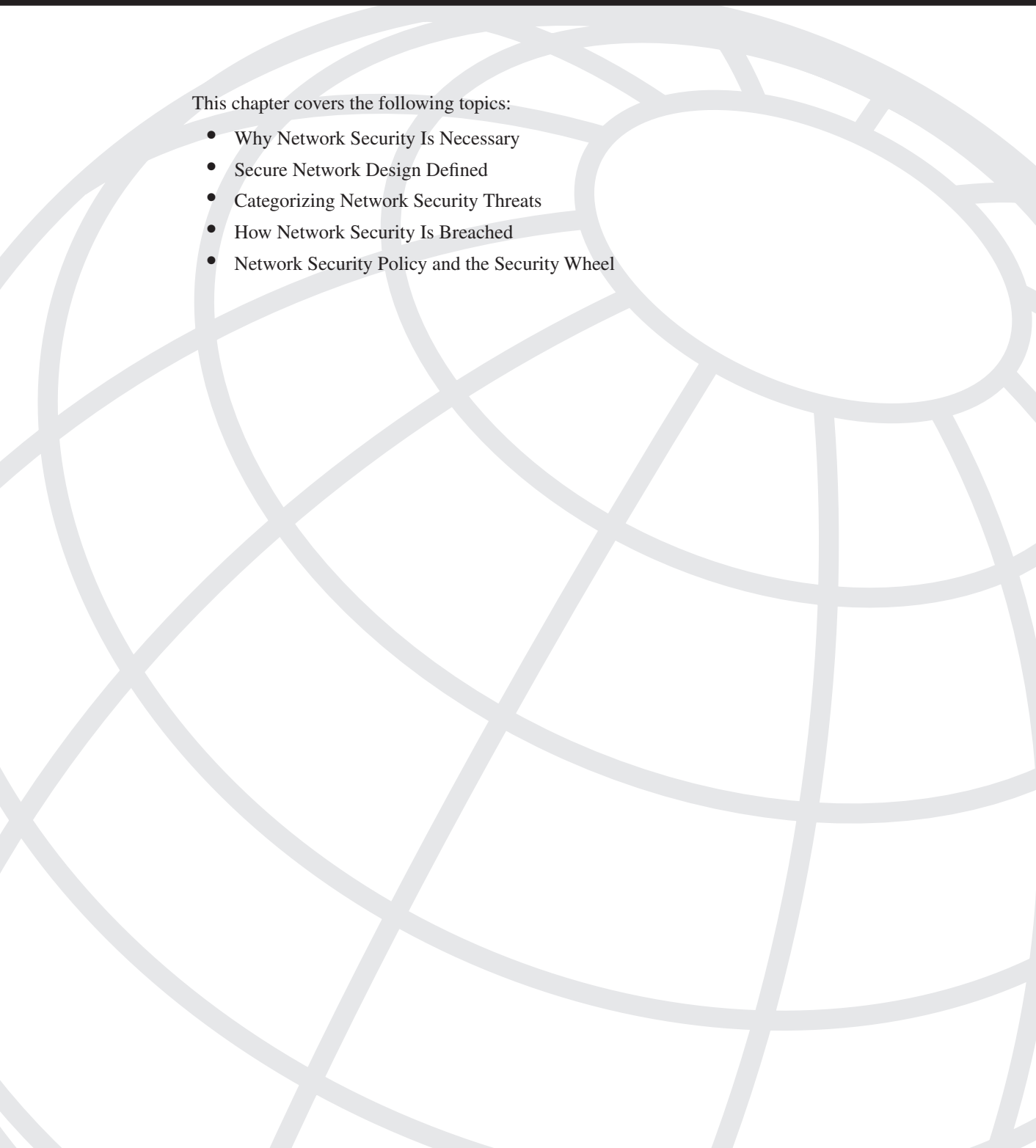


This chapter covers the following topics:

- Why Network Security Is Necessary
- Secure Network Design Defined
- Categorizing Network Security Threats
- How Network Security Is Breached
- Network Security Policy and the Security Wheel

CHAPTER 1

Introduction to Network Security

Computers, networks, and the Internet affect our lives every day. The fast-paced, technologically savvy world we live in today is ever more dependent upon computers and networking. This did not happen overnight. Although the advances in computer technology are occurring at a very fast rate, computers have been around for quite some time.

In the beginning of this wave of computer technology, many were unsure how far the wave was going to go. Some were hesitant to place much time and effort into something that might have turned out to be a fad. The number of people who were working on the advancement of computer technology was relatively small, compared to today's widespread needs. In their small community, computer enthusiasts were comfortable working with each other, and they trusted each other. Participation was invited. In such a freewheeling environment, the security of computers and the software that ran those computers was not given a very high priority. Much of the time security was an afterthought.

Why Network Security Is Necessary

Today, the Internet is made up of tens of thousands of networks, interconnected without boundary. Network security is essential in this environment because any organizational network is accessible from any computer in the world and, therefore, potentially vulnerable to threats from individuals who do not require physical access to it.

In a recent survey conducted by the Computer Security Institute (CSI), 70 percent of the organizations polled stated that their network security defenses had been breached and that 60 percent of the incidents came from within the organizations themselves.

While it is difficult to measure how many companies have had Internet-related security problems and the financial losses due to those problems, it is clear that the problems do exist.

Secure Network Design Defined

An *internetwork* is made up of many networks that are connected. When accessing information in an internetwork environment, secure areas must be created. The device that

separates each of these areas is known as a *firewall*. While it is true that a firewall usually separates a private network from a public network, that is not always the case. It is not unusual to use a firewall to separate network segments within a private network.

NOTE A firewall, as defined in Cisco Press's *Dictionary of Internetworking Terms and Acronyms*, is a "router or access server, or several routers or access servers, designated as a buffer between any connected public networks and a private network. A firewall router uses access lists and other methods to ensure the security of the private network."

A firewall usually has at least three interfaces, although many early implementations had two interfaces. It is still common to install a two-interface firewall. When using a firewall that has three interfaces, at least three networks are created. The three areas that are created by the firewall are described as follows:

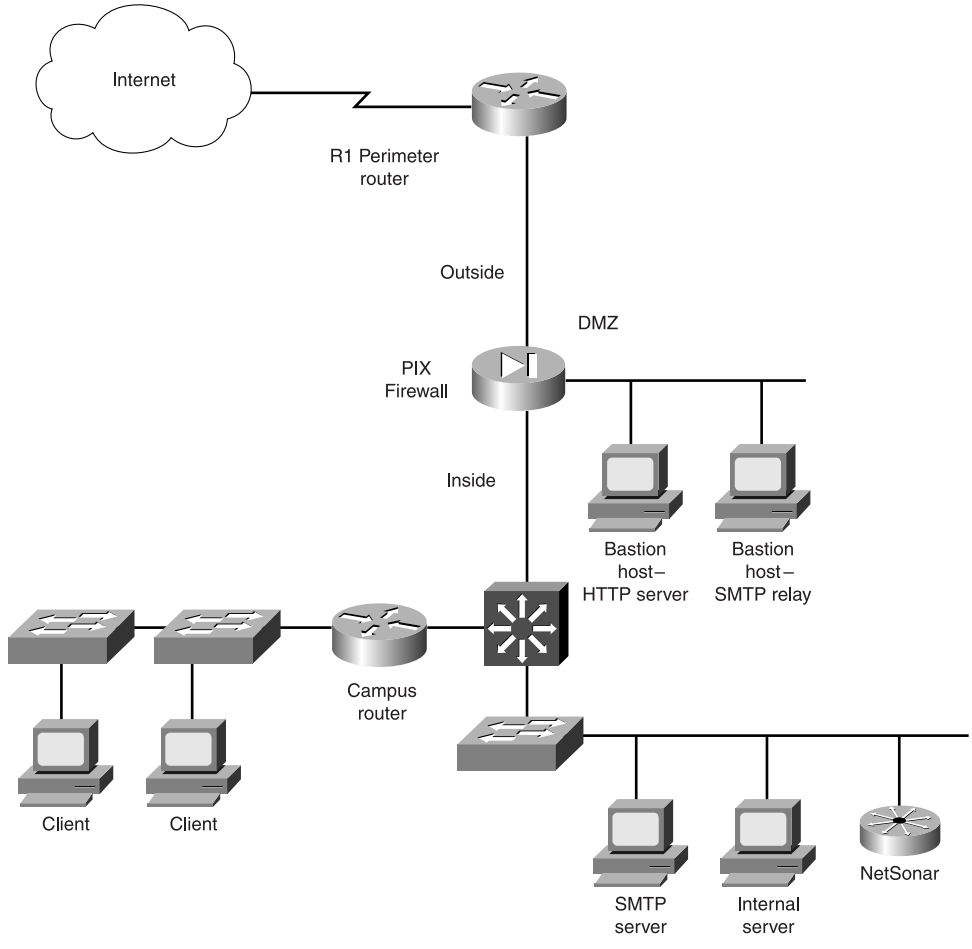
- **Inside**—The *Inside* is the *trusted* area of the internetwork. The devices on the Inside are the organization's private network (or networks). These devices share a common security policy relative to the Outside (the Internet) network. It is, however, a common practice to have a firewall to segment the trusted environment. If one department, such as Human Resources, needs to be protected from the rest of the trusted users, a firewall may be used.
- **Outside**—The *Outside* is the *untrusted* area of the internetwork. The firewall secures the devices on the Inside and DMZ from the devices on the Outside. In the course of doing business, organizations typically allow access to the DMZ from the Outside. If necessary, a firewall should be carefully configured for selective access from the Outside to hosts and services on the DMZ. If unavoidable, a firewall can be configured to allow access from a device on the Outside to a trusted device on the Inside. This is a much greater risk than permitting access from the Outside to the isolated DMZ.
- **DMZ (Demilitarized Zone)**—The DMZ is an isolated network, or networks, which is usually accessible to the Outside users. The firewall must be configured to allow access from the Outside or Inside to the DMZ. The creation of a DMZ allows an organization to make information and services available to Outside users in a secure and controlled environment. This permits access to Outside users, without allowing access to the Inside.

  The hosts or servers that reside on the DMZ are commonly referred to as *bastion hosts*. In this case, a bastion host is a host that is current with regard to its operating system and patches to that operating system. The action of being current will usually make it less vulnerable to attack because the vendor has fixed or "patched" any known security flaws. The bastion host is a host that is running only those services necessary

to make it perform its application duties. Unnecessary (and sometimes more vulnerable) services are turned off or removed from the host.

Figure 1-1 illustrates this general network design.

Figure 1-1 *General Network Design Using a Firewall*



The baseline perspective for a firewall is to perform the following functions:

- Permit no access from the Outside to the Inside.
- Permit limited access from the Outside to the DMZ.

- Permit all access from the Inside to the Outside.
- Permit limited access from the Inside to the DMZ.

In many network designs there are exceptions to some or all of these rules. For example, it may be necessary to allow SMTP messages from the Outside directly to the Inside. If an environment does not have an SMTP server in the DMZ or does not have an SMTP mail relay host in the DMZ, then it would be necessary to allow SMTP directly to the SMTP server that physically resides on the Inside. Permitting this traffic will significantly increase the risk to the internal network.

Another exception may be that all traffic is not permitted to traverse from the Inside to the Outside. Potentially an IP address, a subnet, or the entire Inside network may be restricted from utilizing a particular application (port). Another restriction imposed upon Inside to Outside data traffic may be URL filtering. Establishing an HTTP filter, such as a WebSense filter, and other exceptions will be discussed in later chapters.

Categorizing Network Security Threats

Network security threats can be categorized into four broad themes:

- **Unstructured threats**—These originate mostly from inexperienced individuals using easily available hacking tools from the Internet. Some of the people in this category are motivated by malicious intent but most are motivated by the intellectual challenge and are commonly known as *script kiddies*. They are not the most talented or experienced computer operators, programmers, or users, but they have the time and motivation.

  Script kiddies pose a very serious threat to network security. Many times a script kiddie unleashes a virus or Trojan Horse without actually knowing the full ramifications. The virus they unleash may reach worldwide proportions and cause millions of dollars of damage. In some cases, a virus may be unleashed that contains information that actually points back to the author of the virus.

NOTE A **virus** is malicious software that is attached to another trusted (or thought to be trusted) program to execute a particular unwanted function on a user's workstation. An example of a **virus** is a program that is attached to command.com (the primary interpreter for Windows systems) which deletes certain files and infects any other versions of command.com that it can find. A **Trojan horse** is different only in that the entire application was written to look like something else, when in fact it is an attack tool. An example of a **Trojan horse** is a software application that

runs a simple game on the user's workstation. While the user is occupied with the game, the **Trojan horse** mails a copy of itself to every user in the user's address book. Then other users get the game and play it, thus spreading the **Trojan horse**.

Unstructured threats that are only executed with the intent of testing and challenging a script kiddie's skills can still do a lot of damage to a company. For example, if your company's external web site is hacked, your company's integrity is damaged. Even if your external web site is separate from your internal information that sits behind a protective firewall, the public does not know that. All they know is that if your web site was hacked, then it is an unsafe place to conduct business.

- **Structured threats**—These originate from individuals who are more highly motivated and technically competent than script kiddies. They usually understand network systems design and the vulnerabilities of those systems. They can understand as well as create hacking scripts to penetrate those network systems. An individual who presents a structured threat typically targets a specific destination or group. These threats are from groups that may be involved with the major fraud and theft cases reported to law enforcement agencies. Occasionally, these hackers are hired by organized crime, industry competitors, or state-sponsored intelligence organizations.
- **External threats**—These originate from individuals or organizations working outside your organization, who do not have authorized access to your computer systems or network. They usually work their way into a network from the Internet or dialup access servers.
- **Internal threats**—Typically, these threats originate from individuals who have authorized access to the network. These users either have an account on a server or physical access to the network. An internal threat may come from a disgruntled former or current employee or contractor. Some studies have shown that a majority of security incidents originate from Internal threats.

How Network Security Is Breached

The three types of network attacks are

- **Reconnaissance attacks**—An intruder attempts to discover and map systems, services, and vulnerabilities.
- **Access attacks**—An intruder attacks networks or systems to retrieve data, gain access, or escalate their personal access privileges.
- **Denial of Service attacks**—An intruder attacks your network in such a way that damages or corrupts your computer system, or denies you and other authorized users access to your networks, systems, or services.

Reconnaissance Attacks

Reconnaissance is an unauthorized user's attempt to discover and map network system devices, services available on those systems, and the vulnerabilities of those systems. It is also known as *information gathering* and, in most cases, precedes an actual *access* or *Denial of Service (DoS)* attack.

The malicious intruder typically ping sweeps the target network first to determine what IP addresses are active and responsive. This can lead to the intruder finding information about what services or ports are active on the live IP addresses. From the active IP address information, the intruder queries the application ports to determine the application type and version as well as the type and version of operating system running on the target host.

NOTE A **ping sweep** is network reconnaissance technique that uses ping (ICMP echo and echo-reply) to map a known network.

Reconnaissance is somewhat analogous to a thief investigating a neighborhood for vulnerable homes to break into, such as an unoccupied residence, or an easy-to-open door or window. Just as a thief may rattle the door handle of a door without going in immediately if it is unlocked, the computer user on reconnaissance seeks to discover vulnerable services to be exploited at a later time, when there is less likelihood that anyone is paying attention.

Access Attacks

Access is a broad term that refers to the capability of a specific source (that is, a user on a computer, connected to a network that is connected to the Internet) to connect to a specific destination (that is, a computer on a network that is connected to the Internet). When a destination has been targeted, the attacker will attempt to use some software application to reach the destination. An access attack can come in the form of unauthorized data retrieval and manipulation, system access, or privileged escalation. Access attacks can also be used to gain control of a system and install and hide software that will be used later by the hackers.

Unauthorized Data Retrieval

Unauthorized Data Retrieval is simply reading, writing, copying, or moving files that are not intended to be accessible to the intruder. Sometimes this is as easy as finding share folders in Windows 9*x* or NT, or NFS exported directories in UNIX systems with read or read and write access to everyone. The intruder will usually have no problem getting to the files and, more often than not, the easily accessible information is highly confidential and

completely unprotected to prying eyes, especially if the attacker is already an internal user. The intruder *will* have a problem if the file is encrypted and cannot be read.

Unauthorized System Access

A *System Access* attacker gains access to a system without authorization. An intruder may gain system access through any of a number of ways. Some systems may not be password protected, providing easy access to the intruder. Gaining access into systems that do have some form of security may involve running a script or using a software tool that exploits a known vulnerability of the system or application being attacked.

Operating system weaknesses can also be exploited to provide unauthorized system access. Some aspects of an operating system were developed without security concerns in mind. Those security flaws may be patched in later operating system code, but if the patch is not installed, the flaw will exist.

Unauthorized Privilege Escalation

Legitimate users with a low level of access privilege perform this kind of attack. An intruder who simply gains a low level of access may also perform it. The intent is to get information or execute procedures that are not authorized at their lower level of access. In many cases, this involves gaining root access in a UNIX system and installing a sniffer to record network traffic. The ultimate goal is to find usernames and passwords that can be used to access another target.

In some cases, intruders only want to gain access without wanting to steal information—especially when the motive is intellectual challenge, curiosity, or ignorance.

DoS Attacks

DoS is when an attacker disables or corrupts networks, systems, or services in order to deny the service to its intended users. It usually involves crashing the system or slowing it down to the point that it is unusable. DoS attacks can also be as simple as wiping out or corrupting information necessary for business. In most cases, performing the attack simply involves running a hack, script, or tool. The attacker does not need prior access to the target, only a path to the target. Once the path is realized, great paralyzing damage can be caused. Because many DoS attacks are relatively easy to initiate and can be performed anonymously, it is the most feared attack on the Internet.

A *Distributed* Denial of Service (DDoS) attack is one in which the source of the attack is many computers (usually spread across a large geographic area) making it very difficult to find and stop the source(s).

Network Security Policy and the Security Wheel

Network security is a continuous process. It is necessary because of the continuous advancement in computer technology and use of that technology. With an understanding of the potential threats to network security, security for a system or group of systems should be built around a security policy.

According to RFC 2196, "Site Security Handbook":

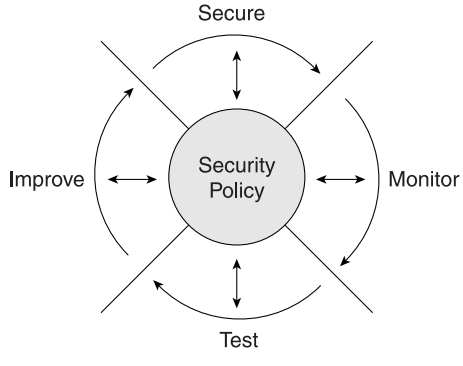
> A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide.

A security policy needs to accomplish the following tasks:

- Identify the organization's security objectives. Determine what you want to protect and how to do it. Understanding weak points in a network and how they can be exploited is a step toward strengthening those weak points.
- Document the resources to be protected. Learn how systems normally function so that you understand how devices are used and how data flows.
- Identify the network infrastructure with current maps and inventories. Consider the physical security of your network and how to protect it. Physical access to a device may give a user control over that device.

A continuous security policy is most effective because it promotes re-testing and reapplying of updated security measures on a continuous basis. The Security Wheel graphically represents this continuous security process. Figure 1-2 illustrates the four steps of the Security Wheel.

Figure 1-2 *The Security Wheel*



The security policy is the hub around which the four steps of the Security Wheel are based:

Step 1 *Secure* the system. Implement security devices and/or systems, with the intent to prevent unauthorized access to network systems:

(a) *Identification Authentication Systems*, such as One-Time Passwords (OTP), give access to authenticated and authorized users. Some examples of Identification Authentication Systems are Cisco Secure Access Control Server (CSACS), Windows Dial-up Networking, S/Key, CrytpoCard, and SecurID.

(b) *Encryption* can disguise traffic. Encrypting traffic can prevent unwanted disclosure to unauthorized or malicious users. This can ensure the confidentiality of the data traffic. IP Security (IPSec) is the standard encryption used on the Internet (The main RFC covering IPSec is RFC 2401) and will be covered in Chapter 11, "Configuring IPSec for Cisco PIX Firewalls."

(c) *Firewalls* can permit and deny specific data to allow only valid traffic and services.

(d) *Vulnerability Patching* is the act of applying fixes or measures to stop the exploitation of known vulnerabilities. This includes turning off services that are not needed on every system; the fewer services that are enabled, the harder it is for hackers to gain access.

(e) *Physical Security* is a very important, and sometimes overlooked aspect of securing the system. If someone is able to walk away with system hardware, all other security is moot. It is also important to protect unauthorized installation of promiscuous mode devices that could capture important data.

Step 2 *Monitor* the network for violations and attacks against the corporate security policy. Violations can occur within the secured perimeter of the network from a disgruntled employee or from the outside of the network from a hacker. A real-time intrusion detection system, such as the Cisco Secure Intrusion Detection System (CSIDS) can discover and prevent unauthorized entry. CSIDS can ensure that the security devices in Step 1 have been configured properly. Logging is an important aspect of monitoring. Keeping track of the data traffic that is flowing into a network can be the difference between discovering an attack and acting on it before it becomes a problem, and not discovering an attack and having the attack disable the network.

Step 3 *Test* the effectiveness of the security safeguards in place. Validation is a necessity. You may have a very sophisticated network security system, but if it is not configured or working properly, your network can be compromised. One tool that may be used to identify the security posture of the network is Cisco Secure Scanner.

Step 4 Continuously *Improve* the corporate security policy. Collect and analyze information from the monitoring and testing phases to make security improvements.

New network vulnerabilities and risks are created every day. In order to keep your network as secure as possible, all four steps—secure, monitor, test, and improve—should be repeated on a continuous basis and should be incorporated into updated versions of the corporate security policy.

Summary

Computers and networks are integrated into our everyday lives in many ways. Understanding data flow and security is necessary when working with networks. When security is an issue, being informed is essential. Network design, the applications used, traffic flow, and understanding of security threats are just some of the topics that should be known.

When the issue is sending data to, or receiving data from an untrusted environment, a firewall should be the centerpiece of your security solution. The focus of this book is using the Cisco Secure PIX Firewall as a part of the solution to network security. The next chapter details the Cisco Secure PIX Firewall software and hardware.

Review Questions

To test what you have learned in this chapter, answer the following questions and then refer to Appendix F for the answers.

1. I want to install a web server and allow Internet users access, but I don't want those users inside my network. How can I accomplish this?
2. A script kiddie poses what type of network security threat?
3. Of all of the different types of threats that exist, which one should I fear most?
4. What is used to allow only specified users access to a network?