



Using PIX Firewall Commands

This chapter introduces the Cisco PIX Firewall Command Reference and contains the following sections:

- [Introduction](#)
- [Access Modes](#)
- [Ports](#)
- [Protocols](#)

Introduction

This section provides detailed descriptions of the PIX Firewall commands.

The following notes can help you as you configure the PIX Firewall:

- View your configuration at any time with the **write terminal** command.
- Save your configuration frequently with the **write memory** command.
- Always check the syntax before entering a command. Enter a command and press the **Enter** key to view a quick summary, or precede a command with **help**, as in, **help aaa**.
- View syslog messages as you work on the PIX Firewall. Start accumulating messages with the **logging buffered debugging** command, view messages with the **show logging** command, and clear the message buffer with the **clear logging** command. Syslog messages are described in the *Cisco PIX Firewall Syslog Guide*.
- Abbreviate commands, such as, using the **conf t** command to start configuration mode, the **wr t** command statement to list the configuration, and **wr m** to write to Flash memory. Start logging with the **lo b 7** command and show logging messages with the **sh lo** command statement.
- After changing or removing the **alias**, **access-list**, **conduit**, **global**, **nat**, **outbound**, and **static** commands, use the **clear xlate** command to make the IP addresses available for access.
- You can view possible port and protocol numbers at the following IANA websites:
<http://www.iana.org/assignments/port-numbers>
<http://www.iana.org/assignments/protocol-numbers>
- Create your configuration on a text editor and then cut and paste it into the configuration. PIX Firewall lets you paste in a line at a time or the whole configuration. Always check your configuration after pasting large blocks of text to be sure everything copied.

Access Modes

The PIX Firewall contains a command set based on Cisco IOS technologies, which provides three administrative access modes:

- Unprivileged mode is available when you first access the PIX Firewall and displays the “>” prompt. This mode lets you view restricted settings.
- Privileged mode displays the “#” prompt and lets you change current settings. Any unprivileged command also works in privileged mode. Use the **enable** command to start privileged mode and the **disable**, **exit**, or **quit** commands to exit.
- Configuration mode displays the “(config)#” prompt and lets you change system configurations. All privileged, unprivileged, and configuration commands work in this mode. Use the **configure terminal** command to start configuration mode and the **exit** or **quit** commands to exit.

Ports

The following literal names can be used instead of a numerical port value in command lines:

PIX Firewall permits the following TCP literal names: **bgp**, **chargen**, **cmd**, **daytime**, **discard**, **domain**, **echo**, **exec**, **finger**, **ftp**, **ftp-data**, **gopher**, **h323**, **hostname**, **http**, **ident**, **irc**, **klogin**, **kshell**, **lpd**, **nntp**, **pop2**, **pop3**, **pptp**, **rpc**, **smtp**, **sqlnet**, **sunrpc**, **tacacs**, **talk**, **telnet**, **time**, **uucp**, **whois**, and **www**.



Note

PIX Firewall uses port 1521 for SQL*Net. This is the default port used by Oracle for SQL*Net; however, this value does not agree with IANA port assignments.

PIX Firewall listens for RADIUS on ports 1645 and 1646. If your RADIUS server uses ports 1812 and 1813, you will need to reconfigure it to listen on ports 1645 and 1646.

To assign a port for DNS access, use **domain**, not **dns**. The **dns** keyword translates into the port value for **dnsix**.

Permitted UDP literal names are **biff**, **bootpc**, **bootps**, **discard**, **dnsix**, **echo**, **mobile-ip**, **nameserver**, **netbios-dgm**, **netbios-ns**, **nntp**, **rip**, **snmp**, **snmptrap**, **sunrpc**, **syslog**, **tacacs**, **talk**, **tftp**, **time**, **who**, and **xdmcp**.

Port numbers can be viewed online at the IANA website:

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

Table 1-1 lists the literal values.

Table 1-1 Port Literal Values

Literal	Value	Description
bgp	179	Border Gateway Protocol, RFC 1163
biff	512	Used by mail system to notify users that new mail is received
bootpc	68	Bootstrap Protocol Client
bootps	67	Bootstrap Protocol Server
chargen	19	Character Generator

Table 1-1 Port Literal Values (continued)

Literal	Value	Description
cmd	514	Similar to exec except that cmd has automatic authentication
daytime	13	Day time, RFC 867
discard	9	Discard
domain	53	DNS (Domain Name System)
dnsix	195	DNSIX Session Management Module Audit Redirector
echo	7	Echo
exec	512	Remote process execution
finger	79	Finger
ftp	21	File Transfer Protocol (control port)
ftp-data	20	File Transfer Protocol (data port)
gopher	70	Gopher
hostname	101	NIC Host Name Server
nameserver	42	Host Name Server
ident	113	Ident authentication service
irc	194	Internet Relay Chat protocol
isakmp	500	ISAKMP
klogin	543	KLOGIN
kshell	544	Korn Shell
lpd	515	Line Printer Daemon - printer spooler
login	513	Remote login
mobile-ip	434	MobileIP-Agent
netbios-ns	137	NETBIOS Name Service
netbios-dgm	138	NETBIOS Datagram Service
nntp	119	Network News Transfer Protocol
ntp	123	Network Time Protocol
pim-auto-rp	496	Protocol Independent Multicast, reverse path flooding, dense mode
pop2	109	Post Office Protocol - Version 2
pop3	110	Post Office Protocol - Version 3
radius	1645, 1646	Remote Authentication Dial-In User Service
rip	520	Routing Information Protocol
smtp	25	Simple Mail Transport Protocol
snmp	161	Simple Network Management Protocol
snmptrap	162	Simple Network Management Protocol - Trap
sqlnet	1521	Structured Query Language Network
sunrpc	111	Sun RPC (Remote Procedure Call)
syslog	514	System Log

Table 1-1 Port Literal Values (continued)

Literal	Value	Description
tacacs	49	TACACS+ (Terminal Access Controller Access Control System Plus)
talk	517	Talk
telnet	23	RFC 854 Telnet
tftp	69	Trivial File Transfer Protocol
time	37	Time
uucp	540	UNIX-to-UNIX Copy Program
who	513	Who
whois	43	Who Is
www	80	World Wide Web
xdmcp	177	X Display Manager Control Protocol, used to communicate between X terminals and workstations running UNIX

Protocols

Possible literal values are **ahp**, **eigrp**, **esp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **ipsec**, **nos**, **ospf**, **pcp**, **snp**, **tcp**, and **udp**. You can also specify any protocol by number. The **esp** and **ah** protocols only work in conjunction with Private Link.

Protocol numbers can be viewed online at the IANA website:

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



Note

PIX Firewall does not pass multicast packets. Many routing protocols use multicast packets to transmit their data. If you need to send routing protocols across the PIX Firewall, configure the routers with the Cisco IOS software **neighbor** command. We consider it inherently dangerous to send routing protocols across the PIX Firewall. If the routes on the unprotected interface are corrupted, the routes transmitted to the protected side of the firewall will pollute routers there as well.

Table 1-2 lists the numeric values for the protocol literals.

Table 1-2 Protocol Literal Values

Literal	Value	Description
ah	51	Authentication Header for IPv6, RFC 1826
eigrp	88	Enhanced Interior Gateway Routing Protocol
esp	50	Encapsulated Security Payload for IPv6, RFC 1827
gre	47	General Routing Encapsulation
icmp	1	Internet Control Message Protocol, RFC 792
igmp	2	Internet Group Management Protocol, RFC 1112
igrp	9	Interior Gateway Routing Protocol
ip	0	Internet Protocol

Table 1-2 Protocol Literal Values (continued)

Literal	Value	Description
ipinip	4	IP-in-IP encapsulation
nos	94	Network Operating System (Novell's NetWare)
ospf	89	Open Shortest Path First routing protocol, RFC 1247
pcp	108	Payload Compression Protocol
snp	109	Sitara Networks Protocol
tcp	6	Transmission Control Protocol, RFC 793
udp	17	User Datagram Protocol, RFC 768

