Lesson Proper for Week 2

NETWORK SECURITY FUNDAMENTALS (CONT.)

Goals of Network Security

Providing Secure Connectivity

In the early days of the Internet, network security primarily emphasized blocking attackers and other unauthorized users from accessing the corporate network. Today the priority is secure connectivity with trusted users and networks. When people go online to conduct business, they often engage in activities that could make them vulnerable:

- Placing orders for merchandise online, revealing both personal and financial information during payment
- Paying bills by transferring funds online
- Accessing account information
- Looking up personnel records
- Creating authentication information, such as usernames and passwords

The growth of the Internet and e-commerce is not likely to slow down, so methods to secure these transactions must be set up and maintained. Several methods can be combined in a layered security scheme, as you learn in the next section.

Secure Remote Access

One of the biggest security challenges for organizations that communicate via the Internet is the need to provide secure remote access for contractors and employees who are traveling. A VPN, with its combination of encryption and authentication, is often provided by the industry standard, IP security (IPsec), and is a simple and cost-effective solution (see Figure 1-1). VPNs are explained in more detail in Chapter 11.

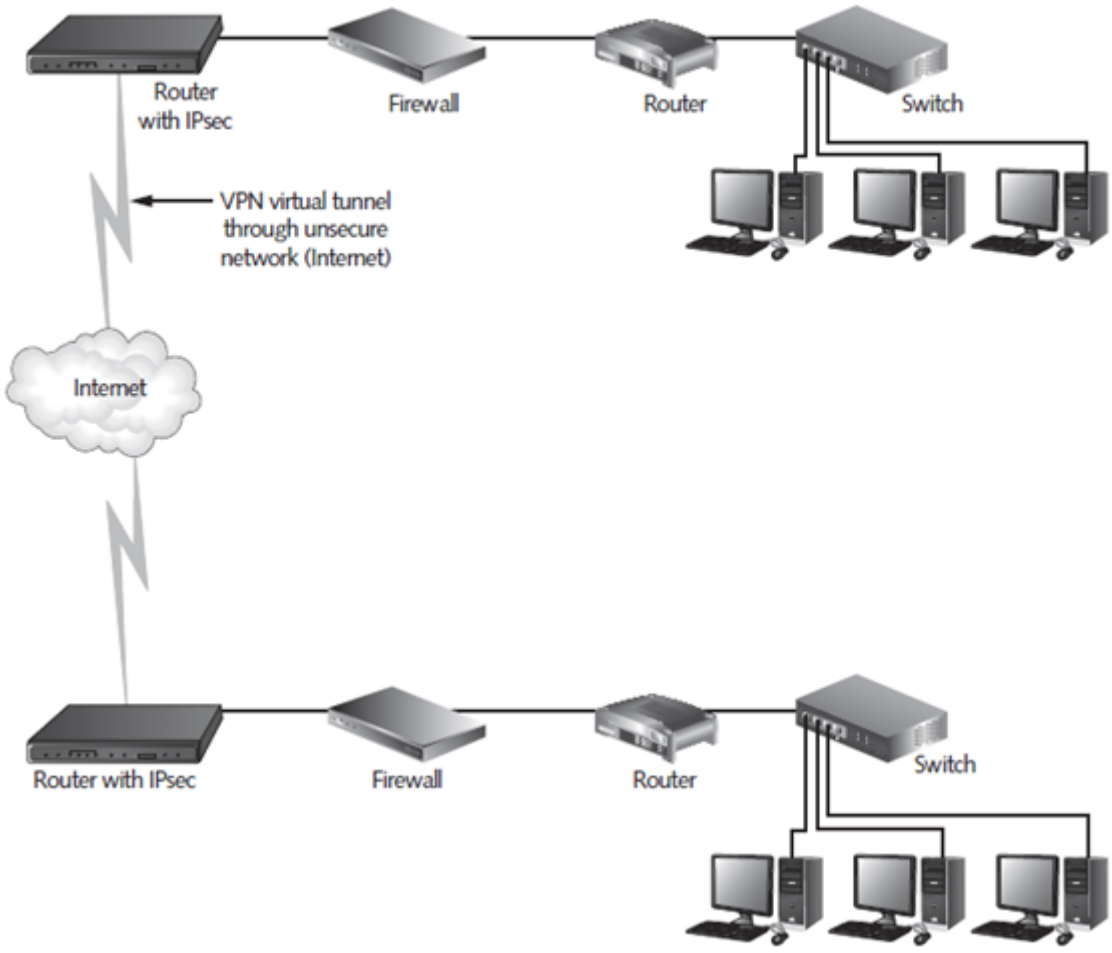

Figure 1-1 Many businesses provide secure remote access using VPNs

Ensuring Privacy

Corporations, hospitals, and other organizations that maintain databases of personal and financial information need to maintain privacy, not only to protect their customers but to maintain the integrity and credibility of their own companies. In addition, U.S. law protects private information and mandates severe penalties for failure to protect it adequately. Examples of these laws include Sarbanes-Oxley (SOX) for publicly traded companies, the Health Insurance Portability and Accountability Act (HIPAA) for medical organizations, the Family Educational Rights and Privacy Act (FERPA) in education, the Payment Card Industry Data Security Standard (PCI DSS) for organizations that accept credit cards, and the Gramm-Leach-Bliley Act in banking. If you work in an industry affected by laws that govern privacy protection, you may have a compliance department that can help you keep current with legal requirements.

One of the most important and effective ways to maintain the privacy of an organization's network is to educate all employees about security dangers and to explain security policies. Employees are likely to detect security breaches and to cause security breaches accidentally through their own behavior. They can also be mindful of their coworkers' activities and be alert to suspicious actions that could indicate a security problem. Providing Nonrepudiation Encryption protects the integrity, confidentiality, and authenticity of digital information. Encryption can also provide nonrepudiation, which is the capability to prevent a participant in an electronic transaction from denying that it performed an action. Nonrepudiation simply means ensuring that the sender cannot deny sending a message and the recipient cannot deny receiving it. Nonrepudiation is an important aspect of establishing trusted communication between organizations that do business across a network rather than face to face.

Confidentiality, Integrity, and Availability

The three primary goals of information security are data confidentiality, data integrity, and data availability. It is hard to imagine any aspect of information technology that has no responsibility for ensuring one or more of these three fundamental goals. Confidentiality is the prevention of intentional or unintentional disclosure of communications between a sender and recipient. Integrity ensures the accuracy and consistency of information during all processing (creation, storage, and transmission). Availability is the assurance that authorized users can access resources in a reliable and timely manner.

Using a Layered Defense Strategy: Defense in Depth

At this comparatively early stage in the development of information security, no single security component or method can be expected to ensure complete protection for a network—or even an individual host computer. Instead, you need to assemble a group of methods that work in a coordinated fashion to provide protection against a variety of threats. Even then, it is not realistic to think that all security threats can be stopped. Security is more a state of mind than a tangible, absolute state.

The components and approaches described throughout the rest of this book should be arranged to provide layers of network defense. This layering approach to network security is often called defense in depth (DiD). The National Security Agency (NSA) originally designed DiD as a best practices strategy for achieving information assurance. When beginning with an unprotected system, the first layer of defense added is always the most effective. As more layers are stacked on the first, potential attackers must successfully breach each layer to gain access to the next one. However, adding layers also adds increasing complexity for system administrators. Security enhancements must be balanced against the cost to maintain and monitor defenses. DiD does eventually reach a point where the cost of implementing additional security outweighs the potential benefits.

Another goal of implementing DiD should be to find ways that the security layers can work together, each using data generated by others to enhance the overall effectiveness of the systems.

In general, the layers are as follows. Each layer is discussed in the following sections.

- Physical security
- Authentication and password security
- Operating system security
- Antivirus protection
- Packet filtering
- Firewalls
- Demilitarized zone (DMZ)
- Intrusion detection and prevention system (IDPS)
- Virtual private networks (VPNs)

- Network auditing and log files
- Routing and access control methods

Physical Security

The term physical security refers to measures taken to protect a computer or other network device from theft, fire, or environmental disaster. Examples of physical security include installing computer locks that attach a computer device to a piece of furniture in your office, and keeping critical servers in a room protected by a lock and/or burglar alarm. If the bad guys can touch it, they own it. This statement means that a computer can easily be compromised if a malicious intruder has physical access to it. Within minutes, an attacker can defeat most common physical locks and steal anything from a password file to the whole server. More insidiously, attackers can plant malware that could give them control of the system without the owner's knowledge.

Authentication and Password Security

After you have physically secured your computers, you can begin to protect them from the inside as well. One simple but reasonably effective strategy is a password security policy, which requires your employees to select good passwords, keep them secure, and change them regularly. Using multiple passwords, including screen-saver passwords and passwords for protecting critical applications, is also a good idea to guard against unauthorized employees gaining control of unattended computers. But, unless password policies are in place to ensure the use of complex passwords and their safekeeping can be enforced through technical means, passwords can become a serious vulnerability. These days, more stringent methods of authentication are becoming common.

Authentication—verifying the identity of a user, service, or computer—uses one of three methods: verifying something the user knows, something the user possesses, or something the user is. In the field of network computing, authentication is performed in one of several ways. Basic authentication involves using something the user knows, such as a username/ password pair. In challenge/response authentication, the authenticating device generates a random code or number (the challenge) and sends it to the user who wants to be authenticated. The user resubmits the number or code and adds a secret PIN or password (the response), or uses a possession such as a smart card to swipe through a card reader.

In large organizations, a centralized server typically handles authentication. The use of biometrics—physical information that identifies a person, such as retinal scans, voiceprints, and fingerprints—is growing in popularity because of the security limitations of relying on username and password combinations alone.

Operating System Security

Another way to secure computers and their data from the inside is by installing operating system (OS) patches that have been issued to address security flaws. It is your responsibility to keep up with patches, hot fixes, and service packs and to test and install them when they become available. In addition, stopping any unneeded services and disabling guest user accounts helps make an OS more secure.

Antivirus Protection

Virus scanning refers to the process of examining files or e-mail messages for filenames, file extensions such as .exe (for executable code) or .zip (for zipped files), and other indications that viruses are present. Many viruses have suspicious file extensions, but some seem innocuous. Antivirus software uses several methods to look for malware, including comparisons to the software's current signature files, which contain a pattern of known viruses. Signature files are the primary reason for keeping your antivirus software updated; antivirus software vendors frequently create updates and make them available for customers to download. When antivirus software recognizes the presence of viruses, it deletes them from the file system or places them in a storage area called a quarantine where they cannot replicate themselves or do harm to other files.

Firewalls and IDSs, by themselves, are not equipped to scan for viruses and eliminate them. However, many enterprise-level firewalls come with integrated antivirus protection. Antivirus software is a must-have for every computer in a network; if your firewall does not provide antivirus software, you need to install it on the computer that hosts the firewall and on all network computers.

Packet Filtering

Packet filters block or allow the transmission of packets of information based on port, IP address, protocol, or other criteria. Packet filtering can be performed by different types of systems. Some are hardware devices, such as routers and firewalls placed at a network gateway. Others are software programs that can be installed on a gateway or a computer. Here are a few examples:

- Routers—These devices are probably the most common packet filters. Routers process packets according to an access control list (ACL) the administrator defines.
- Operating systems—Some systems, such as Windows and Linux, have built-in utilities for packet filtering on the TCP/IP stack of the server software. Linux has a kernel-level packet filter called Iptables; Windows Server 2008 and Windows 7 have a feature called Windows Filtering Platform.
- Software firewalls—Most enterprise-level programs, such as Check Point Firewall Software Blade, perform packet filtering. Personal firewalls such as ZoneAlarm perform basic stateless packet filtering based on simple rules. You use ZoneAlarm in the hands-on projects at the end of this chapter.

Whatever type you use, the packet-filtering device evaluates information in the packet header and compares it to the established rules. If the information corresponds to one of the "allow" rules, the packet is allowed to pass; if the information matches one of the "deny" rules, the packet is dropped.

Firewalls

The foundation for installing and configuring a firewall is your organization's overall security policy. After you have a solid security policy as your guide, you can design security configurations to support your organization's goals. Specifically, you can create a packet-filtering rule base for your firewall that reflects your overall approach to network security. (You learn about security policies in Chapter 13 and about

firewalls in more detail in Chapters 9 and 10.) The following section describes two ways that a firewall can control the amount of protection a network receives: permissive versus restrictive policies.

Permissive vs. Restrictive Policies

A firewall, following the direction given in a security policy, typically adopts one of the following general approaches to security (see Figure 1-2):

- Permissive policy—Calls for a firewall and associated security components to allow all traffic through the network gateway by default and then to block services on a case by case basis.
- Restrictive policy—Calls for a firewall and associated network security components to deny all traffic by default. The first rule denies all traffic on any service and using any port. To allow a specific type of traffic, a new rule must be placed ahead of the "deny all" rule.

A firewall should enforce the overall policy established by the network administrator. Enforcement is handled primarily through setting up packet-filtering rules; a rule base contains a set of these rules. The order of rules in the rule base is important to how the firewall processes traffic.

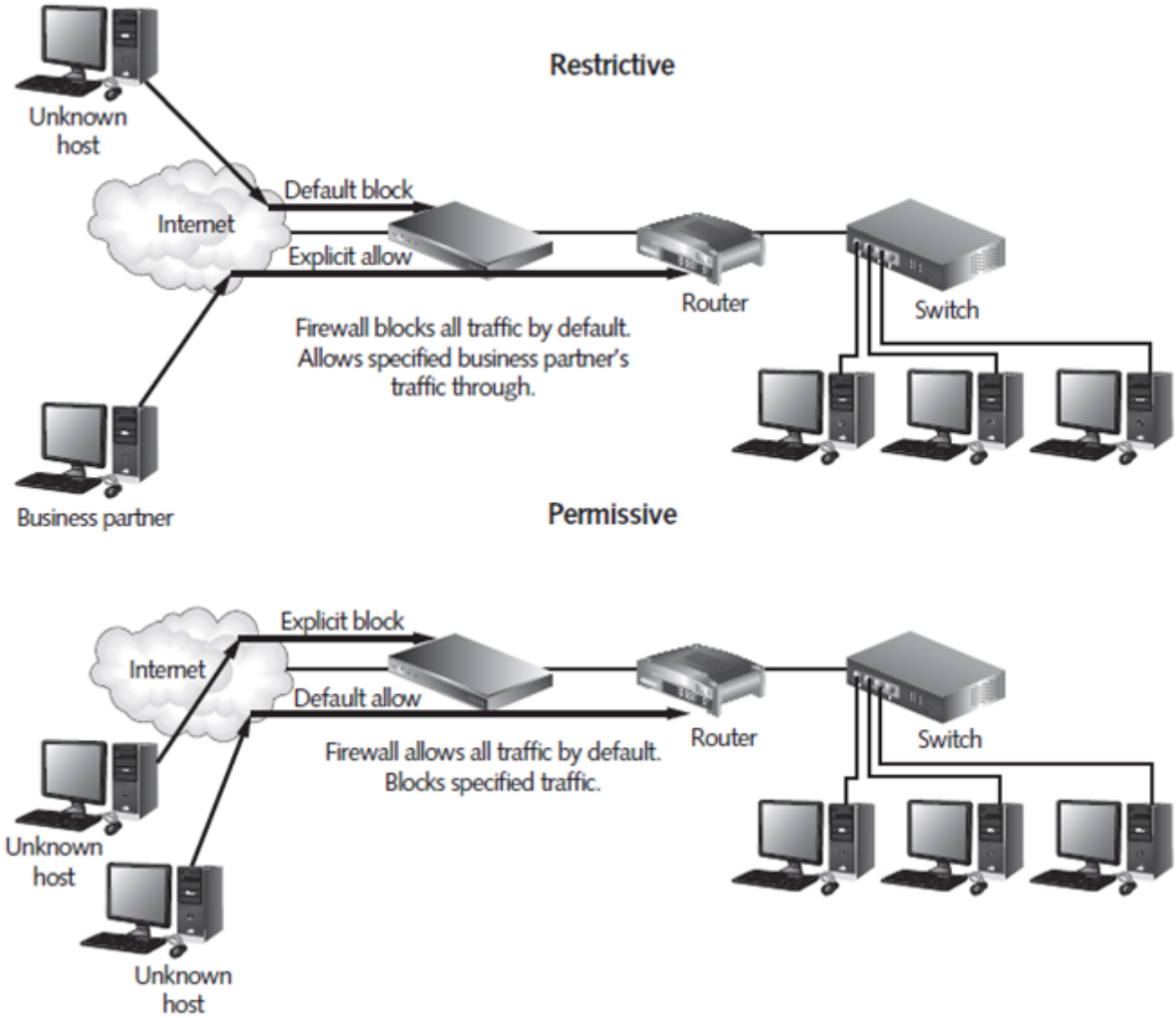

Figure 1-2 Permissive vs. restrictive firewall policies

Demilitarized Zone (DMZ)

A subnet called a demilitarized zone (DMZ) is a network that sits outside the internal network but is connected to the firewall. A DMZ makes services like HTTP (Web server) and FTP (File Transfer Protocol) publicly available, yet protects the internal LAN. A DMZ might also contain a DNS server that resolves fully qualified domain names to IP addresses. The subnet attached to the firewall and contained in the DMZ is sometimes called a service network or perimeter network. A common DMZ configuration is shown in Figure 1-3.

Intrusion Detection and Prevention System (IDPS)

Ideally, firewalls and proxy servers block intruders or malicious code from entering a network. However, using an IDPS with these tools offers an additional layer of protection for a network. An intrusion detection and prevention system (IDPS) works by recognizing the signs of a possible attack and sending a notification to an administrator that an attack is under way (intrusion detection). Some traffic can trigger a response that attempts to actively combat the threat (intrusion prevention).

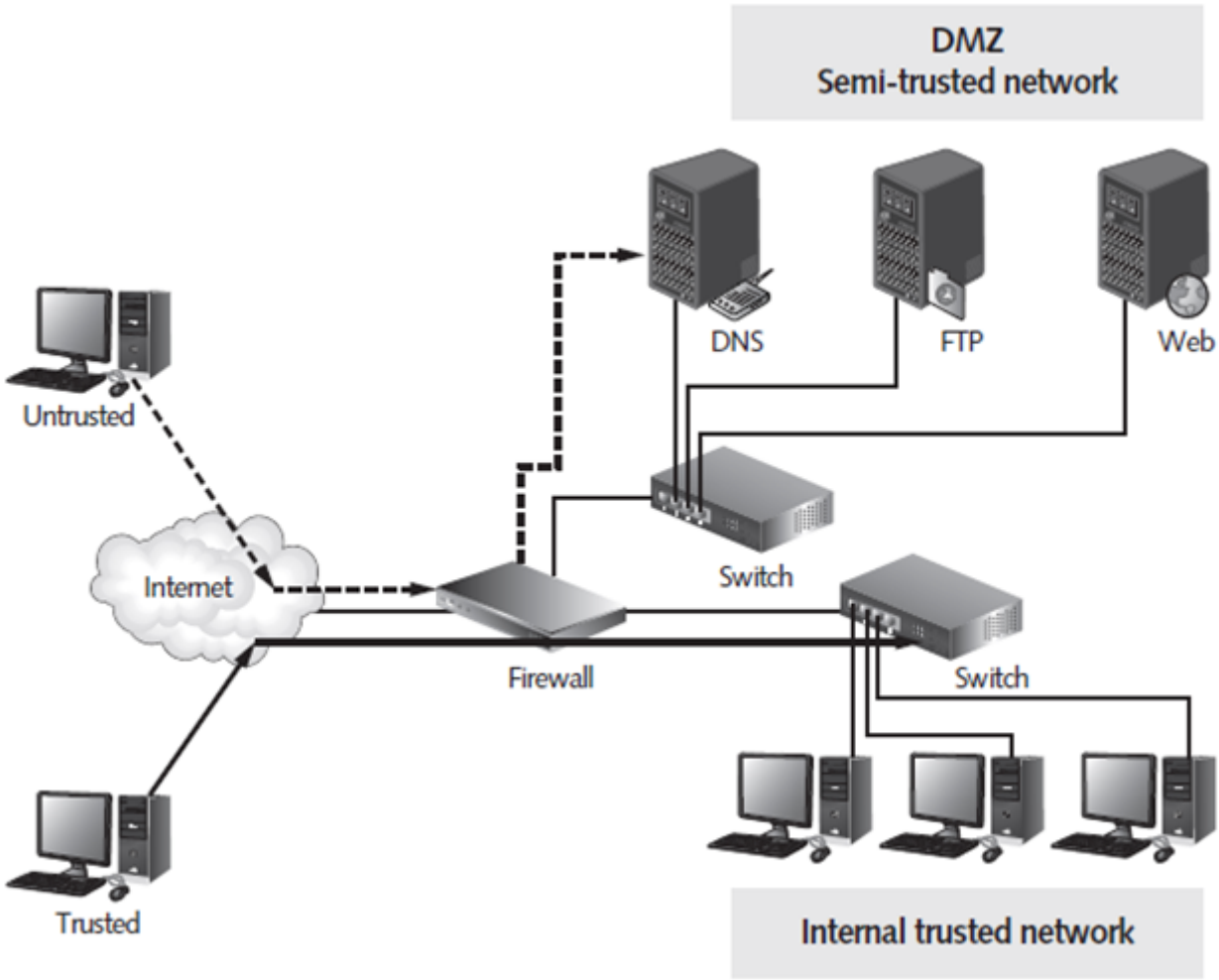

Figure 1-3 Firewall used to create a DMZ and protect the internal network

Note that the term intrusion prevention is not precise because there is no known method for preventing all possible intrusions. The signs of possible attacks are commonly called signatures—combinations of IP addresses, port numbers, and the frequency of access attempts. You learn the details of IDPS concepts and implementation in Chapter 8.

Virtual Private Networks (VPNs)

Companies that share files or exchange confidential financial information traditionally used expensive leased lines provided by telecommunications companies. Although these lines created a point-to-point connection between company networks and therefore ensured a high level of security, the monthly costs were excessively high for many budget-conscious companies. Today, a more common approach to protecting confidential data in transit is the use of VPNs, which provide a low-cost and secure connection that uses the public Internet. A virtual private network (VPN) is a network that uses public telecommunications infrastructure, such as the Internet, to provide secure access to corporate assets for remote users. VPNs use authentication to verify users' identities and encrypt and encapsulate traffic to protect it in transit. VPNs are covered in detail in Chapter 11.

Network Auditing and Log Files

Auditing is the process of recording which computers are accessing a network and what resources are being accessed, and then recording the information in a log file. IT managers often overlook detailed reviews of log files generated by firewalls and IDPS. By reviewing and maintaining log files, you can detect suspicious patterns of activity, such as regular and unsuccessful connection attempts that occur at the same time each day. You can identify those who have attacked your network, or at least gather enough information to begin to identify them. You can set up rules to block attacks and keep your network defense systems up to date by examining attack attempts that have penetrated firewalls and other protective devices. Effective management of log files is an essential activity that goes hand in hand with any perimeter security configuration.

Log File Analysis

- Compiling, reviewing, and analyzing log files are among the most tedious and time consuming tasks associated with network security. Network administrators read and analyze log files to see who is accessing their networks from the Internet. All connection attempts that are rejected should be recorded in the hope of identifying possible intruders or pinpointing vulnerable points in the system.

- When you first install intrusion detection or firewalls on your network, you will probably be asked to prepare reports that describe how the network is being used and what kinds of filtering activities the device is performing. It is a good idea to sort logs by time of day and per hour. (Sorting log files produces material that is more organized and easier to review than the log files produced by the server, firewall, or other device.)

- Be sure to check logs to learn the peak traffic times on your network, and try to identify the services that consume the largest part of your available bandwidth. If your firewall or IDPS can display log file entries graphically (as shown in Figure 1-4), you should consider showing the graphs to management as needed. Graphs illustrate trends more effectively than lists of raw data.

If your firewall or IDPS cannot display log files graphically, it is well worth the time to locate and install a compatible product that can.

Configuring Log Files

Typically, the log files compiled by a firewall or IDPS give you different options. You can view active data (data compiled by the firewall as traffic moves through the gateway in real time) or data that the device has recently recorded. You can also view the information in the following ways:

- System events—These events usually track the operations of the firewall or IDPS, making a log entry whenever it starts or shuts down.

- Security events—These events are records of any alerts the firewall or IDPS has issued.

- Traffic—This is a record of the traffic that passes through the firewall.

- Packets—Some programs enable you to view information about packets that pass through them.

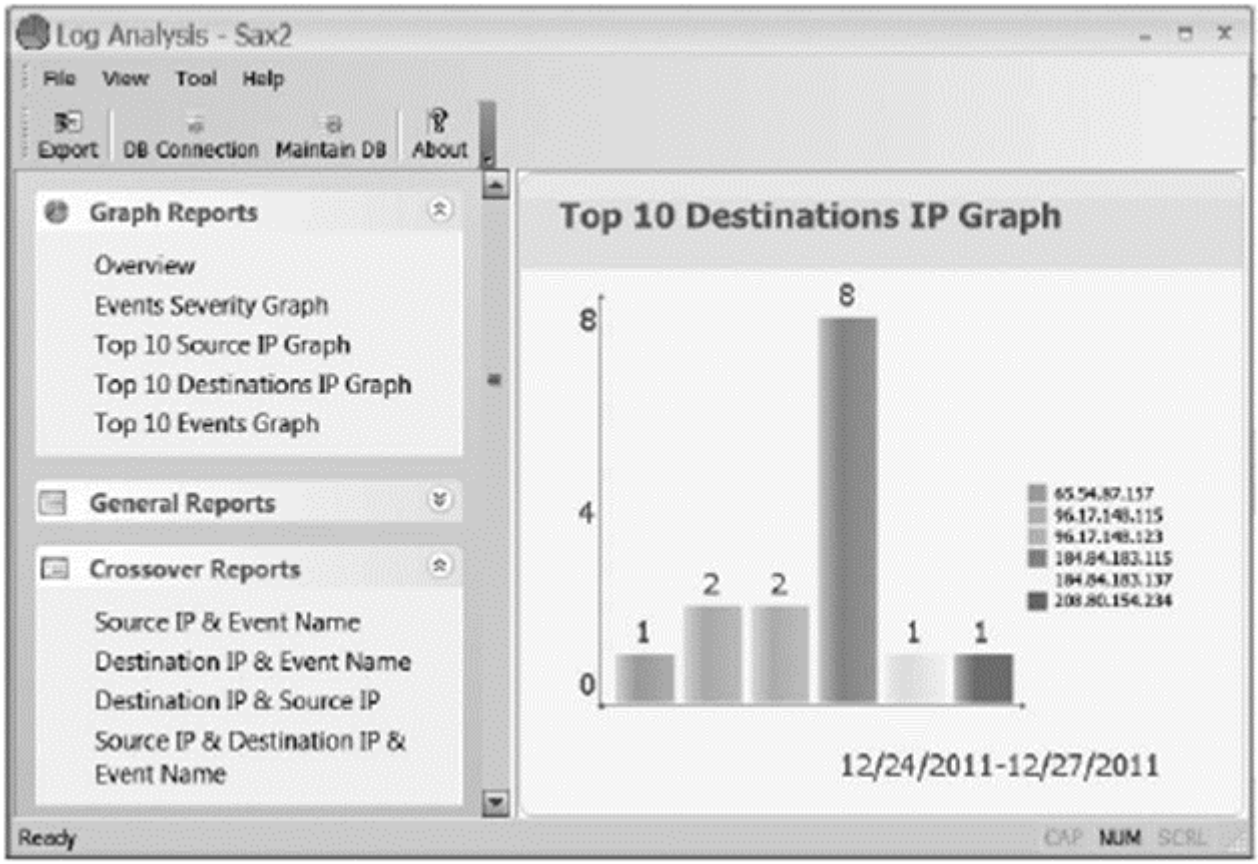

Figure 1-4 Graphic display of log file entries

With more elaborate programs, you can customize what you see in log files and search for specific items or events.

Routing and Access Control Methods

Routers at the perimeter of a network are critical to the movement of all network traffic, regardless of whether the traffic is legitimate or harmful. Because routers are positioned on a network's perimeter, they can be equipped with their own firewall software to perform packet filtering and other functions.

To set up a defense, you need to know what kinds of attacks to expect and which of your services and computers might present openings that can be exploited. As a security professional, your goal is ensuring that no unauthorized access occurs. You must identify areas that would allow attackers to gain access to your network. An attacker might attempt to access the following open points of entry:

- Vulnerable services—The attacker might be able to exploit known vulnerabilities in an application.
- E-mail gateways—The attacker might be able to attach a virus payload to an e-mail message. If a recipient clicks the attachment to open it, the program runs and the virus installs itself on the user's system.
- Porous borders—Computers on the network might be listening (that is, waiting for connections) on a port that has no functional use. If an attacker discovers a port that the computer has left open and that is not being used, the open port can give the attacker access to that computer's contents.

Users must have access to the resources necessary to do their jobs, but unauthorized people must not be able to gain access to those resources. Access control is a vital facet of network security and encompasses everything from complex permission configurations on domain controllers to locked doors. You should know about three main methods of access control:

- Mandatory access control (MAC)—This is an uncompromising method for controlling how information can be accessed. With the MAC method, all access capabilities are defined in advance. System administrators establish what information users can and cannot share.
- Discretionary access control (DAC)—With this method, network users are given more flexibility in accessing information. This method allows users to share information with other users; however, the risk of unauthorized disclosure is higher than with the MAC method.
- Role-based access control (RBAC)—This method establishes organizational roles to control access to information. The RBAC method limits access by job function or job responsibility. An employee could have one or more roles that allow access to specific information.

The Impact of Defense

Although the cost of securing systems and their data might seem high, in terms of return on investment (ROI) the cost of a security breach can be much higher. As mentioned, several laws exist to protect privacy, and violation of those laws can carry severe monetary penalties. When added to the direct and indirect costs of a security breach, implementing a sound security scheme can seem inexpensive by comparison.

A key factor in securing systems successfully is the support you gain from upper management. Before security efforts ever start, executives and managers have to be sold on the idea. This support serves several key purposes:

- The project will cost money, and you need to have funding for the project approved beforehand.
- The project will require IT staff time, and managers, supervisors, and employees from all departments must participate to paint a clear picture of priorities and carry out the security plan.
- The process of implementing security systems might require down time for the network, which translates into lost productivity and inconvenience for everyone.
- Most importantly for the long-term success of security efforts, executives and management need to support the project from start to finish. If they do not, development, testing, implementation, and maintenance are nearly impossible to complete. The necessary resources and enforcement will not be available. Besides, if management does not seem to care and does not support the initiative, why would anyone else?

In addition, remember that it is not enough simply to plan and implement security systems. Probably the most challenging facet of information security is keeping up to date on new threats and other developments in the industry. Security systems must be maintained and updated continuously to provide protection against new threats.

◀ Preliminary Activity for Week 2 Jump to...

Analysis, Application, and Exploration for Week 2 ▶

Navigation

Home
Dashboard
Site pages
My courses
Capstone Project 2
Network Defense and Remote Access Configuration
Participants
General
02 [Enter Module Title Here]
Preliminary Activity for Week 2
Lesson Proper for Week 2
Analysis, Application, and Exploration for Week 2
Generalization for Week 2
Evaluation for Week 2
Assignment for Week 2
03 [Enter Module Title Here]
04 [Enter Module Title Here]
OJT/Practicum 2
Seminars and Tours
Courses

Fair Warning

PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

Activities

- Assignments
- Forums
- Quizzes
- Resources