

Configuring and Testing PIX Firewall

You can configure PIX Firewall by entering commands on your console computer or terminal that are similar in context to those you use with Cisco routers.

Help Information

Help information is available by entering a question mark by itself for a listing of all commands, or with a command for command syntax. For example:

```
pixfirewall> int ?  
usage: interface ethernet inside|outside 10baseT|100baseTX|auto
```

Abbreviating Commands

You can abbreviate most commands down to the fewest unique characters for a command; for example, you can enter **wri te t** to view the configuration instead of entering the full command **write terminal**, or you can enter **en** to start privileged mode and **conf t** to start configuration mode.

Configuring PIX Firewall

Configuring PIX Firewall consists of the following steps:

- Step 1** Using the terminal or computer you connected to the console port during the PIX Firewall installation, connect to the firewall using a modem program such as Procomm.
- Step 2** Once you get to the unprivileged command prompt, which should appear as `pixfirewall>`, proceed to configuration mode by first entering the **enable** command and then the **config terminal** command.
- Step 3** Initially configure PIX Firewall using the commands described in the section that follows, “Initially Configuring the PIX Firewall.”
- Step 4** Exit configuration mode and save the configuration in flash memory with the **write memory** command.
- Step 5** Change the default privileged mode password with the **enable password** command.
- Step 6** Monitor the network interface traffic with the **show interface** command. If both interfaces show that packets are input and output, then the firewall is functioning. If not, ensure that the **interface** and **route** commands are specified correctly.
- Step 7** Use the **ping** command to ensure that hosts on the inside and outside of the network are visible to the firewall.

- Step 8** Test the network to ensure that you can ping between inside hosts, between outside hosts, and from an inside host to an outside host.

The configuration is now complete.

Connecting to the PIX Firewall

You can configure the PIX Firewall from the console or across the network with either Telnet or from a network browser such as Netscape Navigator. Before entering commands on the console, you need to have connected a workstation to the console port and started a modem program so that you can enter the initial configuration commands.

Before you can use Telnet, you need to enter the **telnet** command. Before you use a network browser, enter the **http** command. After you add these commands to the configuration, you can perform configuration remotely across the network.

Starting a Console Session

To start a console session, connect the console cable and start a terminal program such as Procomm. Set the baud rate to 9600, use 8 data bits, and no parity. Set the initialization string as follows so that the terminal program will communicate directly to the PIX Firewall instead of another modem:

```
ATE1V1X4Q0&C1&D2 S7=255 S0=0^M
```

Initially Configuring the PIX Firewall

Access configuration mode and enter the following commands to initially configure the firewall:

- 1 pixfirewall(config)# **interface ethernet inside auto**
- 2 pixfirewall(config)# **interface ethernet outside auto**
- 3 pixfirewall(config)# **ip address inside ip_address netmask**
- 4 pixfirewall(config)# **ip address outside ip_address netmask**
- 5 pixfirewall(config)# **nat 1 0.0.0.0**
- 6 pixfirewall(config)# **global 1 ip_address_pool**
- 7 pixfirewall(config)# **route inside router_ip_address**
- 8 pixfirewall(config)# **route outside router_ip_address**
- 9 pixfirewall(config)# **^z**
- 10 pixfirewall# **write memory**

Alternatively, you can enter lines 1 through 4 and then complete your configuration with a network browser and the HTTP configuration feature of PIX Firewall. Refer to the next section “Configuring with HTTP.” The use of the HTTP configuration feature also requires you to enter the **http** command as explained in “Configuring with HTTP.”

Line 1 indicates that you are using an Intel 10/100 automatic speed sensing network interface card. This statement and that in line 2 set the interface speed. If your system contains 3Com Ethernet boards, replace **auto** with **10baseT**. If your system contains Token-Ring cards, replace **ethernet** with **token** and **auto** with either **4mbps** or **16mbps**.

Lines 3 and 4 assign the IP addresses to the inside and outside network interface cards.

Line 5 disables network address translation until you can configure the system as required.

Line 6 assigns a pool of NIC-registered IP addresses for use by outbound connections. Enter a class address such as this example address of 192.168.42.0 to assign IP addresses 192.168.42.1 through 192.168.42.254.

Lines 7 and 8 let you assign default routes to the inside and outside network interfaces. If your system lets routers advertise default routes, these lines can be omitted.

Line 9 exits configuration mode and line 10 writes the current configuration to flash memory.

Configuring with HTTP

PIX Firewall provides a graphical user interface to help simplify configuration tasks. Once you have specified the network interface speed and IP addresses (as described in the last section), you need to enter two additional commands and you can then use a network browser, such as Netscape, to complete the configuration.

To access PIX Firewall from a network browser, enter these commands to specify an access password and your workstation's IP address and network mask:

```
pixfirewall(config)# passwd access_password  
pixfirewall(config)# http ip_address network_mask
```

At your workstation, start a network browser. Then open a URL and specify the IP address of the PIX Firewall's inside IP address.

The network browser then prompts you for a user name and password as shown in Figure 3-1.

Figure 3-1 HTML Management Interface User Name and Password Prompt



Always use **admin** for the user name and enter the password you specified with the **passwd** command.

The main configuration screen then appears as shown in Figure 3-2.

Figure 3-2 HTML Management Interface Configuration Screen

PIX Firewall Configuration Home

Welcome to the PIX Firewall configuration home page. This interface provides access to most of the features available in the command-line interface. The [PIX Firewall Configuration](#) page lets you view the current configuration. If you make changes, and click the submit button, the configuration is updated.

After you have completed the configuration, you should [save the new or changed configuration](#).

Additionally, you can view a snapshot of the current state of the PIX Firewall by clicking one of the options below. Note: If your browser supports client-pull (for example, Netscape), these pages refresh every 10 seconds. Otherwise, you must manually reload to view the current state.

- [ARP Tables](#)
- [Current Translations and Connections](#)
- [Routing Table](#)

© 1996 Cisco Systems, Inc.

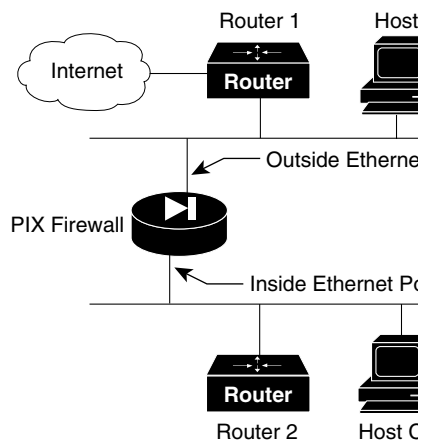
NMS518

Testing the Configuration

Note Use the PIX Firewall **ping** command to test network connections. Hosts on either side of the PIX Firewall cannot ping the opposite PIX Firewall Ethernet port.

The troubleshooting information in this section is based on Figure 3-3.

Figure 3-3 Example Network Setup



Use the steps that follow to determine that your PIX Firewall is ready for use.

- Step 1** Use the **show interface** command to ensure that the interface and line protocol are up. If the display contains “inside is up,” then the interface is functioning on the firewall. If the display contains “line protocol is up,” then the cable is correct and connected to the firewall. If both of these are true, ensure that packets are input and output. If this is occurring, the firewall is correctly configured and a cable is attached. However, even with these, the firewall may still not be reachable from other hosts.
- Step 2** Use the **show ip address** command to ensure that the IP address you expect is associated with each network interface.
- Step 3** Use the **show arp** command to see if ARP requests are being processed.
- Step 4** Can you ping the inside Ethernet port on the PIX Firewall from a host on the inside network? If no, the problem is on your internal network.
- Step 5** Can you ping another host on the same segment; for example, C to D? If no, the problem is on the inside network and not with the PIX Firewall. If yes, check the routing setup on the internal network(s). Check default gateways for the problem, if RIP listening is not in effect.
- Step 6** Can you ping the outside Ethernet port from a host on the outside network; for example, from A or B? If no, can you ping another host on the outside network; for example, A to B? If no, the problem is not the PIX Firewall but is on the outside network.
- Step 7** Can you ping a host on the outside segment from a host on the inside; for example D to A? If no, check the default gateways to the respective hosts if RIP listening is not in effect. If a router is present on the inside network, hosts on the inside segment must have gateways pointing to the router, and the router must point to the PIX Firewall. For example, the default routes for C and D must point to Router 2, and the default route for Router 2 must point to the PIX Firewall.

Adding to Your Configuration

Once your initial configuration is complete and tested, you should add commands to tailor the configuration for your site.

Table 3-1 lists configuration commands by PIX Firewall features.

Table 3-1 Configuration Commands by PIX Firewall Feature

Feature	Command	Access Mode
ARP cache:		
• Adjust	arp	Configuration
• Flush	clear arp-cache	Privileged
Configuration:		
• Read from floppy	conf floppy	Privileged
• Store on floppy	write floppy	Privileged
• View current configuration in RAM	write term	Privileged
Ethernet, configure	interface ethernet 10baseT	Configuration
Failover cable (optional):		
• Configure	failover	Configuration
• Force PIX Firewall to active	failover active	Configuration
• Force PIX Firewall to standby	no failover active	Configuration
• Show status	show failover	Unprivileged
Fast Ethernet, configure	interface ethernet auto	Configuration
Flash memory access:		
• Clear	write erase	Privileged
• Display configuration in flash memory	show configuration	Privileged
• Reload from	reload	Privileged
• Write to	write memory	Privileged
Floppy disk access:		
• Read from	configure floppy	Privileged
• Save configuration to	write floppy	Privileged
IP address, set	ip address	Configuration
Private Link		
• Age links	age	Configuration
• Configure	link and linkpath	Configuration
• V2 compatibility	lnko and lnkopath	Configuration
Processes, show thread information	show processes	Unprivileged
Prompt host name, change	hostname	Configuration
RIP listening, enable or disable	rip	Configuration
Routing table:		
• Adjust	ip route	Configuration
• Show	show ip route	Unprivileged

Feature	Command	Access Mode
Syslog:		
• Address, view	show ip address	Unprivileged
• Dump buffer to console	syslog console	Configuration
• Hosts, view current	show syslog	Unprivileged
• Messages, change facility and level	syslog output	Configuration
• Server, assign	syslog host	Configuration
Token Ring interface, configure	interface token	

Configuration Guidelines

Observe the following guidelines during configuration:

- If your network connects to the Internet, ensure that any global pool IP address you specify is NIC-registered.
- When you enter commands, you can erase characters with the Backspace key and with **^h**. You can erase the previous word with **^w** and erase the line with **^u**.

