This chapter covers the following subjects:

- User Interface
- Configuring the Cisco Security Appliance
- Time Settings and NTP Support

CHAPTER 6

Getting Started with the Cisco Security Appliance Family of Firewalls

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

How to Best Use This Chapter

This chapter provides an overview of the initial configuration steps required to get a Cisco Security Appliance operational. Besides explaining the basic configuration steps, it also explains the operation of the Security Appliance user interface. If you are at all familiar with the Security Appliance, you will probably find the topics in this chapter easy to understand. Test yourself with the "Do I Know This Already?" quiz.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide if you really need to read the entire chapter. If you already intend to read the entire chapter, you do not necessarily need to answer these questions now.

The ten-question quiz, derived from the major sections in the "Foundation Topics" portion of the chapter, helps you determine how to spend your limited study time. Table 6-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 6-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundations Topics Section	Questions Covered in This Section	Score
User Interface	5, 7	
Configuring the Security Appliance	1 to 4	
Configuring Transparent Mode	8	
Time Settings and NTP Support	6	
DHCP Server Configuration	9	

CAUTION The goal of self assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark this question wrong for purposes of the self assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which command tests connectivity?
   a. **ping**
   b. **nameif**
   c. **ip address**
   d. **write terminal**

2. Which 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. Which command assigns security levels to interfaces on the PIX Firewall?
   a. **ip address**
   b. **route**
   c. **security-level**
   d. **secureif**

4. Which command flushes the ARP cache of the PIX Firewall?
   a. **flush arp cache**
   b. **no arp cache**
   c. **clear arp**
   d. **You cannot flush the ARP cache**

5. Which of following configures a message when a firewall administrator enters the **enable** command?
   a. **banner motd enter the enable password**
   b. **banner enable enter the enable password**

c. **banner exec enter the enable password**

d. **banner login enter the enable password**

6. Why would you want authentication enabled between the PIX and the NTP server?

a. To ensure that the PIX does 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. How do you access the enable 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 only the command **privilege**.

8. How do you view the current configuration on your PIX Firewall?

a. **show running-config**

b. **show current**

c. **write memory**

d. **save config**

9. What command enables transparent mode?

a. **firewall mode transparent**

b. **firewall transparent**

c. **transparent enable**

d. **no ip firewall standard**

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**

The answers to the “Do I Know This Already?” quiz are found in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Q&A Sections.” The suggested choices for your next step are as follows:

- **8 or less overall score—**Read the entire chapter. This includes the “Foundation Topics,” “Foundation Summary,” and “Q&A” sections.
- **9 or 10 overall score—**If you want more review on these topics, skip to the “Foundation Summary” section and then go to the “Q&A” section. Otherwise, move to the next chapter.

Foundation Topics

Access Modes

The Cisco Security Appliance family of firewalls 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 Security Appliance 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 from > to #. In this mode, you can change a few of the current settings and view the existing Cisco Security Appliance configuration. Any unprivileged command also works in privileged mode. To exit privileged mode, enter the **disable** or **exit** command.
- You access configuration mode by entering the **configure terminal** command. This changes the prompt from # to (config)#. 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 and later, as well as ASA Security Appliance version 7.0 and later, supports 16 privilege levels. This feature enables you to assign Cisco Security Appliance commands to one of the 16 levels. These privilege levels can also be assigned to users. This is discussed in detail in Chapter 4, "System Management/ Maintenance."

Configuring a Cisco Security Appliance

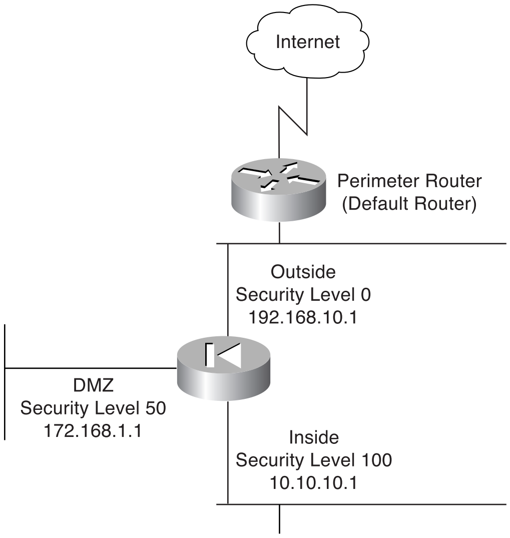
Eight important commands are used to produce a basic working configuration for a Security Appliance:

- **interface**
- **security-level**
- **nameif**
- **ip address**
- **nat**
- **nat-control**

- **global**
- **route**

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

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



interface Command

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

```
interface physical_interface[.subinterface] | mapped_name[shutdown]*
```

NOTE The **interface** command and the configuration of interfaces changed with software version 7.0. The method used to configure an interface is now similar to how you would configure an interface on Cisco IOS routers.

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

Table 6-2 *interface Command Parameters*

Command Parameter	Description
physical_interface	Indicates the interface's physical location on the Cisco Security Appliance. Based on your Security Appliance, the choices would be • **ethernet** • **gigabitethernet** • **management**
subinterface	(Optional) An integer between 1 and 4,294,967,293 designating a logical subinterface. This can be used with VLANs to create multiple VLAN segments on a single physical interface.
mapped_name	In multiple context mode, enter the mapped name if it was assigned using the **allocate-interface** command. This is described in more detail in Chapter 9, "Security Contexts."
shutdown	Administratively shuts down the interface. This parameter performs a very similar function in Cisco IOS Software. However, unlike with Cisco 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.

Example 6-1 shows some examples of the **interface** command.

Example 6-1 *Sample Configuration for the* **interface** *Command*

```
Pix(config)# interface ethernet0
Pix(config-if)# speed 100
Pix(config-if)# duplex full
```

You can only set the speed through two commands that must be used in the interface configuration mode. Use the **speed** command to set the speed of the interface, and use the **duplex** command to set the duplex of the interface.

security-level Command

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. The **security-level** command is new to version 7.0 and replaces the older **nameif** command feature that assigned the security level for an interface. Two interfaces, the **inside** and **outside** interfaces, have set security levels but can be overridden using this command. The **inside** interface has a default security level of 100; the **outside** interface has a default security level of 0. Newly added interfaces receive a default security level of 0. To assign a new security level to an interface, use the **security-level** command in the interface command mode. The syntax of the **security-level** command is as follows:

```
security-level number
```

where *number* can be a numerical value from 1 to 99 indicating the security level.

nameif Command

As the name intuitively indicates, the **nameif** command is used to name an interface. 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.

> **NOTE** The **nameif** command can also be used to assign security values of 0 and 100. The names "inside" and "outside" are merely reserved for security levels 100 and 0, respectively, and are assigned by default, but they can be changed.

To assign a name for an interface, use the command in interface configuration mode. The syntax of the **nameif** command is as follows:

```
nameif hardware-id if-name
```

Table 6-3 describes the command parameters for the **nameif** command.

Table 6-3 **nameif** *Command Parameters*

Command Parameter	Description
hardware-id	Indicates the interface's physical location on the Cisco Security Appliance.
if-name	Specifies the name by which you refer to this interface. The name cannot have any spaces and must not exceed 48 characters.

Example 6-2 shows some examples of the **nameif** command.

Example 6-2 *Sample Configuration for the* **nameif** *Command*

```
nameif ethernet0 outside
nameif ethernet1 inside
nameif ethernet2 dmz
```

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

ip address Command

All the interfaces on a Security Appliance 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 Security Appliance small office/home office (SOHO) models. DHCP is discussed later in this chapter.

The **ip address** command, while in interface configuration mode, is used to configure IP addresses on the Security Appliance interfaces. The **ip address** command binds a logical address (IP address) to the hardware ID. Additionally, you can use the **ip address** command to assign a standby IP address for a Security Appliance that will be used during a failover situation. Table 6-4 describes the parameters for the **ip address** command, the syntax of which is as follows:

```
ip address ip-address [netmask] [standby ip_address]
```

Table 6-4 ip address *Command Parameters*

Command Parameter	**Description**
ip-address	Specifies the IP address of the interface.
netmask	Specifies the appropriate network mask. If the mask value is not entered, the firewall assigns a classful network mask.
standby *ip_address*	Specifies the IP address for the standby unit for failover.

Example 6-3 shows configuration of the inside interface with an IP address of 10.10.10.14/24.

Example 6-3 *Sample Configuration for the* **ip address** *Command*

```
Pix(config)# interface ethernet0
Pix(config-if)# ip address 10.10.10.14  255.255.255.0
```

In addition to manually assigned IP addresses, the Security Appliance can act as a DHCP client. With version 7.0, the **ip address** command can use **dhcp** as an entry instead of an IP address.

This will allow a DHCP server to assign an IP address and netmask to the interface. A default gateway will also be assigned to the Security Appliance if it is required. You can flush and renew the IP address assignment through the DHCP server by reentering the **ip address dhcp** command.

Use the **show ip** command to view the configured IP address on a Security Appliance interface.

nat Command

The **nat** (Network Address Translation) command lets you dynamically translate a set of IP addresses (usually on the inside) to a global set of IP addresses.

> **NOTE** PIX version 6.2 and later support 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 6-5 describes the command parameters for the **nat** command, the syntax of which is as follows:

```
nat (if-name) nat-id local-ip [netmask] [dns] [[tcp] tcp_max_conns [emb_limit]
[norandomseq]]] [udp udp_max_conns]
```

Table 6-5 **nat** *Command Parameters*

Command Parameter	Description
(if-name)	Specifies the internal network interface name.
nat-id	Specifies the ID number to match with the global address pool.
local-ip	Specifies the IP address that is translated. This is usually the inside network IP address. It is possible to assign all of the inside network for the local-ip through **nat** (**inside**) **1 0 0**.
netmask	Specifies the network mask for the local IP address.
dns	Informs NAT[1] to use an existing translation to rewrite the DNS[2] address records.
tcp	Specifies that the maximum TCP connections and embryonic limit are set for the TCP protocol. This is optional.
tcp_max_conns	The maximum number of simultaneous TCP connections that the local_ip hosts allow. Idle connections are closed after the time that is specified. This is optional and used in conjunction with **tcp**.
emb_limit	The maximum number of embryonic connections per host. (An embryonic connection is a connection request that has not finished the necessary handshake between source and destination.) Set a small value for slower systems and a higher value for faster systems. The default is 0, which allows unlimited embryonic connections.
udp	Specifies a maximum number of UDP[3] connection parameters that can be configured. This is optional.
udp_max_conns	Sets the maximum number of simultaneous UDP connections that the local_IP hosts are each allowed to use. Idle connections are closed. This is optional and used in conjunction with **udp**.

[1] NAT = Network Address Translation

[2] DNS = Domain Name System

[3] UDP = User Datagram Protocol

Example 6-4 shows an example of the **nat** command.

Example 6-4 *Sample Configuration for the* **nat** *Command*

```
nat (inside) 1 10.10.10.0 255.255.255.0 0 0
nat (inside) 2 172.16.1.0 255.255.255.0 0 0
```

Chapter 5, "Understanding Cisco Security Appliance Translation and Connection," discusses NAT in greater detail.

Configuring Port Address Translation

Port Address Translation (PAT) can be configured using the same command as NAT. PAT maps a single global IP address to many local addresses. 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 address has up to 65,535 ports available for making connections. For PAT, the port number uniquely identifies each connection.

PAT translates a group of local addresses to a single global IP address with a unique source port (above 1024). When a local host accesses the destination network, the Firewall services module assigns it the global IP address and then a unique port number. Each host receives the same IP address, but because the source port numbers are unique, the responding traffic, which includes the IP address and port number as the destination, can be assigned to the correct host. It is highly unlikely that you would run out of addresses in PAT configuration because there are more than 64,000 ports available.

PAT enables you to use a single global address, thus conserving routable addresses. You can even use the destination actual interface IP address as the PAT IP address (this type of configuration is used, but not limited to, the outside interface). PAT does not work with multimedia applications that have an inbound data stream different from the outgoing control path.

In large enterprise environments, to use NAT, you must have a large number of routable addresses in the global pool. If the destination network requires registered addresses, such as the Internet, you might encounter a shortage of usable addresses. This can be a disadvantage.

PAT does not work with applications that have an inbound data stream on one port and the outgoing control path on another, such as multimedia applications. For those situations, it is more advantageous to use NAT. Example 6-5 shows a sample configuration for PAT.

Example 6-5 *Sample Configuration for Configuring PAT on the Inside Interface*

```
nat  (inside)  1  10.10.30.0  255.255.255.0
global  (outside)  1  interface
```

speed Command

The **speed** command is used to set the communication speed of the interface. The speed setting is only used on copper Ethernet interfaces (RJ-45), with the fiber Gigabit Ethernet interfaces set to a speed of 1000 Mbps by default using the nonegotiate syntax. You can use the **speed** command to set the speed on the interface to 10 Mbps or 100 Mbps. Additionally, you can set the **speed** command to autodetect the speed of the interface from the line connected to the interface using the **auto** syntax. Table 6-6 describes the command parameters for the **speed** command, which must be used in the interface configuration mode. The syntax for the speed command is as follows:

```
speed {auto | 10 | 100 | nonegotiate}
```

Table 6-6 speed *Command Parameters*

Command Parameter	Description
auto	Autodetects the speed of the interface.
10	Sets the speed to 10BASE-T (10 Mbps)
100	Sets the speed to 100BASE-T (100 Mbps)
nonegotiate	For SFP[1] media type, sets the speed to 1000 Mbps. SFP does not allow any other setting.

[1] SFP = Small Form-factor Pluggable

duplex Command

The **duplex** command is used to set an interfaces duplex mode. The duplex for an interface can be set manually by defining if the interface should be in half-duplex or full-duplex mode. Additionally, you can set the interface to autodetect the duplex from the line connected to the interface.

Table 6-7 describes the command parameters for the **duplex** command, which must be used in the interface configuration mode. The syntax for the **duplex** command is as follows:

```
duplex {auto | full | half}
```

Table 6-7 duplex *Command Parameters*

Command Parameter	Description
auto	Auto detects the duplex of the interface.
full	Sets the duplex to full duplex.
half	Sets the duplex to half duplex.

nat-control Command

The **nat-control** command is used to enforce address hinding on the inside and outside interfaces of a Security Appliance. With **nat-control** enabled, all packets that flow through the Security Appliance require a NAT rule, or the packets will be denied access through the appliance. If an inside NAT policy is enabled on an interface, each inside address must have an inside NAT rule configured or communication will not be permitted through the Security Appliance. Additionally, if an outside NAT policy is enabled on an interface, all outside addresses must have an outside NAT rule configured or communication will not be permitted through the Security Appliance.

The **nat-control** command is not enabled by default, requiring that only hosts that undergo NAT need a NAT rule.

global Command

The **global** command is used to define the address or range of addresses into which the addresses defined by the **nat** command are translated. 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 as follows:

```
global  (if-name) nat-id global-ip | global-ip-global-ip [netmask  netmask]
```

Table 6-8 describes the parameters and options for the **global** command.

Table 6-8 **global** *Command Parameters*

Command Parameter	Description
(if-name)	Specifies the external network where you use these global addresses.
nat-id	Identifies the global address and matches it with the **nat** command with which it is pairing.
global-ip	Specifies a single IP address. When a single IP address is specified, the Security Appliance automatically performs PAT. A warning message indicating that the Security Appliance will use PAT for 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	Specifies 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 are not, you can leverage the shortage of global addresses by PAT entry, which permits more than 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 65,535

PAT assigns a unique source port for each User Datagram Protocol (UDP) or Transmission Control Protocol (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 then assigns it to the conversation. PAT has some restrictions in its use. For example, it cannot support H.323. Example 6-6 shows a configuration using a range of global IP addresses and a single IP address for PAT.

Example 6-6 *Sample Configuration for NAT and PAT*

```
nat (inside) 1 10.0.0.0 255.0.0.0
global (outside) 1 192.168.100.20-192.168.100.50 netmask 255.255.255.0
global (outside) 1 192.168.100.55 netmask 255.255.255.0
```

When a host or device tries to start a connection, the Security Appliance checks the translation table to see whether there is an entry for that particular IP address. If there is no existing translation, a new *translation slot* is created. The default time that a translated IP address 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 Security Appliance 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 Security Appliance using the **route** command.

Table 6-9 describes the **route** command parameters, the syntax of which is as follows:

```
route if-name ip-address netmask gateway-ip [metric | tunneled]
```

Table 6-9 **route** *Command Parameters*

Command Parameter	Description
if-name	Specifies the name of the interface from which the data leaves.
ip-address	Specifies the IP address to be routed.
netmask	Specifies the network mask of the IP address to be routed.
gateway-ip	Specifies the IP address of the next-hop address. Usually, this is the IP address of the perimeter router.

Table 6-9 **route** *Command Parameters (Continued)*

metric	The administrative distance of this route. This can be used to create floating static routes.
tunneled	Specifies the route as the default tunnel gateway for VPN[1] traffic.

[1] VPN = virtual private network

Example 6-7 shows a default route configuration on a Cisco Security Appliance.

Example 6-7 *Default Route of 192.168.1.3*

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

NOTE On a Security Appliance, such as the PIX Firewall, several default routes are permitted. To allow more then a single default route, each additional default route must be set up as a floating static route.

The **1** at the end of the route 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 a Security Appliance. It is good practice to use the **clear arp** command to clear the Address Resolutions Protocol (ARP) cache of a Security Appliance before testing your new route configuration.

Routing Information Protocol

The Routing Information Protocol (RIP) can be enabled to build the Cisco Security Appliance routing table. RIP configuration specifies whether the Security Appliance 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. When using RIP version 2 with Security Appliance software versions earlier than 5.3, it is important to configure the router providing the RIP updates with the network address of the Security Appliance interface. The default version is 1 if not explicitly specified. The syntax to enable RIP is as follows:

```
rip if-name default | passive [version [1 | 2]] [authentication [text | md5
 key (key-id)]]
```

Table 6-10 describes the **rip** command parameters.

Table 6-10 **rip** *Command Parameters*

Command Parameter	Description
if-name	Specifies the interface name.
default	Broadcasts a default route on the interface.
passive	Enables passive RIP on the interface. The Cisco Security Appliance listens for RIP routing broadcasts and uses that information to populate its routing tables.
version	Specifies the RIP version number. Use version 2 for RIP update encryption. Use version 1 to provide backward compatibility with the earlier versions.
authentication	Enables authentication for RIP version 2.
text	Sends RIP updates in clear text.
md5	Encrypts RIP updates using MD5 encryption.
key	Specifies 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 up to 16 characters in length.
key-id	Specifies the key identification value. The *key-id* can be a number from 1 to 255. Use the same *key-id* that is used on the routers and any other device that provides RIP version 2 updates.

NOTE RIP is not supported in transparent mode. This is due to transparent mode relying on Layer 2 bridging instead of Layer 3 routing to pass packets.

Testing Your Configuration

Making sure that the configuration you entered works is an important part of the configuration process. At this point, you 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 Internet Control Message Protocol (ICMP) echo request message to the target IP address and expects an ICMP echo reply. By default, the Security Appliance denies all inbound traffic through the outside interface. Based on your network security policy, you should consider configuring the Security Appliance 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 Security Appliance. If no ICMP control list is configured, the Security Appliance accepts all ICMP traffic that terminates at any interface (including the outside interface). For example, when you first configure a PIX Firewall, 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
```

The **icmp permit any any outside** command is used during the testing/debugging phase of your configuration process. Make sure that you change it so it does not respond to ping requests after you complete testing. It is a security risk to leave it set to accept and respond to ICMP packets.

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

```
ping outside 192.168.1.1
```

You also can monitor ping results by starting **debug icmp trace**. The **debug** command will display messages that contain **icmp** type values. Table 6-11 describes the **icmp**-type values supported in version 7.0.

Table 6-11 **icmp** *Type Values*

Type Values	Description
0	Echo-reply
3	Unreachable
4	Source-quench
5	Redirect
6	Alternate-address
8	Echo
9	Router-advertisement
10	Router-solicitation
11	Time-exceeded
12	Parameter-problem
13	Timestamp-request
14	Timestamp-reply
15	Information-request
16	Information-reply
17	Mask-request
18	Mask-reply
31	Conversion-error
32	Mobile-redirect

Saving Your Configuration

Configuration changes that you have made stay in the random access memory (RAM) of the Security Appliance unless you save them to Flash memory. If for any reason the Security Appliance 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 by using 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 change that you cannot back out from, you simply reboot and return to the settings you had before you made the changes.

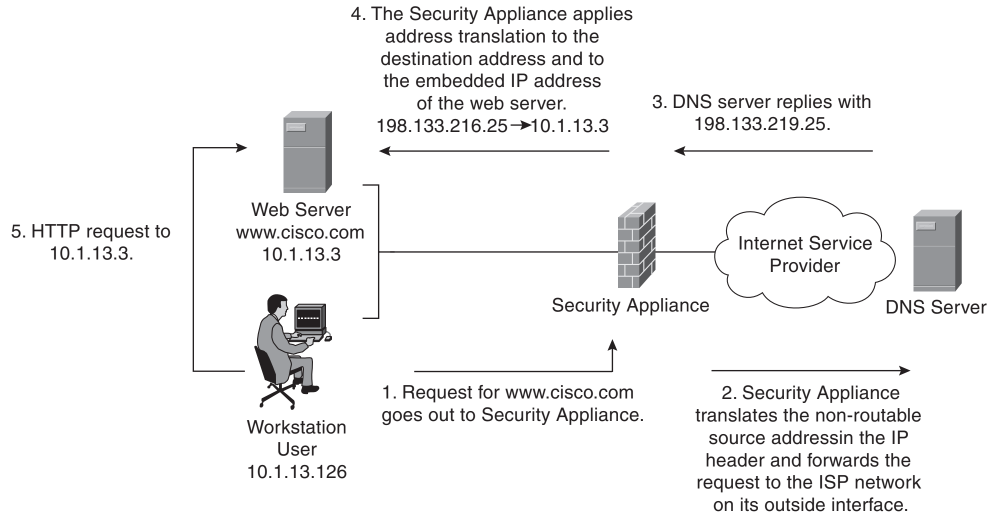
You are now finished configuring the Cisco Security Appliance. This basic configuration lets protected network users start connections and prevents users on unprotected networks from accessing (or attacking) protected hosts.

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

Support for Domain Name System Messages

Security Appliance fully supports NAT and PAT Domain Name System (DNS) messages originating from either a more secure interface or less secure interfaces. This means that if a client on an inside network requests DNS resolution of an inside address from a DNS server on an outside interface, the DNS record is translated correctly. To illustrate this point, Figure 6-2 shows a user from inside obtaining DNS resolution from the outside (maybe from an Internet service provider) for a web server on the inside. This process is called *DNS reply modification* or *DNS doctoring*.

Figure 6-2 *User Obtaining DNS Resolution from the Outside*


4. The Security Appliance applies address translation to the destination address and to the embedded IP address of the web server. 198.133.216.25→10.1.13.3
3. DNS server replies with 198.133.219.25.
5. HTTP request to 10.1.13.3.
Web Server www.cisco.com 10.1.13.3
Internet Service Provider
Security Appliance
DNS Server
Workstation User 10.1.13.126
1. Request for www.cisco.com goes out to Security Appliance.
2. Security Appliance translates the non-routable source addressin the IP header and forwards the request to the ISP network on its outside interface.

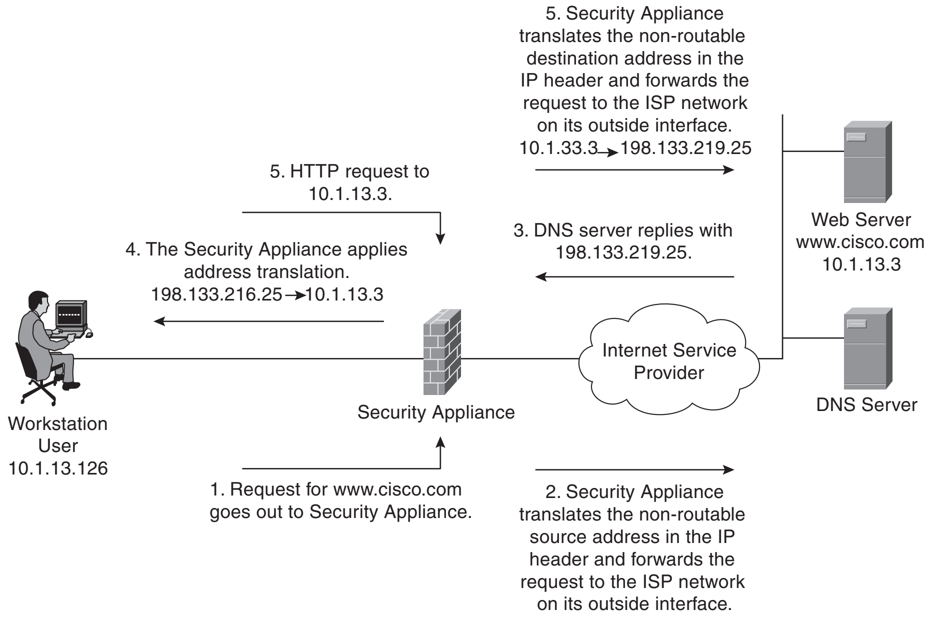
Before the release of version 7.0, you would use the **alias** command to modify DNS server replies. As for version 7.0, this feature has been integrated into the translation commands, such as the **static** command. Using the example shown in Figure 6-2, you would use the following command to create the DNS reply modification:

```
Pix(config)# static (inside,outside) 198.133.219.25 10.1.33.3 netmask 255.255.255.255
```

You can use DNS doctoring to manipulate the DNS replies for servers that exist outside your network, with **Outside NAT** enabled. Using this process will allow you to restrict your users to only destination IP addresses that reside on the Inside subnet, shielding them from the possibility of relying on outside DNS problems. Using the example shown in Figure 6-3, you would use the following command to create the DNS reply modification:

```
Pix(config)# static (outside,inside) 10.1.33.3 198.133.219.25 netmask
  255.255.255.255
```

Figure 6-3 *DNS Reply Modification Using Outside NAT*


5. Security Appliance translates the non-routable destination address in the IP header and forwards the request to the ISP network on its outside interface.
10.1.33.3 → 198.133.219.25
5. HTTP request to 10.1.13.3.
3. DNS server replies with 198.133.219.25.
Web Server
www.cisco.com
10.1.13.3
4. The Security Appliance applies address translation.
198.133.216.25 → 10.1.13.3
Internet Service Provider
Security Appliance
DNS Server
Workstation User
10.1.13.126
1. Request for www.cisco.com goes out to Security Appliance.
2. Security Appliance translates the non-routable source address in the IP header and forwards the request to the ISP network on its outside interface.

Configuring Dynamic Host Configuration Protocol on the Cisco Security Appliance

The Cisco Security Appliance can be configured as either of the following:

- DHCP server
- DHCP client

Using the Cisco Security Appliance DHCP Server

The DHCP server is usually used in, but not limited to, SOHO environments. The address pool of a Cisco Security Appliance DHCP server must be within the same subnet of the Security Appliance interface that is enabled, and you must specify the associated Security Appliance interface with *if- name*. In other words, the client must be physically connected to the subnet of a Security Appliance interface. The size of the pool is limited to 32 addresses with a 10-user license and 128 addresses with a 50-user license on the PIX 501. The unlimited user license on the PIX 501 and all other Security Appliance platforms supports 256 addresses. To configure DHCP on a Security Appliance, use the **dhcpd** command. The following is the syntax for the **dhcpd** command:

```
dhcpd address ip1[-ip2] if-name
dhcpd auto-config [outside]
dhcpd dns dns1 [dns2]
dhcpd wins wins1 [wins2]
dhcpd lease lease-length
dhcpd domain domain-name
dhcpd enable if-name
dhcpd option 66 ascii {server-name | server-ip-str}
dhcpd option 150 ip server-ip1 [ server-ip2]
dhcpd ping-timeout timeout
debug dhcpd event
debug dhcpd packet
```

Table 6-12 describes the different **dhcpd** command parameters.

Table 6-12 **dhcpd** *Command Parameters*

Parameter	Description
address *ip1*- [*ip2*]	Specifies the IP pool address range.
auto-config	Enables the Security Appliance to configure DNS, Windows Internet Naming Service (WINS), and domain name values automatically from the DHCP client to the DHCP server. If the user also specifies DNS, WINS, and domain parameters, the command-line interface (CLI) parameters overwrite the **auto-config** parameters.
binding	Specifies the binding information for a given server IP address and its associated client hardware address and lease length.
code	Specifies the DHCP option code, either 66 or 150.
dns *dns1* [*dns2*]	Specifies the IP addresses of the DNS servers for the DHCP client.
domain*domain-name*	Specifies the DNS domain name; for example, cspfa2.com.
if-name	Specifies the interface on which to enable the DHCP server.
lease *lease-length*	Specifies the length of the lease, in seconds, granted to the DHCP client from the DHCP server. The lease indicates how long the client can use the assigned IP address. The default is 3600 seconds. The minimum lease length is 300 seconds, and the maximum lease length is 2,147,483,647 seconds.
option 150	Specifies the Trivial File Transfer Protocol (TFTP) server IP address(es) designated for Cisco IP Phones in dotted-decimal format. DHCP **option 150** is site-specific; it gives the IP addresses of a list of TFTP servers.
option 66	Specifies the TFTP server IP address designated for Cisco IP Phones and gives the IP address or the host name of a single TFTP server.
outside	Specifies the outside interface of the firewall.
ping-timeout	Specifies the timeout value of a ping, in milliseconds, before an IP address is assigned to a DHCP client.
server-ip(1,2)	Specifies the IP address(es) of a TFTP server.

continues

Table 6-12 **dhcpd** *Command Parameters (Continued)*

Parameter	**Description**
server-ip-str	Specifies the TFTP server in dotted-decimal format, such as 1.1.1.1, which is treated as a character string by the Security Appliance DHCP server.
server-name	Specifies an American Standard Code for Information Interchange (ASCII) character string representing the TFTP server.
statistics	Provides statistical information, such as address pool, number of bindings, malformed messages, sent messages, and received messages.
wins *wins1 [wins2]*	Specifies the IP addresses of the Microsoft NetBIOS name servers (Windows Internet Naming Service servers). The second server address is optional.

In addition to supporting a DHCP client and DHCP server configuration, the Security Appliance also supports a DHCP relay configuration. The DHCP relay configuration enables the Security Appliance to assist in dynamic configuration of IP device hosts on any Ethernet interface. When the Cisco Security Appliance receives a request from a host on an interface, it forwards the request to a user-configured DHCP server on another interface. The DHCP relay agent is a feature that is provided by security software version 6.3.

A Security Appliance allows any number of integrated DHCP servers to be configured, and on any interface. The DHCP client can be configured only on the outside interface, and the DHCP relay agent can be configured on any interface. The DHCP server and DHCP relay agent cannot be configured concurrently on the same Security Appliance, but the DHCP client and DHCP relay agent can be configured concurrently.

As with all other DHCP servers, DNS, Windows Internet Naming Service (WINS), IP address lease time, and domain information on the Security Appliance can be configured. The following six steps are required to enable the DHCP server feature on the Security Appliance:

Step 1 Enable the DHCP daemon on the Cisco Security Appliance to listen to DHCP requests from clients:

```
pix(config)#dhcpd enable inside
```

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

```
pix(config)#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):

```
pix(config)#dhcpd lease 2700
```

Step 4 Specify a DNS server (optional):

```
pix(config)#dhcpd dns 192.168.10.68 192.168.10.73
```

Step 5 Specify a WINS server (optional):

```
pix(config)#dhcpd wins 192.168.10.66
```

Step 6 Configure the domain name the client will use (optional):

```
pix(config)#dhcpd domain axum.com
```

Configuring the Security Appliance DHCP Client

DHCP client support on the Cisco Security appliance is designed for use in SOHO environments in which digital subscriber line (DSL) and cable modems are used. The DHCP client can be enabled only on the outside interface of the Security Appliance. 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 a Security Appliance is enabled by the **ip address dhcp** command:

```
ip address dhcp [setroute] [retry retry-cnt]
```

The **setroute** option tells the Cisco Security Appliance 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 **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 outside dhcp
```

The partial configuration in Example 6-8 demonstrates how to use three new features that are associated with each other: DHCP server, DHCP client, and PAT using the interface IP address to configure a Security Appliance in a SOHO environment with the inside interface as the DHCP server.

Example 6-8 *Sample Configuration for the* **dhcpd** *Command*

```
ip address dhcp setroute
ip address 10.100.1.1 255.255.255.0
dhcpd address 10.100.1.50-10.100.1.60 inside
dhcpd dns 192.168.1.106 192.168.1.107
dhcpd wins 192.168.1.106
dhcpd lease 1200
dhcpd domain cspfa.com
dhcpd enable inside
nat (inside) 1 0 0
global (outside) 1 interface
```

> **NOTE** To configure DHCP client features for a VPN connection, you must use **dhcp-server** command in a tunnel-group. This will assign an IP address from an outside DHCP server. The **ip address dhcp** command cannot be used in this way.

Configuring Time Settings on the Cisco Security Appliance

The Security Appliance obtains its time setting information in two ways:

- By Network Time Protocol (NTP) server
- By system clock

NTP

The NTP is used to implement a hierarchical system of servers that provide a source for a precise synchronized time among network systems. It is 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 if there is a time inconsistency between network devices on the network. Furthermore, some time-sensitive operations, such as validating certificates and certificate revocation lists (CRLs), require precise time stamps.

Cisco PIX Firewall version 6.2 and later, as well as ASA Security version 7.0, enable you obtain the system time from NTP version 3 servers.

The syntax to enable an NTP client on the Security Appliance is as follows:

```
ntp server ip-address [key number] source if-name [prefer]
```

Table 6-13 describes the parameters of the **ntp** command.

Table 6-13 **ntp** *Command Parameters*

CommandParameter	Description
ip-address	Specifies the IP address of the time server with which the Security Appliance synchronizes.
key	This keyword indicates that you are configuring the NTP client to use the specified authentication key (identified by number) when sending packets to the NTP server.
number	Specifies the authentication key. This value is useful when you use multiple keys and multiple servers for identification purposes.
source	Specifies the interface. If the **source** keyword is not specified, the routing table is used to determine the interface.
if-name	Specifies the interface name used to send packets to the NTP server.
prefer	Specifies the preferred time server. This option reduces switching back and forth between servers by making the specified server the preferred time server.

Communication of messages between the Security Appliance and the NTP servers can be authenticated to prevent the Security Appliance 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
```

NOTE NTP uses port 123 for communication.

The **ntp authenticate** command enables NTP authentication and refuses synchronization with 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 4,294,967,295). The **md5** option 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 that the NTP server is required to provide in its NTP packets for the Security Appliance to accept synchronization with that NTP server. The Cisco Security Appliance requires the NTP server to provide this key number in its NTP packets, which provides protection against synchronizing the Security Appliance system clock with an NTP server that is not trusted.

NTP configuration on the Security Appliance can be verified and viewed by using the following **show** commands:

- The **show ntp** command displays the current NTP configuration.
- The **show ntp associations** [**detail**] command displays the configured network time server associations.
- The **show ntp status** command displays the NTP clock information.

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

Cisco Security Appliance System Clock

The second method of configuring the time setting on the Security Appliance is by using the system clock. The system clock is usually set when you answer the initial setup interview question when you are configuring a new Cisco Security Appliance. 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 the following:

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

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

Cisco PIX Firewall version 6.2 included 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 weekday month hh:mm week weekday
 month hh:mm [offset]]
```

Table 6-14 describes the parameters for the **clock** command.

Table 6-14 **clock** *Command Parameters*

Command Parameter	Description
summer-time	Automatically switches to summer time (for display purposes only).
zone	Specifies 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.

Table 6-14 **clock** *Command Parameters (Continued)*

CommandParameter	Description
week	Specifies the week of the month. The week is 1 through 4.
week day	Sets the day of the week (Sunday, Monday).
month	Specifies the full name of the month, such as April.
hh:mm	Specifies the time in 24-hour clock format.
offset	Specifies the number of minutes to add during summer. The default is 60 minutes.

Time zones are set only for display. Setting a time zone does not change the internal Security Appliance time, which is kept according to Coordinated Universal Time (UTC). To set the time zone, use the **clock timezone** command. The syntax for the command is as follows:

```
clock timezone zone hours [minutes]
```

The following **clock summer-time** command specifies that summer time 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
```

You can check your clock configuration by simply entering the **show clock** command as shown in Example 6-9.

Example 6-9 **show clock** *Sample Output*

```
PIXFW# show clock
10:04:06.334 PDI Thu Feb 13 2004
```

NOTE In 2007, the United States will be extending Daylight Savings Time (DST) by a month. Starting in 2007, DST will start on the second Sunday in March and will end on the first Sunday in November. The following **clock** command will set the Security Appliance to the new DST setting (to be precise, summer begins on June 21, or thereabouts):

```
pix(config)# clock summer-time PDT recurring 2 Sunday March 2:00 1 Sunday
November 2:00
```

Configuring Login Banners on the Cisco Security Appliance

PIX Firewall version 6.3 introduced support for message-of-the-day (MOTD), EXEC, and login banners, similar to the feature included in Cisco IOS Software. Banner size is limited only by available system memory or Flash memory.

You can create a message as a warning for unauthorized use of the firewall. In some jurisdictions, civil and/or criminal prosecution of crackers who break into your system are made easier if you have incorporated a warning banner that informs unauthorized users that their attempts to access the system are in fact unauthorized. In other jurisdictions, you may be forbidden to monitor the activities of even unauthorized users unless you have taken steps to notify them of your intent to do so. One way of providing this notification is to put the information into a banner message configured with the Security Appliance **banner** command.

Legal notification requirements are complex and vary in each jurisdiction and situation. Even within jurisdictions, legal opinions vary, and this issue should be discussed with your own legal counsel. In cooperation with counsel, you should consider which of the following information should be put into your banner:

- A notice that the system can be logged in to or used only by specifically authorized personnel, and perhaps information about who may authorize use
- A notice that any unauthorized use of the system is unlawful and may be subject to civil and/or criminal penalties
- A notice that any use of the system may be logged or monitored without further notice and that the resulting logs may be used as evidence in court
- Specific notices required by specific local laws

From a security, rather than a legal, point of view, your login banner usually should not contain any specific information about your router, its name, its model, what software it is running, or who owns it; such information may be abused by crackers.

The banner messages can be displayed when a user enters privileged EXEC mode, upon line activation, on an incoming connection to a virtual terminal, or as a MOTD. To create a banner message, use the following command:

```
banner {exec | login | motd} text
```

Table 6-15 describes the parameters of the **banner** command.

Table 6-15 **banner** *Command Parameters*

Parameter	Description
exec	Configures the system to display a banner before displaying the enable prompt.
Login	Configures the system to display a banner before the password login prompt when accessing the firewall using Telnet.
motd	Configures the system to display a MOTD banner.
text	Specifies the line of message text to be displayed in the firewall command-line interface. Subsequent *text* entries are added to the end of an existing banner unless the banner is cleared first. The tokens $(domain) and $(hostname) are replaced with the host name and domain name of the firewall.

Spaces are allowed, but tabs cannot be entered using the CLI. You can dynamically add the host name or domain name of the Security Appliance by including $(hostname) and $(domain) in the string. Example 6-10 shows a sample configuration using the **banner** command.

Example 6-10 *A Sample Configuration of the **banner** Command*

```
pixfw(config)# banner login Warning Notice
This is a U.S. Government computer system, which may be accessed and used only
for authorized Government business by authorized personnel. Unauthorized access
or use of this computer system may subject violators to criminal, civil, and/or
administrative action.
All information on this computer system may be intercepted, recorded, read, copied,
and disclosed by and to authorized personnel for official purposes, including criminal
investigations. Such information includes sensitive data encrypted to comply with
confidentiality and privacy requirements. Access or use of this computer system
by any person, whether authorized or unauthorized, constitutes consent to these
 terms. There is no right of privacy in this system.    ^d
```

To replace a banner, use the **no banner** command before adding the new lines. The **no banner** {**exec** | **login** | **motd**} command removes all the lines for the banner option specified. The **no banner** command removes all the lines for the banner option specified and does not selectively delete text strings. The **clear banner** command removes all the banners.

Configuring Transparent Mode

With the release of Security software version 7.0, a Security Appliance can run as a Layer 2 firewall. Standard firewalls act in a similar fashion as a router, routing packets through the firewall instead of switching them. This creates an extra hop in the IP path that a user can detect. With transparent firewall enabled, the Security Appliance will act as a Layer 2 filtering bridge, switching the packets instead of routing them, and the user will not see an additional hop within the IP path. This allows the Security Appliance to bridge packets from one interface to another, instead of routing them. These interfaces are usually on the same VLAN or IP subnet.

Because transparent firewalls perform MAC address lookup instead of routing, a Security Appliance with this feature enabled can be placed in a network without a need to reconfigure any part of the network, including NAT or IP readdressing. With the change from routing to switching, enabling transparent firewalling removes or restricts support for several Security Appliance features:

- **Interface limits—**A Security Appliance with transparent firewalls enabled can only use two interfaces. Each interface must be on a different VLAN to support transparent firewalls. This restriction is based on a single context. If multiple contexts have been enabled, each context created can use only two interfaces. These interfaces can only be used by one context and cannot be shared between multiple contexts in transparent mode.

- **NAT—**NAT does not apply when the Security Appliance is running in a Layer 2 mode. NAT would be done by a Layer 3 device in this design.
- **Dynamic routing protocols—**Because the Security Appliance is set to be a bridge, dynamic routing protocols are not needed, as they are used in an environment to assist in routing packets. Static routes can be configured for traffic that may originate from the Security Appliance.
- **IPv6—**IPv6 is not supported due to transparent mode working at Layer 2 and not Layer 3.
- **DHCP relay—**The Security Appliance cannot act as a DHCP relay, although it can act as a DHCP server.
- **Quality of service (QoS)—**Most QoS options rely on the TCP header, which is not used in transparent mode.
- **Multicast—**Multicast traffic is not supported by default in transparent mode. To pass multicast traffic through the Security Appliance in transparent mode, you must use extended access lists.
- **VPN termination for through traffic—**The Security Appliance with transparent firewalls enabled can only support site-to-site VPN tunnels for the management connections.

A Security Appliance in transparent mode can still run virtual firewalls. Each context must be configured with an IP address to use for management access. This IP address assigned to the port must be part of the connecting network, since the Security Appliance cannot route a subnet that is not directly connected. Additionally, each connecting network must reside in the same subnet to be supported in transparent mode.

NOTE A Security Appliance can be set to either transparent or router mode. If multiple contexts are enabled, all contexts must be set to the same mode.

The bridging of traffic by the Security Appliance does not work like a normal switch by default. A Security Appliance in transparent mode will only pass ARP traffic between the two interfaces until an extended access list or EtherType access list is configured. With either of these access lists configured, you can allow Layer 3 traffic to pass through the Security Appliance.

Enabling Transparent Mode

When you decide to enable transparent mode, ensure that your configuration has been backed up. When this feature is enabled, it will clear the current configuration to avoid any command conflicts that may exist with the currently deployed configuration. To enable transparent mode, use the **firewall transparent** command in the global configuration mode. If you are using multiple contexts, you must execute this command in the system configuration mode, which will affect all configured contexts. Use the **show firewall** command in privileged mode to verify that the firewall has accepted the new transparent mode, as shown in Example 6-11.

Example 6-11 *Enabling Transparent Mode Output*

```
Pix(config)# firewall transparent
Pix(config)# exit
Pix# show firewall
Firewall mode: Transparent
```

The last configuration required to enable transparent mode is to assign an IP address to an interface for management access to the Security Context:

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

This will allow you to manage the Security Appliance remotely. The IP address will also be used as the source address for any traffic that originates from the Security Appliance, or for syslog and Simple Network Management Protocol (SNMP) alarm messages. If you are using multiple contexts, you must assign an IP address for each context configured. To configure an IP address, use the **ip address** command in global-configuration mode. The IP address used must be in the same subnet as a network directly connected to the Security Appliance. You can display the current management-port configuration using the **show ip address** command in privileged mode, as shown in Example 6-12. Example 6-13 uses the same process but in multicontext mode.

Example 6-12 *Assigning an IP Address to Management Port in Single-Context Mode*

```
Pix(config)# ip address 10.10.10.1 255.255.255.0
Pix(config)# exit
Pix# show ip address
     Management System IP Address:
     ip address 10.10.10.1 255.255.255.0
Management Current IP Address:
     ip address 10.10.10.1 255.255.255.0
```

Example 6-13 *Assigning an IP Address to Management Ports in Multiple-Context Mode*

```
Pix/admin(config)# ip address 10.10.10.1 255.255.255.0
Pix/admin(config)# changeto context1
Pix/context1(config)# ip address 10.10.11.1 255.255.255.0
Pix/context1(config)# changeto context2
Pix/context2(config)# ip address 10.10.12.1 255.255.255.0
```

Traffic Management in Transparent Mode

Now that you have transparent mode enabled on the Security Appliance, you must allow more than just ARP traffic through the firewall. Extended access lists must be configured for each traffic type you wish to allow through the firewall. For non-IP traffic, you must configure EtherType access lists. Both types of access lists, once configured, must be assigned to one of the two interfaces, or both, to be enabled. The syntax for extended access lists is the same as those used in nontransparent mode, and detailed configuration of these access lists can be found in Chapter 7, "Configuring Access." EtherType access lists are used when non-IP traffic is required to pass through the firewall. EtherType access lists are connectionless and must be applied to both interfaces to operate correctly. To create an EtherType access list, use the **ethertype** attribute with the **access-list** command:

```
access-list id ethertype {deny | permit}{ipx | bpdu | mpls-unicast | mpls-multicast | any
| hex_number}
```

Table 6-16 describes the parameters for the **access-list ethertype** command.

Table 6-16 **access-list ethertype** *Command Parameters*

Parameter	Description
id	Name or number of an access list.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
ipx	Specifies access to IPX.
npdu	Specifies access to bridge protocol data units.
mpls-unicast	Specifies access to MPLS unicast.
mpls-multicast	Specifies access to MPLS multicast.
any	Specifies access to anyone.
hex_number	A 16-bit hexadecimal number greater than or equal to 0x600 by which an EtherType can be identified.

NOTE In transparent mode, the Security Appliance relies on EtherTypes to determine traffic selection. This forces the Security Appliance to only pass Ethernet II frames, due to 802.3 frames requiring a length field instead of EtherType.

Remember that the Security Appliance defaults do not allow any non-ARP traffic through the firewall.

You can manage the ARP traffic through inspection on the Security Appliance. Inspection can help restrict malicious users from attempting ARP floods on or through the firewall or connected networks. Using the **arp-inspection** command in global-configuration mode, you can check each request to flood ARP requests through an interface for mismatched IP addresses, MAC addresses, or fake interfaces, and you can drop the request packets before they can cause problems. The full command syntax for the **arp-inspection** command is as follows:

```
arp-inspection interface_name enable [flood | no-flood]
```

Table 6-17 describes the parameters for the **arp-inspection ethertype** command.

Table 6-17 **arp-inspection ethertype** *Command Parameters*

Parameter	Description
interface_name	The interface on which you want ARP inspection.
enable	Enables ARP inspection.
flood	(Default) Specifies that packets not matching any element of a static ARP entry are flooded out of all interfaces except the originating interface. If a mismatch occurs between the MAC address, IP address, or interface, the Security Appliance drops the packet.
no-flood	(Optional) Specifies that packets not exactly matching a static ARP entry are dropped.

Monitoring in Transparent Mode

All traffic flows based on MAC address lookup via bridging. MAC addresses are either statically assigned by the administrator or dynamically learned through traffic over an interface. The Security Appliance lists all known MAC addresses in the MAC address table. This table is used by the Security Appliance to switch traffic that passes through it, based on any filters applied to each interface. To display the current MAC address table, you can use the **show mac-address-table** command in privileged mode, as shown in Example 6-14.

Example 6-14 **show mac-address-table** *Command Output*

```
pix# show mac-address-table
interface mac  address         type      Age(min)
inside  0010.7cbe.6101         static
inside  0008.e3bc.5ee0         dynamic    5
outside 0050.8DFB.19C2         dynamic    5
```

The Security Appliance will learn MAC addresses from the interface by default. This can be a dangerous setting to allow on a secured network. If a malicious user spoofed (faked) the MAC address of a network device already connected to the network, or just used a random MAC address, that user could gain access to the secured network. The Security Appliance would see the new MAC address and add it to the MAC table, giving the user access to that part of the network. You can disable the Security Appliance's ability to learn new MAC addresses using the **mac-learn** command in global-configuration mode:

```
mac-learn interface_name disable
```

This will allow only static MAC addresses into the MAC address table. If the same malicious user attempted to spoof the MAC address of an entry in the static table but on the wrong interface, or tried to use a random MAC address not in the table, the MAC address and all packets from that user would be dropped. An administrator can assign static MAC addresses through the following command:

```
mac-address-table static interface_name mac_address
```

Sample Security Appliance Configuration

Examples 6-15 and 6-16 show sample output for a Security Appliance configuration in routed and transparent mode. Included are some of the commands discussed in this chapter.

Example 6-15 *Sample PIX Configuration in Routed Mode*

```
pix#  show  config
: Saved
: Written by deguc at 11:29:39.859 EDT Fri Aug 8 2005
PIX Version 7.0(4)
interface Ethernet 0
 nameif outside
 security-level 0
 speed 100
 duplex full
 ip address 192.168.1.1 255.255.255.224
interface Ethernet 1
 nameif inside
 security-level 100
 speed 100
 duplex full
 interface Ethernet 2
 nameif dmz
 security-level 20
 speed 100
 duplex full
enable password GgtfiV2tiXAndr3w encrypted
passwd kP3Eex5gnkza7.lan encrypted
```

Example 6-15 *Sample PIX Configuration in Routed Mode (Continued)*

```
hostname pix
domain-name axum.com clock timezone EST -5
clock summer-time EDT recurring
class-map ips_class
   match access-list IPS
class-map inspection_default
   match default-inspection-traffic
policy-map global_policy
   class inspection_default
      inspect dns maximum length 512
      inspect ftp
      inspect h323 h225
      inspect h323 ras
      inspect netbios
      inspect sunrpc
      inspect rsh
      inspect rtsp
      inspect sip
      inspect skinny
      inspect esmtp
      inspect sqlnet
      inspect tftp
      inspect xdmcp
      inspect icmp
   class ips-class
      ips promiscuous fail-close
service-policy global_policy global
Hyphenate in command, as for "service-policy"?
access-list IPS permit ip any any
pager lines 24
no logging on
ip audit info action alarm
ip audit attack action alarm no failover

route outside 0.0.0.0 0.0.0.0 192.168.1.3 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
```

continues

Example 6-15 *Sample PIX Configuration in Routed Mode (Continued)*

```
no snmp-server enable traps
telnet 10.10.10.14  255.255.255.255 inside
telnet timeout 5
 terminal width 80
Cryptochecksum:62a73076955b1060644fdba1da64b15f
```

Example 6-16 *Sample PIX Configuration in Transparent Mode*

```
pix# show config
: Saved
: Written by deguc at 11:49:39.859 EDT Fri Aug 8 2005
PIX Version 7.0(4)
interface Ethernet 0
 nameif outside
 security-level 0
 speed 100
 duplex full
interface Ethernet 1
 nameif inside
 security-level 100
 speed 100
 duplex full
interface Ethernet 2
 speed 100
 duplex full
 shutdown
enable password GgtfiV2tiXAndr3w encrypted
passwd kP3Eex5gnkza7.lan encrypted
firewall transparent
hostname pix
domain-name axum.com clock timezone EST -5
clock summer-time EDT recurring
ip address 192.168.1.1 255.255.255.0
route outside 0.0.0.0 0.0.0.0 192.168.1.3 1
telnet 10.10.10.14  255.255.255.255 inside
arp outside 198.168.1.1 0009.7cbe.2100
arp-inspection outside enable
access-list ACLIN permit icmp 192.168.1.0 255.255.255.0 192.168.1.0 255.255.255.0
access-list ETHER ethertype permit ipx
access-group ETHER in interface inside
access-group ETHER in interface outside
access-group ACLIN in interface inside
access-group ACLIN in interface outside
pager lines 24
no logging on
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
```

Example 6-16 *Sample PIX Configuration in Transparent Mode (Continued)*

```
         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
        no snmp-server location
        no snmp-server contact
        snmp-server community public
        no snmp-server enable traps
        telnet timeout 5
         terminal width 80
Cryptochecksum:62a73076955b1060644fdba1da64b15f
```

Foundation Summary

The "Foundation Summary" provides a convenient review of many key concepts in this chapter. If you are already comfortable with the topics in this chapter, this summary can help you recall a few details. If you just read this chapter, this review should help solidify some key facts. If you are doing your final preparation before the exam, this summary provides a convenient way to review the day before the exam.

Table 6-18 provides a quick reference to the commands needed to configure the Cisco Security Appliance, time server support, and the DHCP server.

Table 6-18 *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.
security-level	Assigns a security level to an interface.
nameif	Enables you to name interfaces.
ip address	Identifies addresses for network interfaces and enables you to set how many times the PIX Firewall polls for DHCP information.
nat	Enables you to 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	Specifies 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 Security Appliance 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.

With software version 7.0, Cisco Security Appliances can now support transparent firewalls. You can configure the Security Appliance to bridge traffic at Layer 2 instead of route traffic to allow for seamless integration into an existing network. Layer 3 traffic can pass through a transparent firewall through access lists and connection tables, the same as in routed mode.

Q&A

As mentioned in the Introduction, the questions in this book are more difficult than what you should experience on the exam. The questions are designed to ensure your understanding of the concepts discussed in this chapter and adequately prepare you to complete the exam. You should use the simulated exams on the CD to practice for the exam.

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

1. How do you access privileged mode?
2. What is the function of the **nameif** command?
3. Which seven commands produce a basic working configuration for a Cisco Security Appliance?
4. Why is the **route** command important?
5. What is the command to flush out the ARP cache on a Cisco PIX Firewall?
6. What is the syntax to configure a MOTD banner that says, "System shall not be available on 18:00 Monday January 19th for 2 hours due to system maintenance?"
7. What is the command used to configure PAT on a Cisco Security Appliance?
8. Which 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?
11. What is the difference between a Security Appliance in transparent mode and a Security Appliance in routed mode?