

# Acronyms and Abbreviations

---

This appendix lists the acronyms and abbreviations used in this document. Refer to Chapter 6, “Command Reference,” for information on the commands described in this section.

**Table B-1 Acronyms and Abbreviations**

Acronym	Description
AAA	Authentication, Authorization, and Accounting.
AH	Authentication Header.
ARP	Address Resolution Protocol—A low-level TCP/IP protocol that maps a node’s hardware address (called a “MAC” address) to its IP address. Defined in RFC 826. An example hardware address is 00:00:a6:00:01:ba. (The first three groups specify the manufacturer, the rest identify the host’s motherboard.)
BGP	Border Gateway Protocol—While PIX Firewall does not support use of this protocol, you can set the routers on either side of the PIX Firewall to use RIP between them and then run BGP on the rest of the network before the routers.
BOOTP	Bootstrap Protocol—Lets diskless workstations boot over the network and is described in RFC 951 and RFC 1542. You can set access to this feature with the <b>outbound</b> and <b>conduit</b> commands.
CA	Certification Authority.
chargen	Character Generation—Via TCP, a service that sends a continual stream of characters until stopped by the client. Via UDP, the server sends a random number of characters each time the client sends a datagram. Defined in RFC 864.
conn	Connection slot in PIX Firewall—Refer to the <b>xlate</b> command page for more information.
CRL	Certificate Revocation List.
DES	Data Encryption Standard.
DNS	Domain Name System—Operates over UDP unless zone file access over TCP is required. You can permit or deny access to this feature with the <b>conduit</b> and <b>outbound</b> commands.
EGP	Exterior Gateway Protocol—While PIX Firewall does not support use of this protocol, you can set the routers on either side of the PIX Firewall to use RIP between them and then run EGP on the rest of the network before the routers.

---

**Table B-1 Acronyms and Abbreviations (Continued)**

<b>Acronym</b>	<b>Description</b>
EIGRP	Enhanced Interior Gateway Routing Protocol—While PIX Firewall does not support use of this protocol, you can set the routers on either side of the PIX Firewall to use RIP between them and then run EIGRP on the rest of the network before the routers.
ESP	Encapsulated Security Protocol. Refer to RFC 1827 for more information.
FDDI	Fiber Distributed Data Interface—Fiber optic interface.
FTP	File Transfer Protocol—You can permit or deny access to this feature with the <b>aaa</b> , <b>conduit</b> , and <b>outbound</b> commands.
gaddr	Global address—An address set with the <b>global</b> and <b>static</b> commands.
GRE	Generic Routing Encapsulation protocol—Commonly used with Microsoft's implementation of PPTP. You can set access to this feature with the <b>conduit</b> command.
HSRP	Hot-Standby Routing Protocol.
HTTP	Hypertext Transfer Protocol—The service that handles access to the World Wide Web.
IANA	Internet Assigned Number Authority—Assigns all port and protocol numbers for use on the Internet. You can view port numbers at:  <a href="http://www.isi.edu/in-notes/iana/assignments/port-numbers">http://www.isi.edu/in-notes/iana/assignments/port-numbers</a>  You can view protocol numbers at:  <a href="http://www.isi.edu/in-notes/iana/assignments/protocol-numbers">http://www.isi.edu/in-notes/iana/assignments/protocol-numbers</a>
ICMP	Internet Control Message Protocol—This protocol is commonly used with the <b>ping</b> command. You can view ICMP traces through the PIX Firewall with the <b>debug trace on</b> command. Conduits can be pinged, but statics cannot. If an internal host needs to be pinged, you can provide this access with the <b>conduit</b> command by opening a port just for ICMP. Refer to RFC 792 for more information.
IGMP	Internet Group Management Protocol.
IGRP	Interior Gateway Routing Protocol.
IKE	Internet Key Exchange
IKMP	Internet Key Management Protocol
IP	Internet Protocol.
IPinIP	IP-in-IP encapsulation protocol.
IPSec	IP Security Protocol efforts in the IETF (Internet Engineering Task Force).
IRC	Internet Relay Chat protocol—The protocol that lets users access chat rooms. You can permit or deny access to this service with the <b>outbound</b> and <b>conduit</b> commands.
ISAKMP	Internet Security Association and Key Management Protocol
KDC	Key Distribution Center
laddr	Local address—The address of a host on a protected interface.

---

**Table B-1 Acronyms and Abbreviations (Continued)**

<b>Acronym</b>	<b>Description</b>
MD5	Message Digest 5—An encryption standard for encrypting VPN packets. This same encryption is used with the <b>aaa authentication console</b> command to encrypt Telnet sessions to the console.
MIB	Management Information Base—Used with SNMP.
MTU	maximum transmission unit—The maximum number of bytes in a packet that can flow efficiently across the network with best response time. For Ethernet, the default MTU is 1500 bytes, but each network can have different values, with serial connections having the smallest values. The MTU is described in RFC 1191.
NAT	Network Address Translation.
NIC	Network Information Center.
NNTP	Network News Transfer Protocol—News reader service. You can permit or deny access to this service with the <b>outbound</b> and <b>conduit</b> commands.
NOS	Network Operating System.
NTP	Network Time Protocol—Set system clocks via the network. You can permit or deny access to this service with the <b>outbound</b> and <b>conduit</b> commands.
NVT	Network virtual terminal.
OSPF	Open Shortest Path First protocol.
PIX	Private Internet Exchange.
PAT	Port Address Translation.
PFSS	PIX Firewall Syslog Server.
PKI	Public Key Infrastructure
POP	Post Office Protocol.
PPTP	Point-to-Point Tunneling Protocol.
RADIUS	Remote Authentication Dial-In User Service—User authentication server specified with the <b>aaa-server</b> command.
RAS	The registration, admission, and status protocol. Provided with H.323 support.
RFC	Request For Comment—RFCs are the defacto standards of networking protocols.
RIP	Routing Information Protocol.
RPC	Remote Procedure Call—You can permit or deny access to this service with the <b>outbound</b> and <b>conduit</b> commands.
SMTP	Simple Mail Transfer Protocol—Mail service. You can permit or deny access to this service with the <b>conduit</b> and the <b>fixup protocol smtp 25</b> command. The <b>fixup protocol smtp</b> command enables the Mail Guard feature. The PIX Firewall Mail Guard feature is compliant with both the RFC 1651 EHLO and RFC 821 section 4.5.1 commands.
SNMP	Simple Network Management Protocol—Set attributes with the <b>snmp-server</b> command.
SPI	Security parameter index—A number which, together with a destination IP address and security protocol, uniquely identifies a particular security association.

---

**Table B-1 Acronyms and Abbreviations (Continued)**

<b>Acronym</b>	<b>Description</b>
SQL*Net	SQL*Net is a protocol Oracle uses to communicate between client and server processes. (SQL stands for Structured Query Language.) The protocol consists of different packet types that PIX Firewall handles to make the data stream appear consistent to the Oracle applications on either side of the firewall. SQL*Net is enabled with the <b>fixup protocol sqlnet</b> command, which is provided in the default configuration. You can also specify access to SQL*Net with the <b>outbound</b> and <b>conduit</b> commands. Refer to the <b>outbound/apply</b> command page for more information on the <b>outbound</b> command.
SYN	Synchronize sequence numbers flag in the TCP header.
TACACS+	Terminal Access Controller Access Control System Plus.
TCP	Transmission Control Protocol. Refer to RFC 793 for more information.
TFTP	Trivial File Transfer Protocol.
TripleDES	Triple Data Encryption Standard. Also known as 3DES.
uauth	User authentication.
UDP	User Datagram Protocol.
VPN	Virtual Private Network.
WWW	World Wide Web.
XDMCP	X Display Manager Control Protocol.
xlate	Translation slot in PIX Firewall.