PIX Command Reference

General Commands

`aaa accounting` – Enable/view LOCAL, TACACS+, RADIUS user accounting
`aaa authentication` – Enable/view LOCAL, TACACS+, RADIUS user authentication
`aaa authorization` – Enable/disable LOCAL or TACACS+ user authorization services
`aaa mac-exempt` – Exempt a list of MAC addresses from authentication and authorization
`aaa proxy-limit` – Specify the number of concurrent proxy connections allowed per user
`aaa-server` – Define the AAA server group
`access-group` – Bind the access list to an interface
`access-list` – Create access list
`activation-key` – Update activation key and check key running on PIX Firewall against Flash key
`alias` – Administer overlapped addresses w/dual NAT
`arp` – Configure/view ARP cache and parameters
`auth-prompt` – Change AAA challenge text for through-the-firewall user sessions
`auto-update` – How often to poll Auto Update Server
`banner` – Configure session, login, or MOTD banners
`ca` – Interoperate with a certification authority
`ca generate rsa key` – Generate RSA key-pairs
`capture` – Enable packet capture for packet sniffing
`clear` – Remove configuration files/reset commands
`clock` – Set PIX Firewall clock for Syslog and PKI
`conduit` – Add, delete, or show conduits through the PIX Firewall for incoming connections. NOTE: `conduit` has been superseded by `access-list`.
`configure` – Config from terminal, memory, network
`console` – Set idle timeout for serial-cable console
`copy` – Change software images without requiring access to the TFTP monitor mode, or copy a capture file to a TFTP server.
`crashinfo` – Configure crash info to write to Flash
`crypto dynamic-map` – Create, view, delete dynamic crypto map entry
`crypto ipsec` – Create, view, delete IPSec security associations and parameters
`crypto map` – Create or modify crypto map entry
`debug` – Provide info to help troubleshoot protocols
`dhcpd` – Configure the DHCP server

IIUSA
Excellence in Information Technology
http://iiusatech.com

General Commands (continued)

`dhcprelay` – Configure DHCP relay agent
`disable` – Exit priviliged mode
`domain-name` – Change the IPSec domain name
`dynamic-map` – View/delete dynamic crypto map entry
`eeprom` – PIX525 only: Display/update EEPROM
`enable` – Start privileged mode
`established` – Permit return connections on ports other than those used for originating connection
`exit` – Exit an access mode
`failover` – Enable or disable the PIX Firewall failover feature on a standby PIX Firewall
`filter` – Enable/display URL, Java, or ActiveX filtering
`fixup protocol` – Modify fixups for services
`flashfs` – Clear, display, or downgrade filesystem info
`floodguard` – Enable Flood Defender against attacks
`fragment` – Additional mgmt of packet fragments
`global` – Create entries in pool of global addresses
`help` – Display help information
`hostname` – Change hostname in command-line prompt
`http` – Enable PIX HTTP server
`icmp` – Configure access rules for ICMP traffic
`igmp` – IGMP support is implemented as a subcommand to the `multicast` command
`interface` – Set network interface parameters
`ip address` – Set IP address and subnet mask
`ip audit` – Configure IDS signature use
`ip local pool` – Identify addresses for a local pool
`ip verify reverse-path` – Implement Unicast RPF IP spoofing protection
`isakmp` – Configure Internet Security Association Key Management Protocol (ISAKMP) for IPSec Internet Key Exchange (IKE)
`isakmp policy` – Configure specific IKE parameters
`kill` – Terminate a telnet session
`logging` – Enable syslog and SNMP logging
`login` – Initiate login prompt for starting a session
`mac-list` – Add list of MAC addresses
`management-access` – Enable access to internal management interface on the firewall
`mgcp` – Configure additional support for MGCP fixup
`mroute` – Configure static multicast route
`mtu` – Specify maximum transmission unit for interface
`multicast` – Enable multicast traffic to flow through PIX
`name/names` – Associate a name with an IP address
`nameif` – Name interfaces and assign security level
`nat` – Associate a network with a global IP address pool
`ntp` – Synchronize PIX using Network Time Protocol
`object-group` – Define object groups to optimize config
`outbound/apply` – Create an Internet access list

General Commands (continued)

`pager` – Enable or disable screen paging
`password` – Set password for console telnet access
`pdm` – Support browsing for Cisco PIX Device Manager
`perfmon` – View performance information
`ping` – Determine if other IP addresses are visible
`prefix-list` – Configure prefix list for Area Border Router type 3 link-state advertisement filtering
`privilege` – Configure command privilege levels
`quit` – Exit configuration or privileged mode
`reload` – Reboot and reload the configuration
`rip` – Change Routing Information Protocol settings
`route` – Enter a static or default route for interface
`route-map` – Define conditions for redistributing routes
`router ospf` – Configure global parameters for OSPF
`routing interface` – Config interface-specific OSPF
`service` – Enable system services
`setup` – Use Cisco PIX Device Manager for a new PIX
`show` – View command information
`show blocks/clear blocks` – System buffer info
`show checksum` – Display the configuration checksum
`show conn` – Display all active connections
`show cpu usage` – Display CPU utilization
`show crypto engine [verify]` – Show crypto engine statistics or run Known Answer Test
`show crypto interface [counters]` – Show VPN accelerator cards installed in chassis
`show history` – Show previously entered commands
`show local-host/clear local-host` – View local host network states
`show memory` – Show system memory utilization
`show ospf` – Show OSPF routing process general info
`show ospf border-routers` – Show internal OSPF routing table entries to an ABR and ASBR
`show ospf database` – Show LSA info in database
`show ospf flood-list` – Display a list of OSPF LSA's waiting to be flooded over an interface
`show ospf interface` – Show OSPF interface info
`show ospf neighbor` – Show OSPF neighbor info
`show ospf request-list` – Show all requested LSAs
`show ospf retransmission-list` – Display a list of all LSAs waiting to be resent
`show ospf summary-address` – Display a list of all OSPF summary address redistribution information
`show ospf virtual links` – Show OSPF link states
`show processes` – Display processes
`show routing` – Show non-default routing config
`show running-config` – Display running config
`show startup-config` – Display PIX startup config
`show tech-support` – Info to help a support analyst
`show tcpstat` – Show TCP stack status
`show traffic/clear traffic` – Send/rcv activity

General Commands (continued)

`show uauth/clear uauth` – Authorization caches
`show version` – View PIX operating info
`show xlate/clear xlate` – Translation slot info
`shun` – Enable dynamic response to attacking host
`snmp-server` – Provide PIX event info through SNMP
`ssh` – Specify host for Secure Shell console access
`static` – Configure a 1-to-1 IP address mapping
`syslog` – Enable syslog message facility
`sysopt` – Change firewall system options
`telnet` – Specify host for telnet console access
`terminal` – Change console terminal settings
`tftp-server` – Specify IP address of TFTP server
`timeout` – Set the maximum idle time duration
`url-block` – Filter long URLs
`url-cache` – Cache pending Webserver responses
`url-server` – Designate N2H2 or Websense server
`username` – Specify username for a privilege level
`virtual` – Access PIX Firewall virtual server
`vpdn` – Configure Virtual Private Dial-up Networking
`vpnclient` – Configure Easy VPN Remote
`vpngroup` – Support VPN Client/Easy VPN Remote
`who` – Show active telnet sessions on the Firewall
`write` – Store, view, or erase current config

Port Literal Values

Literal	*TCP/UDP:Value*	*Description*
aol	TCP:5190	*America On-Line*
bgp	TCP:179	*Border Gateway Protocol, RFC 1163*
biff	UDP:512	*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*

Port Literal Values (Continued)

Literal	*TCP/UDP:Value*	*Description*
hostname	TCP:101	*NIC Host Name Server*
ident	TCP:113	*Ident authentication service*
imap4	TCP:143	*Internet Message Access Protocol, v4*
irc	TCP:194	*Internet Relay Chat protocol*
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	*LDAP (SSL version)*
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 Authen. 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	*SNMP - Trap*
sqlnet	TCP:1521	*Structured Query Language Network*
ssh	TCP:22	*Secure Shell*
sunrpc (rpc)	TCP,UDP:111	*Sun Remote Proced. Call*
syslog	UDP:514	*System Log*
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*

http://iiusatech.com

Port Literal Values (Continued)

Literal	*TCP/UDP:Value*	*Description*
who	UDP:513	*Who*
whois	TCP:43	*Who Is*
www	TCP:80	*World Wide Web*

Protocol Literal Values

Literal	*Value*	*Description*
ah	51	Authentication header for IPv6
eigrp	88	Enhanced IGRP
esp	50	Encapsulating Security Payload
gre	47	General routing encapsulation
icmp	1	Internet Control Message Protocol
igmp	2	Internet Group Management Protocol
igrp	9	Interior Gateway Routing Protocol
ipinip	4	IP-in-IP encapsulation
nos	94	Network Operating System (Novell)
ospf	89	Open Shortest Path First protocol
pcp	108	Payload Compression Protocol
snp	109	Sitara Networks Protocol
tcp	6	Transmission Control Protocol
udp	17	User Datagram Protocol

Recovering a Lost Password on the PIX

1) Download the file for the PIX Firewall software from:
`www.cisco.com/warp/public/110/34.shmtl`

2) Move the binary file downloaded in step (1) to the TFTP home folder on your TFTP server.

3) Reboot the PIX and interrupt the boot process to enter monitor mode (use Esc or ctrl+Break).

4) Specify the PIX firewall interface to use for TFTP. For the Inside interface (Ethernet1), use:

```
monitor> interface 1
```

5) Specify PIX interface's IP address (ex: 10.10.10.1):

```
monitor> address 10.10.10.1
```

6) Specify default gateway (this usually isn't required):

```
monitor> gateway ip_address
```

7) Specify address of TFTP server (ex: 10.10.10.100):

```
monitor> server 10.10.10.100
```

8) Verify connectivity to the TFTP server:

```
monitor> ping 10.10.10.100
```

9) Specify the filename of the password-recovery file (version 5.3(1) in the following example):

```
monitor> file np53.bin
```

10) Start the TFTP process:

```
monitor> tftp
```

11) When prompted, press **y** to erase the password:

```
Do you wish to erase the passwords? [yn] y
Passwords have been erased
```

The password is erased and the PIX reboots.

Rev 4.4