Using PIX Firewall Commands

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

Introduction

This section provides a brief introduction to using PIX Firewall commands and where to go for more information on configuring and using your PIX Firewall.

The following table lists some basic PIX Firewall commands.

Task	Related Command
Saving my configuration	**write memory**
Viewing my configuration	**write terminal**
Accumulating system log (syslog) messages	**logging buffered debugging**
Viewing system log (syslog) messages	**show logging**
Clearing the message buffer	**clear logging**

Tips

Tip When using the PIX Firewall command-line interface (CLI), you can do the following:

- 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**.
- Abbreviate commands. For example, you can use the **config t** command to start configuration mode, the **write t** command statement to list the configuration, and the **write m** command to write to Flash memory. Also, in most commands, **show** can be abbreviated as **sh**. This feature is called command completion.
- 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.
- Review 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 in 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.

For more information

For information about how to build your PIX Firewall configuration, please refer to the *Cisco PIX Firewall and VPN Configuration Guide*.

Syslog messages are fully described in *Cisco PIX Firewall System Log Messages*.

For information about how to use Cisco PIX Device Manager (PDM), please refer to the online Help included in the PDM software (accessed through the PDM application Help button). For information about how to install PDM, please refer to the *Cisco PIX Device Manager Installation Guide*.

PIX Firewall technical documentation is located online at the following website:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/

Command Modes

The PIX Firewall contains a command set based on Cisco IOS technologies and provides configurable command privilege modes based on the following command modes:

- Unprivileged mode. When you first access the firewall, it displays the ">" prompt. This is unprivileged mode, and it lets you view firewall settings. The unprivileged mode prompt appears as follows:

```
pixfirewall>
```

- Privileged mode, which displays the "#" prompt and lets you change current settings. Any unprivileged mode command also works in privileged mode. Use the **enable** command to start privileged mode from unprivileged mode as follows:

```
pixfirewall> enable
Password:
pixfirewall#
```

  Use the **exit** or **quit** commands to exit privileged mode and return to unprivileged mode as follows:

```
pixfirewall# exit

Logoff

Type help or '?' for a list of available commands.
pixfirewall>
```

  Use the **disable** command to exit privileged mode and return to unprivileged mode as follows:

```
pixfirewall# disable
pixfirewall>
```

- Configuration mode, which displays the "(config)#" prompt and lets you change the firewall configuration. All privileged, unprivileged, and configuration mode commands are available in this mode. Use the **configure terminal** command to start configuration mode as follows:

```
pixfirewall# configure terminal
pixfirewall(config)#
```

  Use the **exit** or **quit** commands to exit configuration mode and return to privileged mode as follows:

```
pixfirewall(config)# quit
pixfirewall#
```

  Use the **disable** command to exit configuration mode and return to unprivileged mode as follows:

```
pixfirewall(config)# disable
pixfirewall>
```

Ports

Literal names can be used instead of a numerical port value in **access-list** commands.

The 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.

The PIX Firewall listens for RADIUS on ports 1645 and 1646. If your RADIUS server uses ports 1812 and 1813, you must 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**.

Note By design, the PIX Firewall drops DNS packets sent to UDP port 53 (usually used for DNS) that have a packet size larger than 512 bytes.

Port numbers can be viewed online at the IANA website:

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

Table 2-1 lists the port literal values.

Table 2-1 Port Literal Values

Literal	TCP or UDP?	Value	Description
aol	TCP	5190	America On-line
bgp	TCP	179	Border Gateway Protocol, RFC 1163
biff	UDP	512	Used by mail system to notify users that new mail is received
bootpc	UDP	68	Bootstrap Protocol Client
bootps	UDP	67	Bootstrap Protocol Server
chargen	TCP	19	Character Generator
citrix-ica	TCP	1494	Citrix Independent Computing Architecture (ICA) protocol
cmd	TCP	514	Similar to **exec** except that **cmd** has automatic authentication
ctiqbe	TCP	2748	Computer Telephony Interface Quick Buffer Encoding
daytime	TCP	13	Day time, RFC 867
discard	TCP, UDP	9	Discard
domain	TCP, UDP	53	DNS (Domain Name System)
dnsix	UDP	195	DNSIX Session Management Module Audit Redirector
echo	TCP, UDP	7	Echo
exec	TCP	512	Remote process execution
finger	TCP	79	Finger
ftp	TCP	21	File Transfer Protocol (control port)
ftp-data	TCP	20	File Transfer Protocol (data port)
gopher	TCP	70	Gopher
https	TCP	443	Hyper Text Transfer Protocol (SSL)
h323	TCP	1720	H.323 call signalling
hostname	TCP	101	NIC Host Name Server
ident	TCP	113	Ident authentication service
imap4	TCP	143	Internet Message Access Protocol, version 4
irc	TCP	194	Internet Relay Chat protocol

Table 2-1 Port Literal Values (continued)

Literal	TCP or UDP?	Value	Description
isakmp	UDP	500	Internet Security Association and Key Management Protocol
kerberos	TCP, UDP	750	Kerberos
klogin	TCP	543	KLOGIN
kshell	TCP	544	Korn Shell
ldap	TCP	389	Lightweight Directory Access Protocol
ldaps	TCP	636	Lightweight Directory Access Protocol (SSL)
lpd	TCP	515	Line Printer Daemon - printer spooler
login	TCP	513	Remote login
lotusnotes	TCP	1352	IBM Lotus Notes
mobile-ip	UDP	434	MobileIP-Agent
nameserver	UDP	42	Host Name Server
netbios-ns	UDP	137	NetBIOS Name Service
netbios-dgm	UDP	138	NetBIOS Datagram Service
netbios-ssn	TCP	139	NetBIOS Session Service
nntp	TCP	119	Network News Transfer Protocol
ntp	UDP	123	Network Time Protocol
pcanywhere-status	UDP	5632	pcAnywhere status
pcanywhere-data	TCP	5631	pcAnywhere data
pim-auto-rp	TCP, UDP	496	Protocol Independent Multicast, reverse path flooding, dense mode
pop2	TCP	109	Post Office Protocol - Version 2
pop3	TCP	110	Post Office Protocol - Version 3
pptp	TCP	1723	Point-to-Point Tunneling Protocol
radius	UDP	1645	Remote Authentication Dial-In User Service
radius-acct	UDP	1646	Remote Authentication Dial-In User Service (accounting)
rip	UDP	520	Routing Information Protocol
secureid-udp	UDP	5510	SecureID over UDP
smtp	TCP	25	Simple Mail Transport Protocol
snmp	UDP	161	Simple Network Management Protocol
snmptrap	UDP	162	Simple Network Management Protocol - Trap
sqlnet	TCP	1521	Structured Query Language Network
ssh	TCP	22	Secure Shell
sunrpc (rpc)	TCP, UDP	111	Sun Remote Procedure Call
syslog	UDP	514	System Log

Table 2-1 Port Literal Values (continued)

Literal	TCP or UDP?	Value	Description
tacacs	TCP, UDP	49	Terminal Access Controller Access Control System Plus
talk	TCP, UDP	517	Talk
telnet	TCP	23	RFC 854 Telnet
tftp	UDP	69	Trivial File Transfer Protocol
time	UDP	37	Time
uucp	TCP	540	UNIX-to-UNIX Copy Program
who	UDP	513	Who
whois	TCP	43	Who Is
www	TCP	80	World Wide Web
xdmcp	UDP	177	X Display Manager Control Protocol

Protocols

Literal names can be used instead of a numerical port value in **access-list** commands.

Protocol numbers can be viewed online at the IANA website:

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

Note Many routing protocols use multicast packets to transmit their data. If you send routing protocols across the PIX Firewall, configure the surrounding routers with the Cisco IOS software **neighbor** command. If routes on an unprotected interface are corrupted, the routes transmitted to the protected side of the firewall will pollute routers there as well.

The PIX Firewall supports the protocol literal values listed in Table 2-2 .

Table 2-2 Protocol Literal Values

Literal	Value	Description
ah	51	Authentication Header for IPv6, RFC 1826
eigrp	88	Enhanced Interior Gateway Routing Protocol
esp	50	Encapsulating Security Payload (ESP) 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
ipinip	4	IP-in-IP encapsulation
nos	94	Network Operating System (Novell NetWare)
ospf	89	Open Shortest Path First routing protocol, RFC 1247

Table 2-2 Protocol Literal Values (continued)

Literal	Value	Description
pcp	108	Payload Compression Protocol
snp	109	Sitara Networks Protocol
tcp	6	Transmission Control Protocol, RFC 793
udp	17	User Datagram Protocol, RFC 768

Deprecated Commands

The following commands are no longer used to configure the firewall: **sysopt route dnat**, **sysopt security fragguard**, **fragguard,** and **session enable**.

The **sysopt route dnat** command is ignored, starting in PIX Firewall software Version 6.2. Instead, overlapping configurations (network addresses and routes) are automatically handled by outside NAT.

The **sysopt security fragguard** and **fragguard** commands have been replaced by the **fragment** command.

The **session enable** command is deprecated because the AccessPro router it was intended to support no longer exists.