

# Configuration Forms

---

PIX Firewall has multiple features and functions for controlling access to and from your company's network. Installing this product requires a thorough knowledge of your company's network topology and security policy. The forms in this appendix are provided for your convenience and can help you prepare for the PIX Firewall installation, making the process easier and faster.

You can configure the PIX Firewall for immediate operation and network protection using a small subset of the information requested in these forms. To get the PIX Firewall up and running immediately, fill in the information in Tables A-1 to A-4, and follow the configuration instructions in Chapter 2, "Configuring PIX Firewall," or use the PIX Firewall Setup Wizard program to complete the initial configuration.

The purpose of these forms is to capture the information you need to complete the initial configuration of your PIX Firewall unit, and to help gather the information you need for more complicated configuration tasks. The forms do not capture all options available with some of the configuration commands, such as the *em\_limit* and **norandomseq** options in the **nat** command. Additionally, the forms do not have one-to-one correspondence with PIX Firewall command syntax, meaning that information may not appear in the same order in the forms as it does in command syntax. Chapter 5, "Command Reference" has complete information on all PIX Firewall commands. Refer to these commands as needed during the actual installation process.

Cisco recommends completing the forms in the order presented, as later forms use information defined in earlier forms. After you complete the forms in Tables A-1 to A-4, you have the information you need to enter the PIX Firewall unit's initial configuration. With the initial configuration, you can test your PIX Firewall to verify the system is running properly in your network environment.

This appendix provides the following forms:

- PIX Firewall Network Interface Information
- Routing Information
- Outside (Global) Network Address or Address Range
- Inside (Local) or Perimeter Network Address Translation
- Static Address Mapping
- Conduit Configuration
- Access Control
- Authorization and Authentication Information

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. You must configure each interface with an IP address, network speed, maximum transmission unit (MTU) size, and so on. Refer to Chapter 5, “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 (Ethernet or Token Ring)	Hardware ID	Interface IP Address	Interface Speed	MTU Size	Interface Security Level
Outside		0				0
Inside		1				100

---

Each PIX Firewall interface requires a name. Outside is the default name for the PIX Firewall interface with the lowest security level (0) and which is typically the interface connection to the outside world. Inside is the default name for the PIX Firewall interface with the highest security level (100), making it the most secure interface connection to the inside (local) networks. If the PIX Firewall has three or more interfaces, choose names for the perimeter interfaces and assign a security level to each perimeter interface between 1 and 99. You can pick any number you choose, but for simplicity, we recommend when there are three interfaces, assign the third interface to security level 50. If there are four interfaces, use 40 for one and 60 for the other. Each security level must be unique.

Security levels become important when you need to permit users on one interface to access another. When accessing an interface with a higher security level from a lower level interface, you use the **static** and **conduit** commands. When accessing an interface with a lower security level from a higher level interface, you use the **nat** and **global** commands.

The PIX Firewall supports both Ethernet and Token Ring interfaces. The interface speed values for each type of interfaces are shown below:

- Ethernet
  - 10baseT—Set 10 Mbps Ethernet half-duplex communications.
  - 100baseTX—Set 100 Mbps Ethernet half-duplex communications.
  - 100full—Set 100 Mbps Ethernet full-duplex communications.
  - au—Set 10 Mbps Ethernet half-duplex communications for an AUI cable interface.
  - auto—Set Ethernet speed automatically. The auto keyword is valid only with the Intel 10/100 automatic speed sensing network interface card, which shipped with the PIX Firewall in units manufactured after November 1996.
  - bnc—Set 10 Mbps Ethernet half duplex communications for a BNC cable interface.
- Token Ring
  - 4mbps—Set 4 Mbps data transfer speed.
  - 16mbps—Set 16 Mbps (default) data transfer speed.

Set the hardware IDs sequentially; use ethernet0 for an Ethernet interface associated with the outside interface, or use token0 for a Token Ring interface associated with the interface named “outside.” Use ethernet1 for an Ethernet interface associated with the interface named “inside.” Continue the sequential numbering for each additional interface.

For the maximum transmission unit value, RFC 1191 [Mogul and Deering 1990] recommends 1,500 bytes for Ethernet, 17,914 for 16 Mbps Token Ring, and 4,464 for 4 Mbps Token Ring.

## Routing Information

Each inside or perimeter PIX Firewall interface is configurable for route and RIP (Routing Information Protocol) information. To determine what route information is required, consider what routers are in use in your network and are adjacent to the planned installation point of the firewall.

Specifying a route tells the PIX Firewall where to send information that is exiting a specific interface and destined for a particular network address. You can specify more than one route per interface, allowing you control over where to send network traffic. Configuring a route requires the following information: PIX Firewall interface name, destination network IP address, network mask, and IP address of the router (gateway) that routes traffic to the destination network. Refer to the **route** command for more information.

The PIX Firewall learns where everything is on the network by “passively” listening for RIP network traffic. When the PIX Firewall interface receives RIP traffic, the PIX Firewall updates its routing tables. You can also configure the PIX Firewall to broadcast an inside or perimeter interface as a “default” route. Broadcasting an interface as a default route is useful if you want all network traffic on that interface to go out through that interface. Refer to the **rip** command for more information.

Table A-2 provides a form for entering route information. Router IP addresses must 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)

When defining a route, you must specify the IP address and network mask for the destination network. Use 0.0.0.0 for both the IP address and network mask as the default value.

The gateway IP address is the router that routes the traffic to the destination network IP address.

The RIP information specifies whether the PIX Firewall updates its routing tables by passive listening to RIP traffic, and whether the interface broadcasts itself as a default route for network traffic on that interface. If you configure the PIX Firewall interface to listen for RIP updates, be sure to configure the router supplying the RIP information with the network address for the PIX Firewall interface.

---

**Note** Before testing your configuration, flush the ARP caches on any routers that feed traffic into or from the PIX Firewall and between the firewall and the Internet. For Cisco routers, use the **clear arp** command to flush the ARP cache.

---

## Network Address Translation

The Network Address Translation (NAT) feature works by substituting, or translating, host addresses on an internal interface with a “global address” associated with an outside interface. This protects internal host addresses from being exposed on other network interfaces. To understand whether you want to use NAT, you must decide if you want to expose internal addresses on other network interfaces connected to the PIX Firewall. If you choose to protect internal host addresses using NAT, you must identify the pool of addresses you want to use for translation.

If the addresses that you want to protect access only other networks within your organization, you can use any set of “private” addresses for the pool of translation addresses. For example, if you want to protect the host addresses on the Finance Department’s network (connected to the inside interface on the PIX Firewall) from exposure when connecting to the Sales Department network (connected to the perimeter interface on the PIX Firewall), you can set up translation using any available set of addresses on the Sales network. The effect is that hosts on the Finance network appear as local addresses on the Sales network.

If the addresses that you want to protect require Internet access, you must use only NIC-registered addresses (official Internet addresses registered with the Network Information Center for your organization) for the pool of translation addresses. For example, if you want to protect host addresses on the Sales network (connected to a perimeter interface of the PIX Firewall) from exposure when making connections to the Internet (accessible through the outside interface of the PIX Firewall), you can set up translation using a pool of registered addresses on the outside interface. The effect is that hosts on the Internet see the only the Internet addresses for the Sales network, not the addresses on the perimeter interface.

If you are installing the PIX Firewall in an established network that has host- or network-registered addresses, you might not want to do translation for those hosts or networks since that would require using another registered address for the translation.

When considering NAT, it is also important to consider whether you have an equal number of addresses for internal hosts. If not, some internal host might not get network access when making a connection. In this case you can either apply for additional NIC-registered addresses or use Port Address Translation (PAT).

Mapping a range of global IP addresses to an inside or perimeter address, or to a set of addresses, is known as Network Address Translation (NAT). Mapping a single global IP address to many inside or perimeter addresses is known as Port Address Translation (PAT). PAT extends the range of available outside addresses at your site by dynamically assigning unique port numbers to the outside address as a connection is requested. A single IP addresses has up to 64,000 ports that are available for making connections. For PAT, the port number uniquely identifies each connection.

The PIX Firewall associates internal addresses with global addresses using a NAT identifier (NAT ID). For example, if the inside interface has NAT ID5, then hosts making connections from the inside interface to another interface (perimeter or outside) get a substitute (translated) address from the pool of global addresses associated with NAT ID5.

If you decide not to use NAT to protect internal addresses from exposure on outside networks, you must assign those addresses NAT ID 0, which indicates to the PIX Firewall that translation is not provided for those addresses.





## Conduits

---

**Note** Table A-6 defines advanced configuration settings. Cisco recommends completing the initial (basic) installation from Tables A-1 to A-4 and testing the PIX Firewall with these configuration settings prior to configuring static address mappings and conduits. Refer to the Chapter 5, “Command Reference” for complete information on the **conduit** command.

---

The mechanism by which the PIX Firewall permits hosts on an outside interface to initiate connections with hosts on an inside interface is known as a conduit.

To understand whether you need to configure conduits at your site, you must decide if you want external hosts to access internal (PIX Firewall protected) hosts. By default, all external attempts to access internal hosts are denied, and you must configure specific access. If you want external hosts to access internal hosts or networks, you must consider whether you want to control access by IP address, or by both IP address and by user. To control access by IP address, you must configure a conduit. To control access by user, you must set up authentication, as shown in Table A-8.

A global or static address must exist for an internal host or network before you can set up a conduit. See Tables A-3 and A-5 to configure a global or static entry for an internal host. Use the deny option to create exceptions for broadly applied conduits. For example, you can configure one conduit that permits a host on the Internet (foreign host) to access your corporate (internal) network using any port service, while another conduit specifically denies that same outside host FTP services. Table A-6 provides a form for entering conduit information.

**Table A-6 Conduit Configuration**

Permit/Deny a Connection from this Outside Host	Network Protocol: ESP, UDP, TCP, GRE, PPTP or Number	Static IP Address and Network Mask from Table A-5 <sup>1</sup>	Ports (Services) Authorized for the Static IP Address <sup>2</sup>	Foreign Host or Network IP Address(es) and Network Mask	Ports (Services) Authorized for the Foreign IP Address <sup>2</sup>

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 a conduit: 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 must have two conduit 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.

---

## Access Control

---

**Note** Table A-7 defines advanced configuration settings. Cisco recommends completing the initial (basic) installation from Tables A-1 to A-4 and testing the PIX Firewall with configuration settings prior to configuring access control settings. Refer to the Chapter 5, “Command Reference” for complete information on the **conduit** command.

---

You can configure the PIX Firewall with access lists that permit, deny, or except (create an exception case) network connections or services. These services include World Wide Web (port 80), Telnet (port 23), H.323 (port 1720), and many others. For example, access control can permit a specific network or port access to the World Wide Web but deny that same network or port access to Java applet downloads.

To understand whether you need access control at your site, you must decide if you want to enforce restrictions on outbound network traffic; that is, network traffic initiated by hosts on an inside network to an outside network. By default, all internally initiated connections are allowed out, and you must configure restrictions. You can control access by IP address, or by both IP address and user authentication. To configure access control by IP address, follow the form provided in Table A-7. To control access by user, you must set up authentication, as defined in Table A-8.

**Table A-7** Access Control

Access Control List ID Number (1 to 65,000)	Host or Network IP Address on Which to Apply Access Control	Network Mask	Java <sup>1</sup> or Ports (Services) You Want to Control	Permit, deny, except <sup>2</sup> services	Protocol(s): UDP, TCP, ICMP, etc.	Comments

- 1 Java applet downloads are permitted by default; use the “java” keyword with “Deny” to block applet downloads from the IP address for this entry.
- 2 The **except** keyword creates an exception to a previously defined access control list, allowing more flexible control over broadly applied access control lists.

Refer to the “Protocols” section in Chapter 1, “Introduction” for a list of protocol values. In addition, you can specify protocols by number.

---

## Authentication and Authorization

---

**Note** Table A-8 defines advanced configuration settings. Cisco recommends completing the initial (basic) installation from Tables A-1 to A-4 and testing the PIX Firewall with configuration settings prior to configuring authentication and authorization settings. Refer to the Chapter 5, “Command Reference” for complete information on the **aaa** command.

---

If you want to control network access by user, or you want to authorize users for certain network services, use PIX Firewall authentication and authorization features.

Table A-8 defines the information needed applications that provide user authentication and authorization for network connections. Authentication servers include the Terminal Access Controller Access Control System Plus (TACACS+) developed by Cisco Systems, Inc.

Understanding the relative relationship of the PIX Firewall interfaces is important for configuring authentication or authorization schemes. In the PIX Firewall, you use two interfaces to make a connection from a local host or network to an outside, or foreign, host or network. The interface with the highest security level, relative to the two interfaces, is always the local interface. The interface with the lower security level, relative to two interfaces, is always the outside interface. Table A-1 defines the security level for each interface on the PIX Firewall.

If you want authentication and authorization to occur when a local host initiates a connection to the outside network, you configure the local interface. If you set up authentication and authorization to occur when an outside host initiates a connection, you configure the outside interface. In other words, you determine how to configure the interfaces based on the origination point of the connection.

---

**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, you must create a static and a conduit for that connection as defined in Tables A-3 and A-6.

---

Prior to defining authentication and authorization requirements, you must 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 below:

Authentication server (TACACS+ or RADIUS): \_\_\_\_\_

IP address: \_\_\_\_\_

Encryption key: \_\_\_\_\_

If you have additional authentication servers, list them separately. The PIX Firewall allows up to 16 authentication servers in the configuration.

