

PIX Security Appliance Contexts, Failover, and Management

Upon completion of this chapter, you should be able to answer the following questions:

- How do I configure a Pix Security Appliance to perform in multiple context mode?
- How do I configure a PIX Security Appliance failover?
- How do I configure transparent firewall mode?
- What is PIX Security Appliance management?

Key Terms

This chapter uses the following key terms. You can find the definitions in the glossary at the end of the book.

security contexts page 718

transparent firewall mode page 718

failover protection page 718

Secure Shell (SSH) page 741

This chapter provides an overview and explanation of *security contexts*. You can partition a single PIX Security Appliance into multiple virtual firewalls, known as security contexts. Each context is an independent firewall, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone firewalls. This chapter continues with a discussion of configuring and managing of security contexts.

A firewall system working properly provides network protection against many threats. What happens when a power loss occurs, or some other problem, to the firewall? Is network protection to be sacrificed to preserve network availability, or should the network be protected by cutting links until the problem is fixed? Fortunately, you can avoid these situations by establishing *failover protection* to keep the system going in the event of a firewall failure.

This chapter introduces you to the two methods of PIX Security Appliance failover: hardware failover and stateful failover. Instructions are given on how to configure each one of these in a network environment.

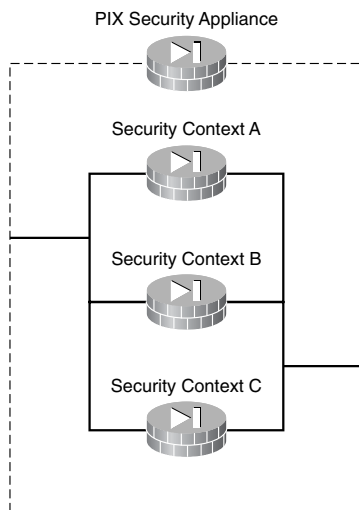
This chapter also provides a discussion of *transparent firewall mode*. A transparent firewall is a Layer 2 firewall that is not seen as a router hop to connected devices. Because the PIX Security Appliance is not a routed hop, a transparent firewall can easily be introduced into an existing network.

The last topic covered in this chapter is PIX Security Appliance management. You learn how to conduct system management via remote access, how to configure a PIX Security Appliance to support command authorization, and how to perform image and activation key upgrades on PIX Security Appliances. Because password recovery is important to the management of PIX Security Appliances, this chapter includes step-by-step instructions on how to accomplish password recovery.

Configure a PIX Security Appliance to Perform in Multiple Context Mode

You can partition a single PIX Security Appliance into multiple virtual firewalls, known as security contexts, as shown in Figure 8-1. Each context is an independent firewall, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone PIX Security Appliances.

Each context has its own configuration that identifies the security policy, interfaces, and almost all the options that can be configured on a standalone PIX Security Appliance. If desired, individual context administrators can be allowed to implement the security policy on the context. Some resources are controlled by the overall system administrator, such as VLANs and system resources, so that one context cannot affect other contexts inadvertently.

Figure 8-1 Security Contexts

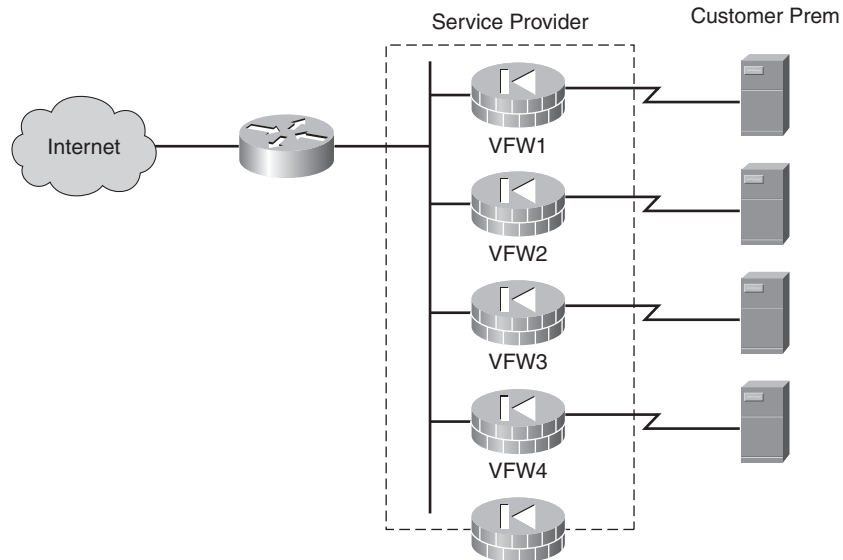
The system administrator adds and manages contexts by configuring them in the system configuration, which identifies basic settings for the PIX Security Appliance. The system administrator has privileges to manage all contexts. The system configuration does not include any network interfaces or network settings for itself. Instead, when the system needs to access network resources, such as downloading the contexts from the server, it uses one of the contexts that is designated as the admin context.

The admin context is just like any other context, except that when a user logs in to the admin context, for example, over an Secure Shell (SSH) connection, that user has system administrator rights and can access the system execution space and all other contexts. Typically, the admin context provides network access to networkwide resources, such as a syslog server or context configuration server.

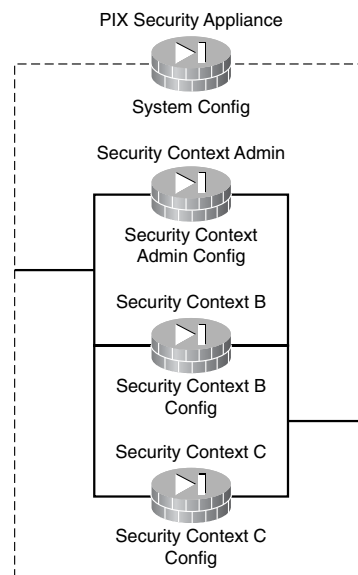
Just a few situations that call for the consideration of using multiple security contexts are as follows:

- A service provider wanting to sell firewall services to many customers
- A large enterprise or a college campus wanting to keep departments completely separate

In the example in Figure 8-2, a service provider is using a single PIX Security Appliance divided into multiple contexts to deliver the same service as multiple standalone small PIX units. By enabling multiple security contexts on the PIX, the service provider can implement a cost-effective, space-saving solution that keeps all customer traffic separate and secure (and also eases configuration).

Figure 8-2 Multiple Contexts Example

Each context has its own configuration file that identifies the security policy, interfaces, and almost all the options that you can configure on a standalone PIX Security Appliance. The firewall appliance also includes a system configuration that identifies basic setting for the appliance, including a list of contexts, as shown in Figure 8-3. Context configurations can be stored on the local disk partition on the Flash memory card or they can be downloaded from a TFTP, FTP, or HTTP(S) server.

Figure 8-3 Context Configuration Files

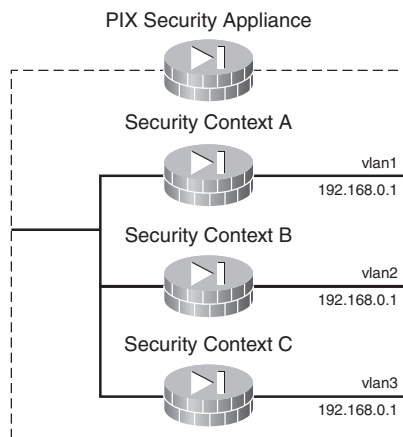
In addition to individual security contexts, the firewall appliance also includes a system configuration that identifies basic settings for the firewall appliance, including a list of contexts. Like the single-mode configuration, this configuration resides as the “startup” configuration in the Flash partition.

Each packet that enters the PIX Security Appliance must be classified so that the PIX can determine to which context to send a packet. The PIX checks for the following characteristics:

- Source interface, the source VLAN
- Destination address

The PIX Security Appliance uses the characteristic that is unique and not shared across contexts. For example, if a VLAN is shared across contexts, the classifier uses the IP address. A VLAN interface can be shared as long as each IP address space on that VLAN is unique, or overlapping IP addresses can be used as long as the VLANs are unique. The example in Figure 8-4 shows multiple contexts sharing an outside VLAN, while the inside VLANs are unique, allowing overlapping IP address.

Figure 8-4 Packet Classification

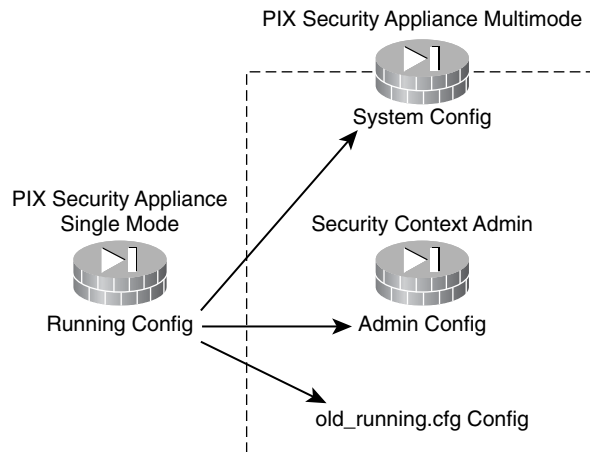


Enabling Multiple Context Mode

When the PIX Security Appliance is changed from single mode to multiple mode, the PIX converts the running configuration into two files:

- A new startup configuration, stored in Flash, that comprises the system configuration
- `admin.cfg`, stored in the disk partition, that comprises the admin context, as shown in Figure 8-5

The original running configuration is saved to disk as `old_running.cfg`. The original startup configuration is not saved; so if it differs from the running configuration, you should back it up before proceeding.

Figure 8-5 Backing Up the Single-Mode Configuration

The Admin Context

The system configuration does not include any network interfaces or network settings for itself. When the system needs to access the network, it uses the designated admin context. If the system is already in multiple context mode, or if it is converted from single mode, the admin context is created automatically as a file on the disk partition called `admin.cfg`.

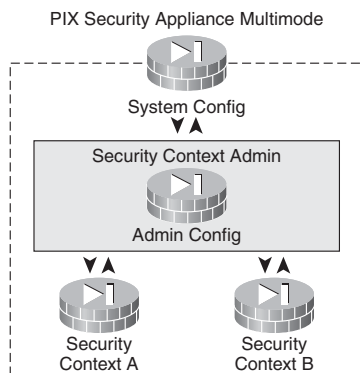
The admin context has the following characteristics (represented graphically in Figure 8-6):

- The system execution space has no traffic-passing interfaces and uses the policies and interfaces of the admin context to communicate with other devices.
- Used to fetch configurations for other contexts and send system-level syslogs.
- Users logged in to the admin context can change to the system context and create new contexts.
- Because the admin context is special, it does not count against the licensed context count.
- Aside from the significance to the system, it could be used as a regular context.

Setting the Security Context Mode

Use the **show mode** command in privileged EXEC mode to display the security context mode for the running software image and for any image in Flash memory. The mode will be either of the following:

- **Single**—Multiple mode disabled
- **Multiple**—Multiple mode enabled

Figure 8-6 Admin Context

To set the security context mode to single or multiple, use the **mode** command in global configuration mode. In single mode, the PIX Security Appliance has a single configuration and behaves as a single device. In multiple mode, multiple contexts, each with its own configuration, can be created. The number of contexts allowed depends on the license.

When converting from multiple mode to single mode, an administrator might want to first copy a full startup configuration, if one is available, to the PIX Security Appliance. The system configuration inherited from multiple mode is not a complete functioning configuration for a single-mode device.

Configuring a Security Context

Use the **context** command in global configuration mode to create a security context in the system configuration and enter context configuration mode. The security context definition in the system configuration identifies the context name, configuration file URL, VLAN, and interfaces that a context can use.

If an admin context is not present—for example, if the configuration has been cleared—the first context that is added must be the admin context. After the admin context is specified, you can use the **context** command to configure the admin context.

Allocating Interfaces

To allocate interfaces to a security context, use the **allocate-interface** command in context configuration mode. You can enter this command multiple times to specify different ranges. For transparent firewall mode, you can use only two interfaces per context. If the PIX Security Appliance model includes a management interface, you can configure that interface for management traffic in addition to the two network interfaces. The same interfaces can be assigned to multiple contexts in routed mode, if desired. Transparent mode does not allow shared interfaces.

If you specify a range of subinterfaces, you can also specify a matching range of mapped names. Follow these guidelines for ranges:

- The mapped name must consist of an alphabetic portion followed by a numeric portion. The alphabetic portion of the mapped name must match for both ends of the range. For example, enter the following range: **int0-int10**.

- The numeric portion of the mapped name must include the same quantity of numbers as the subinterface range. For example, if both ranges include 100 interfaces, enter the following range: **gigabitethernet0/ 0.100-gigabitethernet0/ 0.199 int1-int100**.

Context Configuration Files

Each context on the PIX Security Appliance has its own configuration file, which is specified using the **config-url** command. Until you enter this command, the context is not operational. As soon as you enter the **config-url** command, the context becomes operational.

The configuration files can be stored in a variety of locations. Note that HTTP(S) locations are read-only. Also, all remote URLs must be accessible from the admin context.

To identify the URL from which the system downloads the context configuration, use the **config-url** command in context configuration mode. Note the following:

- When a context URL is added, the system immediately loads the context so that it is running.
- The admin context file must be stored on the Flash memory dual in-line memory module (DIMM).
- If the system cannot retrieve the context configuration file because the server is unavailable, or the file does not yet exist, the system creates a blank context that is ready to be configured with the command-line interface.
- To change the URL, reenter the **config-url** command with a new URL.

The PIX Security Appliance merges the new configuration with the current running configuration. Reentering the same URL also merges the saved configuration with the running configuration. A merge adds any new commands from the new configuration to the running configuration. If the configurations are the same, no changes occur. If commands conflict or if commands affect the running of the context, the effect of the merge depends on the command. Errors or unexpected results might occur. If the running configuration is blank, as in the case that the server was unavailable and the configuration was never downloaded, the new configuration is used.

To avoid merging the configurations, clear the running configuration, which disrupts any communications through the context, and then reload the configuration from the new URL.

The running configuration that is edited in configuration mode, or that is used in the **copy** or **write** commands, depends on the location. When in the system execution space, the running configuration consists only of the system configuration. When in a context, the running configuration consists only of that context.

After you activate the context, you configure it much the same as PIX Security Appliance standalone device. Individual device configuration changes made in the context are stored in the configuration specified by the **config-url** command. You cannot change or view the location of the startup configuration file from within the context.

Note

Enter the **allocate-interface** command or commands before entering the **config-url** command. The PIX Security Appliance must assign interfaces to the context before it loads the context configuration. The context configuration might include commands that refer to interfaces, such as **interface**, **nat**, or **global** commands. If the **config-url** command is entered first, the PIX loads the context configuration immediately. If the context contains any commands that refer to interfaces, those commands fail.

Managing Security Contexts

You can remove a context only by editing the system configuration. To remove a context, use the **no** form of the **context** command. The current admin context cannot be removed unless all other contexts are removed. To clear all context configurations in the system configuration, use the **clear configure context** command in global configuration mode. You can create or remove contexts without a reboot.

Use the **admin-context** command in global configuration mode to set the admin context for the system configuration. Any context can be set to be the admin context, as long as the context configuration resides on the Flash memory DIMM.

As an administrator, when you are logged in to the system execution space or the admin context, you can change between contexts and perform configuration and monitoring tasks within each context. Use the **changeto** command in privileged EXEC mode to change between security contexts and the system context.

Use the **show context** command to display all contexts. From the system execution space, you can view a list of contexts including the name, interfaces, and configuration file. In the system execution space, the PIX Security Appliance displays all contexts if you do not specify a context name.

The **show context detail** command reveals additional details about the context(s), including the running state and information for internal use.

Use the **show context count** command to list the number of contexts configured.

Configure PIX Security Appliance Failover

The failover function for the PIX Security Appliance provides a safeguard in case a PIX fails. Specifically, when one PIX fails, another immediately takes its place. In the failover process, there are two PIX units: the primary PIX and the secondary PIX. The primary PIX functions as the active PIX, performing normal network functions. The secondary PIX functions as the standby PIX, ready to take control should the active PIX fail to perform. When the primary PIX fails, the secondary PIX becomes active while the primary PIX goes on standby. This entire process is called *failover*.

Understanding Failover

There are two types of hardware failover:

- **Active/standby**—In active/standby, one PIX Security Appliance is the actively processing traffic while the other is a hot standby. All traffic flows through the active PIX. In the example in Figure 8-7, the active/standby scenario consists of two PIX units, the primary and secondary. When the primary fails, the secondary becomes active and processes all the traffic. The primary PIX becomes the standby unit.

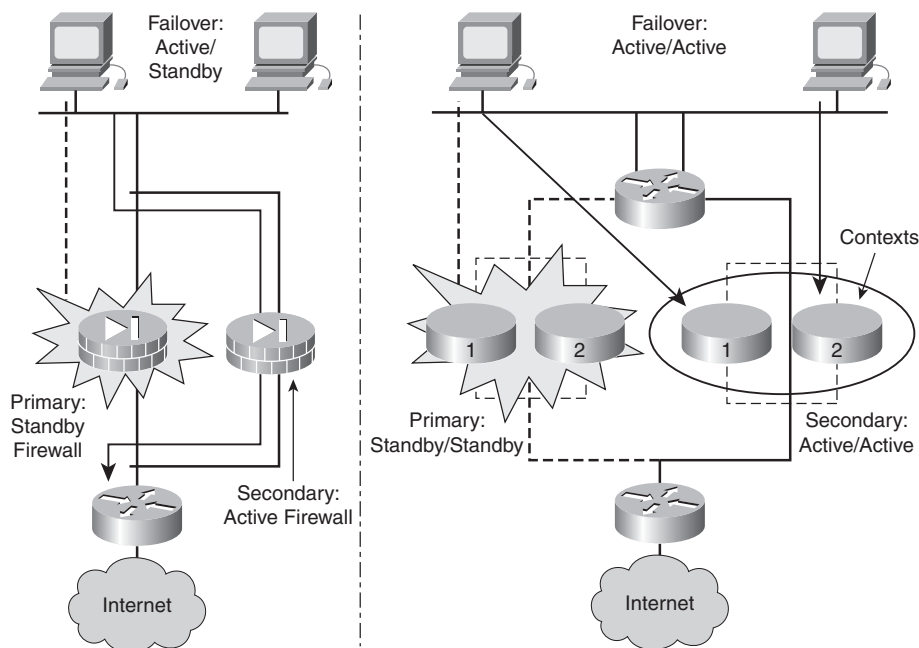
Note

If failover is used, a delay occurs between when the context is removed on the active unit and when the context is removed on the standby unit. An error message indicating that the number of interfaces on the active and standby units are not consistent might display. This error is temporary and can be ignored.

- **Active/active**—In active/active, an administrator logically divides a PIX Security Appliance into multiple contexts. Each PIX can process traffic and serve as backup units. In the example in Figure 8-7, each PIX is composed of two contexts. Under normal conditions, each PIX has one active and one standby context. The active context processes approximately 50 percent on the traffic load, while the other context is a standby unit for the other PIX.

In the active/active example in Figure 8-8, the primary PIX Security Appliance on the left fails, so the standby context in the secondary PIX becomes active. In the secondary PIX, both contexts are active, active/active. The PIX on the right handles 100 percent of the traffic using both contexts.

Figure 8-7 Hardware Failover: Active/Standby and Active/Active



A failover occurs when one of the following situations takes place:

- A power-off or a power-down condition occurs on the active PIX Security Appliance.
- The active PIX Security Appliance is rebooted.
- A link goes down on the active PIX Security Appliance for more than 30 seconds.
- The command **failover active** is typed on the standby PIX Security Appliance, which forces control back to that unit.
- Block memory exhaustion occurs for 15 consecutive seconds or more on the active PIX Security Appliance.

There are two types of failover:

- **Hardware failover**—Hardware failover provides hardware redundancy. When the active PIX Security Appliance fails, the standby PIX becomes active. All connections are lost, and client applications must perform a new connection to restart communication through the PIX. The disconnection happens because the active PIX does not pass the stateful connection information to the standby PIX. Failover messages are exchanged over a serial failover cable or a LAN-based failover connection.
- **Stateful failover**—The stateful failover feature passes per-connection stateful information to the standby unit. After a failover occurs, the same connection information is available at the new active unit. End-user applications are not required to do a reconnect to keep the same communication session. The state information passed to the standby unit includes information such as the global pool addresses and status, connection and translation information and status, the negotiated H.323 UDP ports, the port allocation map for Port Address Translation (PAT), and other details necessary to let the standby unit take over processing if the primary unit fails.

Depending on the failure, the PIX Security Appliance switchover takes from 15 to 45 seconds. Applications not handled by stateful failover then require time to reconnect before the active unit becomes fully functional.

Failover Requirements

The Cisco PIX Security Appliance 515/515E, 525, 535 and the Adaptive Security Appliance 5510, 5520, and 5540 can be used for failover. For failover to work, a pair of devices must be identical in the following requirements:

- Model number
- Software version
- Activation keys (DES or 3DES)
- Amount of Flash memory and RAM
- Proper licensing

One important factor for the PIX Security Appliance is failover licensing. The primary failover units must have an unrestricted (UR) license, whereas the secondary can have an UR or a failover (FO) license. The PIX failover (FO) license can be either an active/standby only or an active/active failover only. To perform active/active failover on a PIX with a failover license, the failover license must be an active/active-only failover license. A restricted license cannot be used for failover, and two units with FO licenses cannot be used in a single failover pair.

Note

Neither the Security Appliance 501 nor the Security Appliance 506E can be used for failover.

Failover Interface Test

Both the primary and secondary PIX Security Appliances send special failover hello packets to each other over all network interfaces and the failover cable every 15 seconds to make sure that everything is working. When a failure occurs in the active PIX, and it is not because of a loss of power in the standby PIX, failover begins a series of tests to determine which security appliance has failed. The purpose of these tests is to generate network traffic to determine which, if either, security appliance has failed.

At the start of each test, each PIX clears its received packet count for its interfaces. At the conclusion of each test, each PIX looks to determine whether it has received any traffic. If it has, the interface is considered operational. If one PIX receives traffic for a test and the other PIX does not, the PIX that did not receive traffic is considered failed. If neither PIX has received traffic, the tests then continue.

The following are the four different tests used to test for failover:

- **LinkUp/Down**—This is a test of the network interface card (NIC) itself. If an interface card is not plugged into an operational network, it is considered failed. For example, the hub or switch has failed, has a failed port, or a cable is unplugged. If this test does not find anything, the network activity test begins.
- **Network Activity**—This is a received network activity test. The PIX Security Appliance counts all received packets for up to 5 seconds. If any packets are received at any time during this interval, the interface is considered operational and testing stops. If no traffic is received, the Address Resolution Protocol (ARP) test begins.
- **ARP**—The ARP test consists of reading the ARP cache of the PIX Security Appliance for the 10 most recently acquired entries. The PIX sends ARP requests one at a time to these machines, attempting to stimulate network traffic. After each request, the PIX counts all received traffic for up to 5 seconds. If traffic is received, the interface is considered operational. If no traffic is received, an ARP request is sent to the next machine. If at the end of the list no traffic has been received, the ping test begins.
- **Broadcast ping**—The ping test consists of sending out a broadcast ping request. The PIX Security Appliance then counts all received packets for up to 5 seconds. If any packets are received at any time during this interval, the interface is considered operational and testing stops. If no traffic is received, the testing starts over again with the ARP test.

Failover Cabling

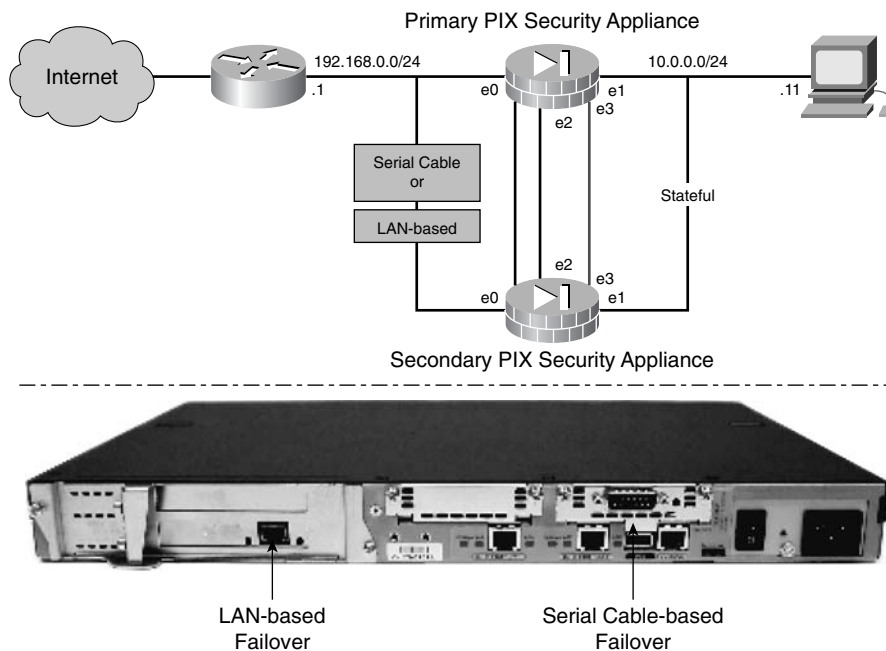
The failover PIX Security Appliances communicate failover information between the PIX units. The communications identifies the unit as primary or secondary, identifies the power status of the other unit, and serves as a link for various failover communications between the two units.

The majority of the failover communications are passed over dedicated failover links. There are three types of failover links, as shown in Figure 8-8:

- **Serial failover cable**—The serial failover cable is a modified RS-232 serial link cable that transfers data at 115 Kbps.
- **LAN-based failover cable**—PIX Security Appliance Software Version 6.2 introduced support for LAN-based failover, so a special serial failover cable is no longer required to connect the primary and secondary units. LAN-based failover overcomes the distance limitations imposed by the 6-foot length of the serial failover cable. With LAN-based failover, failover messages are transmitted over Ethernet connections. LAN-based failover provides message encryption and authentication using a manual pre-shared key for added security. LAN-based failover requires an Ethernet connection to be used exclusively for passing failover communications between two PIX units.
- **Stateful cable**—The stateful failover cable passes per-connection stateful information to the standby unit. Stateful failover requires an Ethernet interface with a minimum speed of 100 Mbps full duplex to be used exclusively for passing state information between the two PIX Security Appliance units. The stateful failover interface can be connected to either a 100BASE-TX or 1000BASE-TX full duplex on a dedicated switch or dedicated VLAN of a switch.

Data is passed over the dedicated interface using IP Protocol 8. No hosts or routers should be on this interface.

Figure 8-8 Types of Failover Cabling

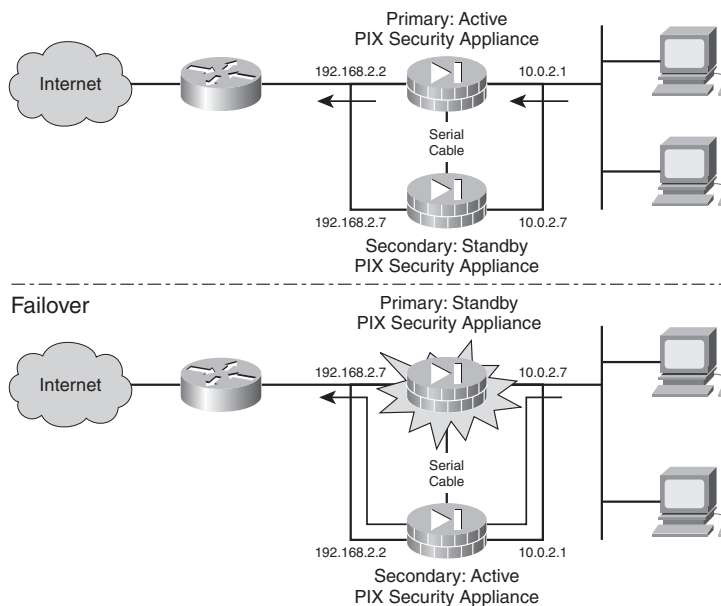


Serial Cable-Based Failover Configuration

In serial cable-based active/standby failover, two PIX Security Appliances are interconnected with a serial failover cable. One unit is the primary unit, the other is the secondary unit. In the top example in Figure 8-9, the primary PIX is active and passes traffic. The IP addresses of the outside and inside interfaces are 192.168.2.2 and 10.0.2.1. The secondary unit is standby and has interface IP addresses of 192.168.2.7 and 10.0.2.7.

In the bottom example in Figure 8-9, notice the primary PIX failed. In active/standby applications, the type of failover unit did not change. The primary unit is still the primary unit. What changed are the roles, active and standby, and the interface IP addresses. The secondary unit is now the active unit passing the traffic. The interface IP addresses were swapped. The secondary unit inherited the IP addresses of the primary unit, 192.168.2.2 and 10.0.2.1.

Figure 8-9 Serial Cable: Active/Standby Failover



Complete the following steps to configure failover with a serial failover cable. Before starting this procedure, if the standby PIX Security Appliance is powered on, power it down and leave it off until instructed to power it on.

- Step 1.** Attach a network cable for each network interface that is planned to be used.
- Step 2.** Connect the failover cable between the primary PIX Security Appliance and the secondary PIX.
- Step 3.** Configure the following failover parameters on the PIX Security Appliance:
 - Failover
 - Standby IP addresses

- Stateful failover interface (This is optional, for use with stateful failover.)
- Failover poll time (Optional)

When this configuration is finished, save it to the Flash memory of the primary unit.

Step 4. Power on the secondary PIX Security Appliance.

Active/Standby LAN-Based Failover Configuration

LAN-based failover overcomes the distance limitations imposed by the 6-foot failover cable. With LAN-based failover, an Ethernet cable can be used to replicate configuration from the primary PIX Security Appliance to the secondary PIX. The special failover cable is not required. Instead, LAN-based failover requires a dedicated LAN interface and a dedicated switch, hub, or VLAN. You should not use a crossover Ethernet cable to connect the two units.

The same LAN interface used for LAN-based failover can also be used for stateful failover. However, the interface needs enough capacity to handle both the LAN-based failover and stateful failover traffic. If the interface does not have the necessary capacity, use two separate, dedicated interfaces.

LAN-based failover allows traffic to be transmitted over Ethernet connections that are relatively less secure than the special failover cable. To secure failover transmissions, LAN-based failover provides message encryption and authentication using a manual pre-shared key.

Complete the following steps to configure LAN-based failover:

- Step 1.** Install a LAN-based failover connection between the two PIX Security Appliances. Verify that any switch port that connects to a PIX interface is configured to support LAN-based failover. Disconnect the secondary PIX.
- Step 2.** Configure the primary PIX Security Appliance for failover.
- Step 3.** Save the configuration of the primary unit to Flash memory.
- Step 4.** Power on the secondary PIX Security Appliance.
- Step 5.** Configure the secondary PIX Security Appliance with the LAN-based failover command set.
- Step 6.** Save the configuration of the secondary unit to Flash memory.
- Step 7.** Connect the PIX Security Appliance LAN-based failover interface to the network.
- Step 8.** Reboot the secondary unit.

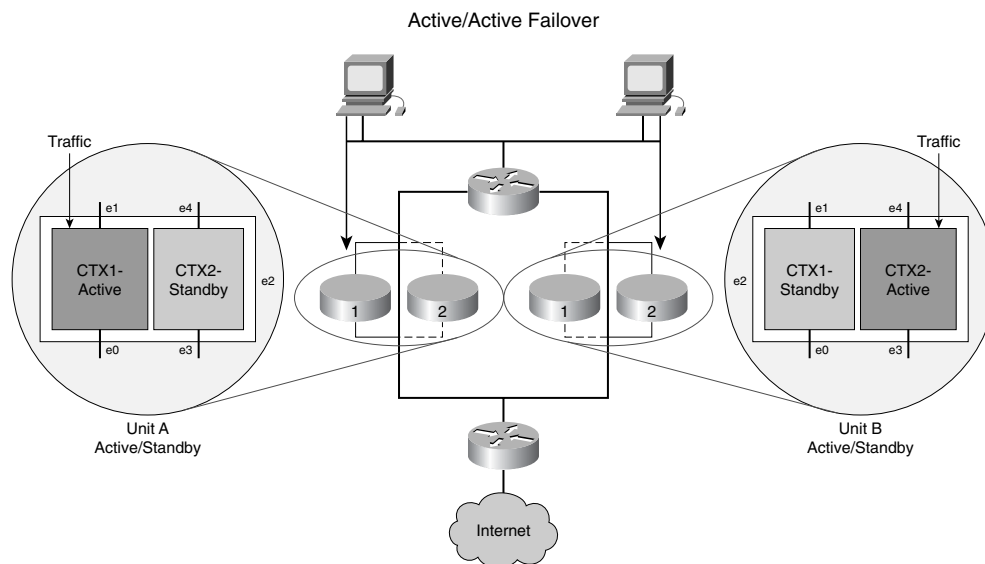
Active/Active Failover

Previously, under the active/standby failover model, only one PIX Security Appliance could be actively processing user traffic (while the other unit acted as a hot standby and prepared to take over if the active unit failed). Cisco PIX and ASA Security Appliances Software Release 7.0

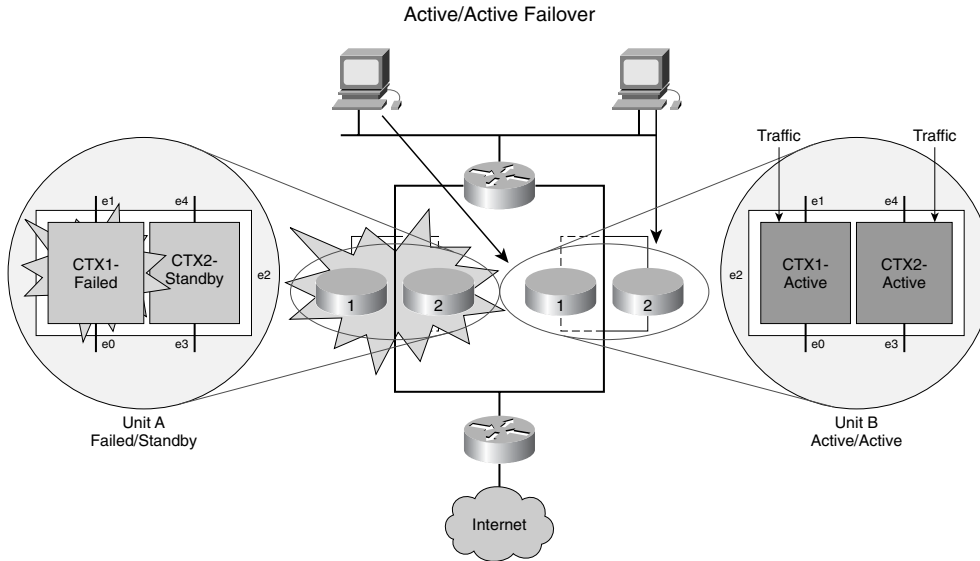
adds the capability of active/active failover. When two devices are configured to function in active/active failover, both units can actively process traffic while at the same time serving as a backup for their peer unit.

The active/active failover feature leverages the virtual context feature. In the example in Figure 8-10, two PIX Security Appliances are configured for active/active failover, Unit A and Unit B. Each PIX is partitioned into two contexts, ctx1 and ctx2. In the two-unit active/active scenario, under normal conditions, there is one active context and one standby context per unit. In Unit A, ctx1 is active and passing traffic. Ctx1 in Unit B is in standby state. In Unit B, ctx2 is active and passing traffic while ctx2 in Unit A is in standby state. Under normal conditions, each unit handles 50 percent of the traffic. The PIX active/active cluster itself does not perform load balancing. It is the administrator's responsibility to engineer the network to route 50 percent of the traffic to each unit. This can be accomplished either statically or with the use of an upstream router to do load balancing on the traffic.

Figure 8-10 Active/Active Failover - 1



In Figure 8-10, Unit A ctx1 was active while ctx2 was standby. Unit B ctx1 was standby while ctx2 was active. Active/active failover logic enables each PIX Security Appliance to determine whether a failure is a context-based or unit-based failure. If an active context fails, the active context transitions to a failed state. In the peer PIX, the standby context changes from standby to active. For example in Figure 8-11, if Unit A interface e0 fails, the Unit A can determine the failure is a context-based failure. The Unit A can place ctx1 in a failed state. Unit A can communicate with Unit B the change in state of ctx1. Unit B can change the state of its ctx1 to active. After the state change, both contexts on Unit B are active and passing traffic. Failover can be context based or unit based. When a failure affects the whole unit, the peer unit can take over by activating any standby contexts and start processing 100 percent of the traffic.

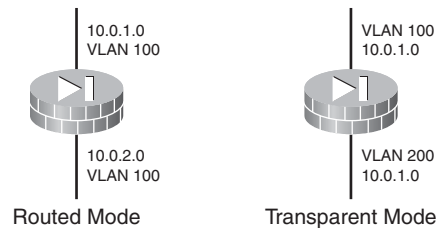
Figure 8-11 Active/Active Failover - 2

Configure Transparent Firewall Mode

The PIX Security Appliance can run in two firewall settings:

- The routed setting based on IP address
- The transparent setting based on MAC address

Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a bump in the wire, or a stealth firewall, and is not seen as a router hop to connected devices, as shown in Figure 8-12.

Figure 8-12 Transparent Versus Router Firewall

Transparent Firewall Mode Overview

The PIX Security Appliance connects the same network on the inside and outside ports, but each interface resides on a different VLAN.

Note the following:

- Transparent mode supports only two interfaces, typically an inside interface and an outside interface.
- Transparent mode can run both in single and multiple mode.
- The PIX Security Appliance bridges packets from one VLAN to the other instead of routing them.
- MAC lookups are performed instead of routing table lookups.

Because the PIX Security Appliance is not a routed hop, it is easy to introduce a transparent firewall into an existing network. IP readdressing is unnecessary. Maintenance is facilitated because there are no complicated IP routing patterns to troubleshoot and no Network Address Translation (NAT) configuration.

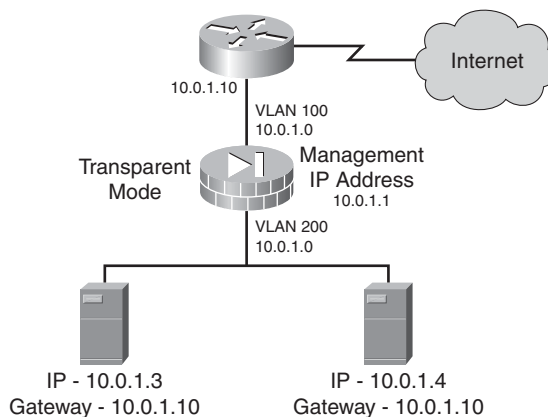
Note

The transparent PIX Security Appliance does not pass Cisco Discovery Protocol (CDP) packets.

Even though transparent mode acts as a bridge, Layer 3 traffic, such as IP traffic, cannot pass through the PIX Security Appliance. The transparent firewall, however, can allow any traffic through using either an extended access list, for IP traffic, or an EtherType access list, for non-IP traffic. The only traffic allowed through the transparent firewall without an access list is ARP traffic. ARP traffic can be controlled by ARP inspection.

Because the PIX Security Appliance is now acting a bridge, device IP addressing should be configured as if the PIX is not in the network. Layer 3 traffic must be explicitly permitted. Each directly connected network must be on the same subnet. A management IP address is required for connectivity to and from the PIX itself. The management IP address must be on the same subnet as the connected network as shown in Figure 8-13. Keep in mind that as a layer 2 device the PIX interfaces must be on different VLANs to differentiate the traffic flow. Do not specify the PIX Security Appliance management IP address as the default gateway for connected devices, because devices need to specify the router on the other side of the PIX Security Appliance as the default gateway.

Figure 8-13 Transparent Firewall Guidelines



The following features are not supported in transparent mode:

- **NAT**—NAT is performed on the upstream router.
- **Dynamic routing protocols**—The administrator can, however, add static routes for traffic originating on the PIX Security Appliance. Dynamic routing protocols can be allowed through the PIX using an extended access list.
- **IPv6**—There is no fix for this limitation.
- **DHCP relay**—The transparent firewall can act as a DHCP server, but it does not support the **DHCP relay** commands. DHCP relay is not required because DHCP traffic can be allowed to pass through using an extended access list.
- **Quality of service**—QoS must be performed by upstream router.
- **Multicast**—The administrator can, however, allow multicast traffic through the PIX Security Appliance by allowing it in an extended access list.
- **VPN termination for through traffic**—The transparent firewall supports site-to-site VPN tunnels for management connections only. It does not terminate VPN connections for traffic through the PIX Security Appliance. VPN traffic cannot pass through the PIX using an extended access list, but it does not terminate nonmanagement connections.

Enable Transparent Firewall Mode

To view the current firewall mode, enter the **show firewall** command as follows:

```
Pixfirewall(config)#show firewall
Firewall mode: transparent
```

The mode will either be routed or transparent.

To set the firewall mode to transparent mode, use the **firewall transparent** command in global configuration mode as follows:

```
Pixfirewall(config)#firewall transparent
Switched to transparent mode
```

To restore routed mode, use the no form of this command.

For multiple context mode, only one firewall mode can be used for all contexts. The mode must be set in the system configuration. The **firewall transparent** command also appears in each context configuration for informational purposes only. This command cannot be entered in a context.

When the mode is changed, the PIX Security Appliance clears the configuration because many commands are not supported for both modes.

If a text configuration that changes the mode with the **firewall transparent** command is downloaded to the PIX Security Appliance, be sure to put the command at the top of the configuration. The PIX changes the mode as soon as it reads the command, and then continues reading the configuration that was downloaded. If the command is later in the configuration, the PIX clears all the preceding lines in the configuration.

Note

If a configuration already exists, be sure to back up the configuration before changing the mode. You can use this backup for reference when creating a new configuration.

A transparent firewall does not participate in IP routing. The only IP configuration required for the PIX Security Appliance is to set the management IP address. This address is required because the PIX uses this address as the source address for traffic originating on the PIX, such as system messages or communications with authentication, authorization, and accounting (AAA) servers. This address can also be used for remote management access. This address must be on the same subnet as the upstream and downstream routers. For multiple context mode, set the management IP address within each context.

ACLs

The transparent firewall as shown in Figure 8-14 can allow any traffic through using either an extended access control list (ACL), for IP traffic, or an EtherType access list, for non-IP traffic. For example, routing protocol adjacencies can be established through a transparent firewall. Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Extended Interior Gateway Routing Protocol (EIGRP), or Border Gateway Protocol (BGP) traffic can be allowed through based on an extended access list. Protocols such as Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP) can also pass through the PIX Security Appliance. Remember that by default, no traffic is allowed through the firewall, regardless of the security level assigned to the interface.

To specify the traffic that should be allowed to pass through the firewall, use the following command:

```
pixfirewall(config)#access-list id [line line-number] [extended] {deny | permit} {object-group network_obj_grp_id | protocol} source_address mask dest_address mask
```

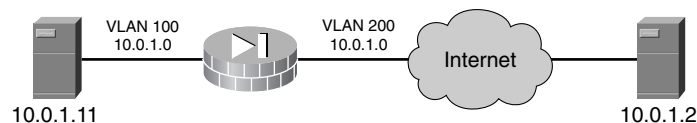
For the transparent firewall in Figure 8-14, for example, you might enter the following:

```
Pixfirewall (config)#access-list ACLIN permit icmp 10.0.1.0 255.255.255.0 10.0.1.0 255.255.255.0
```

```
Pixfirewall(config)#access-group ACLIN in interface inside
```

```
Pixfirewall(config)#access-group ACLIN in interface outside
```

Figure 8-14 Configure ACLs to Permit Traversal Through the Transparent Firewall



For features that are not directly supported on the transparent firewall, traffic can be allowed to pass through so that upstream and downstream routers can support the functionality. For example, by using an extended access list, DHCP traffic, instead of the unsupported DHCP relay feature, or multicast traffic such as that created by IP/TV can be allowed.

To configure an access list that controls traffic based on its EtherType, use the following command in global configuration mode:

```
Pixfirewall(config)#access-list id ethertype {deny | permit} {ipx | bpdu | mpls-unicast | mpls-multicast | any | hex_number}
```

For instance, to allow IPX packets through the firewall, you would enter the following:

```
Pixfirewall(config)#access-list ETHER ethertype permit ipx
Pixfirewall(config)#access-group ETHER in interface inside
Pixfirewall(config)#access-group ETHER in interface outside
```

Because EtherTypes are connectionless, you must apply the ACL to both interfaces for traffic to pass in both directions.

The PIX Security Appliance can control any EtherType identified by a 16-bit hexadecimal number. EtherType ACLs support Ethernet V2 frames. 802.3-formatted frames are not handled by the ACL because they use a length field as opposed to a type field. Bridge protocol data units, which are handled by the ACL, are the only exception. They are (SNAP) encapsulated, and the PIX is designed to specifically handle bridge protocol data units (BPDUs).

Only one ACL of each type, extended and EtherType, can be applied to each direction of an interface. The same ACLs can be applied on multiple interfaces.

Predefined EtherTypes are as follows:

- IPX.
- BPDU.
- MPLS.
- Other Ethernet V2/DIX-encapsulated frames can be allowed based on their 2-byte EtherType.
- 802.3-encapsulated frames cannot pass through the firewall at this time.

ARP Inspection

ARP inspection prevents malicious users from impersonating, or spoofing, other hosts or routers. ARP spoofing can enable a man-in-the-middle attack. Configure static ARP entries using the **arp** command before enabling ARP inspection. When ARP inspection is enabled, the PIX Security Appliance compares the MAC address, IP address, and source interface in all ARP packets to static entries in the ARP table and takes the following actions:

- If the IP address, MAC address, and source interface match an ARP entry, the packet is passed through.
- If there is a mismatch between the MAC address, the IP address, or the interface, the PIX Security Appliance drops the packet.
- If the ARP packet does not match any entries in the static ARP table, the PIX Security Appliance can be set to either flood the packet out all interfaces or to drop the packet.

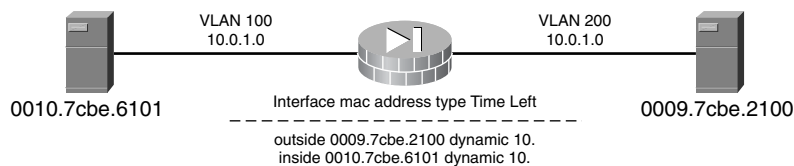
Note

The management-specific interface, if present, never floods packets even if this parameter is set to flood.

Monitor and Maintain a Transparent Firewall

The PIX Security Appliance learns and builds a MAC address table in a similar way as a normal bridge or switch. When a device sends a packet through the PIX, it adds the MAC address to its table, as shown in Figure 8-15. The table associates the MAC address with the source interface so that the PIX knows to send any packets addressed to the device out the correct interface.

Figure 8-15 MAC Address Table



Because the PIX Security Appliance is a firewall, if the destination MAC address of a packet is not in the table, the PIX does not flood the original packet on all interfaces as a normal bridge does. Instead, it generates the following packets for directly connected devices or for remote devices:

- **Packets for directly connected devices**—The PIX Security Appliance generates an ARP request for the destination IP address so that PIX can learn which interface receives the ARP response.
- **Packets for remote devices**—The PIX Security Appliance generates a ping to the destination IP address so that the PIX can learn which interface receives the ping reply.

The Original Packet Is Dropped

By default, each interface automatically learns the MAC addresses of entering traffic, and the PIX Security Appliance adds corresponding entries to the MAC address table. MAC address learning can be disabled if desired; however, unless MAC addresses are statically added to the table, no traffic can pass through the PIX. To disable MAC address learning, enter the following command:

```
Pixfirewall(config)#mac-learn interface_name disable
```

To reenable MAC address learning, use the **no** form of this command:

```
Pixfirewall(config)#no mac-learn interface_name disable
```

By default, each interface automatically learns the MAC addresses of entering traffic, and the PIX Security Appliance adds corresponding entries to the MAC address table.

Normally, MAC addresses are added to the MAC address table dynamically as traffic from a particular MAC address enters an interface. If desired, you can add static MAC addresses to the MAC address table by using the following command:

```
Pixfirewall(config)# mac-address-table static interface_name mac_address
```

One benefit to adding static entries is to guard against MAC spoofing. If a client with the same MAC address as a static entry attempts to send traffic to an interface that does not match the static entry, PIX Security Appliance drops the traffic and generates a system message.

You can view the entire MAC address table, including static and dynamic entries for both interfaces, or you can view the MAC address table for just a single interface can.

Two new **debug** commands have been introduced with regard to transparent firewall mode:

- **debug arp inspection**—Displays debug messages for ARP inspection
- **debug mac-address-table**—Displays debug messages for the MAC address table



Lab 8.3.3 Configure a PIX Security Appliance as a Transparent Firewall

In this lab activity, you configure a PIX Security Appliance is transparent mode.

PIX Security Appliance Management

This section deals with the management of the PIX Security Appliance. You examine managing Telnet and SSH access, command authorization, PIX Security Appliance password recovery, and Adaptive Security Appliance password recovery. This section ends with a discussion on file management and image upgrade and activation keys.

Managing Telnet Access

The serial console permits a single user to configure the PIX Security Appliance, but often this is not convenient for a site with more than one administrator. By configuring console access using Telnet, a maximum of 5 concurrent Telnet connections per context can be allowed, if available, with a maximum of 100 connections divided between all contexts.

Telnet access to the PIX Security Appliance can be enabled on all interfaces; however, the PIX requires that all Telnet traffic to the outside interface be IPsec protected. To enable a Telnet session to the outside interface, configure IPsec on the outside interface to include IP traffic generated by the PIX, and enable Telnet on the outside interface.

The following are the Telnet configuration commands:

- **telnet**—Specifies which hosts can access the PIX Security Appliance console using Telnet. Up to 16 hosts or networks can be specified. The syntax for this command is as follows:

```
Pixfirewall# telnet {{hostname | IP_address mask interface_name} {IPv6_address
interface_name} | {timeout number}}
```

- **telnet timeout**—Sets the maximum time a console Telnet session can be idle before being logged off by the PIX Security Appliance. The default is 5 minutes. The syntax for this command is as follows:

```
Pixfirewall(config)#telnet timeout minutes
```

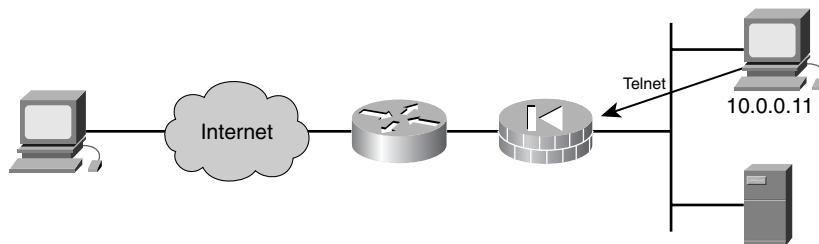
- **passwd**—Sets the password for Telnet access to the PIX Security Appliance. The default value is **cisco**. The syntax for this command is as follows:

```
Pixfirewall(config)#{passwd | password} password [encrypted]
```

For the network in Figure 8-16, host 10.0.0.11 on the internal interface is allowed to access the PIX Security Appliance console using Telnet with the password telnetpass. If the Telnet session is idle more than 15 minutes, the PIX closes it. The command sequence to enable this is as follows:

```
Pixfirewall(config)#telnet 10.0.0.11 255.255.255.255 inside
Pixfirewall(config)#telnet timeout 15
Pixfirewall(config)#passwd telnetpass
```

Figure 8-16 Configure Telnet Access



The following commands enable the administrator to view and clear Telnet configuration and Telnet sessions:

- **show running-config telnet**—Displays the current list of IP addresses authorized to access the PIX Security Appliance using Telnet. This command can also be used to display the number of minutes that a Telnet session can remain idle before being closed by the PIX.
- **clear configure telnet**—Removes the Telnet connection and the idle timeout from the configuration.

- **who**—Enables the administrator to view the IP addresses that are currently accessing the PIX Security Appliance console using Telnet.
- **kill**—Terminates a Telnet session. When a Telnet session is killed, the PIX Security Appliance lets any active commands terminate and then drops the connection without warning the user.

Managing SSH Access

Secure Shell (SSH) provides another option for remote management of the PIX Security Appliance. SSH provides a higher degree of security than Telnet, which provides lower-layer encryption and application security. The PIX supports the SSH remote functionality, which provides strong authentication and encryption capabilities. SSHv1 server was introduced in the PIX Security Appliance Software Version 5.2 and SSHv2 server was introduced in the PIX Security Appliance Software Version 7.0. SSH, an application running on top of a reliable transport layer such as TCP, supports logging on to another computer over a network, executing commands remotely, and moving files from one host to another.

Both ends of an SSH connection are authenticated, and passwords are protected by being encrypted. Because SSH uses Rivest, Shamir, and Adleman (RSA) public key cryptography, an Internet encryption and authentication system, an RSA key pair must be generated for the PIX Security Appliance before clients can connect to the PIX console. The PIX must also have an Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) activation key.

The PIX Security Appliance allows up to five SSH clients to simultaneously access the console. Specific hosts or networks that are authorized to initiate an SSH connection to the PIX can be defined, and how long a session can remain idle before being disconnected.

To establish an SSH connection to the PIX Security Appliance console, enter the username **pix** and the Telnet password at the SSH client. When starting an SSH session, the PIX displays a dot (.) on the console before the SSH user authentication prompt appears, as follows:

```
pixfirewall(config)# .
```

The display of the dot does not affect the functionality of SSH. The dot appears at the console when generating a server key or decrypting a message using private keys during SSH key exchange before user authentication occurs. These tasks can take up to 2 minutes or longer. The dot is a progress indicator that verifies that the PIX Firewall is busy and has not hung.

Note

The PIX Security Appliance SSH implementation provides a secure remote shell session without IPsec, and only functions as a server, which means that the PIX cannot initiate SSH connections.

In Example 8-1, an RSA key pair is generated for the PIX Security Appliance using the default key modulus size of 1024. Host 172.26.26.50 is authorized to initiate an SSH connection to the PIX.

```
Example 8-1    Generation of RSA Key Pair
pixfirewall(config)# crypto key zeroize rsa
pixfirewall(config)# write memory
pixfirewall(config)# domain-name cisco.com
pixfirewall(config)# crypto key generate rsa modulus 1024
pixfirewall(config)# write memory
pixfirewall(config)# ssh 172.26.26.50 255.255.255.255 outside
pixfirewall(config)# ssh timeout 30
```

Use the **show ssh sessions** command to list all active SSH sessions on the PIX Security Appliance. The **ssh disconnect** command enables the administrator to disconnect a specific session. Use the **clear configure ssh** command to remove all **ssh** command statements from the configuration, and use the **no ssh** command to remove selected **ssh** command statements. The **debug ssh** command displays information and error messages associated with the **ssh** command.

Command Authorization

Command authorization is a way of facilitating and controlling administration of the PIX Security Appliance. You can use three types of command authorizations to control which users execute certain commands:

- Enable-level command authorization with passwords
- Command authorization using the local user database
- Command authorization using Access Control Server (ACS)

The first type of command authorization, enable-level with passwords, allows the administrator to use the **enable** command with the *priv_level* option to access a PIX Security Appliance privilege level, and then use any command assigned to that privilege level or a lower privilege level. To configure this type of command authorization, the administrator must create and password-protect the privilege levels, assign privilege levels to commands, and enable the command-authorization feature.

The PIX Security Appliance supports up to 16 privilege levels, levels 0 through 15. You can create and secure privilege levels by using the following command:

```
pixfirewall(config)#enable password password [level level] [encrypted]
```

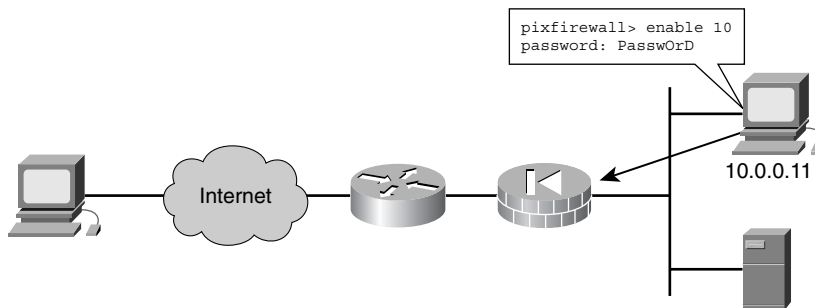
Access to a particular privilege level can be gained from the > prompt by entering the **enable level** command with a privilege-level designation and entering the password for that level when prompted.

The following command sequence shows how to create and access a privilege for the network displayed in Figure 8-17:

```
pixfirewall(config)#enable password Passw0rd level 10
```

```
pixfirewall> enable 10
Password: Passw0rd
pixfirewall#
```

Figure 8-17 Creating and Accessing Password-Protect Privilege Levels



When inside a privilege level, the commands assigned to that level and commands assigned to lower privilege levels can be executed. For example, from privilege level 15, every command can be executed because this is the highest privilege level. If a privilege level is not specified when entering enable mode, the default of 15 is used. Therefore, creating a strong password for level 15 is important.

To assign commands to privilege levels, use the **privilege** command. Replace the level argument with the privilege level, and replace the command argument with the command to assign to the specified level. The **show**, **clear**, or **configure** parameter can be used to optionally set the privilege level for the **show**, **clear**, or **configure** command modifiers of the specified command. The **privilege** command can be removed by using the **no** keyword.

To configure user-defined privilege levels for PIX Security Appliance commands, use the following command:

```
pixfirewall(config)#privilege [show | clear | configure] level level [mode {enable | configure}] command command
```

Use the **privilege** command without a **show**, **clear**, or **configure** parameter to set the privilege level for all the modifiers of the command. For example, to set the privilege level of all modifiers of the **access-list** command to a single privilege level of 10, enter the following command:

```
privilege level 10 command access-list
```

For commands that are available in multiple modes, use the **mode** parameter to specify the mode in which the privilege level applies. Do not use the **mode** parameter for commands that are not mode specific.

Next, to enable command authorization, use the following command:

```
pixfirewall(config)#aaa authorization command {LOCAL | tacacs-server-tag}
```

Consider the following example where privilege levels are set for the different command modifiers of the **access-list** command:

```
pixfirewall(config)#enable password Password level 10  
pixfirewall(config)#privilege show level 8 command access-list  
pixfirewall(config)#privilege configure level 10 command access-list  
pixfirewall(config)#aaa authorization command LOCAL
```

The first **privilege** command entry sets the privilege level of **show access-list** to 8. The second **privilege** command entry sets the privilege level of the **configure** modifier to 10. The **aaa authorization command LOCAL** command is then used to enable command authorization. The user knows the highest privilege level to which the **access-list** command is assigned and also knows the password for that level. The user is therefore able to view and create ACLs by entering level 10.

To view the command assignments for each privilege level, use the following command:

```
pixfirewall#show running-config [all] privilege [all | command command | level level]
```

The system displays the current assignment of each command-line interface (CLI) command to a privilege level.

Use the **show privilege level** command with the *level* option to display the command assignments for a specific privilege level. Use the **show privilege command** *command* to display the privilege level assignment of a specific command. To view the user account that is currently logged in, enter the **show curpriv** command.



Lab 8.4.3a Configure User Authentication and Command Authorization Using ASDM

In this lab exercise, you configure command authorization, local user authentication, and SSH.



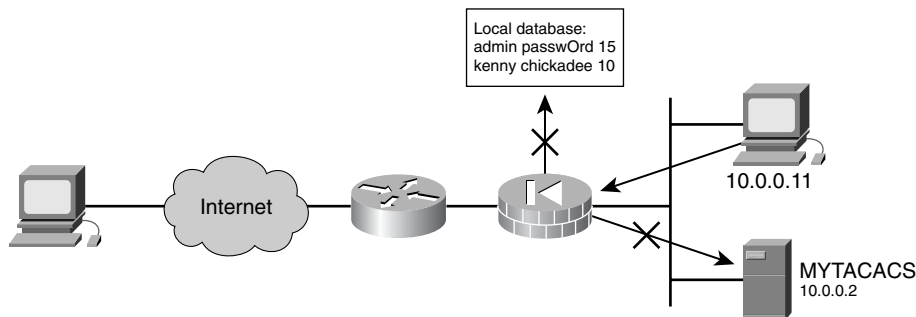
Lab 8.4.3b Configure SSH, Command Authorization, and Local User Authentication Using CL

In this lab exercise, you configure and verify SSH operation. You then configure command authorization and local user authentication.

PIX Security Appliance Password Recovery

When configuring the command-authorization feature, do not save the configuration until it works as required. If an administrator gets locked out of the PIX Security Appliance, the administrator can usually recover access by simply reloading it. If the configuration has already been saved, and authentication using the LOCAL database has been configured, but no user-names have been configured, a lockout problem is created. A lockout problem can also be encountered when configuring command authorization using a TACACS+ server if the TACACS+ server is unavailable, down, or misconfigured, as shown in Figure 8-18.

Figure 8-18 Lockout



If access to the PIX Security Appliance cannot be recovered by restarting the PIX, use a web browser to access <http://www.cisco.com/warp/customer/110/34.shtml>.

This website provides a downloadable file with instructions for using it to remove the lines in the PIX Security Appliance configuration that enable authentication and cause the lockout

Note

If AAA has been configured on the PIX Security Appliance, and the AAA server is down, the PIX Security Appliance can be accessed by entering the Telnet password initially, and then **pix** as the username and the enable password for the password. If there is no enable password in the PIX configuration, enter **pix** for the username and press **Enter**. If the enable and Telnet passwords are set but not known, you must continue with the password-recovery process.

Note

Password recovery for PIX Security Appliance versions through 6.3 requires a TFTP server.

problem. If there are Telnet or console **aaa authentication** commands in PIX Security Appliance Software Versions 6.2 and later, the system also prompts to remove these.

The PIX Password Lockout Utility is based on the PIX Security Appliance software version that is running. Use one of the following files, depending on the PIX software in use:

- np63.bin (6.3 version)
- np62.bin (6.2 version)
- np61.bin (6.1 version)
- np60.bin (6.0 version)
- np53.bin (5.3 version)
- np52.bin (5.2 version)
- np51.bin (5.1 version)

A different type of lockout problem can be encountered when the **aaa authorization** command and *tacacs-server-tag* argument are used and the administrator is not logged in as the correct user. For every command that is entered, the PIX Security Appliance displays the following message:

```
Command Authorization failed
```

This occurs because the TACACS+ server does not have a user profile for the user account that was used for logging in. To prevent this problem, make sure that the TACACS+ server has all the users configured with the commands that they can execute. Also, make sure to be logged in as a user with the required profile on the TACACS+ server.

**Lab 8.4.4 Perform Password Recovery on the PIX Security Appliance**

In this lab exercise, you learn to upgrade the PIX Security Appliance software image. You also learn to perform password-recovery procedures.

Adaptive Security Appliance Password Recovery

On the Adaptive Security Appliance, if the password is forgotten, you can boot the ASA into ROMMON by doing the following:

- Step 1.** Press the **Esc** key on the terminal keyboard when prompted during startup.
- Step 2.** Set the ASA to ignore the startup configuration by changing the configuration register using the **config-register** command. For example, if the configuration register is the default 0x1, change the value to 0x41 by entering the **config-register 0x41** command.
- Step 3.** After reloading, the ASA loads a default configuration, and you can enter privileged EXEC mode using the default passwords.

- Step 4.** Load the startup configuration by copying it to the running configuration and reset the passwords.
- Step 5.** Set the ASA to boot as before by setting the configuration register to the original setting. For example, enter the **config-register 0x1** command in global configuration mode.

On the Adaptive Security Appliance, the **no** version of the **config-register** command prevents a user from entering ROMMON with the configuration intact. When a user enters ROMMON, the ASA prompts the user to erase all Flash file systems. The user cannot enter ROMMON without first performing this erasure. If a user chooses not to erase the Flash file system, the ASA reloads. Because password recovery depends on using ROMMON and maintaining the existing configuration, this erasure prevents the password from being recovered. However, disabling password recovery prevents unauthorized users from viewing the configuration or inserting different passwords. In this case, to recover the system to an operating state, load a new image and a backup configuration file, if available. The **service password-recovery** command, which enables password recovery, appears in the configuration file for informational purposes only—this command is on by default. When the command is entered at the CLI prompt, the setting is saved in nonvolatile random-access memory (NVRAM). The only way to change the setting is to enter the command at the CLI prompt. Loading a new configuration with a different version of the command does not change the setting. If password recovery is disabled when the ASA is configured to ignore the startup configuration at startup, in preparation for password recovery, the ASA changes the setting to boot the startup configuration as usual. If failover is used, and the standby unit is configured to ignore the startup configuration, the same change is made to the configuration register when the **no service password recovery** command replicates to the standby unit:

```
Ciscoasa(config)#no service password-recovery
```

```
WARNING: Executing "no service password-recovery" has disabled the password recovery mechanism and disabled access to ROMMON. The only means of recovering from lost or forgotten passwords will be for a ROMMON to erase all file systems including configuration files and images. You should make a backup of your configuration and have a mechanism to restore images from the ROMMON command line.
```

File Management

Use the following command to display the directory contents:

```
pixfirewall(config)#dir [/all] [all-file systems] [/recursive] [disk0: | disk1: | flash: | system: ] [path]
```

The **dir** command without keywords or arguments displays the directory contents of the current directory.

The **pwd** command option displays the current working directory.

Example 8-2 demonstrates output from the **dir** command.

Example 8-2 Viewing Directory Contents

```

pixfirewall# dir
Directory of disk:/
 1 -rw- 1519 10:03:50 Jul 14 2003 my_context.cfg
 2 -rw- 1516 10:04:02 Jul 14 2003 my_context.cfg
 3 -rw- 1516 10:01:34 Jul 14 2003 admin.cfg
60985344 bytes total (60973056 bytes free)

```

Use the following command to display the contents of a file:

```
pixfirewall# more [/ascii] | [/binary] [filesystem:] path
```

Example 8-3 demonstrates output from the **dir** command.

Example 8-3 Viewing File Contents

```

pixfirewall#more test.cfg
: Saved
: Written by enable_15 at 10:04:01 Apr 14 2005
xxx Version x.x(x)
nameif vlan300 outside security10
enable password 8Ty2YjIyt7RRXU24 encrypted

```

Use the **mkdir** command to create a new directory. If a directory with the same name already exists, the new directory is not created. To remove the existing directory, use the **rmdir** command. If the directory is not empty, the **rmdir** command fails. Use the **cd** command to change the current working directory to the one specified. If a directory is not specified, the directory is changed to the root directory. The syntax for the **mkdir**, **rmdir**, and **cd** commands is as follows:

```

pixfirewall#mkdir [/noconfirm] [dik0: | disk1: | flash:] path
pixfirewall#rmdir [/noconfirm] [dik0: | disk1: | flash:] path
pixfirewall#cd [dik0: | disk1: | flash:] path

```

To copy a file from one location to another, use the following command:

```

pixfirewall(config)#copy [/options] {url | local:[path] | running_config | startup-config}
{running-config | startup-config | url | local:[path | image | pdm]}

```

For example:

```

pixfirewall(config)#copy disk:my_context/my_context.cfg startup-config
pixfirewall(config)#copy disk:my_context/my_context.cfg running-config

```

When the PIX Security Appliance software is installed, the existing activation key is extracted from original image and stored in a file in PIX file system. On systems that support removable Flash media, when you log in to the security appliance during normal operation, you can copy

the application software or Cisco Adaptive Security Device Manager (ASDM) software to the Flash file system from a TFTP, FTP, HTTP, or HTTPS server using the following command:

```
pixfirewall(config)#copy tftp://server[/path]/filename flash://filename
```

For example:

```
pixfirewall(config)#copy tftp://10.0.0.3/cisco/123file.bin flash://123file.bin
```

Image, configuration, and ASDM files can be installed in either internal or removable media, or both. Images stored on removable media are not booted by default, unless the **boot system** command exists in the startup configuration and points to that image.

For multiple context mode, the administrator must be in the system execution space. Make sure to have network access to the server:

- For single context mode, configure any interface, the IP address of the interface, and any static routes required to reach the server.
- For multiple context mode, first add the admin context and configure interfaces, IP addresses, and routing to provide network access.

In single context mode, or from the system configuration in multiple mode, the startup configuration, running configuration, or a configuration file by name on disk, such as the admin.cfg, can be copied.

To copy the configuration file from an FTP server, enter the following command:

```
pixfirewall(config)#copy ftp://[user[:password]@]server[/path]/filename[;type=xx]startup-config
```

To copy the configuration file to an FTP server, enter the following command:

```
Hostname#(config)#copy {startup-config | running-config | disk0: [path/]filename} ftp://[user[:password]@]server[/path]/filename[;type=xx]
```

For example:

```
pixfirewall(config)#copy ftp://admin:letmin@10.0.0.3/configs/startup.cfg;type=an startup-config
```

Image Upgrade and Activation Keys

The **show version** command enables the administrator to display the software version, operating time since the last reboot, processor type, Flash partition type, interface boards, serial number, or BIOS ID, activation key value, license type, such as R or UR, and time stamp for when the configuration was last modified, as demonstrated in Example 8-4. The serial number listed with the **show version** command is for the Flash partition BIOS. This number is different from the serial number on the chassis. When a software upgrade is obtained, the serial number that appears in the **show version** command will be needed, not the chassis number.

Example 8-4 Viewing Version Information

```

pixfirewall#show version
This machine has a Restricted (R) License.
Serial Number:12345678
Running Activation Key: 0xbd27f269 0xbc7ebd46 0x1c73e474 0xbb782818 0x071dd0a6
Configuration has not been modified since last system restart.

```

The **copy tftp flash** command enables the administrator to change software images without accessing the TFTP monitor mode. The full syntax for this command is as follows:

```
pixfirewall(config)#copy tftp://server [/path]/filename flash:/filename
```

This command can be used to download a software image via TFTP with any PIX Security Appliance model running version 5.1 or later. The image that is downloaded is made available to the PIX on the next reload.

Be sure to configure the TFTP server to point to the image to be downloaded. For example, to download the `pix611.bin` file from the D: partition on a Windows system whose IP address is 10.0.0.3, access the Cisco TFTP Server **View > Options** menu and enter the filename path, such as `D:\pix_images`, where the image is located. Then, to copy the file to the PIX Security Appliance, use the following command:

```
pixfirewall#copy tftp://10.0.0.3/pix700.bin flash
```

The TFTP server receives the command and determines the actual file location from its root directory information. The server then downloads the TFTP image to the PIX.

Note

The TFTP server must be running when the **copy tftp** command is entered on the PIX Security Appliance.

Entering a New Activation Key

You can upgrade the license for the PIX Security Appliance using the following command:

```
Pixfirewall(config)#activation-key [activation-key-four-tuple | activation-key-five-tuple]
```

Before entering the activation key, ensure that the image in Flash and the running image are the same. You can do so by rebooting the PIX before entering the new activation key. The PIX also needs to be rebooted after the new activation key is entered for the change to take effect.

Enter the *activation-key-four-tuple* as a four-element hexadecimal string with one space between each element, or *activation-key-five-tuple* as a five-element hexadecimal string with one space between each element, as follows:

```
0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

The leading **0x** specifier is optional. All values are assumed to be hexadecimal. The key is not stored in the configuration file. The key is tied to the serial number.

Use the **activation-key** command to enter an activation key. In this command, replace *activa-*

tion-key-four-tuple with the activation key obtained with the new license, as follows:

```
activation-key 0x12345678 0xabcdef01 0x2345678ab 0xcdef01234
```

After the activation key is entered, the system displays an indication that the activation key has been successfully changed.

Reload the PIX Security Appliance to activate the Flash activation key.

Upgrading the Image and the Activation Key

If the image is being upgraded to a newer version and the activation key is also being changed, reboot the system twice. After the key update is complete, the system is reloaded a second time so that the updated licensing scheme can take effect.

If an image is being downgraded, the PIX Security Appliance needs to be rebooted only one time, after installing the new image. In this situation, the old key is both verified and changed with the current image.

To view the current activation key, enter the **show activation-key** command. Table 8-1 shows error messages that might be returned in the output from this command, along with steps that you can take to resolve the errors.

Table 8-1 Troubleshooting the Activation Key Upgrade

Message	Problem and Resolution
The activation key you entered is the same as the running key.	Either the activation key has already been upgraded or you need to enter a different key.
The Flash image and the running image differ.	Reboot the PIX Firewall and reenter the activation key.
The activation key is not valid.	Either you made a mistake entering the activation key or you need to obtain a valid activation key.

Summary

Having completed this chapter, you should be familiar with virtual firewalls and how they allow the PIX Security Appliance to be separated into multiple, independent firewalls called security contexts. You should be able to discuss how security contexts can be managed and configured independently of one another.

You should also be familiar with methods of PIX Security Appliance failover, why it is necessary, and how to configure it. Failover options and their configurations were discussed. Also discussed in this chapter was the transfer of state information between failover peers. Hardware-based and stateful failover were discussed, and precautions about the type of interconnection between the peers were introduced.

This chapter also discussed the configuration of a PIX Security Appliance as a Layer 2, or transparent, firewall. You should be able to discuss the configuration and available features of a PIX Security Appliance that is in this mode.

Remote-access techniques for maintenance of PIX Security Appliances were introduced. This included the use of SSH and Telnet as access methods. The command-authorization system was discussed, along with how to assign users to levels and levels to command words.

Check Your Understanding

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. Answers are listed in Appendix A, “Check Your Understanding Answer Key.”

1. The system configuration does not include any network interfaces or network settings for itself. Instead, when the system needs to access network resources, such as downloading the contexts from the server, it uses one of the contexts that is designated as the admin context.
 - a. True
 - b. False
2. The security context mode has one of the following configurations:
 - a. single or double mode
 - b. single or multiple mode
 - c. enabled or disabled mode
 - d. static or dynamic mode
3. What are the two types of hardware failover? (Choose two.)
 - a. Active/standby
 - b. Primary/secondary
 - c. Active/active
 - d. Active/passive
4. A failover occurs when block memory exhaustion occurs for how many consecutive seconds:
 - a. 5 seconds
 - b. 10 seconds
 - c. 15 seconds
 - d. 20 seconds
5. What are the three types of failover links?
 - a. Serial failover cable
 - b. LAN-based failover cable
 - c. Ethernet failover cable
 - d. Stateful cable

6. A transparent firewall is a Layer 2 firewall that acts like a bump in the wire, or a stealth firewall, and is seen as a router hop to connected devices.
 - a. True
 - b. False
7. Which of the following is true of the transparent firewall mode?
 - a. Transparent mode only supports two interfaces, typically an inside interface and an outside interface, and it can run both in single and multiple mode.
 - b. Transparent mode only supports one interface, typically an inside interface, and it can run both in single and multiple mode.
 - c. Transparent mode only supports two interfaces, typically an inside interface and an outside interface, and it can run only in the single mode.
 - d. Transparent mode only supports one interfaces, typically an outside interface, and it can run only in the multiple mode.
8. The transparent PIX Security Appliance does not pass Cisco Discovery Protocol (CDP) packets.
 - a. True
 - b. False
9. The PIX Security Appliance supports up to how many privilege levels?
 - a. 2
 - b. 5
 - c. 10
 - d. 16
10. Password recovery for PIX Security Appliance versions through 6.3 requires a TFTP server.
 - a. True
 - b. False