



Firewall Configuration Forms

Installing PIX Firewall requires a thorough knowledge of your company's network topology and security policy. To get the PIX Firewall running immediately, fill in the information in [Table A-1](#) to [Table A-4](#), and proceed to [Chapter 2, "Basic Firewall Configuration."](#) To configure the PIX Firewall for specific types of network traffic, fill in the information in [Table A-5](#) through [Table A-8](#), and follow the instructions in [Chapter 3, "Managing Network Access and Use."](#)

Information may not appear in the same order in the forms as it does in command syntax. page within the [Cisco PIX Firewall Command Reference](#) provides the complete syntax for all PIX Firewall commands.

This appendix includes the following sections:

- [PIX Firewall Network Interface Information](#)
- [Routing Information](#)
- [Network Address Translation](#)
- [Static Address Translation](#)
- [Inbound Access Control](#)
- [Outbound Access Control](#)
- [Authentication and Authorization](#)

For specific information about your network environment, contact your network administrator.

PIX Firewall Network Interface Information

Each PIX Firewall has two or more physical network interfaces. Configure each interface with an IP address, network speed, maximum transmission unit (MTU) size, and so on. Refer to page within the [Cisco PIX Firewall Command Reference](#) for complete information on the **interface** command. [Table A-1](#) provides a form for entering PIX Firewall network interface information.

Table A-1 PIX Firewall Network Interface Information

Interface Name	Interface Type	Hardware ID	Interface IP Address	Interface Speed	MTU Size	Interface Security Level
Outside						0
Inside						100

Routing Information

[Table A-2](#) provides a form for entering route information. Refer to the [Cisco PIX Firewall Command Reference](#) for complete information on the **route** command and the **rip** command. The router IP addresses should not be the same as the PIX Firewall interface IP address, or the same as any global address specified in [Table A-3](#).

Table A-2 Routing Information

Interface Name	Destination Network IP Address	Network Mask	Gateway (Router) IP Address	(RIP) Enable Passive Listening for Routing Information? (Yes, No)	(RIP) Broadcast This Interface as a Default Route? (Yes, No)

Inbound Access Control

Before attempting advanced configuration, we recommend completing the information on [Table A-1](#) to [Table A-4](#) and completing the instructions provided in [Chapter 2, “Basic Firewall Configuration.”](#) After completing and testing your basic configuration, complete the information in [Table A-6](#), which defines advanced configuration settings for inbound access control. Then refer to [Chapter 3, “Managing Network Access and Use,”](#) for instructions about how to use this information. Refer to the [Cisco PIX Firewall Command Reference](#) for complete information on the **access-list** and **access-group** commands.

To control access by IP address, configure an **access-list** command statement. To control access by user, set up authentication, as shown in [Table A-8](#). A global or static address should exist for an internal host or network before you can set up a **access-list** command statement. See [Table A-3](#) and [Table A-5](#) to configure a global or static entry for an internal host.

Table A-6 Inbound Access Control

Access List Identifier	Permit or Deny	Network Protocol: UDP, TCP, ICMP, or Number	Source Address: External Host or Network IP Address(es) and Network Mask	Destination Address: Static IP Address and Network Mask from Table A-5 ¹	Destination Ports ²	Interface To Bind List

1. Use the keyword “any” to specify all global IP addresses.
2. To specify a single port or a range of ports, you can use operands: greater than, less than, equal, not equal, and range.

The following is a list of literal port names that you can use when configuring an **access-list** command statement: DNS, ESP, FTP, H323, HTTP, IDENT, NNTP, NTP, POP2, POP3, PPTP, RPC, SMTP, SNMP, SNMPTRAP, SQLNET, TCP, Telnet, TFTP, and UDP. You can also specify these ports by number. Port numbers are defined in RFC 1700.

You should have two **access-list** command statement definitions to permit access to the following ports:

- DNS, Discard, Echo, Ident, NTP, RPC, SUNRPC, and Talk each require one definition for TCP and one for UDP.
- PPTP requires one definition for port 1723 on TCP and another for port 0 and GRE.
- TACACS+ requires one definition for port 65 on TCP and another for port 49 on UDP.

Outbound Access Control

Before performing advanced configuration, we recommend completing the information on [Table A-1](#) to [Table A-4](#) and completing the instructions provided in [Chapter 2, “Basic Firewall Configuration.”](#) After completing and testing your basic configuration, complete the information in [Table A-6](#), which defines advanced configuration settings for inbound access control. Then refer to [Chapter 3, “Managing Network Access and Use,”](#) for instructions about how to use this information. Refer to the [Cisco PIX Firewall Command Reference](#) for complete information on the **access-list** and **access-group** commands. To configure access control by IP address, complete the form provided in [Table A-7](#). To control access by user, set up authentication, as defined in [Table A-8](#).

Table A-7 Outbound Access Control

Access List Identifier	Permit or Deny	Network Protocol: UDP, TCP, or Number	Source Address: External Host or Network IP Address(es) and Network Mask	Destination Address or Network IP and Network Mask from Table A-5 ¹	Destination Ports (Services) ²	Interface To Bind Access List To

1. Use the keyword “any” to specify all global IP addresses.
2. To specify a single port or a range of ports, you can use operands: greater than, less than, equal, not equal, and range.

You can also specify a port with the source address, but this is seldom used.

Precede host addresses with the **host** parameter.

Use the interface name with the **access-group** command.

Refer to [Appendix D, “TCP/IP Reference Information,”](#) for a list of protocol values. In addition, you can specify protocols by number.

Authentication and Authorization

Before performing the advanced configuration defined in [Table A-8](#), we recommend completing the information on [Table A-1](#) to [Table A-4](#) and completing the instructions provided in [Chapter 2, “Basic Firewall Configuration.”](#) After completing and testing your basic configuration, complete the information in [Table A-7](#), which defines advanced configuration settings for inbound access control. Then refer to [Chapter 3, “Managing Network Access and Use,”](#) for instructions about how to use this information. Refer to the *Cisco PIX Firewall Command Reference* for complete information on the **aaa** command.

[Table A-8](#) defines the information needed applications that provide user authentication and authorization for network connections. Authentication servers include TACACS+ and RADIUS.



Note

If your configuration requires a host on an outside (lower security level) interface to initiate connections with a host on a local (higher security level) interface, create **static** and **access-list** command statements for that connection as defined in [Table A-5](#) and [Table A-6](#).

Prior to defining authentication and authorization requirements, identify the authentication server you are using, along with the IP address of the server, and the server encryption key on the PIX Firewall. Enter the information in the following form:

Authentication server (TACACS+ or RADIUS): _____

IP address: _____ Encryption key: _____

If you have additional authentication servers, list them separately.

Table A-8 Authentication and Authorization

Select Authentication or Authorization	Interface Name On Which to Authenticate or Authorize Connections	Protocol That Will Be Used to Provide Authentication: ANY, FTP, HTTP, TELNET	Authentication Server Type: TACACS+ or RADIUS	Local Host or Network IP Address ¹ and Network Mask	Foreign Host or Network IP Address ² and Network Mask

1. For a local interface, this is the internal host or network address from which connections originate. For an outside interface, this is the internal host or network address to which connections are sought.

2. For a local interface, this is the internal host or network address to which connections are sought. For an outside interface, this is the external host or network address from which connections originate.