Basics of the PIX Firewall

Terms you'll need to understand:

- ✓ Inside (trusted)
- ✓ Outside (untrusted)
- ✓ DMZ
- ✓ Bastion hosts
- ✓ Packet filters
- ✓ Proxy filters
- ✓ Stateful packet filters
- ✓ Embedded operating system
- ✓ URL filtering
- ✓ Failover, hot standby
- ✓ Activation keys

Techniques you'll need to master:

- ✓ Security levels
- ✓ Software licensing
- ✓ Adaptive Security Algorithm (ASA)
- ✓ Cut-Through proxy
- ✓ Traffic flow
- ✓ Hardware differences between models

There are several areas of a network in a secure environment; the most common are the inside, the outside, and the DMZ firewalls that help divide and control traffic between them. Cisco has designed the PIX series of firewalls to be the primary devices for performing these functions. This chapter covers the basics of the PIX firewall areas that connect to the firewall—the trusted, untrusted, and DMZ.

Trusted, Untrusted, and DMZ Defined

The PIX firewall always contains trusted and untrusted areas that are used to identify the types of areas around the firewall. Firewalls with more than two interfaces can contain areas called DMZs. These areas are created to support servers that need to be accessed from an untrusted area without compromising the trusted locations. This section covers each in more detail.

Trusted

The term *trusted* is used to refer to users and computers that are in an area considered more secure or protected. This area is typically a private section of the network that needs to be protected against malicious hackers and other security threats. Security in the trusted area is established by blocking all traffic from less trusted sections of the firewall.

Untrusted

The term *untrusted* defines areas of the network that might contain malicious hackers or other security threats. One good example of an untrusted area is the Internet side of your firewall or even segments of your own internal network that are exposed to unknown access. Such an area could be a segment exposed to outside use—for example, kiosk computers on a storeroom floor.

DMZ

The *demilitarized zone (DMZ)* sits between both trusted and untrusted areas and usually hosts computers that need to be available to users from both of these areas. For example, a Web server in the DMZ can be accessed by people on the Internet, which is untrusted, as well as by users in the private trusted network. From the perspective of the inside, private, and trusted portion

of your network, the DMZ area is considered untrusted, so traffic initiated from computers in the DMZ is blocked.

Areas of a Network

Areas of the network are defined by where the traffic is initiated from and where it is flowing to. For example, as traffic on the corporate side of a firewall flows toward the Internet, it is known as traffic flowing from the trusted inside (corporate) to the untrusted outside area of the network.

Firewalls help us divide the networks into the trusted, DMZ, and untrusted areas. The most basic firewall configuration contains only two interfaces—the inside (trusted) and the outside (untrusted)—and there is no official DMZ (see Figure 3.1). If two basic firewalls are stacked together, a DMZ area can be created between them, as shown in Figure 3.2. However, most high-end models of firewalls contain at least three interfaces and are correspondingly called *three-pronged* firewalls, as shown in Figure 3.3. The inside interface connects to the trusted area; the outside connects to the untrusted area; and the DMZ connects to the semi-trusted area. In all these types of setups, most environments contain a perimeter router used to provide Internet service provider (ISP) connection.

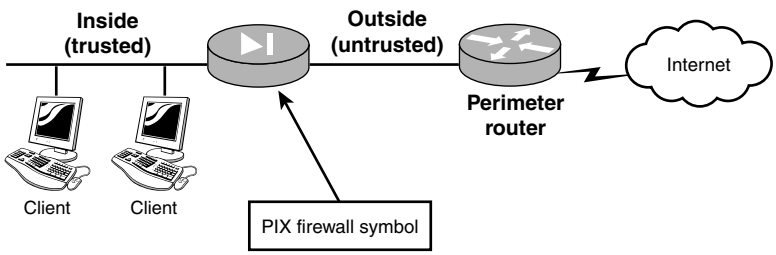

Figure 3.1 Standard firewall without a DMZ.

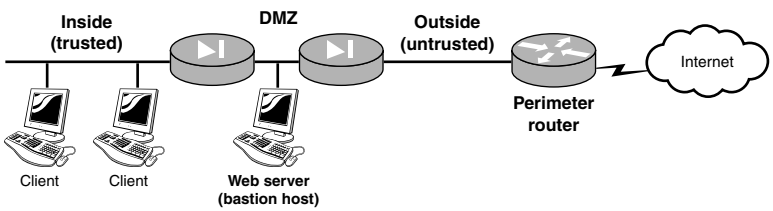

Figure 3.2 Stacked firewall with a DMZ.

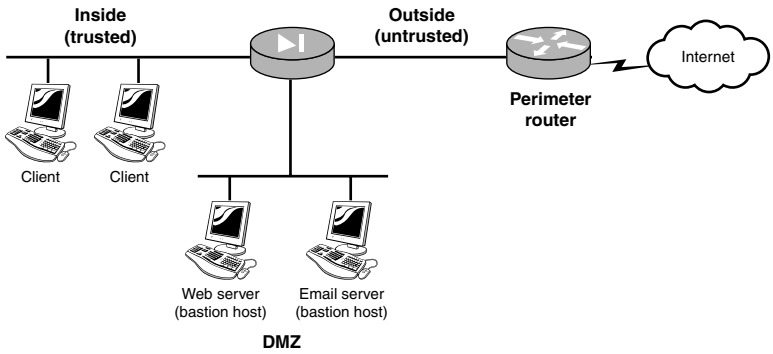

Figure 3.3 Three-pronged firewall.

Inside (Trusted)

The inside interface connects the trusted section of the network to untrusted areas such as the DMZ and Internet. It's worth keeping in mind that trusted areas might not always be made up of users needing protection only from the Internet; they might also require protection from other internal corporate users. For example, an engineering team might need to protect its secret widget network from the probing eyes of other users within the company; the computers hosting the top-secret widget data would then be attached to the inside interface of a PIX firewall.

Outside (Untrusted)

The outside interface connects the firewall to the most untrusted areas, such as the Internet. A firewall's primary function is to protect the DMZ and inside areas from undesired traffic originating from the outside interface. Traffic from the inside and DMZ can travel through the outside interface to the untrusted area, but traffic from the untrusted area is blocked from entering. Consider Jack, for example, a user on the inside interface who is allowed to connect to the Internet and check for the latest GPS software release dates. On the other hand, Jimmy the evil hacker cannot connect to Jack's computer because Jimmy's traffic is originating on the outside interface.

If necessary, a firewall can allow traffic initiated from the outside to connect to computers within the DMZ or inside area. However, you must manually configure the firewall to allow this traffic, and in doing so you effectively

allow a security hole. So, be careful. The more traffic you allow from the outside to inside or DMZ areas, the higher probability a hacker will find an open IP address or port and send an attack toward it. So, typically a few holes are created to allow only what is required through. For example, port 80 might be opened to allow traffic to pass through the firewall to a Web server in a DMZ area and all other traffic would be blocked.

Demilitarized Zone Details

The demilitarized zone is an isolated portion of the network that contains computers called *bastion hosts*. Bastion hosts are systems that have been hardened by applying lock-down procedures, turning off unnecessary services, and installing security patches. These hosts are placed in the DMZ when access from the outside areas need to reach services on these computers. Web, email, and FTP programs are a few of these types of services with which you might be familiar. As an example, if Company B has a Web server that it needs to allow Internet users to access, Company B places the Web server in the DMZ, hardens the system, and configures the firewall so that outside users can have access to this single system. Because bastion hosts can be accessed from the Internet or other untrusted areas, always remember that Jimmy the evil hacker can potentially be attacking this system. So, always have backups of your bastion hosts!

Computers in the DMZ can be non-bastion hosts also, meaning they have not been hardened with software patches and have had unused services and programs removed or disabled. However, they are high-risk systems just looking for trouble from hackers.

Perimeter Routers

Perimeter routers, also called *border routers*, provide the final connection to the Internet or untrusted networks. Typically, these devices do not provide many security features; their function is simply to provide an interface to an ISP or a wide area network (WAN) connection. A perimeter router can, for instance, connect an Ethernet local area network (LAN) to a digital subscriber line (DSL) modem—or, better yet, a high-speed, enterprise-grade satellite link. They can provide a basic isolation from the ISP and also provide basic packet filtering to traffic before it reaches the firewall, adding to your security suite.

Types of Firewall Filtering Technologies

Basic firewalls provide protection from untrusted traffic while still allowing trusted traffic to pass through. Packet filters, proxy filters, and stateful packet filters are some of the technologies used to accomplish this protection. Each one works in a different way to filter and control traffic.

In Table 3.1, the seven-layer Open System Interconnect (OSI) model is shown as a reference for the discussion of these three types of technologies.

Table 3.1 The OSI Model

Layer	Name	Examples
7	Application	Telnet, HTTP, FTP, SSH, and so on
6	Presentation	ASCII, PDF, MP3, BMP, GIF, JPG and so on
5	Session	RPC, SQL, NetBIOS
4	Transport	TCP and UDP
3	Network	IP and ICMP
2	Data Link	Ethernet and Token Ring
1	Physical	Wireless, fiber, and copper wire

The next section describes in more detail the three methods of providing protection to a network. Each method works from the seven-layer OSI model to provide protection to a network or networks.

Packet Filter

Packet filters are the most basic traffic control mechanism of the three technologies. By inspecting layer 3 and layer 4 information, these filters allow traffic to pass through, provided that the source and destination information match the configured rule. The types of information in layers 3 and 4 that are used by packet filters include

- Source IP address
- Source port
- Destination IP address
- Destination port
- Protocol, such as TCP, UDP, IP, and ICMP

Packet filters can be implemented using access control lists (ACLs), which are commonly found on most Cisco IOS routers. Figure 3.4 shows a router between the private network and the Internet.

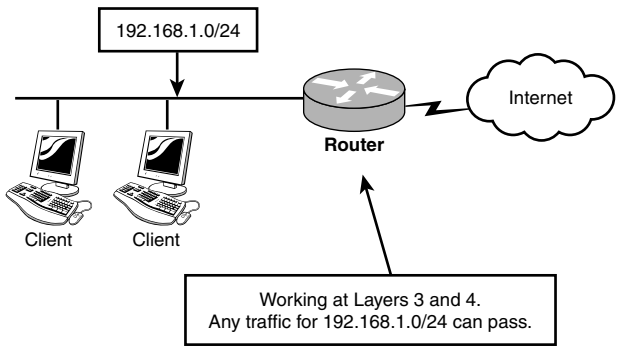

Figure 3.4 Basic packet filter.

The packet filter (Cisco IOS) examines every packet against the ACLs for matches. If a match is found, the packet is either permitted or denied passage through the interface. If a match is not found, the packet is implicitly denied passage. Packet filters process information only up to layer 4, making them very fast and efficient. However, packet filters don't track the TCP session information generated when two computers are communicating with one another. When computers first start to communicate using TCP, they perform a three-way handshake, which is used to establish the TCP session. Because these sessions aren't monitored by packet filters, the computers become vulnerable to spoofing.

Spoofing is the process by which a hacker modifies source information with the intention of bypassing a standard packet filter. The filter examines the packet, determines that the (modified) source is acceptable, and passes it. This enables a hacker to disguise *(spoof)* his attacks as legitimate traffic originating from a computer internal to the network.

Proxy Filter (Server)

Proxy filters, also known as *application proxy servers*, extend beyond the reach of packet filters by examining information from layers 4–7. A proxy server sits between the client and the destination working as a middleman between the two communicating parties (see Figure 3.5). It requires the client to establish a session with the proxy itself, which in turn creates a second session between itself and the destination. Consider, for instance, a client computer that requests information from a remote Web site. The client creates

a session with the proxy server, which can then authenticate the user for valid access to the Internet before creating a second session between the Web site and itself. As the information comes back from the Web site, the proxy server examines layers 4–7 for a valid connection to the inside network.

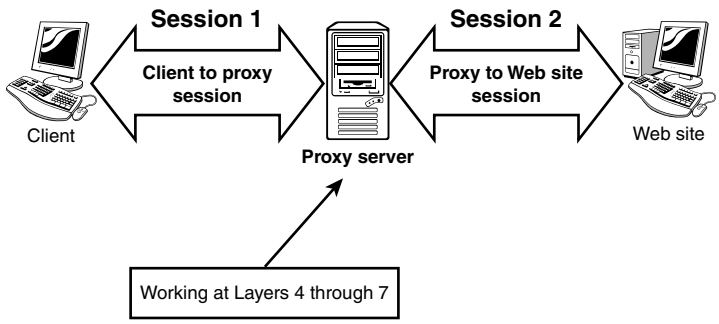

Figure 3.5 Proxy server sessions.

Although proxies can provide some of the most effective measures of protection, they can introduce speed and performance issues, particularly when a large number of sessions are being simultaneously negotiated. They are also built on general-purpose operating systems such as Unix, Linux, or Microsoft Windows, which can make them vulnerable to OS-related attacks.

Stateful Packet Filter—Stateful Inspection

This type of firewall combines the speed of packet filters with the enhanced security of stored session information typified by proxies. While traffic is being forwarded through the firewall, stateful inspections of the packets create slots in session flow tables. These tables contain source and destination IP addresses, port numbers, and TCP protocol information. Before traffic can travel back through the firewall, stateful inspections of the packets are cross-referenced to the session flow tables for an existing connection slot. If a match is found in the tables, the packets are forwarded; otherwise, the packets are dropped or rejected. The Cisco PIX firewall uses stateful inspection as its primary method to control traffic flow. Figure 3.6 shows the client and session flow tables being used.

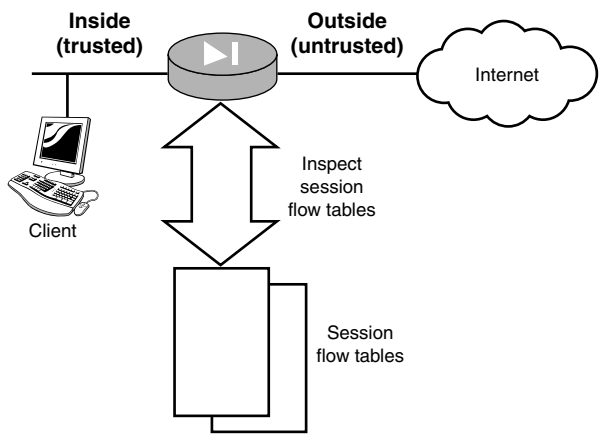

Figure 3.6 Stateful inspection.

Cisco PIX Firewall Features

Cisco PIX firewalls bring together a plethora of powerful features that make the PIX series one of the best choices in the appliance firewall market. Embedded operating system, Adaptive Security Algorithm, cut-through proxy, VPN support, URL filtering control, and hot standby failover capabilities are just some of the features that make it one of the best choices.

Embedded Operating System

The PIX firewall appliance is a dedicated system providing one main function, and that is to be a firewall. Unlike other firewalls that run on general-purpose operating systems such as Linux, Unix, or Microsoft Windows, the PIX series runs on a proprietary embedded operating system using a simplified kernel. This allows for both enhanced speed and protection against known operating system vulnerabilities.

Adaptive Security Algorithm

The adaptive security algorithm (ASA) is the heart of the PIX firewall. It controls all traffic flow through the PIX firewall, performs stateful inspection of packets, and creates remembered entries in connection and translations tables. These entries are referenced every time traffic tries to flow back

through from lower security levels to higher security levels. If a match is found, the traffic is allowed through. Finally, the ASA provides an extra level of security by randomizing the TCP sequence numbers of outgoing packets in an effort to make them more difficult to predict by hackers.

Cut-Through Proxy

Cut-through proxy is the capability of the PIX firewall to control which users have access to the system. It does this by requiring a username and password authentication for users who want to use HTTP, Telnet, or FTP across the firewall. The authentication occurs only once, making the process extremely fast and efficient, especially when compared to the same type of technologies available on application proxies that authenticate every packet. If you need to support other protocols that fall out of the HTTP, Telnet, or FTP realm, you can use a technology named Virtual Telnet. This is covered in a later chapter.

Virtual Private Networks

Virtual private network (VPN) support by the PIX firewall is one of the core features that enables flexibility in a variety of environments. The PIX supports both site-to-site and remote-access VPNs encryption. This dual support provides the ability to connect two branch offices together using only PIX firewalls on each side (site-to-site), or to connect remote users to the office via a VPN across the Internet (remote-access). IPSec, PPTP, and L2TP are the main VPN technologies supported.

URL Filtering

In many situations, a set of valid and invalid Web site addresses might be an appropriate and effective way to filter network traffic. In response to this, Cisco PIX firewalls have integrated an advanced feature of URL filtering that enables the PIX firewall to work with content filtering services. These services allow the capturing of World Wide Web requests to support the enforcement of policies or monitor user traffic. For example, if Jack requests to go to `www.JackGPS.com`, the PIX forwards this request to a content server that references a database of valid or invalid Web sites. If the content server gives the PIX the okay, Jack is allowed to access this Web site. The PIX firewall supports only two content servers: WebSense and N2H2. These products enable administrators to create acceptable and unacceptable Web site lists for their users' Internet access.

Failover/Hot Standby

Today's applications are often mission critical, requiring the reliability of a resilient network infrastructure to support them. In response to this, Cisco PIX firewalls support hot standby failover features. *Failover* is the capability to link two PIX firewalls together, creating an active and a standby failover configuration. If the active firewall fails, the standby firewall assumes the IP and MAC addresses of the once-active, failed firewall. *Hot standby* means that this failover occurs without the need for a power reset that other systems can require. This failover capability helps provide a fault-tolerant firewall system with reduced human intervention.

ASA Security Rules

A PIX firewall has a very simple mechanism to control traffic between interfaces. The ASA uses a concept of security levels to determine whether traffic can pass between two interfaces. The higher the security level setting on an interface, the more trusted it is.

Security Levels

The ASA allows traffic to pass from trusted to untrusted, but not the reverse. Therefore, traffic can pass from interfaces with higher security levels to interfaces with lower security levels. Correspondingly, ASA blocks traffic from interfaces with lower settings from passing through to interfaces with higher settings. To illustrate, consider a common scenario where the inside interface has a security level number of 100 and the outside has a level of 0. The ASA allows traffic to pass from the inside to the outside; however, the ASA prevents traffic from flowing from the outside to the inside because the inside has a higher security level.

Figure 3.7 shows a three-pronged firewall with different security levels on each interface. Interface e0 has security a level of 0, which makes it the lowest security level of all the interfaces. Any traffic initiated on this side of the firewall will not be able to communicate with computers on the other side of the firewall.

The following are the primary security levels created and used on the PIX firewall:

- *Security level 100*—The highest possible level, it is used by the inside interface by default. Using the trusted-untrusted terminology, this level is considered the most trusted.

- *Security level 0*—The lowest possible level, it's used by the outside interface by default, making it the most untrusted interface. Traffic can pass from this interface to other interfaces only if manually configured to do so.
- *Security levels 1–99*—Can be assigned to any other interface on the PIX. On a three-pronged PIX firewall, the inside is typically 100, the outside is 0, and the third interface could be 50. Traffic from interfaces between 1 and 99 can pass through to the outside (0), but it is prevented from passing to the inside (100). This is because the interface has a lower security level setting than the inside.

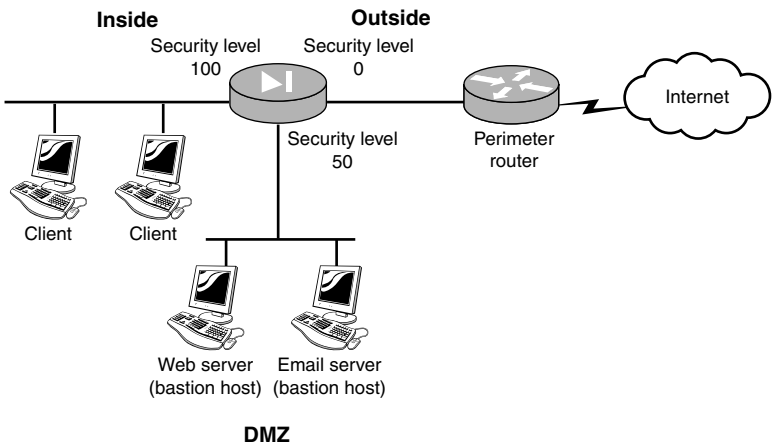

Figure 3.7 Security levels.

Security levels are a very import concept with PIX configuration. Remember, only higher security-level traffic can pass to lower security-level interfaces by default. The default value for the inside interface is 100, and the outside value is 0.

Connection and Translation Tables

The ASA uses two tables to track traffic flowing through the PIX—the connection table and the translation (xlate) table. The *connection* table contains a reference to the session connection between the two computers that are talking. The *translation* table maintains a reference between the inside IP address and the translated global IP address. These topics are covered in further detail later.

PIX Firewall Models

The Cisco PIX firewall comes in several models. Unlike the Cisco router series that requires different software for each model, software on the PIX is the same for all models. The only differences across firewall models are size of the unit, power supply capabilities, number of interfaces supported, and failover capabilities.

The four main PIX models are listed here. Table 3.2 displays the firewall model specifications in detail.

The models are as follows:

- PIX 501
- PIX 506E
- PIX 515E
- PIX 525
- PIX 535

Table 3.2 displays the default capabilities found on the PIX firewall hardware models.

Table 3.2 PIX Firewall Models

Model	501	506E	515E	525	535
Processor	133MHz	300MHz	433MHz	600MHz	1GHz
RAM	16MB	32MB	32MB, 64MB	256MB	1GB
Flash memory	8MB	8MB	16MB	16MB	16MB
Throughput	10Mbps	20Mbps	188Mbps	360Mbps	1Gbps
Connections	7,500	25,000	130,000	280,000	500,000
Max. number of interfaces	1, + 1 four-port switch	2	6	8	10
Failover	No	No	Yes	Yes	Yes
VAC available	No	No	Yes	Yes	Yes
Solution for	Small-office/ home-office (SOHO)	Remote-office/ branch-office (ROBO)	Medium-size office	Enterprise	Enterprise or solution provider

Make sure you know for which solution each firewall model is designed and the simultaneous connections each supports.

Cisco PIX 501 Firewall

The PIX 501 is the entry model into Cisco's firewall family and is intended for small-office/home-office (SOHO) locations. This model has a fixed physical configuration that supports two network interfaces and a single console port for configuration. The inside interface, Ethernet 1, contains a four-port 10/100Mbps Ethernet switch, and the outside interface, Ethernet 0, is a single 10Mbps Ethernet port. The model runs on a 133MHz AMD processor with 16MB of RAM and 8MB of flash memory. The 501, like all PIX firewalls, supports VPN capabilities. A free license for DES IPSec encryption can be acquired; alternatively, for a fee an upgrade to triple DES–level encryption can be obtained. The basic model comes with a 10-user license with VPN DES IPSec support out of the box and can be later upgraded to a 50-user license as required for enhanced scalability.

Figure 3.8 shows the interfaces and console port on the back of the PIX 501. Interfaces 1, 2, 3, and 4 are a four-port switch for the Ethernet 1 interface.

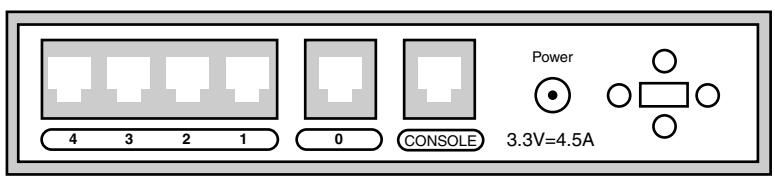

Figure 3.8 The PIX 501's back panel.

Cisco PIX 506E Firewall

The 506E is a newer, enhanced model of the earlier 506 versions and is intended for remote-office/branch-office (ROBO) locations. This model, similar to the 501, has a fixed physical configuration, supporting two 10/100MHz Ethernet interfaces and a single console port for configuration. The 506E, however, has a 300MHz Intel Celeron processor with 32MB of RAM and 8MB of flash memory. The throughput and processor speed are double that of the 501 model, resulting in a compact and efficient firewall package. Lastly, a USB port is reserved for future enhancements.

Figure 3.9 shows the interfaces on the back of a PIX 506. Notice it has only a single interface on Ethernet 1, unlike the PIX 501 that contains a four-port switch for Ethernet 1.

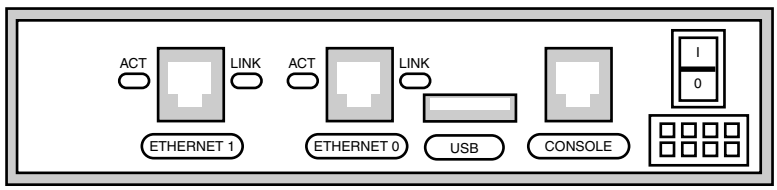

Figure 3.9 The PIX 506's back panel.

Cisco PIX 515E Firewall

The 515E is a newer, enhanced model of the earlier 515 versions and is intended for the small to medium-size enterprise market. The model comes in a 1U form factor and has expandable capability that allows for up to six interfaces, as well as failover features and a VPN accelerator card (VAC) available with additional licensing options. The 515E uses a 433MHz Intel Celeron processor with 32MB or 64MB of RAM and 16MB of flash memory.

Figure 3.10 shows an example to the PIX 515E back view. The 15-pin connection on the right is used for the failover cable that can be connected to another PIX 515E to provide failover capability. The USB port is used for future enhancements.

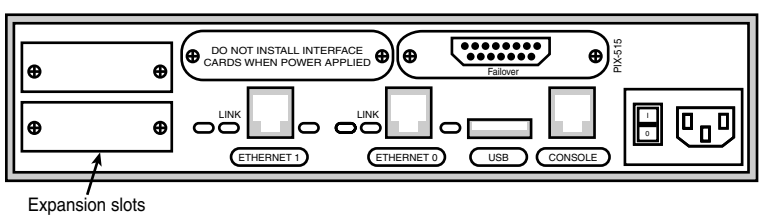

Figure 3.10 The PIX 515E's back panel.

Cisco PIX 525 Firewall

The 525 is the replacement model for its predecessor, the PIX 520. The 520 actually contained a floppy drive, whereas the 525 does not. The model is extremely powerful and is designed for large enterprise environments in which speed and failover capabilities are a must. It ships in a 2U form factor

with expandability that allows for up to eight interfaces, failover features, and a VAC. The PIX 525 uses a 600MHz Intel Pentium III processor with up to 256MB of RAM and 16MB of flash memory. The license schema on this model is based on the number of interfaces and failover support. Lastly, it contains a USB port reserved for future enhancements.

Figure 3.11 displays a typical 525 PIX firewall back view.

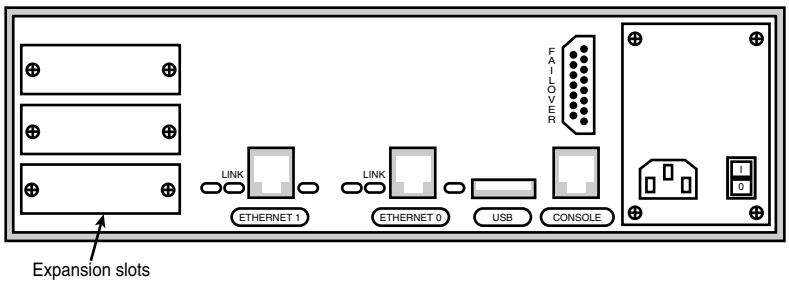

Figure 3.11 The PIX 525's back panel.

Cisco PIX 535 Firewall

The 535 is Cisco's enterprise-class firewall. This model is a 3U form factor that is highly configurable, supporting up to 10 interfaces, some of which can be fiber interfaces. The specification sheet boasts 1Gbps throughput; 500,000 concurrent connections; and 2,000 VPN tunnels. The speed and power of this firewall come from the 1GHz Intel Pentium III with 1GB of RAM. The 535 can contain four 66MHz/64-bit PCI slots and five 33MHz/32-bit PCI slots. The PIX 535 also contains dual redundant power supplies. Figure 3.12 displays the back view of a PIX 535. As you can see in Figure 3.12, three buses are available for Cisco expansion cards.

The PIX 535 supports two main types of PCI interface slots: 32-bit and 64-bit. Table 3.3 displays slot speeds.

Table 3.3 PIX 535 Interface Slots

Interface Slots	Bus Speed
Slots 0 and 1	64-bit/66MHz
Slots 2 and 3	64-bit/66MHz
Slots 4–8	32-bit/33MHz

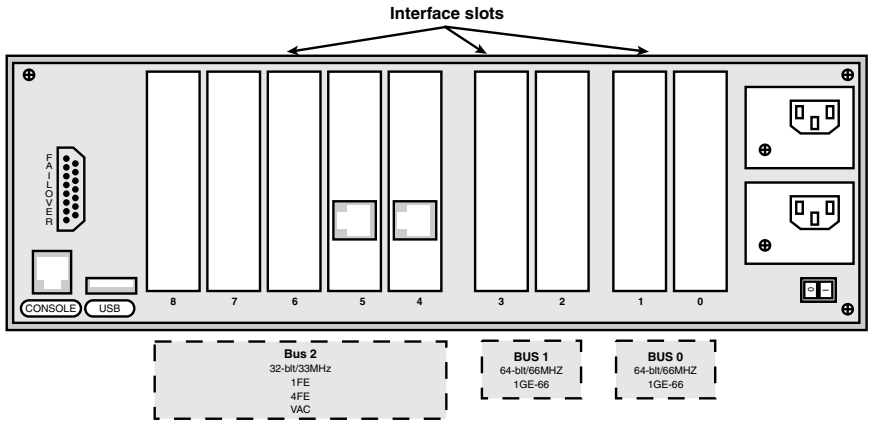

Figure 3.12 The PIX 535's back panel.

Cisco PIX Expansion Cards

Cisco provides several optional cards that can expand the PIX's capabilities and performance. The PIX-4FE card is a 33MHz/32-bit card that adds four Ethernet interfaces to your PIX. The PIX-VPN-ACCEL is designed to offload encryption and decryption from the main processor by using an onboard processor and hardware random number generator to increase VPN tunneling performance.

Table 3.4 displays several of the Cisco proprietary cards and their bus speeds.

Table 3.4 PIX Expansion Cards

Interface Card	Maximum Bus Speed	Description
PIX-1FE	32-bit/33MHz	Single-port 10/100 Fast Ethernet PCI expansion card
PIX-4FE	32-bit/33MHz	Four-port 10/100 Fast Ethernet PCI expansion card
PIX-VPN-ACCEL	32-bit/33MHz	3DES IPSec hardware VAC
PIX-1GE-66	64-bit/66MHz	Single-port Gigabit Ethernet 64-bit/66MHz PCI expansion card

The PIX-4FE and PIX-VPN-ACCEL 32-bit/33MHz cards can be installed only in 32-bit/33MHz slots. Other 32-bit/33MHz cards can be installed in either 66MHz slots or 33MHz slots.

The Console Port and Basic Connection

The console port is a serial null-modem connection used to configure the PIX. Most models, such as the ones mentioned here, use an RJ-45 connector, whereas older models use a standard DB-9 connector. You can use HyperTerm or other ANSI terminal emulation applications to connect to the PIX via the serial port on your PC.

Software Licensing and Activation Keys

The PIX firewall licensing is unique compared to some of Cisco's other products. PIX licensing usually doesn't require the installation of new software, unlike licensing for Cisco routers. The PIX uses activation keys to enable extra features such as adding more RAM, failover, extra interface cards, and so on. Activation keys are acquired by sending Cisco your serial number and the feature you want enabled (oh, and don't forget the cash, too!). Cisco then sends you a unique activation key computed from both the hardware serial number and the required new feature. Because the activation key is unique to each feature, you must get a new activation key if you replace your flash.

Displaying activation key information is straightforward. By using the `show version` command, you can display information such as the software version, hardware platform, enabled licensed features, serial number, and running activation key. Listing 3.1 displays the `show version` command and its output.

Listing 3.1 The show version Command

```
Pixfirewall# show version

Cisco PIX Firewall Version 6.2(2)
Cisco PIX Device Manager Version 2.1(1)
Compiled on Fri 07-Jun-02 17:49 by morlee
pixfirewall up 16 days 21 hours
Hardware:   PIX-501, 16 MB RAM, CPU Am5x86 133 MHz
Flash E28F640J3 @ 0x3000000, 8MB
BIOS Flash E28F640J3 @ 0xfffd8000, 128KB
0: ethernet0: address is 000c.3085.5640, irq 9
1: ethernet1: address is 000c.3085.5641, irq 10
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES:           Disabled
```

Listing 3.1 The show version Command *(continued)*

```
Maximum Interfaces: 2
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       10
Throughput:         Limited
IKE peers:          5

Serial Number: 807082785 (0x301b1b21)
Running Activation Key: 0x2d284af1 0xd032aa26 0x38b7db1f 0x70cfa8ee
Configuration last modified by enable_15 at 09:57:56.047 UTC Sun Mar 30 2003
```

The `show activation-key` command shows information about the activation key. Listing 3.2 displays the output of this command.

Listing 3.2 The show activation-key Command

```
pixfirewall# show activation-key
Serial Number: 807082785 (0x301b1b21)
Running Activation Key: 0x2d284af1 0xd032aa26 0x38b7db1f 0x70cfa8ee
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES:           Disabled
Maximum Interfaces: 2
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       10
Throughput:         Limited
IKE peers:          5
```

Updating the activation keys on the latest software release is a simple process. After you have received your new activation key from Cisco, you can use the `activation-key` command, like so:

```
activation-key <activation-key-four-tuple>
```

Here's another example of the `activation-key` command in use:

```
Pixfirewall(config)# activation-key 2d284af1 d032aa26 38b7db1f 70cfa8ee
```

Licensing

Cisco has three main types of licenses: restricted, unrestricted, and failover. Based on the original purchase agreement, *restricted* licenses support only certain features and allow a fixed number of users. As you need more functionality, you can just bolt them on by ordering activation keys. An *unrestricted* license is exactly what it sounds like: You get all the features your PIX can provide. However, as expected, these licenses can be expensive. Lastly,

failover licenses enable operation as an active or standby PIX firewall and are necessary only in failover scenarios. Additional licenses outside of the main three are available to address more advanced encryption features. For example, various licenses are available if you want to enable DES, triple DES (3DES), or AES encryption.