Firewall of a Private Link.
<i>netmask</i>	Specifies a subnet mask to apply to <i>dest_net</i> .
<i>remote_global</i>	IP address in the global pool of the remote PIX Firewall in a Private Link environment.

mailhost *global_ip local_ip [max_conns] [em_limit]*

<i>global_ip</i>	A registered IP address.
<i>local_ip</i>	The local IP address from the inside network.
<i>max_conns</i>	The maximum mail connections permitted. Set this value to less than or equal to your connection license. Use show actkey to view the maximum number of connections for your firewall.
<i>em_limit</i>	The embryonic mail connection limit. The default is 0, which means unlimited connections. The maximum is 65535 and the minimum is 1. A rule of thumb for the limit is the maximum number of connections on your connection license plus 30%; for example, on a 64-session license, set it to at least 40. Set it lower for slower systems, higher for faster systems.

mtu insideloutside *bytes*

inside	Specify outbound MTU value.
outside	Specify inbound MTU value.
<i>bytes</i>	The number of bytes in the MTU in the range of 64 to 65535 bytes.

name *ip_address name*

<i>ip_address</i>	The IP address of the host being named.
<i>name</i>	The name assigned to the IP address.

names**nat** *global_id ip_address [netmask] [max_conns] [em_limit]*

<i>global_id</i>	Up to 256 global IDs previously specified with the global command. Specify 0 to indicate that no address translation be used with <i>ip_address</i> .
<i>max_conns</i>	The maximum mail connections permitted. Set this value to less than or equal to your connection license. Use show actkey to view the maximum number of connections for your firewall.
<i>em_limit</i>	The embryonic connection limit.

no [*command*]

The **no** commands are:

no aaa authentication *service inbound|outbound address mask*
no aaa authorization *service inbound|outbound address mask*
no alias *inside_net*
no apply *num outgoing_src|outgoing_dest*
no arp [*inside|outside ip_address*]
no conduit *global_ip port tcp|udp ip_address netmask*
no established *udp|tcp*
no failover [*active*]
no global *global_id [ip_address]*
no http *ip_address netmask*
no link *remote_ip_address key-id key*
no linkpath *dest_net netmask remote_ip*
no lno *remote_global key*
no lnkopath *dest_net netmask remote_global*
no mailhost
no mtu *inside|outside*
no name *ip_address [name]*
no names
no nat *global_id ip_address [netmask]*
no outbound *num permit|deny ip_address [netmask [port[-port]]]*
no radius-server *host ip_address key*
no rip *inside|outside default|passive*
no route *inside|outside dest_net_ip*
no snmp-server *contact|location text*
no snmp-server *host ip_address*
no static *global_ip*
no syslog *console*
no syslog *host ip_address*
no syslog *output facility.level*
no tacacs-server *host ip_address key*
no telnet *ip_address netmask*

outbound *num* **permit|deny** *ip_address* [*netmask* [*port*[-*port*]]] [**java**]

<i>num</i>	A tag number for the access list.
permit	Allow the access list to access the specified IP address and port.
deny	Deny the access list access to the specified IP address and port.
java	Block Java applets being downloaded from <i>ip_address</i> depending on use of the apply command.

passwd *password*

<i>password</i>	A password of up to 15 alphanumeric characters, which is not case sensitive. PIX Firewall converts the password to all lowercase.
-----------------	---

ping **inside|outside** *ip_address*

radius-server host *server_ip* *key*

<i>server_ip</i>	The IP address of the authentication server.
<i>key</i>	An alphanumeric keyword of up to 127 characters defined by what the authentication server accepts. This is a public key between the client and server for encrypting data between them. The <i>key</i> must be the same on both the client and server systems. PIX Firewall changes to lowercase any letters in the key. Spaces are not permitted in the key, but other special characters are.

reload

rip **inside|outside** **default|passive**

default	Causes the PIX Firewall to broadcast a default route to the inside network.
passive	Enables passive RIP on either the inside or outside interface. The PIX Firewall listens for RIP routing broadcasts and uses that information to populate its routing tables.

route **inside|outside** *dest_net_ip* *netmask* *gateway_ip* [*metric*]

<i>dest_net_ip</i>	The destination network IP address. Use 0.0.0.0 to specify a default route.
<i>netmask</i>	Specifies a network mask to apply to <i>dest_net_ip</i> . Use 0.0.0.0 to specify a default route.
<i>gateway_ip</i>	Specifies the IP address of the gateway router (the next hop address for this route).
<i>metric</i>	Specifies the number of hops to <i>dest_net_ip</i> . If you are not sure, enter 1 .

session comm_port

comm_port Specifies the PIX Firewall communications port to which a router inside the fire-wall connects. Possible values are **0**, **1**, **2**, or **3**. The default is port **3**.

show [command]

The **show** commands are:

- show aaa**
- show actkey**
- show age**
- show alias**
- show apply** [*number outgoing_src|outgoing_dest*]
- show arp** [*inside|outside ip_address mac alias*]
- show arp timeout**
- show blocks**
- show conduit**
- show configure**
- show conn**
- show established**
- show failover**
- show global**
- show http*
- show hw*
- show interface**
- show ip**
- show link**
- show linkpath**
- show lno**
- show lnoopath**
- show mailhost**
- show memory**
- show mtu**
- show names**
- show nat**
- show outbound**
- show passwd**
- show processes**
- show radius-server**
- show rip**
- show route**
- show session**
- show snmp-server**
- show static**
- show syslog**
- show telnet**
- show timeout**
- show uauth**
- show version**
- show who** [*ip_address*]
- show xlate** [*global_ip*] [*local_ip*]

snmp-server contact*location text*

snmp-server host *ip_address*

contact	Indicate that you are supplying your name or that of the PIX Firewall system administrator.
location	Indicate that you are specifying your PIX Firewall location.
host	Indicate that you are specifying an IP address of a host to which SNMP traps should be sent. You can specify a maximum of 5 host IP addresses.
<i>text</i>	When used with contact , specify your name or that of the PIX Firewall system administrator. When used with location , specify your PIX Firewall location. If the location name contains spaces, surround the string in single quotes; for example, 'building 42'.
<i>ip_address</i>	When used with host , the IP address of a host to which SNMP traps should be sent. You can specify a maximum of 5 host IP addresses.

static *global_ip local_ip [max_conns] [em_limit]*

<i>global_ip</i>	The registered IP address. Use a network address to create a net static.
<i>local_ip</i>	The local IP address from the inside network. Use a network address to create a net static.
<i>max_conns</i>	The maximum number of TCP connections allowed for this static.
<i>em_limit</i>	The embryonic connection limit.

syslog console

syslog host *host_ip*

<i>host_ip</i>	The IP address or network of a host that is authorized to receive SYSLOG messages.
----------------	--

syslog output *facility.level*

<i>facility</i>	Eight facilities LOCAL0(16) through LOCAL7(23); the default is LOCAL4(20). Hosts file the messages based on the <i>facility</i> number in the message.
<i>level</i>	Message type; sets the level above which PIX Firewall suppresses messages to the SYSLOG hosts. Setting the level to 3, for example, allows messages with levels 0, 1, 2, and 3 to display. The default is 3. The levels are: <ul style="list-style-type: none">• 0 — System unusable• 1 — Take immediate action• 2 — Critical condition• 3 — Error message• 4 — Warning message• 5 — Normal but significant condition• 6 — Informational• 7 — Debug message

tacacs-server host *ip_address key*

<i>ip_address</i>	The IP address of the authentication server.
<i>key</i>	An alphanumeric keyword of up to 127 characters defined by what the authentication server accepts. This is a public key between the client and server for encrypting data between them. The <i>key</i> must be the same on both the client and server systems. PIX Firewall changes to lowercase any letters in the key. Spaces are not permitted in the key, but other special characters are.

telnet *ip_address netmask*

<i>ip_address</i>	The IP address or network of a host that is authorized to access the PIX Firewall Telnet management interface.
<i>netmask</i>	The netmask for the network specified in this Telnet command. Use any valid mask, or a network IP address to enable access to all in the subnet; for example if you set <i>netmask</i> to 255.255.255.0, all systems in the Class C subnet can access the firewall over Telnet. If you set <i>netmask</i> to 255.255.255.255, only the IP address you specify can access the firewall.

Command Summary

timeout [**conn** [*hh:mm:ss*]] [**h323** [*hh:mm:ss*]] [**rpc** [*hh:mm:ss*]]
[**uauth** [*hh:mm:ss*]] [**udp** [*hh:mm:ss*]] [**xlate** [*hh:mm:ss*]]

conn <i>hh:mm:ss</i>	Idle time until a connection slot is freed (default value is 12 hours). Use 0:0:0 for the time value to never time out a connection.
h323 <i>hh:mm:ss</i>	Duration for H323 (Internet Phone) inactivity timer. When this time elapses, the port used by the H323 service closes.
rpc <i>hh:mm:ss</i>	Idle time until an RPC slot is freed.
uauth <i>hh:mm:ss</i>	Duration before authentication and authorization cache times out and user has to reauthenticate next connection.
udp <i>hh:mm:ss</i>	Idle time until a UDP slot is freed.
xlate <i>hh:mm:ss</i>	Idle time until a translation slot is freed (default value is 24 hours).

who [*ip_address*]

write erase

write floppy

write memory

write terminal

Commands by Feature

Table A-1 lists configuration commands by feature.

Table A-1 **Commands by PIX Firewall Feature**

Feature	Command	Access Mode
AAA (Authentication, Authorization, and Accounting)	aaa authentication	Configuration
	aaa authorization	Configuration
	radius-server	Configuration
	tacacs-server	Configuration
ARP cache:		
Adjust	arp	Configuration
Flush	clear arp-cache	Privileged
Configuration:		
Read from floppy	conf floppy	Privileged
Store on floppy	write floppy	Privileged
View current configuration in RAM	write term	Privileged
Cut-Through Proxy	aaa authentication	Configuration
	aaa authorization	Configuration
	radius-server	Configuration
	tacacs-server	Configuration
Ethernet, configure	interface ethernet 10baseT	Configuration
Failover (optional):		
• Configure	failover	Configuration
• Force PIX Firewall to active	failover active	Configuration
• Force PIX Firewall to standby	no failover active	Configuration
• Show status	show failover	Unprivileged
Fast Ethernet, configure	interface ethernet auto	Configuration
Flash memory access:		
• Clear	groom	Privileged
• Display configuration in flash memory	show configuration	Privileged
• Reload from	reload	Privileged
• Write to	write memory	Privileged
Floppy disk access:		
• Read from	configure floppy	Privileged
• Save configuration to	write floppy	Privileged
IP address, set	ip address	Configuration
Java applet filtering	outbound deny ... java	Configuration
NAT (Name Address Translation)	alias, nat	Configuration
Private Link:		
• Age links	age	Configuration
• Configure	link and linkpath	Configuration
• V2 compatibility	lko and lkoopath	Configuration
Mail Guard	mailhost	Configuration
Multimedia	established	Configuration
Processes, show thread information	show processes	Unprivileged
Prompt host name, change	hostname	Configuration
RIP listening, enable or disable	rip	Configuration

Command Summary

Routing table:		
• Adjust	route	Configuration
• Show	show route	Unprivileged
SNMP	snmp-server	Configuration
SYSLOG:		
• Display messages as they occur	syslog console	Configuration
• Messages, display log	show syslog	Unprivileged
• Messages, change facility and level	syslog output	Configuration
• Server, assign	syslog host	Configuration
Token Ring interface, configure	interface token	Configuration