This chapter covers the following exam topics for the Secure PIX Firewall Advanced Exam (CSPFA 9E0-511):

5. User interface
6. Configuring the PIX Firewall
8. Time setting and NTP support
13. DHCP server configuration

CHAPTER 6

Getting Started with the Cisco PIX Firewall

This chapter describes the basic preparation and configuration required to use the network firewall features of the Cisco PIX Firewall. It focuses on how to establish basic connectivity from the internal network to the public Internet.

"Do I Know This Already?" Quiz

The purpose of this quiz is to help you determine your current understanding of the topics covered in this chapter. Write down your answers and compare them to the answers in Appendix A. The concepts in this chapter are the foundation of much of what you need to understand to pass the CSPFA Certification Exam. Unless you do exceptionally well on the "Do I Know This Already?" pretest and are 100% confident in your knowledge of this area, you should read through the entire chapter.

1. How do you access privileged mode?
2. What is the function of the **nameif** command?
3. What six commands produce a basic working configuration for a Cisco PIX Firewall?
4. Why is the **route** command important?
5. What is the command to flush out the ARP cache on a Cisco PIX Firewall?
6. True or false: It is possible to configure the outside interface on a Cisco PIX Firewall to accept DHCP requests.
7. What type of environment uses the PIX DHCP client feature?
8. What command releases and renews an IP address on the PIX?
9. Give at least one reason why it is beneficial to use NTP on the Cisco PIX Firewall.
10. Why would you want to secure the NTP messages between the Cisco PIX Firewall and the NTP server?

Foundation Topics

Access Modes

The Cisco PIX Firewall contains a command set based on Cisco IOS Software technologies that provides three administrative access modes:

- Unprivileged mode is available when you first access the PIX Firewall through console or Telnet. It displays the > prompt. This mode lets you view only restricted settings.
- You access privileged mode by entering the **enable** command and the enable password. The prompt then changes to # from >. In this mode you can change a few of the current settings and view the existing Cisco PIX Firewall configuration. Any unprivileged command also works in privileged mode. To exit privileged mode, enter the **disable**, **exit**, or **^z** command.
- You access configuration mode by entering the **configure terminal** command. This changes the prompt to (config)# from #. In this mode you can change system configurations. All privileged, unprivileged, and configuration commands work in this mode. Use the **exit** or **^z** command to exit configuration mode.

NOTE PIX version 6.2 supports 16 privilege levels. This new feature allows Cisco PIX Firewall commands to be assigned to one of the 16 levels. These privilege levels can also be assigned to users. This is discussed in detail in Chapter 4, "System Maintenance."

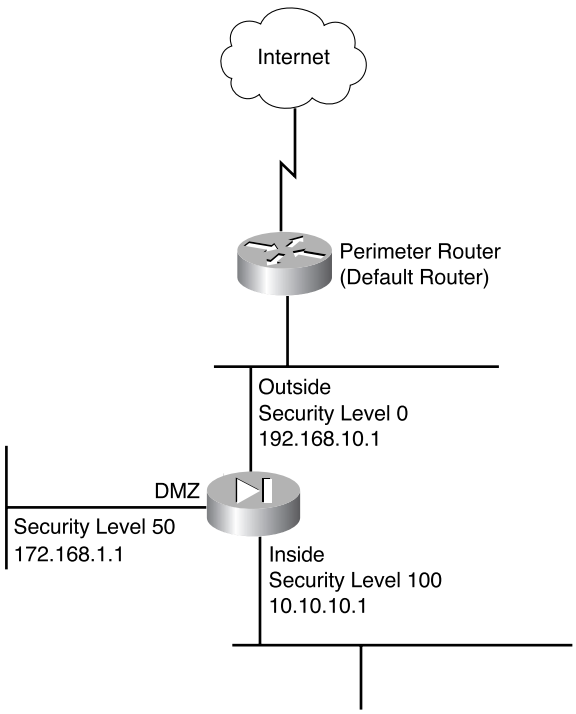
Configuring the PIX Firewall

Six important commands are used to produce a basic working configuration for the PIX Firewall:

interface
nameif
ip address
nat
global
route

Before you use these commands, it can prove very useful to draw a diagram of your Cisco PIX Firewall with the different security levels, interfaces, and IP addresses. Figure 6-1 shows one such diagram that is used for the discussion in this chapter.

Figure 6-1 *Documenting Cisco PIX Firewall Security Levels, Interfaces, and IP Addresses*



interface Command

The **interface** command identifies the interface hardware card, sets the speed of the interface, and enables the interface all in one command. All interfaces on a Cisco PIX Firewall are shut down by default and are explicitly enabled by the **interface** command. The basic syntax of the **interface** command is as follows:

```
interface hardware_id hardware_speed [shutdown]
```

Table 6-1 describes the command parameters for the **interface** command.

Table 6-1 **interface** *Command Parameters*

Command Parameter	Description
hardware_id	Indicates the interface's physical location on the Cisco PIX Firewall.
hardware_speed	Sets the connection speed, depending on which medium is being used. **1000auto** sets Ethernet speeds automatically. However, it is recommended that you configure the speed manually. **1000sxfull**—Sets full-duplex Gigabit Ethernet. **1000basesx**—Sets half-duplex Gigabit Ethernet. **1000auto**—Automatically detects and negotiates full-/half-duplex Gigabit Ethernet. **10baset**—Sets 10 Mbps half-duplex Ethernet (very rare these days). **10full**—Sets 10 Mbps full-duplex Ethernet. **100full**—Sets 100 Mbps full-duplex Ethernet. **100basetx**—Sets 100 Mbps half-duplex Ethernet. Make sure that the *hardware_speed* setting matches the port speed on the Catalyst switch the interface is connected to.
shutdown	The **shutdown** parameter administratively shuts down the interface. This parameter performs a very similar function in Cisco IOS Software. However, unlike with IOS, the command **no shutdown** cannot be used here. To place an interface in an administratively up mode, you reenter the **interface** command without the **shutdown** parameter.

Here are some examples of the **interface** command:

```
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full
```

nameif Command

As the name intuitively indicates, the **nameif** command is used to name an interface and assign a security value from 1 to 99. The outside and inside interfaces are named by default and have default security values of 0 and 100, respectively. By default, the interfaces have their hardware ID. Ethernet 0 is the outside interface, and Ethernet 1 is the inside interface. The names that are configured by the **nameif** command are user-friendly and are easier to use for advanced configuration later.

The syntax of the **nameif** command is

```
nameif hardware_id if_name security_level
```

Table 6-2 describes the command parameters for the **nameif** command.

Table 6-2 **nameif** *Command Parameters*

Command Parameter	Description
hardware_id	Indicates the interface's physical location on the Cisco PIX Firewall.
if_name	The name by which you refer to this interface. The name cannot have any spaces and must not exceed 48 characters.
security_level	A numerical value from 1 to 99 indicating the security level.

Here are some examples of the **nameif** command:

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security20
```

The *security_level* value controls how hosts/devices on the different interfaces interact with each other. By default, hosts/devices connected to interfaces with higher security levels can access hosts/devices connected to interfaces with lower-security interfaces. Hosts/devices connected to interfaces with lower-security interfaces cannot access hosts/devices connected to interfaces with higher-security interfaces without the assistance of access lists or conduits.

You can verify your configuration by using the **show nameif** command.

ip address Command

All the interfaces on the Cisco PIX Firewall that will be used must be configured with an IP address. The IP address can be configured manually or through Dynamic Host Configuration Protocol (DHCP). The DHCP feature is usually used on Cisco PIX Firewall small office/home office (SOHO) models. DHCP is discussed later in this chapter.

The **ip address** command is used to configure IP addresses on the PIX interfaces. The **ip address** command binds a logical address (IP address) to the hardware ID. Table 6-3 describes the parameters for the **ip address** command, the syntax of which is as follows:

```
ip address if_name ip_address [netmask]
```

Table 6-3 **ip address** *Command Parameters*

Command Parameter	Description
if_name	The interface name that was configured using the **nameif** command.
ip_address	The interface's IP address.
netmask	The appropriate network mask. If the mask value is not entered, the PIX assigns a classful network mask.

Here's an example of the **ip address** command:

```
ip address inside 10.10.10.14 255.255.255.0
```

Use the **show ip** command to view the configured IP address on the PIX interface.

nat Command

The **nat** (Network Address Translation) command lets you translate a set of IP addresses to another set of IP addresses.

NOTE PIX 6.2 supports bidirectional translation of inside network IP addresses to global IP addresses and translation of outside IP addresses to inside network IP addresses.

The **nat** command is always paired with a **global** command, with the exception of the **nat 0** command. Table 6-4 describes the command parameters for the **nat** command, the syntax of which is as follows:

```
nat (if_name) nat_id local_ip [netmask]
```

Table 6-4 **nat** *Command Parameters*

Command Parameter	Description
(if_name)	The internal network interface name.
nat_id	The ID number to match with the global address pool.
local_ip	The IP address that is translated. This is usually the inside network IP address. It is possible to assign all the inside network for the *local_ip* through **nat (inside) 1 0 0**.
netmask	Network mask for the local IP address.

Here are some examples of the **nat** command:

```
nat (inside) 1 10.10.10.0 255.255.255.0
nat (inside) 1 172.16.1.0 255.255.255.0
```

Chapter 5, "Understanding Cisco PIX Firewall Translation and Connections," discusses NAT in greater detail.

global Command

The **global** command is used to define the address or range of addresses that the addresses defined by the **nat** command are translated into. It is important that the *nat_id* be identical to the *nat_id* used in the **nat** command. The *nat_id* pairs the IP address defined by the **global** and **nat** commands so that network translation can take place. The syntax of the **global** command is

```
global (if_name) nat_id global_ip | global_ip-global_ip [netmask]
```

Table 6-5 describes the parameters and options for the **global** command.

Table 6-5 **global** *Command Parameters*

Command Parameter	Description
(if_name)	The external network where you use these global addresses.
nat_id	Identifies the global address and matches it with the **nat** command it is pairing with.
global_ip	A single IP address. When a single IP address is specified, the PIX automatically performs Port Address Translation (PAT). A warning message indicating that the PIX will PAT all addresses is displayed on the console.
global_ip-global_ip	Defines a range of global IP addresses to be used by the PIX to NAT.
netmask	The network mask for the global IP address(es).

There should be enough global IP addresses to match the local IP addresses specified by the **nat** command. If there aren't, you can leverage the shortage of global addresses by PAT entry, which permits up to 64,000 hosts to use a single IP address. PAT divides the available ports per global IP address into three ranges:

- 0 to 511
- 512 to 1023
- 1024 to 65535

PAT assigns a unique source port for each UDP or TCP session. It attempts to assign the same port value of the original request, but if the original source port has already been used, PAT starts scanning from the beginning of the particular port range to find the first available port and assigns it to the conversation. PAT has some restrictions in its use. For example, it cannot support H.323 or caching name server use. The following example shows a configuration using a range of global IP and single IP for PAT:

```
nat (inside) 1 10.0.0.0 255.0.0.0
global (outside) 1 192.168.10.15-192.168.1.62 netmask 255.255.255.0
global (outside) 1 192.168.10.65 netmask 255.255.255.0
```

When a host or device tries to start a connection, the PIX Firewall checks the translation table if there is an entry for that particular IP. If there is no existing translation, a new *translation slot* is created. The default time that a translated IP is kept in the translation table is 3 hours. You can change this with the **timeout xlate** *hh:mm:ss* command. To view the translated addresses, use the **show xlate** command.

route Command

The **route** command tells the Cisco PIX Firewall where to send information that is forwarded on a specific interface and that is destined for a particular network address. You add static routes to the PIX using the **route** command.

Table 6-6 describes the **route** command parameters, the syntax of which is as follows:

```
route if_name ip_address netmask gateway_ip [metric]
```

Table 6-6 **route** *Command Parameters*

Command Parameter	Description
if_name	The name of the interface where the data leaves from.
ip_address	The IP address to be routed.
netmask	The network mask of the IP address to be routed.
gateway_ip	The IP address of the next-hop address. Usually this is the IP address of the perimeter router.
metric	Specifies the number of hops to *gateway_ip*.

The following example shows a default route configuration on a Cisco PIX Firewall:

```
route outside 0.0.0.0 0.0.0.0 192.168.1.3 1
```

The **1** at the end indicates that the gateway router is only one hop away. If a metric is not specified in the **route** command, the default is 1. You can configure only one default route on the PIX Firewall. It is good practice to use the **clear arp** command to clear the PIX Firewall's ARP cache before testing your new route configuration.

RIP

The Routing Information Protocol (RIP) can be enabled to build the Cisco PIX Firewall routing table. RIP configuration specifies whether the PIX updates its routing tables by passively listening to RIP traffic and whether the interface broadcasts itself as a default route for network traffic on that interface. It is also important to configure the router providing the RIP updates with the network address of the PIX interface. The syntax to enable RIP is

```
rip if_name default | passive [version [1 | 2]] [authentication [text | md5
  key (key_id)]]
```

Table 6-7 describes the **rip** command parameters.

Table 6-7 **rip** *Command Parameters*

Command Parameter	Description
if_name	The interface name.
default	Broadcasts a default route on the interface.
passive	Enables passive RIP on the interface. The Cisco PIX Firewall listens for RIP routing broadcasts and uses that information to populate its routing tables.
version	The RIP version. Use **version 2** for RIP update encryption. Use **version 1** to provide backward compatibility with the older version.
authentication	Enables authentication for RIP version 2.
text	Sends RIP updates in clear text.
md5	Encrypts RIP updates using MD5 encryption.
key	The key to encrypt RIP updates. This value must be the same on the routers and on any other device that provides RIP version 2 updates. The *key* is a text string of up to 16 characters in length.
key_id	The key identification value. The key_id can be a number from 1 to 255. Use the same key_id that is in use on the routers and any other device that provides RIP version 2 updates.

Testing Your Configuration

Making sure that the configuration you entered works is an important part of the configuration process. At this point you would test basic connectivity from the inside interface out to the other interfaces. Use the **ping** and **debug** commands to test your connectivity.

The **ping** command sends an ICMP echo request message to the target IP and expects an ICMP echo reply. By default, the PIX denies all inbound traffic through the outside interface. Based on your network security policy, you should consider configuring the PIX to deny all ICMP traffic to the outside interface, or any other interface you deem necessary, by entering the **icmp** command. The **icmp** command controls ICMP traffic that terminates on the PIX. If no ICMP control list is configured, the PIX accepts all ICMP traffic that terminates at any interface (including the outside interface). For example, when you first configure the PIX, it is a good idea to be able to ping an interface and get a response. The following makes that possible for the outside interface:

```
icmp permit any any outside
```

NOTE **icmp permit any any outside** is used during the testing/debugging phase of your configuration process. Make sure that you change it to not responding to ping request after you complete testing. It is a security risk to leave it accepting and responding to ICMP packets.

After the **icmp permit** command has been configured, you can ping the outside interface on your Cisco PIX Firewall and ping from hosts on each firewall interface. For example:

```
ping outside 192.168.1.1
```

You can also monitor ping results by starting **debug icmp trace**.

Saving Your Configuration

Configuration changes that you have made stay in the PIX's RAM unless you save them to Flash memory. If for any reason the PIX must be rebooted, the configuration changes you made are lost. So when you finish entering commands in the configuration, save the changes to Flash memory with the **write memory** command, as follows:

```
Pix# write memory
```

NOTE There is one obvious advantage of not having configuration changes committed to Flash memory immediately. For example, if you make a configuration that you cannot back out of, you simply reboot and get back the settings you had before you made the changes.

You are now done configuring the Cisco PIX Firewall. This basic configuration lets protected network users start connections and prevents users on unprotected networks from accessing (or attacking) protected hosts.

Use the **write terminal** or **show running-config** command to view your current configuration.

Configuring DHCP on the Cisco PIX Firewall

The Cisco PIX Firewall has features that let it be configured as a:

- DHCP server
- DHCP client

Using the PIX Firewall DHCP Server

The DHCP server is usually used in SOHO environments with lower-end models of the Cisco PIX Firewall, such as the 501 and 506 units. Table 6-8 shows DHCP clients that are supported by PIX.

Table 6-8 *Cisco PIX Firewall DHCP Client Support*

PIX Firewall Version	Cisco PIX Firewall Platform	Maximum Number of DHCP Client Addresses (Active Hosts)
Version 5.2 and earlier	All platforms	10
Version 5.3 to version 6.0	PIX 506/506E	32
	All other platforms	256
Version 6.1 and higher	PIX 501	32
	PIX 501 with optional 50-user license	128
	PIX 506/506E	256
	All other platforms	256

The PIX DHCP server can be enabled only on the inside interface.

As with all other DHCP servers, you have to configure DNS, WINS, IP address lease time, and domain information on the PIX. Six steps are involved in enabling the DHCP server feature on the PIX:

Step 1 Enable the DHCP daemon on the Cisco PIX Firewall to listen to DHCP requests from clients:

```
dhcpd enable inside
```

Step 2 Specify the IP address range that the PIX DHCP server assigns:

```
dhcpd address 10.10.10.15-10.10.10.100 inside
```

Step 3 Specify the lease length to grant to the client. The default is 3600 seconds:

```
dhcpd lease 2700
```

Step 4 Specify a DNS server (optional):

```
dhcpd dns 192.168.10.68 192.168.10.73
```

Step 5 Specify WINS servers (optional):

```
dhcpd wins 192.168.10.66
```

Step 6 Configure the domain name the client uses (optional):

```
dhcpd domain axum.com
```

Configuring the PIX Firewall DHCP Client

DHCP client support on the Cisco PIX Firewall is designed for use by SOHO environments in which DSL and cable modems are used. The DHCP client can be enabled only on the PIX's outside interface. When the DHCP client is enabled, DHCP servers on the outside provide the outside interface with an IP address.

NOTE The DHCP client does not support failover configuration.

The DHCP client feature on your firewall is enabled by the **ip address dhcp** command:

```
ip address outside dhcp [setroute] [retry retry_cnt]
```

The **setroute** option tells the Cisco PIX Firewall to set its default route using the default gateway parameter that the DHCP server returns. Do not configure a default route when using the **setroute** option.

NOTE The same command, **ip address dhcp,** is used to release and renew the outside interface's IP address.

To view current information about the DHCP lease, enter the following command:

```
show ip address dhcp
```

Configuring Time Settings on the Cisco PIX Firewall

There are at least two ways in which the PIX gets its time setting information:

- NTP server
- System clock

Network Time Protocol (NTP)

The Network Time Protocol (NTP) is used to implement a hierarchical system of servers that provide a source for a precise synchronized time among network systems. It's important to maintain a consistent time throughout all network devices, such as servers, routers, and switches. When analyzing network events, logs are an important source of information. Analyzing and troubleshooting network events can be difficult is there is time inconsistency with network devices on the network. Furthermore, some time-sensitive operations, such as validating certificates and certificate revocation lists (CRLs), require precise time stamps.

NOTE The latest Cisco PIX Firewall OS, version 6.2, lets you obtain the system time from NTP version 3 servers. This feature is available only on Cisco PIX Firewall version 6.2.

The syntax to enable an NTP client on the PIX is

```
ntp server ip_address [key number] source if_name [prefer]
```

Table 6-9 describes the parameters of the **ntp** command.

Table 6-9 **ntp** *Command Parameters*

Command Parameter	Description
ip_address	This is the time server's IP address with which the PIX synchronizes.
key	This option requires an authentication key when sending packets to the NTP server.
number	The authentication key. This number is useful when you use multiple keys and multiple servers for identification purposes.
source	If the **source** keyword is not specified, the routing table is used to determine the interface.
if_name	The interface name used to send packets to the NTP server.
prefer	Reduces switching back and forth between servers by making the specified server the preferred time server.

Communication of messages between the PIX and the NTP servers can be authenticated to prevent the PIX from synchronizing time with rogue NTP servers. The three commands used to enable NTP authentication are as follows:

```
ntp authenticate
ntp authentication-key number md5 value
ntp trusted-key number
```

The **ntp authenticate** command enables NTP authentication and refuses synchronization to an NTP server unless the server is configured with one of the authentication keys specified using the **ntp trusted-key** command.

The **ntp authentication-key** command is used to define authentication keys for use with other NTP commands to provide a higher degree of security. The *number* parameter is the key number (1 to 4294967295). **md5** is the encryption algorithm. The *value* parameter is the key value (an arbitrary string of up to 32 characters).

The **ntp trusted-key** command is used to define one or more key numbers corresponding to the keys defined with the **ntp authentication-key** command. The Cisco PIX Firewall requires the NTP server to provide this key number in its NTP packets. This provides protection against synchronizing the PIX system clock with an NTP server that is not trusted.

To get remove NTP configuration, use the **clear ntp** command.

PIX Firewall System Clock

The second method of configuring the time setting on the PIX Firewall is the system clock. The system clock is usually set during the initial setup interview question when you're configuring a new Cisco PIX Firewall. You can change it later using the **clock set** command:

```
clock set hh:mm:ss month day year
```

Three characters are used for the *month* parameter. The *year* is a four-digit number. For example, to set the time and date to 17:51 and 20 seconds on April 9, 2003, you would enter

```
clock set 17:51:20 apr 9 2003
```

NOTE The system time, unlike NTP, is not synchronized with other network devices.

Cisco PIX Firewall version 6.2 has made some improvements to the **clock** command. The **clock** command now supports daylight saving (summer) time and time zones. To configure daylight saving time, enter the following command:

```
clock summer-time zone recurring [week day month hh:mm week day
  month hh:mm [offset]]
```

Table 6-10 describes the parameters for the **clock** command.

Table 6-10 **clock** *Command Parameters*

Command Parameter	Description
summer-time	Automatically switches to summer time (for display purposes only).
zone	The name of the time zone.
recurring	Indicates that summer time should start and end on the days specified by the values that follow this keyword. The summer time rule defaults to the United States rule.
week day	Sets the day of the week (Sunday, Monday).
month	The full name of the month, such as April.
hh:mm	The time in 24-hour military format.
offset	The number of minutes to add during summer. The default is 60 minutes.

Time zones are set just for the purpose of display. It does not change the internal PIX time, which remains universal time clock (UTC). To set the time zone, use the **clock timezone** command.

The following **clock summer-time** command specifies that summertime starts on the first Sunday in April at 2 a.m. and ends on the last Sunday in October at 2 a.m.:

```
pix(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday
  October 2:00
```

Sample PIX Configuration

Example 6-1 shows sample output for a PIX configuration. Can you identify some of the commands that have been discussed in this chapter?

Example 6-1 *Sample PIX Configuration*

```
pix# show config
: Saved
: Written by deguc at 11:29:39.859 EDT Fri Aug 8 2002
PIX Version 6.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security20
enable password GgtfiV2tiX5zk297 encrypted
passwd kP3Eex5gnkza7.w9 encrypted
hostname pixfirewall
domain-name axum.com
clock timezone EST -5
clock summer-time EDT recurring
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
pager lines 24
no logging on
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full
mtu outside 1500
mtu inside 1500
mtu dmz 1500
ip address outside 192.168.1.10.1 255.255.255.224
ip address inside 10.10.10.1 255.255.0.0
ip address dmz 172.16.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
pdm location 10.10.10.14 255.255.255.255 inside
arp timeout 14400
global (outside) 1 192.168.1.20-192.168.1.110 netmask 255.255.255.224
global (outside) 1 192.168.1.111
global (dmz) 1 172.16.1.10-172.16.1.20 netmask 255.255.255.224

nat (inside) 1 0.0.0.0 0.0.0.0 0 0
nat (dmz) 1 0.0.0.0 0.0.0.0 0 0
```

continues

Example 6-1 *Sample PIX Configuration (Continued)*

```
route outside 0.0.0.0 0.0.0.0 192.168.1.10.3 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00
  sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
 http server enable
http 10.10.10.14 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
no sysopt route dnat
telnet 10.10.10.14  255.255.255.255 inside
telnet timeout 5
 terminal width 80
Cryptochecksum:62a73076955b1060644fdba1da64b15f
```

Foundation Summary

Table 6-11 provides a quick reference to the commands needed to configure the Cisco PIX Firewall, time server and NTP support, and the DNS server.

Table 6-11 *Command Reference*

Command	Description
enable	Specifies to activate a process, mode, or privilege level.
interface	Identifies the speed and duplex settings of the network interface boards.
nameif	Lets you name interfaces and assign security levels.
ip address	Identifies addresses for network interfaces and lets you set how many times the PIX Firewall polls for DHCP information.
nat	Lets you associate a network with a pool of global IP addresses.
global	Defines a pool of global addresses. The global addresses in the pool provide an IP address for each outbound connection and for inbound connections resulting from outbound connections. Ensure that associated **nat** and **global** command statements have the same *nat_id*.
route	Used to enter a default or static route for an interface.
write terminal	Displays the current configuration on the terminal.
rip	Enables IP routing table updates from received RIP broadcasts.
dhcpd	Controls the DHCP server feature.
ntp server	Synchronizes the PIX Firewall with the network time server that is specified and authenticates according to the authentication options that are set.
clock	Lets you specify the time, month, day, and year for use with time-stamped syslog messages.

Q&A

The questions in this section are designed to ensure your understanding of the concepts discussed in this chapter and adequately prepare you to complete the exam. Use the simulated exams on the CD to practice for the exam.

The answers to these questions can be found in Appendix A.

1 What command tests connectivity?

   A **ping**

   B **nameif**

   C **ip address**

   D **write terminal**

2 What command saves the configuration you made on the Cisco PIX Firewall?

   A **write terminal**

   B **show start-running config**

   C **write memory**

   D **save config**

3 What command assigns security levels to interfaces on the PIX?

   A **ip address**

   B **route**

   C **nameif**

   D **secureif**

4 What command flushes the ARP cache on a PIX?

   A **flush arp cache**

   B **no arp cache**

   C **clear arp**

   D You cannot flush the ARP cache.

5 True or false: The DHCP client feature is primarily designed for large corporate enterprise networks and ISPs.

6 Why would you want authentication enabled between the PIX and the NTP server? (Select all that apply.)

A To ensure that the PIX does not synchronize with an unauthorized NTP server

B To maintain the integrity of the communication

C To increase the speed of communication

D To reduce latency

7 True or false: The DHCP client feature can be configured on the PIX's inside interface.

8 How do you access privileged mode?

A Enter the **enable** command and the enable password.

B Enter the **privilege** command and the privilege password.

C Enter the super-secret password.

D Enter the **privilege** command only.

9 How do you view the current configuration on your PIX? (Select all that apply.)

A **write terminal**

B **show current**

C **write memory**

D **save config**

10 In a DHCP client configuration, what is the command to release and renew the IP address on the outside interface?

A **ipconfig release**

B **ip address dhcp outside**

C **outside ip renew**

D **ip address renew outside**