LESSON 4 : Understanding Network Security

OBJECTIVE DOMAIN MATRIX

SKILLS/CONCEPTS	MTA EXAM OBJECTIVE	MTA EXAM OBJECTIVE NUMBER
Using Dedicated Firewalls to Protect a Network	Understand dedicated firewalls.	3.1
Controlling Access with Network Access Protection (NAP)	Understand Network Access Protection (NAP).	3.2
Using Isolation to Protect a Network	Understand network isolation.	3.3
Protecting Data with Protocol Security	Understand protocol security.	3.4
Securing Wireless Networks	Understand wireless security.	1.4

KEY TERMS

application-level firewall

circuit-level firewall

DMZ (demilitarized zone)

DNS Security Extensions (DNSsec)

DNS poisoning

DNS spoofing

firewall

honey net

honeypot

host firewall

intrusion detection systems (IDS)

intrusion prevention systems (IPS)

MAC address

Network Access Protection (NAP)

network firewall

Open Systems Interconnect (OSI)

padded cell

personal firewall

Secure Content Management (SCM)

spoofing

stateful inspection

Unified Threat Management (UTM)

Traditionally, when building an information security infrastructure, the first point of focus was the network. As soon as networks began interconnecting, it was obvious that the network offered the main vector of attack. In other words, it

was the primary way to get to an organization's information from the outside.

At this point, the driving philosophy around network protection was reminiscent of the castles of old. According to this mindset, the best way to secure your network was to build strong walls, dig moats, and control access to the castle through the main gate. In network

terms, this meant deploying multiple layers of firewalls, then controlling who could enter the network with firewall rules, access controls, and demilitarized zones (DMZs). This practice is known as securing the perimeter, or defense in depth.

This model worked quite well until the next round of technological evolution in the late 1990s, when the concept of the virtual private network (VPN) was introduced. VPNs allowed companies to securely extend their network across untrusted networks like the Internet, but this also impacted the perimeter of the network. Next came wireless network technologies, literally moving the perimeter that required protection into the air and offering additional challenges to the layered security model.

The good news is that as network technologies have evolved and securing a networks' perimeter has become more challenging, the security technologies available for addressing these challenges have evolved as well. In this lesson, we will discuss such security solutions and how they can be used to address the challenges you will encounter.

Using Dedicated Firewalls to Protect a Network

> **THE BOTTOM LINE**
> Even today, firewalls remain the foundation of network security technology. There are a number of options, types, and technologies associated with selecting, implementing, and maintaining firewalls in your network. There are also a number of drivers to help you determine the proper solution for your organization.

One of the first things that comes to mind when people talk about information security is the firewall. Firewalls have long been the foundation of an organization's network security infrastructure. But what exactly is a firewall?

A ***firewall*** is a system that is designed to protect a computer or a computer network from network-based attacks. A firewall does this by filtering the data packets that are traversing the network. A typical perimeter firewall is implemented with two (or more) network connections (see Figure 4-1), namely:

> **CERTIFICATION READY**
> Where would most companies place their dedicated firewall?
> 3.1

- A connection to the network being protected; and
- A connection to an external network.

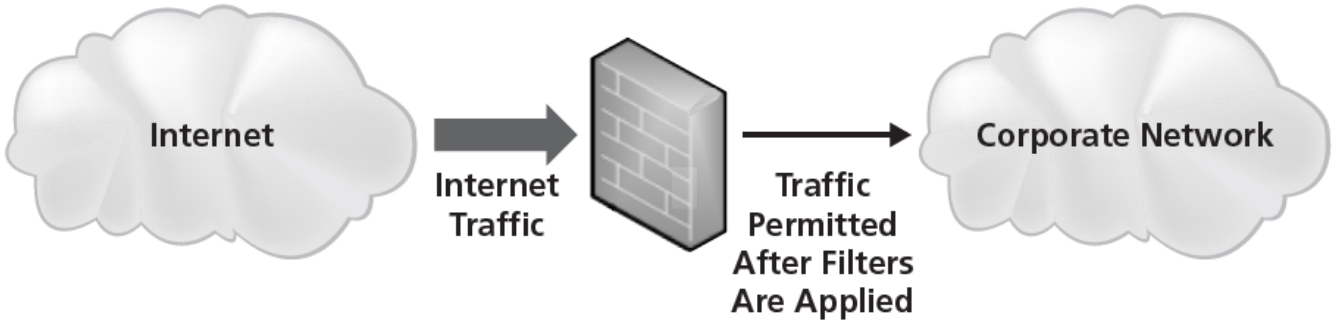

Figure 4-1 A firewall implementation

There are numerous variations on this model, but ultimately, all firewalls protect hosts on one network from hosts on another network.

Firewalls are used to divide and isolate networking areas for an organization. For example, one of the most common uses of a firewall would be to divide the network of your organization (internal network) from the external network (Internet). The internal network may also be referred to as clean, secure, and local while the external network may be referred to as dirty, unsecure, and remote. They all reference the same model, but occasionally, you may find you need to translate a particular term into terminology you are familiar with.

In today's networks, you'll find firewalls used for a number of purposes beyond just securing the perimeter. For instance, many corporate networks are divided into zones secured by firewalls. Thus, you may find that your organization's firewalls are not only securing Internet and extranet connections, but also creating secure zones for your financial systems, securing your research and development servers, or perhaps even securing the production network from the development and test networks.

Given the widely varying uses for firewalls in today's networks, there are a variety of different firewall types. But before we get into a discussion of the different types of firewalls, we need to discuss the OSI model.

Understanding the OSI Model

Any discussion about network security requires an understanding of the ***Open Systems Interconnect (OSI)*** reference model. The OSI model is a conceptual model, created by the International Organization for Standardization (ISO) in 1978 and revised in 1984, to describe a network architecture that allows the passage of data between computer systems. Although never fully utilized as a model for a protocol, the OSI model is nonetheless the standard for discussing how networking works.

As shown in Figure 4-2, the OSI model is built in the same way it is usually discussed, from bottom to top. The seven layers of this model are as follows: physical, data link, network, transport, session, presentation, and application. Here, the physical layer is referred to as layer 1, the data link layer as layer 2, and so on. This is important to remember because you will frequently hear routers referred to as "layer 3 devices" or specific types of firewalls described as "layer 7 devices." This nomenclature refers to where on the OSI model a device interacts. Accordingly, it is important that you are familiar with the high-level concept of the OSI model and what occurs at each layer.

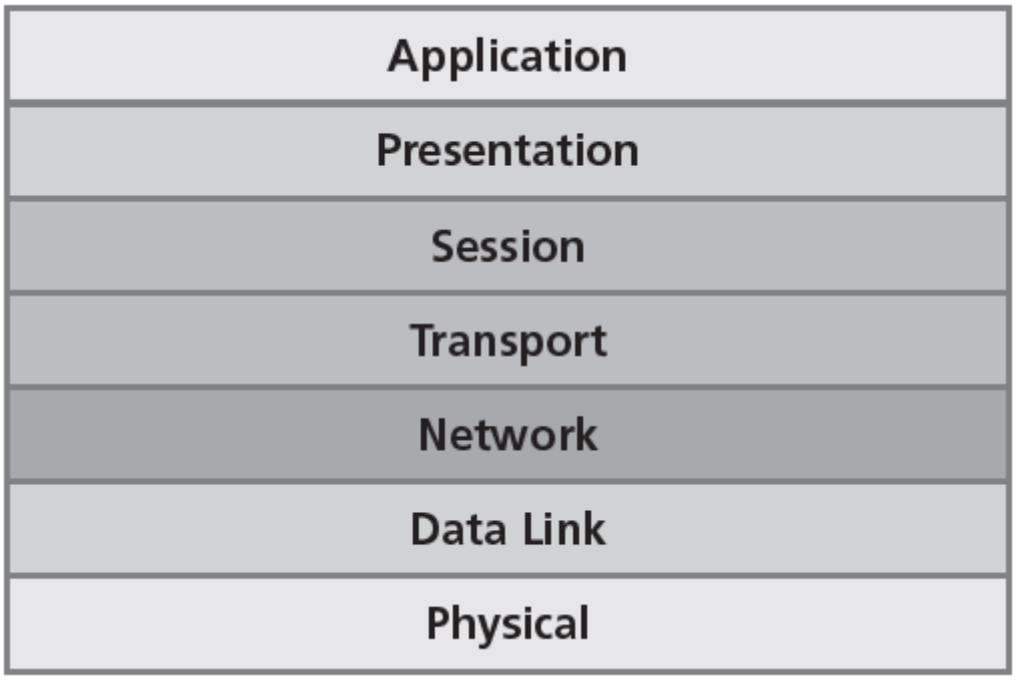

Figure 4-2 The seven-layer OSI model

Each layer of the OSI model has its own specific function. The following sections describe the function of each layer, starting with the physical layer and working upward.

PHYSICAL LAYER (LAYER 1)

The physical layer of the OSI model is used to define the physical characteristics of the network, including the following specifications:

- **Media:** Cabling types, voltage, signal frequency, speed, bandwidth, etc.
- **Hardware:** Type of connector, type of network interface card, etc.
- **Topology:** The topology used in the network, such as ring, mesh, star, or bus

DATA LINK LAYER (LAYER 2)

The data link layer connects the data layer to the physical layer so that data can be transmitted across the network. The data link layer handles error detection, error correction, and hardware addressing (i.e., the address of a network interface card).

The data link layer is broken into two sublayers:

- **Media Access Control (MAC) sublayer:** The MAC address is defined at this layer. The ***MAC address*** is the physical or hardware address burned into each NIC (for example, 96-4C-E5-48-78-C7). The MAC sublayer also controls access to the underlying network media.
- **Logical Link Control (LLC) sublayer:** The LLC layer is the layer responsible for the error and flow control mechanisms of the data link layer. The LLC layer is specified in the IEEE

802.2 standard.

> **TAKE NOTE***
> The IEEE 802.x standards define a variety of networking technologies. For example, 802.1x defines a standard for wireless security. Similarly, Ethernet is defined by the IEEE 802.3 standard.

NETWORK LAYER (LAYER 3)

The network layer is primarily responsible for routing. This layer defines the mechanisms that allow data to be passed from one network to another. To be clear, this layer doesn't specify how the data is passed; rather, it defines the mechanisms that permit this passage. How the data is passed is defined by the routing protocols (which are discussed in more detail later in the lesson.) As a result, a router is typically known as a layer 3 device.

> **TAKE NOTE***
> It's important to remember that in addition to routing (allowing traffic to select the best path), the network layer of the OSI model specifies one other critical function: addressing. In the case of TCP/IP, this is the layer where IP addresses are specified. Although the data link layer uses hard-coded MAC addresses to communicate on the physical layer, network protocols use software-configured addresses and routing protocols to communicate across the network.

TRANSPORT LAYER (LAYER 4)

The transport layer does exactly what its name implies: It provides the mechanisms for carrying data across a network. This layer uses three main mechanisms to accomplish this task:

- **Segmentation:** When, for example, you download an MP3 file from your favorite music site, you are dealing with a large block of data. In order for this file to get from the music site to your PC, it needs to be broken down into smaller, more manageable blocks so the network can handle it. This process is called segmentation, and the transport layer performs this function.
- **Service addressing:** Network protocols (TCP/IP, for example) provide a number of network services, and these services are identified by ports. The transport layer ensures that when data traverses the network, it is passed to the right service and the right port.
- **Error checking:** Transport layer protocols also perform error checking on data and ensure that information is sent or received correctly.

The protocols you will see operating at the transport layer come in two types:

- **Connection oriented:** A connection-oriented protocol (such as Transmission Control

Protocol [TCP]) requires an end-to-end connection between hosts before data can be transmitted. You can think of this like a telephone call. When making a call, you can't start speaking to the person at the other end of the line until you have successfully connected to that person.

- **Connectionless:** A connectionless protocol (such as the User Datagram Protocol [UDP]) allows for the transmission of data without requiring that a connection is already established. Connectionless protocols rely on the network to ensure the proper delivery of data from one host to another. You can think of a connectionless protocol like sending an email. Obviously, you don't have to connect directly to the recipient before sending an email; instead, you type and address your message, then click send. Here, you rely on the network—and not an existing connection—to ensure the email gets to the addressee.

The transport layer has an additional responsibility in the OSI model: handling flow control of data. Flow control determines how the receiving device accepts the data transmissions. There are two common methods of flow control:

- **Buffering:** Buffering flow control temporarily stores data in a buffer and waits for the destination device to become available. Buffering can be problematic if the sending device is able to transmit data much faster than the receiving device is able to receive it. Too high a transmit rate can overload a buffer, which has a limited size, causing data loss.

- **Windowing:** In a windowing environment, data segments are grouped together, and when sent, they require only one acknowledgment. Here, the sending and receiving devices agree to the size of the window (i.e., the number of segments that can be sent at one time). In some cases, the window size is agreed to when the connection is established; in others, the window size varies based on network congestion and device resources. These types of windows are referred to as sliding windows. Windowing improves network performance by reducing the number of acknowledgements that need to be sent between devices.

> **TAKE NOTE***
> If you are familiar with PC hardware, you may recognize these two flow control methods. They are the same methods used for flow control in a PC when moving data into and out of the different types of data storage, including hard drives, cache, and RAM.

SESSION LAYER (LAYER 5)

The session layer is responsible for data synchronization between the applications on the sending device and the receiving device. This layer establishes, maintains, and breaks sessions between the two devices. While the

transport layer is responsible for connections between the two devices, it is the session layer that is actually responsible for transferring the data between the two devices.

PRESENTATION LAYER (LAYER 6)

The presentation layer converts application layer data into a format that can be transmitted across a network. Data formatted for transport across a network is not always natively readable by applications. Some common data formats that are converted by the presentation layer include the following:

- Graphics files
- Text and data files
- Music and video files

The presentation layer is also the layer in which encryption and decryption of data takes place.

APPLICATION LAYER (LAYER 7)

Finally, at the top of the OSI model is the application layer. This layer takes data from the user and passes that data to the lower layers of the OSI model for transport. Responses are then passed up through the layers and displayed to the user.

> **TAKE NOTE***
> It's important to remember that the application layer of the OSI model is not the actual application you see on your computer. Rather, the application layer is used to define how the applications running on your computer can take advantage of the network service. For example, if you wanted to print a document to a network printer, your word processing application would take the file information and pass it to the application layer, which would then pass it down the other layers in the model so that it could be transmitted to the printer. Of course, there are applications (software programs) that may use the network service or application that runs at application layer services, like web browsers.

Although the OSI model provides a framework to categorize technology, this model is not fully implemented on today's networks. Instead, today's networks follow a simplified model that usually consists of the following four layers:

- **Link layer:** This is the lowest layer of the TCP/IP model and is designed to be hardware independent. It is responsible for linking to the hardware networking technology, and it transmits data. TCP/IP has been implemented on top of virtually any hardware networking technology in existence.
- **Internet layer:** This layer is responsible for connecting multiple networks together and for routing packets between networks.
- **Transport layer:** This layer is responsible for end-to-end message transfer capabilities independent of the underlying network. It also handles error control, segmentation, flow control, congestion control, and application addressing (port numbers).

- **Application layer:** The term “application layer” refers to higher-level network protocols and services, such as SMTP or FTP.

Now that you have an understanding of the OSI model, we can discuss various networking technologies and their impact on your information security program.

Examining Hardware Firewalls and Their Characteristics

In today’s network environment, the vast majority of production firewalls are hardware based. A hardware firewall is a firewall that runs on a dedicated platform specifically designed, optimized, and hardened (the process of securing a system) to run the firewall application software.

Although there are a variety of types of firewalls, each with varying characteristics, all firewalls share some basic functions. For one, all firewalls filter traffic based on a set of configured rules. Generally, these rules are based on information contained in the data packets that are traveling across the network. In particular, the header information contained in those data packets provides the firewall with the information it needs to properly apply the rules. These rules are generally defined by a company’s security policies and business requirements.

Although it is possible to configure a firewall to permit all traffic and only block specific traffic based on rules, virtually all firewalls work according to the deny-all permit-specific philosophy. This means that the firewall will, by default, deny all traffic, so any traffic permitted to traverse the firewall must be explicitly configured in the firewall’s rules.

There are a variety of firewall types, and depending on who is doing the defining, you may even find that different people define firewall types in different ways. The key is to understand the basics, because outside of passing the certification test, you will generally not be called upon to identify firewall types in your day-to-day duties.

LOOKING AT PACKET FILTERING

The first type of firewall is known as a packet filtering firewall. This type of firewall is considered first generation because the earliest firewalls functioned as packet filters. As discussed, the primary purpose of a firewall is to filter traffic. Accordingly, and as its name suggests, a packet filtering firewall inspects the data packets that attempt to traverse it, and based on the rules that have been defined on the firewall, it allows or denies each packet as appropriate.

One of the very first versions of this type of firewall was the packet filtering router. Routers have the ability to do some rudimentary packet filtering, such as permitting all outbound traffic while denying all inbound traffic, or blocking specific protocols from passing through the router, such as telnet or ftp.

> **TAKE NOTE***
> Don’t get too hung up on the definitions of firewall types. Instead, seek to understand the functionality of each type. What you call different types of firewalls is not as important as knowing how these firewalls function.

Different from routers, firewalls improve packet filtering by increasing granular control. For example, you might configure a packet filtering firewall to block web browsing from the Internet except to your company’s website, while at the same time permitting outbound web traffic from your internal network to the Internet. Or you could set up a rule that drops any ping requests unless they originate from a network team member’s workstation.

When you are configuring a packet filtering firewall rule, you will generally use one or more of the following TCP/IP attributes:

- Source IP addresses
- Destination IP addresses
- IP protocol (telnet, ftp, http, https, etc.)
- Source TCP and UDP ports (e.g., the http protocol runs on TCP port 80)
- Destination TCP and UDP ports
- The inbound firewall network interface
- The outbound firewall network interface

Some of the more common protocols and ports you will encounter in a production network include the following:

- FTP (file transfer) 20/tcp and 21/tcp
- Telnet (terminal login) 23/tcp
- DNS 53/udp and 53/tcp
- HTTP (web) 80/tcp
- HTTPS (web) 443/tcp
- SMTP (email) 25/tcp
- POP3 (email) 110/tcp
- IMAP3 (email) 220/tcp
- IMAP4 (email) 143/tcp
- LDAP (directory services) 389/tcp
- SQL server 1433/tcp
- RDP (terminal services) 3389/tcp

This is not a comprehensive list, as there are thousands of different protocols and ports, but these are the most common protocols you will see when configuring rules on a packet filtering firewall. For a comprehensive list of protocols and ports, visit **http://www.iana.org/assignments/port-numbers.**

LOOKING AT CIRCUIT-LEVEL FIREWALLS

Circuit-level firewalls are typically considered second-generation firewall technology. They work in a similar fashion to packet-filtering firewalls, but they operate at the transport and session layers of the OSI model.

Instead of analyzing each individual packet, a circuit-level firewall monitors TCP/IP sessions by monitoring the TCP handshaking between packets to validate the session. Traffic is filtered based on specified session rules and may be restricted to authorized computers only. When the session is established, the firewall maintains a table of valid connections and lets data pass through when session information matches an entry in the table. When the session is terminated, the table entry is removed and the circuit is closed. One unique feature of circuit-level firewalls is that sessions that cross this type of firewall appear to originate from that firewall. This allows the internal network to be hidden from the public network.

A circuit-level firewall is also known as a transparent proxy, because (as mentioned) all sessions appear to originate from the firewall. Circuit-level firewalls are almost always used in conjunction with other types of firewalls, as they are only able to permit sessions from authorized computers. Additional granularity is typically required in most production environments.

LOOKING AT APPLICATION-LEVEL FIREWALLS

Application-level firewalls (also known as proxy servers) work by performing a deep inspection of application data as it traverses the firewall. Rules are set by analyzing client requests and application responses, then enforcing correct application behavior. Application-level firewalls can block malicious activity, log user activity, provide content filtering, and even protect against spam and viruses. Microsoft Internet Security and Acceleration Server is an example of an application-level firewall.

Now for the downside—deep inspection of application data is a resource-intensive activity, and significant processing power may be required to reduce the chances that the firewall will negatively impact network performance. The deeper the inspection, the higher the resource requirements and the higher the possibility of a detrimental effect on network performance. Thus, when you deploy an application-level firewall, it is important that you size it appropriately. Cutting corners on processors and RAM on your application-level firewall is an excellent formula for creating unhappy users, and it is always a better idea to go a little more powerful than your immediate needs. Remember to always plan for growth. Network utilization seldom decreases over time. You usually don't want to go back to management in a year to fund an upgrade.

One capability available on some application-level firewalls that can offset the negative performance effects of deep inspection is the addition of caching. Caching allows the firewall to store commonly downloaded data and provide it in response to requests from a user rather than having to retrieve the data from the Internet. Most web browsers have this capability for local storage of commonly used pages; a caching firewall extends this capability to all users on the network. For example, if fifty employees all read the front page of the online version of the *Wall Street Journal* when they come into the office, the firewall will cache the first visit to the site, then serve the stored page to the next forty-nine visitors.

Caching was a much more effective technology during the early days of the Internet, when most of the content was static. In recent years, with the advent of customizable views, mashups, and interactive content, the effectiveness of caching has become more and more limited.

LOOKING AT STATEFUL MULTILEVEL FIREWALLS

Stateful multilevel firewalls are designed to provide the best features of both packet filtering and application-level firewalls. This type of firewall provides network-level packet filtering and is also capable of recognizing and processing application-level data. When configured correctly, these firewalls can provide the highest level of security

of all the firewall types discussed here; however, they are typically the most expensive firewalls. In addition, with all of their available features, they can also be very complex to configure and maintain.

USING UNIFIED THREAT MANAGEMENT AND SECURE CONTENT MANAGEMENT DEVICES

To make your network the most secure, you need to implement a comprehensive solution that goes beyond the normal firewall. Unified Threat Management (UTM) consists of multiple security function including a comprehensive firewall, intrusion prevention, antivirus gateway, antispam filtering, content filtering, and reporting. You should also have a redundant solution that includes load balancing to protect yourself if a device fails. You could even combine an enterprise level firewall with a ***Secure Content Management (SCM)*** appliance. An SCM appliance specializes in content and threat analysis by integrating different functions and features including antivirus, anti-spam, and content filtering.

Using Hardware Firewalls versus Software Firewalls

Before we can consider when it's appropriate to utilize a hardware firewall instead of a software firewall, we need to look at what is meant by the term "software firewall." There are two basic types of software firewall:

- ***Host firewall:*** This type of software firewall is installed on a host and used to protect the host from network-based attacks. One example of this type of application is the Windows firewall included with recent versions of Microsoft operating systems. Host firewalls are also known as ***personal firewalls***.
- ***Network firewall:*** This category of software firewall consists of applications that are installed on servers used to protect network segments from other network segments. These types of firewalls offer similar functionality to hardware firewalls. The most popular network firewalls are those produced by Cisco.

The one circumstance in which it clearly doesn't make sense to use a hardware firewall is to protect a single host. If you need to protect only a single host, the best solution is to install a software firewall on the host with a specific set of rules based on what you're trying to protect. If the host is part of a larger network, which is almost always the case, then any network firewalls deployed on the network will also protect the host.

Host firewalls aside, there are a variety of factors that will impact your decision of whether to use a hardware solution or a software solution to protect your network. Many of these factors are related to some of the challenges associated with software firewalls. They include the following:

- **Host hardware:** Software firewalls run on the server's general-purpose hardware. This can lead to bottlenecks (including processor, memory, or network bottlenecks), especially if the hardware isn't sized appropriately to address the traffic requirements associated with running a firewall application.
- **Host operating system:** Although both hardware and software firewalls run operating systems, a hardware firewall runs a hardened operating system, providing a smaller attack surface than an unhardened operating system. In order to match the security level of the hardened OS provided by a hardware firewall, a software firewall server needs to be similarly

hardened. This can require specialized expertise and additional investments in both time and resources. As a result, most software firewalls have larger attack surfaces than their hardware counterparts.

- **Other applications:** Software firewalls must compete for resources with any other processes running on the host. In contrast, a hardware firewall has dedicated hardware resources that are not shared with any other service. As a result, when using a software firewall, you may find that you need additional hardware to match the performance of a hardware firewall because of the added resource requirements.
- **Availability/stability:** One potential issue associated with using a software firewall is that its reliability is tied to the reliability of the underlying operating system and associated hardware. Although the hardware components in a host will generally be as reliable as the components found in a hardware firewall, they are not always available in a redundant configuration, as hardware firewalls are. Operating systems have come a long way in terms of stability, but a general-purpose operating system such as what you would use with a software firewall is typically not as stable as the hardened operating system used on a hardware firewall.

Despite all the potential challenges associated with software firewalls, there are still a couple of compelling reasons to use software firewalls. First, they are very cost effective. Second, they are generally less complex to install and support than their hardware counterparts.

Therefore, in a medium to large network environment in which performance, availability, and reliability are critical, a hardware firewall is the best solution. Indeed, you will find hardware firewalls in virtually every enterprise network. In contrast, if you have a small network, are trying to keep costs down, or are trying to secure a single host, then using a software firewall may be the right answer.

Using Stateful versus Stateless Inspection

As previously discussed, the most basic firewall systems work by filtering packets. A packet filtering firewall inspects data packets as they attempt to traverse it and, based on the rules that have been defined on the firewall, either allows or denies each packet. The firewall doesn't consider any other information related to the packets when determining which packets are permitted to cross the firewall and which aren't. This type of data packet inspection is known as stateless inspection.

In stateless inspection, the data traversing the firewall are examined for information such as the following:

- The IP address of the sending device
- The IP address of the receiving device
- The type of packet (TCP, UDP, etc.)
- The port number

Stateful inspection takes packet filtering to the next level. In addition to examining the header information of the packets traversing the firewall, a stateful inspection firewall considers other factors when determining whether traffic should be permitted across the firewall. Stateful inspection also determines whether a packet is part of an existing session, and that information can be used to decide whether to permit or deny a packet. The existing session is referred to as the state, which frequently occurs at layer 4 (the transport layer) of the OSI model. Many of today's stateful inspection firewalls can also track communications across layers 5 through 7 as well.

Stateful inspection may sound relatively easy, but it's actually a very complex process, which is why stateful inspection firewalls are typically more expensive and more challenging to configure. A stateful inspection firewall keeps track of all current sessions in a state table stored in memory. In other words, when you initiate a connection to the MSN website to check today's headlines, the firewall stores the information regarding your session in a table. The same is done for every other connection occurring across the firewall. Then, as each packet reaches the firewall, it is analyzed to determine whether it is part of an existing session (state). If it is, and if the session is permitted based on the current firewall rules, then the packet is passed. In contrast, if the packet is not part of an existing session and is not being used to initiate a permitted session, it is dropped.

Another benefit of stateful inspection is that once a session is established, the firewall manages access based on sessions rather than on packets. This permits a simpler set of firewall rules when compared to traditional packet filtering firewalls. A packet filtering firewall requires a rule for each authorized packet. Therefore, if you want to permit a connection between Host A and Host B across a packet filtering firewall, you need a rule that permits packets from Host A to Host B, as well as another rule that permits packets from Host B to Host A. In comparison, when using a stateful inspection firewall, you can define a rule permitting a connection from Host A to Host B, and then the firewall's state table management will automatically allow the return traffic. Stateful inspection firewalls make excellent perimeter firewalls for protecting an internal network from the Internet, for protecting DMZ-based hosts (discussed in more detail later in this lesson) from the Internet, and for protecting extranets from connections to customers, vendors, or business partners.

Controlling Access with Network Access Protection (NAP)

THE BOTTOM LINE

One of the problems that many security programs struggle with is how to ensure that the computers attached to the network are compliant with the organization's security policies. Companies want to be sure that computers that are fully patched, are running up-to-date antivirus software, and belong to the organization before they are allowed to connect to the network. The challenge is finding a mechanism that permits the network to check each system before it connects. As the solution to this problem, Microsoft has developed Network Access Protection as part of Windows Server 2008.

Recognizing the need for administrators to have more granular control over what systems connect to a network, Microsoft introduced ***Network Access Protection (NAP)*** as part of the Windows Server 2008 operating system. NAP is a solution that allows administrators a more powerful way to control access to network resources. NAP's controls are based on the client computer's identity and whether that computer complies with the configured network governance policies.

NAP is a complex set of controls, a full discussion of which could easily fill this entire lesson or even this entire book. Therefore, for the purposes of this section, we will only be examining NAP at a high level, discussing its purpose, components, and requirements.

CERTIFICATION READY

How can you make sure that all computers on your network have an up-to-date antivirus package and current security patches from Microsoft?
3.2

Understanding the Purpose of NAP

NAP allows network administrators to define highly granular levels of network access based on who a client is, which groups the client belongs to, and how compliant the client is based on NAP policy. If a client is not compliant, NAP provides a mechanism to automatically bring the client into compliance. Then, once the client is compliant and all issues have been corrected, NAP will dynamically increase the client's level of network access.

NAP has three distinct components:

- **Health state validation:** In order for NAP to validate the health state of a computer, the administrator must first define health requirement policies. Then, when the computer tries to connect to the network, system health agents (SHAs) and system health validators (SHVs) validate the computer's configuration against the health requirement policy. In addition to defining health requirement policies, administrators must also define what action to take if a computer is not compliant. NAP can be configured to monitor only; here, the results of the system health check are logged for later analysis. If NAP is configured for limited access, computers that do not comply with health requirement policies will have their access limited to a restricted network. Generally, this would involve access to a remediation server so that the computer's issues can be corrected. In contrast, computers that comply with the health requirement policies will be granted unlimited network access.

> **TAKE NOTE***
> If you are going to deploy NAP in your environment, be sure to spend some time running in monitor-only mode. This will allow you to get a better understanding of the impact of the limited access policy if/when you implement it. Although security is important, it's a good idea to roll out new security capabilities with as little user impact as possible.

- **Health policy compliance:** Administrators can enforce compliance with health requirement policies by configuring NAP to automatically update noncompliant computers with missing software updates or configuration changes. It is important to understand that these compliance changes are performed using configuration management software, not NAP natively. When NAP is configured for monitoring only, noncompliant computers have access to the network so that they can be updated with required updates or configuration changes. In comparison, when NAP is configured in limited access mode, noncompliant computers have limited access until the required updates and configuration changes are completed. In

this case, the resources required to update the system should be included in the parts of the network the computer can access. Whether NAP is configured for monitoring or limited access, any NAP-compatible computers can be brought into compliance automatically. For computers that cannot support NAP (older versions of Windows, non-Windows operating systems, etc.), administrators can define exceptions that still allow the computers access to the network.

- **Limited access mode:** The final component that NAP provides to protect a network is limited access mode. This mode permits administrators to protect their networks by limiting the access of noncompliant computers. Noncompliant computers can be limited based on time (how long they can stay connected) or by what portions of the network they can access. If configured for limited access, it's recommended that this access include the resources needed to bring the computer into compliance. Then, after the computer is brought into compliance, NAP can open its access dynamically, without requiring a reboot or reauthentication.

Looking at How NAP Works

There are a variety of components used to make NAP work, including system health agents (SHAs) and system health validators (SHVs). SHAs run on the client computer and report the computer's status to the SHVs, which are running on the network and manage the NAP configuration.

These components provide health state tracking and compliance validation. They are the foundation of the NAP service because they allow NAP to determine what action needs to be taken based on a computer's configuration.

Client operating systems that have a Windows Security Health Validator SHA to monitor Windows Security Center settings include the following:

- Windows Vista Business
- Windows Vista Enterprise
- Windows Vista Ultimate
- Windows 7 Home Premium
- Windows 7 Professional
- Windows 7 Ultimate
- Windows XP Service Pack 3

Windows Server 2008 includes a corresponding Windows Security Health Validator SHV. Although currently leveraged largely by Microsoft, NAP is extensible and has an API that allows any vendor to provide its own SHAs

and SHVs to interoperate with NAP.

The other major part of the NAP puzzle is the enforcement piece. With NAP, enforcement clients (ECs) and enforcement servers (ESs) perform this function. These components require health state validation, and if a computer is not compliant, they enforce limited network access using the Network Policy Server (NPS), which is a component in Windows Server 2008. NPS is the RADIUS (Remote Authentication Dial-In User Service) server and proxy service in Windows Server 2008. When NPS functions as a RADIUS server, it provides authentication, authorization, and accounting (AAA) services for network access. When used for authentication and authorization, NPS interacts with the Active Directory to verify user or computer credentials, as well as to obtain user or computer account properties when a computer attempts an 802.1x-authenticated connection or a VPN connection.

NPS also acts as a NAP health policy server. In particular, administrators define system health requirements in the form of health policies on the NPS server, and the server then evaluates health state information provided by NAP clients to determine whether the clients comply. When a client is determined to be out of compliance, the NPS server offers the set of remediation actions that must be carried out by the NAP client to become compliant.

The role of NPS as an AAA server is independent from its role as a NAP health policy server. These roles can be used separately or combined as needed.

NPS also allows the Windows Server 2008 host to act as the health policy server, enforcing limited access in the following ways:

- **IPsec enforcement:** IPsec enforcement requires that the connecting client be configured to run IPsec before it can connect to other hosts. This is the most stringent of the various limited access mechanisms, because the client computer cannot communicate with anything until it is configured for IPsec communications. IPsec enforcement allows you to enforce anything the Windows IPsec client can be configured for. You can require IPsec communications with other compliant computers on a per-IP address or per-port number basis. This is a highly secure configuration due to the fact that IPsec encrypts all data traversing the network. In fact, you'll rarely see this configuration of NAP unless you're working in a high-security network environment that encrypts all network traffic.
- **802.1x enforcement:** 802.1x enforcement requires that the connecting client be compliant to obtain full access through an 802.1x-authenticated network connection. Here, the client must not only be able to successfully authenticate using 802.1x—it must also comply with the active health policy. The health policy is enforced every time the client attempts to connect to the network and authenticate with 802.1x. For noncompliant computers, network access is limited through a restricted access profile placed on the network device. The restricted profile can specify packet filters or force the computer to join a restricted VLAN. It's important to remember that 802.1x enforcement will also actively monitor the health status of the connected client, and if the client becomes noncompliant, it will apply the restricted access profile to the connection.

TAKE NOTE*

802.1x is an authentication protocol used to secure LANs from client connections. 802.1x authentication involves three parties: a client (also known as the supplicant), a network device (also known as the authenticator), and an authentication server. When the client wants to connect to the network, it makes a request to the network device. The network device then forwards that request to the authentication server using RADIUS. The authentication server next determines whether the client device is permitted on the network. If it's permitted, then the network device allows it to connect.

- **VPN enforcement:** VPN enforcement requires that a computer be compliant in order to obtain unlimited network access through a remote access VPN connection. This can be a huge benefit for organizations with large numbers of remote employees. One of the major challenges facing a company with many remote users is ensuring that these users' computers remain fully patched, are running up-to-date antivirus software, and are securely configured. NAP solves this issue with VPN enforcement. Noncompliant computers receive network access that is restricted by IP packet filters applied by the VPN server. As with 802.1x enforcement, VPN enforcement enforces health policy requirements every time a computer attempts to use a remote access VPN connection to connect to the network. VPN enforcement also actively monitors the health status of the connected client, and if the client becomes noncompliant, it will apply the restricted access profile to the connection.
- **DHCP enforcement:** DHCP enforcement requires that a computer be compliant with the health policy in order to obtain an unlimited-access IPv4 address configuration from a DHCP server. For noncompliant computers, network access is limited by an IPv4 address configuration that allows access to only a restricted network. DHCP enforcement enforces health policy requirements every time a DHCP client attempts to lease or renew an IP address configuration. As with the other modes of limited access, DHCP enforcement also actively monitors the health status of the NAP client and renews the IPv4 address configuration for access only to the restricted network if the client becomes noncompliant.

The last major element of your NAP installation is the remediation servers. These servers, which are not a formal component of NAP (there are no acronyms associated with the remediation servers), consist of the servers, services, or other resources that a noncompliant computer can use to become compliant. Of course, in order for a noncompliant computer to use remediation servers, these servers must be available as part of the limited access granted to the computer.

A remediation server might contain the latest software updates and virus signatures, could be a web server for requesting 802.1x credentials, or might even be a web server with instructions on how to configure IPsec to connect to the network. The makeup of your remediation servers is specific to your environment and your health policy. An SHA can communicate with a remediation server directly, or it can instead use installed client software to remediate issues.

Examining the Requirements for NAP

As previously mentioned, a number of different Microsoft operating systems support NAP, including the following:

- Windows Server 2008 or Windows Server 2008 R2
- Windows Vista Business
- Windows Vista Enterprise
- Windows Vista Ultimate
- Windows 7 Home Premium
- Windows 7 Professional
- Windows 7 Ultimate
- Windows XP Service Pack 3

However, there are a number of additional components you may need in order to successfully implement NAP. These include:

- Active Directory Domain Controller
- Active Directory-based Certificate Authority
- System Health Agents
- System Health Validators
- RADIUS server
- Enforcement clients
- Enforcement servers
- Network Policy Server
- 802.1x network devices
- VPN server
- DHCP server
- Remediation server

Not every NAP implementation will require all these components, but you should be aware that you might need them depending on why and how you are deploying NAP in your organization.

Using Isolation to Protect a Network

THE BOTTOM LINE

In addition to protecting the perimeter, you can use a number of other techniques to guard the computing resources on your internal network. These technologies allow you to isolate portions of your network, provide a special use for your firewalls, or even supplement the security provided by your firewalls. VLANs and routing are network technologies that can help you segregate your network into security zones. You can deploy technologies like Honeypots to help distract attackers from the important portions of your network, and firewalls can also play a part if you need to create DMZs on your network. VPNs, NAT, server isolation, and domain isolation are some additional concepts you can use to secure your network.

Understanding Virtual LANs

Before we can discuss what a virtual LAN is, we need to quickly review the concept of Local Area Networks (LANs). A LAN is a network of hosts covering a small physical area, like an office, a floor in a building, or a small group of buildings. LANs are used to connect multiple hosts. These LANs are then connected to other LANs using a router, which (as discussed) is a layer 3 device.

CERTIFICATION READY

What would you use to isolate your subnet with all of your servers from the rest of the network?
3.3

One of the challenges associated with LANs as they grow larger is that each device on the LAN broadcasts traffic onto the LAN. Although these broadcasts will not cross a router, if there are enough hosts, the aggregate broadcast traffic can saturate a network. One solution is to deploy more routers as a way to divide the network into more manageable segments. However, routers add latency to network traffic, and they require a routing protocol (discussed in the next section) for traffic to find its way from one part of the network to another.

Accordingly, virtual LANs (VLANs) were developed as an alternate solution to deploying multiple routers. VLANs are logical network segments used to create separate broadcast domains, but they still allow the devices on the VLAN to communicate at layer 2 without requiring a router. VLANs are created by switches, and traffic between VLANs is switched not routed, which creates a much faster network connection because there is no need for involvement of a routing protocol. Even though the hosts are logically separated, the traffic between these hosts is switched directly as if the hosts were on the same LAN segment.

VLANs provide a number of benefits over routed networks, including the following:

- Higher performance on medium or large LANs due to reduced broadcast traffic
- Better organization of devices on the network for easier management
- Additional security because devices can be put on their own VLAN

There are several different ways to assign hosts to VLANs. These methods are as follows:

- **VLAN membership by port:** Because the ports on a switch are defined as belonging to a specific VLAN, any device that is plugged into a port is assigned to the corresponding VLAN. For example, a thirty-two port switch might have ports 1–4 assigned to VLAN1, ports 5–16 assigned to VLAN2, and ports 17–32 assigned to VLAN3. Although this seems like a straightforward method for organizing ports, it can be problematic if you work in an environment in which users change office locations frequently. For example, if you've assigned the ports in one section of cubicles to the sales department and two weeks later, management decides to move the department to the other side of the building, you will need to reconfigure the switch to support this move. However, in a relatively static environment, this model works well.
- **VLAN membership by MAC address:** With this model, membership in a VLAN is based on the MAC address of the host. When the VLAN is set up on the switch, the hosts are assigned based on their MAC address. Thus, when a workstation moves to another location and connects to a different switch port, the switch automatically assigns the host to the appropriate VLAN based on the workstation's MAC address. Because the MAC address is generally hard coded into the host's NIC, this model is generally more usable in an environment in which hosts move. One downside to this model is that it requires more initial work to set up because you need to get all the MAC addresses from the hosts and associate them with the appropriate VLANs.
- **Membership by IP subnet address:** In this type of VLAN association, membership is based on the layer 3 header. The switch reads the layer 3 IP address and associates the address range with the appropriate VLAN. Even though the switch accesses layer 3 information in the header, the VLAN assignment is still done at layer 2 of OSI model and no routing takes place. This model is also conducive to environments in which there are frequent user moves. Performance may be affected because the switch needs to read the layer 3 header to determine which VLAN to assign the host to. This is generally not an issue with today's switch technologies, but it is good to be aware of the additional overhead associated with this model.
- **Membership by protocol:** VLANs can also be organized based on protocol. This was a useful solution when many LANs ran multiple network protocols, but with the current dominance of TCP/IP in virtually every network, this model is almost never used anymore.

The next question to think about is: How do VLANs help with security? In short, there are two basic ways to leverage a VLAN in support of security.

First, because a VLAN is logical separation, traffic on one VLAN is not directly accessible to hosts on another VLAN. However, this is of minimal use as there are now techniques called VLAN hopping that can provide access to

traffic on other VLANs.

The second use for VLANs from a security perspective is that they allow you to better organize your hosts for assigning access permissions. This technique is used in conjunction with firewalls or access control lists. For example, if you have a section of your building that your administrators sit in, you can create a VLAN for that area and give it access through your firewalls so that these employees can access all sections of the network. Meanwhile, the sales department might be on a VLAN that has its access restricted to the sales application servers, with access to the HR and finance applications blocked.

Understanding Routing

Routing takes place one step up the OSI model from a VLAN—in other words, at layer 3. Recall that routing is the process of forwarding a packet based on the packet's destination address. At each step in the packet's route across the network, a decision must be made about where to forward the packet. To make these decisions, the IP layer consults a routing table stored in the memory of the routing device. Routing table entries are created by default when TCP/IP initializes, and additional entries are added either manually by a system administrator or automatically through communication with routers.

But what exactly is a router? Previously, we defined routing as the process of forwarding a packet based on the packet's destination address. Thus, in its simplest form, a router is any device that forwards packets from one interface to another. This is a very simple description for a very complex process.

Routers come in two basic types—software and hardware. A software router is a computer running an operating system and multiple services, including a routing service. For example, Windows Server 2008 supports routing. Some benefits of using a software router are as follows:

- **Tight integration with the OS:** The routing service is frequently integrated with the operating system and other services.
- **Consistent/easier user interface:** No retraining is required on a new interface/operating system—the routing functions are configured through the standard user interface.
- **Low cost:** If you are adding routing to an existing server, you do not have to pay for dedicated hardware. This reduces the overall cost, although if you were to dedicate a software router for routing only, any cost savings would be negligible.
- **Flexibility:** Software routers allow you to configure and run multiple services on a single platform.

When would you use a software router? Typically, you will find software routers in small offices that are looking for an inexpensive, easy-to-manage solution. Another circumstance in which you might use a software router is between two LAN segments where traffic requirements are expected to be low. An example of this might be a lab segment where you want to isolate the lab hosts but do not want to invest in a dedicated hardware router.

Although there are benefits to using software routers, there are also some pretty significant drawbacks when compared to hardware routers. These include the following:

- **Slow performance:** Due to the additional overhead associated with the operating system and any additional running services, software routers are typically slower than hardware routers.
- **Lower reliability:** Any software router has the potential for issues with the operating system and other running services, as well as for problems with the greater number of hardware components as compared to a hardware router. As a result, software routers are typically less reliable than hardware routers.
- **Limited scalability:** When scaling a software router to multiple high-speed interfaces, you are subject to the limitations of the computer hardware. Because most PC-based servers are not designed to route multiple high-speed network interface cards, software routers will generally not scale as easily or as large as hardware routers. Also, adding additional services like access control lists or firewall services will impact a software router's performance to a greater degree than a comparable hardware router.
- **Limited protocol support:** Software routers typically do not support anywhere near the number of routing protocols that a hardware router does. For example, Windows Server 2008 is limited to the IP routing protocol RIP, and it does not presently support any of the more advanced IP-based routing protocols like BGP4.

You now understand what a software router entails, but what about a hardware router? In short, a hardware router is a dedicated hardware device whose main function is to route packets. This description is not as accurate now as it was in years past, however, because many of today's hardware routers are multifunction devices—for instance, they may include VPN, DHCP, firewall, caching, or perhaps even intrusion detection services. The benefits of hardware routers (as compared to software routers) include the following:

- **High performance:** Hardware routers run on custom-built, single-purpose hardware platforms, with highly optimized hardware and operating systems.
- **High reliability:** Hardware routers are typically more reliable than their software counterparts, due in large part to the limited software capabilities and dedicated hardware. A hardware router typically has higher modularity than a software router. Hardware routers can also be deployed in pairs so that one router will take over if the other fails. Although this is theoretically possible with a software router, it is very seldom done.
- **Wide routing protocol support:** Hardware routers can typically be configured to support any routing protocol from RIP to OSPF to BGP, as long as you purchase the appropriate functions. They also support a greater number of routing algorithms than software routers. In a larger network environment, this can be critical.

As with anything, hardware routers have their drawbacks, including the following:

- **High cost:** Typically, hardware routers are dedicated platforms, which usually makes them more expensive than software routers that also provide other services. This line is blurring as additional features become available on hardware routers. That being said, a small router can be relatively inexpensive.
- **Lower user friendliness:** Hardware routers are typically configured using a Secure Shell (SSH) connection and are managed through a command-line interface. Although there are graphical tools for managing routers, a lot of router configuration is still done through the command line using an extremely complex list of commands. Thus, an experienced router support engineer can configure or troubleshoot a hardware router without too much difficulty, but for someone new to routers, there is a steep learning curve.
- **Greater complexity:** Although an individual hardware router may not actually be much more complex than its software-based counterpart, as you scale to large networks, a hardware router environment can rapidly become extremely complicated. This issue would also apply to software routers, but software routers are not as common in the real world. In most network environments, hardware routers are used almost exclusively, and software routers are reserved for only the smallest networks or locations.

EXAMINING HOW ROUTING WORKS

When a router receives a packet that must be forwarded to a destination host, the router has to make a decision. In particular, it needs to determine whether it can deliver the packet directly to the destination host, or whether it needs to forward the packet to another router. To make this decision, the router examines the destination network address. If the router has an interface that is connected to the same network as the destination host, it can deliver the packet directly. Where it gets interesting is when the router is not connected to the same network as the destination host—here, the router must determine the best route to the destination host so it can forward the packet correctly.

When a router needs to forward a packet to another router, it uses the information in its routing tables to choose the best path for the packet. Which router to forward the packet to is determined by a number of variables pertaining to the network path to the destination host, including the number of hops, the cost of each hop, and so on. This database is stored in the router's memory to ensure the lookup process is performed very quickly.

> **TAKE NOTE***
> Just because there is a route to a destination doesn't mean there is also a route back.
> Although this is not a common problem in networks with dynamic routing enabled, it can occur, particularly if you are working in a heavily firewalled network environment.

As the packet travels across the network toward its destination, each router along the way makes a decision about where to forward the packet by consulting its routing table. Moreover, when the destination host sends a reply packet, it is possible that this packet may not travel back to the original sender via the same route. The route taken by the reply packet depends on the metrics of each path along the return route. In other words, the way to the destination host may not be the best path back to the sending host.

The information in a routing table can be generated in one of two ways. The first method is to manually configure the routing table with the routes for each destination network. This is known as static routing. Static routing is more suited to small environments in which the amount of information to configure is small and the overhead of dynamic routing is unacceptable. Static routers do not scale well to large or frequently changing networks because of the requirement for manual administration.

The second method for generating routing table information is to make use of a dynamic routing protocol. Because dynamic routing protocols are quite a bit more complex than static routing, we need to take a more in-depth look at this subject.

A general definition of “protocol” is an agreed-upon method for exchanging data between two devices. Accordingly, a routing protocol defines the method for exchanging routing information between two routing devices—and a dynamic routing protocol involves the exchange of routing information that is automatically built and maintained in a routing table. In other words, when you are using a dynamic routing protocol, routing information is exchanged between routers and used to update the information stored in each device’s routing table. This can be done either periodically (at scheduled intervals) or on demand. If set up correctly at the outset, dynamic routers require little administration, outside of ensuring that software updates are applied in a timely fashion. Because they learn routing information dynamically and have the ability to route around failures when the network architecture supports it, dynamic routers are generally used in large network environments in which static routing would be impractical.

> **TAKE NOTE***
> Don’t forget: Routers need to be patched, too!
> Because they run an operating system, routers have security and functionality updates that must be applied.

LOOKING AT ROUTING PROTOCOLS

Routing protocols are based either on a distance vector or a link state algorithm. The differences between the two methods relate to when routing information is exchanged, what information is sent during this exchange, and how quickly the protocol can route around outages when the network topology supports it. Path selection involves apply a routing metric to multiple routes in order to select the best route. Some of the metrics used are bandwidth, network delay, hop count, path cost, load, reliability, and communication costs. (The hop count is the number of routers traversed by a packet between its source and destination.)

Distance vector-based routing protocols require that each router inform its neighbors of its routing table. This is done by sending the entire routing table when the router boots, and then sending it again at scheduled intervals. Each router takes the updates from its neighboring routers and then updates its own routing table based on this information. Using the information from these updates, a router can build a network map in its routing table, and it can then use this map to determine hop counts for each network entry in the routing table. RIP is one example of a distance vector-based routing protocol that is supported by Windows Server 2008.

Routing updates sent using a distance vector-based routing protocol are unacknowledged and unsynchronized, which is one of the drawbacks of these protocols. Some other drawbacks of this type of routing protocol include the following:

- **High overhead:** Because every router on the network sends its entire routing table when it sends an update, distance vector-based protocols produce very large routing tables. This adds overhead to the router memory needed to store the tables, as well as the router

processing power needed to maintain these tables. Large routing tables can also hamper an administrator trying to determine the source of an issue when problems arise.

- **Lack of scalability:** Distance vector-based networks are limited to 15 hops (router traversals) for any given route. In a large network (like the Internet), it is very easy to have network segments that are greater than 15 hops away—and such segments would be unreachable in a distance vector-based network.
- **Intensive bandwith utilization:** Distance vector-based protocols require that routers exchange their entire routing table whenever they are updated. On a large network with large routing tables, these updates can utilize significant amounts of bandwidth, especially across smaller WAN connections or demand dial links.
- **Long convergence time:** Convergence is the amount of time it takes for a routing algorithm to detect and route around a network failure. Distance vector-based protocols typically have longer convergence times than link state-based protocols (described later in the lesson).
- **Routing loop issues:** Distance vector-based protocols can also suffer from routing loop issues when there are multiple paths to a network. A routing loop is when a packet is sent back and forth between two networks or across multiple networks where the packet is eventually sent back to the network that sent it. Since it is a loop, the packet never gets to its destination. If one or more mechanisms are not in place to deal with routing loop issues and packets that are caught in a routing loop are not dropped, your network would eventually be congested as it deals with the lost packets.
- **Count to infinity issues:** Count to infinity issues occur when there is a network outage and the routing algorithm cannot calculate a new router. Here, one router will broadcast a route and increment the hop count for the router, then a second router will broadcast the same route to the first router, also incrementing the hop count, and so on, until the route metric (hop count) reaches 16 and the route is discarded.

Thankfully, some distance vector-based routing protocols have additional mechanisms that allow them to avoid count to infinity issues, as well as to improve convergence. These mechanisms are as follows:

- **Split horizon:** The split horizon mechanism prevents routes from being broadcast out the interface they were received from. Split horizon eliminates count to infinity and routing loops during convergence in single-path internetworks and reduces the chances of count to infinity in multipath internetworks.
- **Split horizon with poison reverse:** The split horizon with poison reverse mechanism allows routes to be broadcast back to the interface they were received from, but they are announced

with a hop count of 16, which indicates that the network is unreachable (in other words, the route has been poisoned and is unusable through that interface).

- **Triggered updates:** Triggered updates allow a router to announce changes in metric values almost immediately, rather than waiting for the next periodic announcement. The trigger is a change to a metric in an entry in the routing table. For example, networks that become unavailable can be announced with a hop count of 16 through a triggered update. If triggered updates were sent by all routers immediately, each triggered update could cause a cascade of broadcast traffic across the IP internetwork.

The advantages of distance-vector routing are that it requires little maintenance and is easy to configure, making it popular in small network environments.

Link state routing—the second type of routing protocol—was designed to overcome the disadvantages of distance vector routing. Routers that use link state routing protocols learn about their network environment by “meeting” their neighboring routers. This is done through a “hello” packet, which tells the neighboring router what networks the first router can reach. Once this introduction is complete, the neighboring router will send the new network information to each of its neighboring routers using a link state advertisement. Open Shortest Path First (OSPF) is an example of a link state routing protocol. The neighboring routers copy the contents of the packet and forward the link state advertisement to each attached network, except for the network the link state advertisement was received on. This is known as flooding.

A router that uses a link state routing protocol builds a tree, or map, of shortest paths using itself as the root. This tree is based on all the link state advertisements seen, and it contains the route to each destination in the network. Once this tree is built, routing information is sent only when changes to the network occur, instead of periodically as with distance vector-based protocols.

There are a number of advantages to the link state method, especially when compared to distance vector-based routing protocols. Some advantages include the following:

- **Smaller routing tables:** Because the router only maintains a table of link states, rather than a copy of every route on the network, it is able to maintain much smaller routing tables.
- **High scalability:** Link state protocols do not suffer from the 16-hop issue that distance vector-based protocols do, so they are able to scale to much larger networks.
- **More efficient use of network bandwidth:** Because link state information is not exchanged after the network has converged, routing updates do not consume precious bandwidth unless there is an outage that forces the network to reconverge.
- **Faster convergence:** Link state routing protocols converge faster than distance vector-based protocols because updates are sent as soon as a change to the network occurs, instead of having to wait for the periodic updates used in distance vector-based protocols.

One disadvantage of link state protocols is that they are more complex to understand and configure than distance vector protocols. They also require additional processing power on the router, due to the need to calculate the routing tree.

Routing can be a key component of network security because it lets you determine which parts of a network can be accessed by other parts of the network. For example, if you have a business partner connection to a third-party network, the third-party network will need to have routing information in order to access any systems that you have put on your extranet DMZ. Although a firewall is the best way to secure this connection, you can add an additional layer of security by restricting the routing available to the third party. In other words, if you only tell the third party's network the routes to the extranet, it will not be able to send packets to any other parts of your network where it should not have access.

Looking at Intrusion Detection and Intrusion Prevention Systems

Two other technologies available to secure networks are ***intrusion detection systems (IDSs)*** and ***intrusion prevention systems (IPSs)***. An IDS is a solution designed to detect unauthorized user activities, attacks, and network compromises. An intrusion prevention system (IPS) is similar to an IDS, except that in addition to detecting and alerting, an IPS can also take action to prevent a breach from occurring.

There are two main types of IDS/IPSs:

- **Network based:** A network-based IDS (NIDS) monitors network traffic using sensors that are located at key locations within the network, often in the demilitarized zone (DMZ) or at network borders. These sensors capture all network traffic and analyze the contents of individual packets for malicious traffic. A NIDS accesses network traffic by connecting to a hub, network switch configured for port mirroring, or network tap.
- **Host based:** A host-based IDS (HIDS) generally has a software agent that acts as the sensor. This agent monitors all activity of the host on which it is installed, including monitoring the file system, logs, and kernel to identify and report suspicious behavior. A HIDS is typically deployed to safeguard the host on which it is installed.

There are two common deployment methodologies used when placing an IDS/IPS to protect a network from the Internet. Each has its own advantages and disadvantages:

- **Unfiltered:** An unfiltered IDS/IPS installation examines the raw Internet data stream before it crosses the firewall. This provides the highest amount of visibility for detecting attacks, but it also means that there is a significantly larger volume of data to be monitored and a higher possibility of false positives. There is also a chance that during periods of high traffic, the IDS/IPS might not be able to process all the packets, so attacks may be missed.
- **Screened:** A screened IDS/IPS solution monitors only that traffic that gets through the screening firewall. The advantage to this model is it dramatically reduces the amount of information that needs to be monitored, thereby also reducing the chances of false positives

and lost packets during high traffic volumes. However, there is a loss of visibility with this model because you cannot see attacks on the screening firewall.

> **TAKE NOTE***
> Historically, IDSs and IPSs have been used to secure Internet connections, because these connections typically present the largest threat to a network. However, with the interconnectivity of networks beyond the Internet and the threat of insider attacks, it may make sense to deploy an IDS or IPS in strategic locations on your internal network. You should especially consider doing so if your internal network has connections to third-party networks, such as those of customers, vendors, or business partners.

Looking at Honeypots

Honeypots, honey nets, and padded cells are complementary technologies to IDS/IPS deployments. A ***honeypot*** is a trap for hackers; it is designed to distract hackers from real targets, detect new vulnerabilities and exploits, and learn about the identity of attackers. A ***honey net*** is a collection of honeypots used to present an attacker with an even more realistic attack environment. Finally, a ***padded cell*** is a system that waits for an IDS to detect an attacker and then transfers the attacker to a special host where he or she cannot do any damage to the production environment. These are all related technologies, and each can be used to add an additional layer to your security infrastructure.

As previously mentioned, a honeypot is a valuable surveillance and early warning tool. However, “honeypot” is also a generic term used to describe anything that would attract an attacker. Thus, although the term usually refers to a host running special software for detecting and analyzing attacks, it can sometimes refer to other things, such as files, data records, or even unused IP address space.

There are a variety of different types of honeypots, including the following:

- **Production:** A production honeypot is a relatively easy solution to deploy. It is used to distract attackers from potentially vulnerable production systems and is relatively simple to use. Production honeypots typically capture limited information, and they can generally be found in corporate networks. This type of honeypot is typically used as an additional early warning system that enhances an IDS/IPS system.
- **Research:** A research honeypot is more complex than a production honeypot and is more difficult to deploy and maintain. This type of honeypot captures extensive information, which can then be used to develop attack signatures, identify new attack techniques and vulnerabilities, and develop a better understanding of an attacker’s mindset. Research honeypots are used primarily for research by universities, the military, or other government organizations.

When deploying a honeypot, you should ensure that the associated server contains no production information and is not being used for production purposes. This ensures that your production data is secure—and, because there is no legitimate reason for traffic or activity on the system, you can safely assume that any activity that occurs on the honeypot is malicious activity.

You should be aware, however, that honeypots can create risks to your environment. Because you are essentially using a honeypot as bait for an attacker, you are actually luring attackers into your network environment. As a result, you need to be absolutely certain that all honeypots are isolated from your production environment. If they are not, an attacker may be able to jump from a honeypot to your production environment and compromise critical systems or infrastructure. It's somewhat like trying to lure a bear to an adjoining campsite to keep them away from yours—there's always a chance the bear may find your campsite anyway.

One area in which honeypots are especially useful is in the battle against spam. One challenge associated with spam and spam filtering is that the spammers are constantly changing the techniques they use to bypass spam filters. They also have a variety of techniques for harvesting email addresses from websites for inclusion in their spam target lists. As a result, the people who develop spam filters spend much of their time working to identify these techniques and to develop new filters to combat them. Honeypots are an essential component of this fight, and there are two types of honeypots that can be used to combat spam:

- **Email address honeypot:** Any email address that is dedicated to receiving spam for analysis can be considered a spam honeypot. An example of this technique is Project Honey Pot, a distributed, open-source project that uses honeypot pages installed on websites around the world in conjunction with uniquely tagged email addresses for analyzing not only spam delivery, but also email address harvesting techniques.
- **Email open relay honeypot:** Email open relays are servers whose job is to relay messages from mail server to mail server. If you have ever used POP3 or IMAP to send email through your personal ISP, you have used a mail relay server. In some instances, these servers are set up so they do not need credentials to send email, which is a significant prize for spammers because it allows them to relay millions of spam emails anonymously. Setting up a honeypot that appears to be an open relay can potentially reveal a spammer's IP address and provide bulk spam capture. This allows for in-depth analysis of the spammer's techniques, response URLs and email addresses, and other valuable information.

Although these are all extremely exciting technologies, they are deployed in very few corporate environments. Instead, these technologies are primarily used by educational institutions and security research firms. Corporate information security professionals are so busy securing their environment from attacks that they don't spend a lot of time researching attack patterns. As long as an attack doesn't succeed, these professionals are satisfied. Still, in high-security environments in which there is extensive Internet-based activity and data that requires additional layers of security, honeypots may be part of the layered security defense.

Looking at DMZs

When most people hear the term ***DMZ*** (short for ***demilitarized zone***), images of barbed wire and machine gun emplacements come to mind. Although not entirely accurate in the scope of information security, this vision is not that far from reality. In computer networking, a DMZ is a firewall configuration used to secure hosts on a network

segment. In most DMZs, the hosts on the DMZ are connected behind a firewall that is connected to a public network like the Internet. Another common configuration is to have the firewall connected to an extranet that has connections to customers, vendors, or business partners. DMZs are designed to provide access to systems without jeopardizing the internal network.

There are two typical DMZ configurations you may encounter in production environments:

- **Sandwich DMZ:** In a sandwich DMZ model (see Figure 4-3), there is both an outer firewall and an inner firewall. The outer firewall secures the DMZ network segment from the external (insecure) network. Servers that are meant to be accessed from the external network (like the Internet) have the appropriate rules configured to permit secure access. The inner firewall is then used to add an additional layer of security between the servers on the DMZ and the internal (secure) network. The main benefit of this model is that in the event that the outer firewall and/or a server on the DMZ is compromised, there is an additional layer of firewall security protecting the internal network. Ideally, the outer and inner firewalls are from different vendors in order to ensure that the same exploit cannot be used to compromise both. The major drawbacks of this model are that it is more complex to implement and maintain, it is more expensive because of the extra firewall, and if you have different firewall vendors, you'll need additional training for your staff.

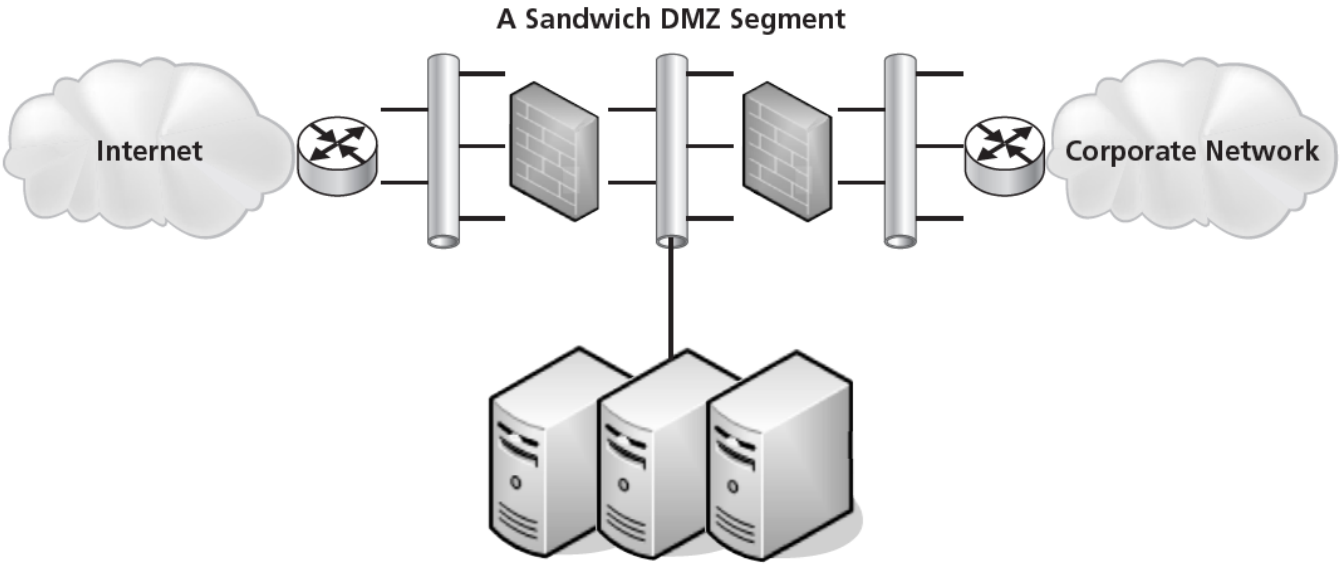

Figure 4-3 Sandwich DMZ

- **Single firewall DMZ:** In a single firewall DMZ (see Figure 4-4), the DMZ is an additional network connection from the firewall. This leaves you with an external network connection, an internal network connection, and a DMZ network connection all connected to the same firewall. Although this architecture still allows the firewall to control access to DMZ resources, if the firewall is compromised, access to the internal network may be breached. This model is less expensive than the sandwich model, but it does not provide as high a level of security.

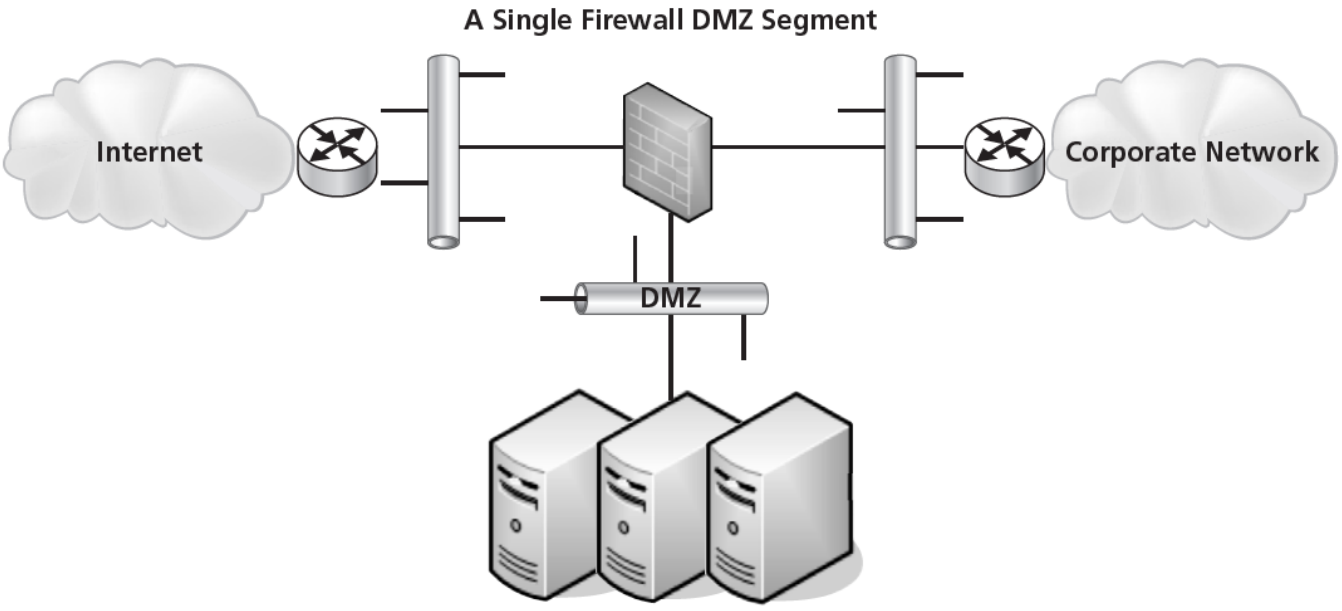

Figure 4-4 Single firewall DMZ

Now that you understand the architecture of a DMZ, you should also understand what types of servers and services you might place on a DMZ. Some of the most common include the following:

- **Web servers:** Web servers are the most common servers found in DMZ networks. Accessed using HTTP over port 80 or HTTPS over port 443 for secure access, web servers are commonly Internet-accessible. In fact, the next time you access a web server on the Internet, you can count on the fact that it is hosted on a DMZ somewhere. Web servers add an additional layer of complexity due to the fact that many web applications need to communicate with an internal database or databases to provide some specialized services. These databases often contain sensitive information, so you should not place them on the DMZ because you do not want them to be accessed from the insecure network (the Internet). An example of this might be an e-commerce application. When you reach a seller's website, the catalog data—including product descriptions, prices, and availability—are contained in the database (sometimes referred to as the back end database). If the database server also contains critical information like Social Security numbers, financial information, or credit card data, you may want to add an application firewall between the web server and the database server. Although this increases the cost and complexity of your solution, it adds an extra layer of security to protect the database.

- **Email relay servers:** Email servers are another type of server that needs to be accessed from the Internet. In the early years of computer networking, it was not unusual for email to be restricted to an organization's corporate network. However, once companies and individuals were increasingly connected to the Internet, the ability to send and receive email from other companies became critical to business success. By placing your email relay servers, which communicate on port 25, on a DMZ, they can receive email from the Internet and then relay it securely to mail servers on the internal network. Spam filtering capabilities are frequently included on these relay servers.

- **Proxy servers:** Proxy servers are used to proxy or act as an intermediary for user requests from the internal network to the Internet, and they are usually used to retrieve website information. These servers can be placed on a DMZ to provide additional security for web browsing. Some proxy servers will filter content (including inappropriate websites), add virus protection and antispyware security, and even improve performance by caching web requests.

- **Reverse proxy servers:** Reverse proxy servers are used to provide secure access to internal applications from an insecure network. Although these servers have largely been replaced by VPN technologies, they are still sometimes used to provide employees access to web-based email servers on the internal network, provide access to internal web applications, and in some cases, even provide secure terminal services connections to an internal network.

Understanding Network Address Translation (NAT)

Network Address Translation (NAT) is a technique used to modify the network address information of a host while traffic is traversing a router or firewall. This technique hides the network information of a private network while still permitting traffic to be transferred across a public network like the Internet.

NAT was originally created as a workaround for IP addressing issues. Recall that the Internet relies on the TCP/IP protocol suite for communications between hosts. A critical component of this protocol suite is IP addressing. In the early days of the Internet, when the TCP/IP protocol and related addressing was being developed, the 32-bit addressing scheme (known as IPv4) was considered more than adequate for any potential network growth. Technically, there were 4,294,967,296 unique addresses available using a 32-bit address, and even discounting the reserved ranges, there were still over 3 billion possible addresses. At the time, that was enough to provide an address for every person on the planet, including children. Unfortunately, the designers of this addressing scheme dramatically underestimated the explosive growth of the Internet, as well as the widespread adoption of TCP/IP in business and home networks—both of which threatened to exhaust the pool of IPv4 IP addresses. Without unique addresses, the Internet would be unable to successfully route TCP/IP traffic. NAT was the resulting solution for maintaining Internet functionality given the limited number of IP addresses available.

Today, one practical use for NAT is that it allows you to use one set of IP addresses on the internal LAN and a second set of IP addresses for the Internet connection. There is a device (usually a router or firewall) located between the two networks that provides NAT services, managing the translation of internal addresses to external addresses. This allows companies to use large numbers of unregistered internal addresses while only needing a fraction of that number of addresses on the Internet, thus conserving the addresses. This permits the reuse of addresses within private networks while ensuring that the addresses used on the Internet remain unique.

The long-term solution for the address issue is IPv6 or Internet Protocol Version 6, the next generation protocol for the Internet. This protocol is designed to offer several advantages over IPv4, including support for addresses that are 128 bits long. This permits 2128 unique IPv6 addresses, or over 340 trillion addresses. However, adoption of IPv6 has been slow, in large part due to the successful use of NAT and proxy servers to conserve the number of IPv4 addresses currently used on the Internet.

TAKE NOTE*
Network Address Translation (NAT) is supported under Windows Server 2008 by the Routing and Remote Access Service.

Today, there are two main types of NAT:

- **Static NAT:** Static NAT maps an unregistered IP address on the private network to a registered IP address on the public network, using a one-to-one basis. This method is used when the translated device needs to be accessible from the public network. For example, a web server on your DMZ network might have an unregistered address of 10.20.30.40 that is translated by a NAT-capable device to an Internet-facing address of 12.4.4.234. Thus, a user trying to connect to that website can enter 12.4.4.234, and the router or firewall at the other end will translate that address to 10.20.30.40 when the packet reaches it. This version of NAT is typically used in conjunction with DMZs or extranet networks.
- **Dynamic NAT:** Dynamic NAT maps an unregistered IP address on the private network to a registered IP address that is selected by the routing device providing the NAT service from a pool of registered addresses. This method is most commonly used when a large number of systems on the internal network need to access the Internet, but they don't have the requirement for a static address. Here, a workstation's address is translated to the next available registered address in the pool as soon as it initiates a connection to the public network.

There are two major security implications associated with the use of NAT. First, NAT can be used to hide private network addresses, which makes it more difficult for an attacker to successfully penetrate a private network. The addresses that are visible to an Internet-based attacker are the NAT addresses typically stored on the firewall, which should be one of the more secure devices on your network.

NAT also presents a unique issue when working with the IPsec protocol (discussed in more detail later in the lesson). Early implementations of IPsec did not support NAT, so the IPsec protocol could not be used when NAT was enabled in an environment. NAT traversal capability was added in later versions of the IPsec protocol, but IPsec still requires that some special steps be taken in order to work successfully with NAT.

Understanding Virtual Private Networks (VPNs)

VPN (Virtual Private Network) is a technology that uses encrypted tunnels to create secure connections across public networks like the Internet. There are a variety of uses for this technology, but three of the most common are shown in Figure 4-5.

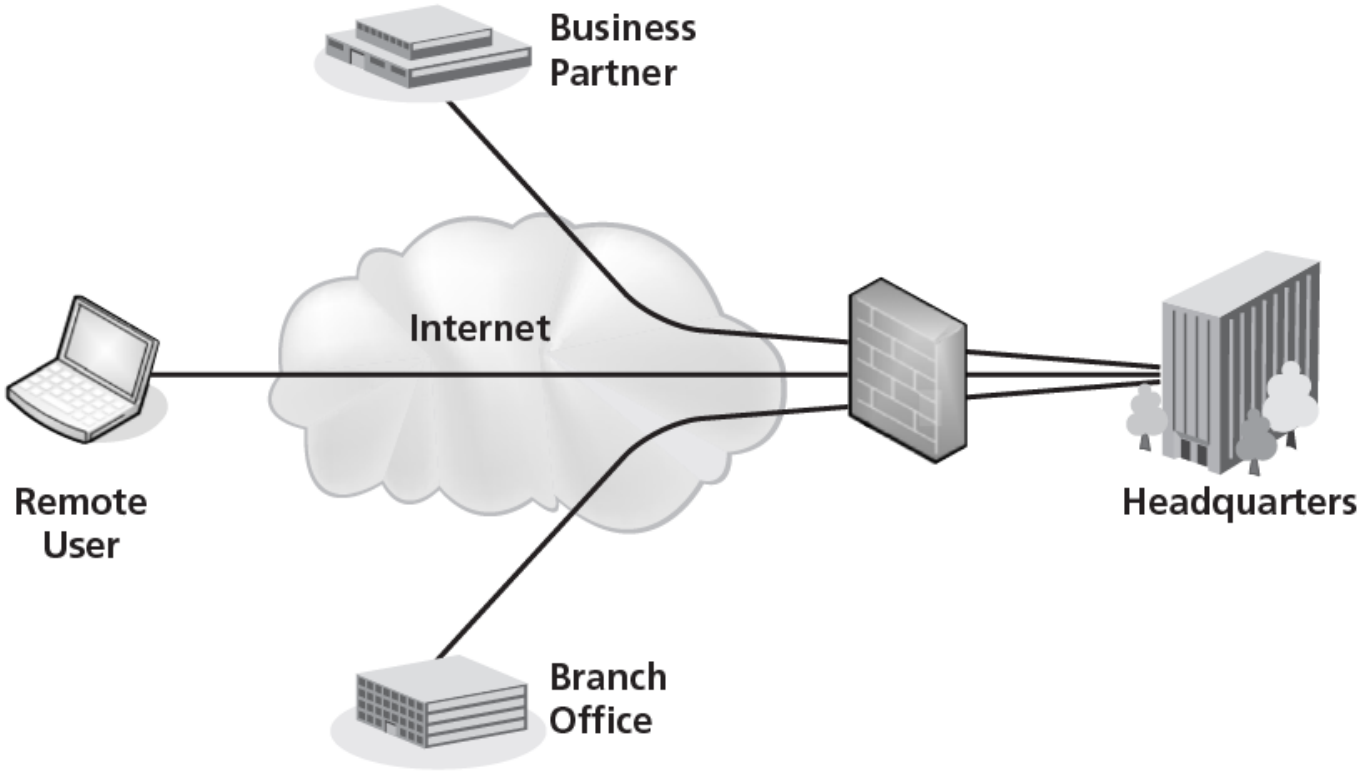

Figure 4-5 Uses for VPN technology

VPNs are commonly used by remote employees for access to the internal network, to create secure network-to-network connections for branch offices or business partner connections, or even to create secure host-to-host connections for additional security and isolation on an internal network. VPNs utilize encryption and authentication to provide confidentiality, integrity, and privacy protection for data.

Remote access VPNs were first introduced in the late 1990s and were initially used in conjunction with modems to provide more secure, more flexible connectivity to corporate networks. All that was required was a dial-up Internet connection and a VPN client, and you could connect to a corporate network over an encrypted connection. Shortly thereafter, with the advent of high-speed Internet connections, the use of VPN technologies exploded. It was now possible in some cases to get a faster connection at home via high-speed Internet than in a branch office via typical dedicated network connections. This technology also allows businesses to migrate from expensive dedicated network connections to less expensive Internet-based VPN connections.

The first standards-based VPNs were based on the IPsec protocol. IPsec-based VPNs quickly overtook some of the proprietary-based VPNs that were the first products marketed.

Understanding Internet Protocol Security (IPsec)

Internet Protocol Security (IPsec) is a standards-based protocol suite designed specifically for securing Internet Protocol (IP) communications. It is also a component of IPv6, the next generation of the IP protocol. IPsec authenticates and encrypts each IP packet in an IP data stream. In addition, IPsec has protocols that can be used to establish mutual authentication and cryptographic keys negotiation during a session. IPsec operates at the network layer of the OSI model.

TAKE NOTE*
Why do layers matter?
The fact that IPsec operates at layer 3 of the OSI model means that it can be used to encrypt any traffic in layers 4 through 7 of the model.

In practical terms, this means that IPsec can be used to encrypt any application traffic.

IPsec was designed to provide interoperable, high-quality, cryptographically based security for IPv4 and IPv6. Today, it offers a comprehensive set of security services, including the following:

- Access control
- Connectionless data integrity checking
- Data origin authentication
- Replay detection and rejection
- Confidentiality using encryption
- Traffic flow confidentiality

The IPsec protocol has three major components:

- **Authentication Header (AH):** AH provides integrity protection for packet headers, data, and user authentication. It can optionally provide replay protection and access protection. AH cannot encrypt any portion of packets. For AH to work in conjunction with NAT, the IP protocol number 51 needs to be allowed across the firewall.
- **Encapsulating Security Payload (ESP):** ESP provides authenticity, integrity, and confidentiality protection of data packets. Unlike AH, ESP cannot protect packet headers—it protects the data only. For ESP to work in conjunction with NAT, the IP protocol number 50 needs to be allowed across the firewall.
- **Internet Key Exchange (IKE):** IKE is used to negotiate, create, and manage security associations (SA), which means that it is the protocol that establishes the secure communication channel to network hosts. For IKE to work in conjunction with NAT, the User Datagram Protocol (UDP) port 500 needs to be allowed across the firewall.

IPsec can be used in two different modes:

- **Transport mode (host-to-host):** In transport mode, only the data packet payload is encapsulated. Because the packet header is left intact, the original routing information is used to transmit the data from sender to recipient. When used in conjunction with AH, this mode cannot be used in a NAT environment because the encryption of the header is not compatible with the translated addressing.
-

Tunnel mode (gateway-to-gateway or gateway-to-host): In tunnel mode, the IP packet is entirely encapsulated and given a new header. The host/gateway specified in the new IP header decapsulates the packet. This is the mode used to secure traffic for a remote access VPN connection from the remote host to the VPN concentrator on the internal network. This is also the mode used to secure site-to-site IPsec connections.

Using Other VPN Protocols

Although IPsec is considered the predominant protocol associated with VPNs, there are other protocols that can also be used to build VPNs or provide VPN-like connectivity.

USING SECURE SOCKETS LAYER (SSL) AND TRANSPORT LAYER SECURITY (TLS)

One of the key VPN protocols used today is SSL/TLS, which is the main alternative to IPsec for implementing a VPN solution.

The SSL protocol standard was originally proposed as a standard by Netscape. Although this protocol is widely used to secure websites, it has since been formalized in the IETF standard known as Transport Layer Security (TLS). The SSL/TLS protocol provides a method for secure client/server communications across a network and prevents eavesdropping and tampering with data in transit. SSL/TLS also provides endpoint authentication and communications confidentiality through the use of encryption.

If you have ever connected to a website using HTTPS, the secure version of HTTP web browsing, you have used the SSL protocol. This protocol provides 128-bit encryption, and it is currently the leading security mechanism for protecting web traffic on banking, e-commerce, email, and essentially any other secure websites you might encounter. In typical end user/browser usage, SSL/TLS authentication is one way. Here, only the server is authenticated when the client compares the information entered to access a server to information on the SSL certificate on the server (the client knows the server's identity), but not vice versa (the client remains unauthenticated or anonymous). However, SSL/TLS can also perform bidirectional authentication by using client-based certificates. This is particularly useful when this protocol is used to access a protected network because it adds an additional layer of authentication to the access.

As discussed in the section on IPsec, a VPN creates a secure tunnel through a public network like the Internet. Although SSL VPNs still leverage the concept of tunneling, they create their tunnels differently than IPsec. An SSL VPN establishes connectivity using the SSL protocol. IPsec works at layer 3 of the OSI model, while SSH functions at layers 4 and 5. SSL VPNs can also encapsulate information at layers 6 and 7, which makes SSL VPNs very flexible.

One additional feature of an SSL VPN is that it usually connects using a web browser, whereas an IPsec VPN generally requires that client software be installed on the remote system.

SSL VPNs are predominantly used for remote access VPN connections in which a client is connecting to applications on an internal network, as opposed to site-to-site connections in which two gateways are used to connect disparate private networks across the Internet.

Some benefits of SSL/TLS VPNs over IPsec VPNs include the following:

•

Lower cost: Because an SSL VPN is typically clientless, you don't have the costs of rolling out, supporting, and updating client software.

- **Platform independence:** Because access to an SSL VPN is granted through the standard SSL interface, which is a component of virtually every web browser, virtually any OS that runs a browser is supported.
- **Increased client flexibility:** As a general rule, IPsec clients are generally installed only on corporate systems. In comparison, due to their additional flexibility, SSL VPNs can be configured to allow access from a variety of clients, including corporate systems, home systems, customer or supplier systems, or even kiosk machines in libraries or Internet cafes. This wider access can greatly increase employee satisfaction.
- **NAT support:** Historically, Network Address Translation (NAT) has caused issues with IPSec VPNs. Virtually all IPsec vendors have created workarounds for this issue. Still, with an SSL VPN, you don't have these issues because SSL works at a higher layer than IPsec.
- **Granular access control:** Depending on your environment, this could be considered either a benefit or a drawback. SSL VPNs require a greater granularity of access than a typical IPsec VPN. In particular, instead of creating a tunnel from the host to the internal network, SSL VPNs require that each resource that is accessed be explicitly defined. The upside is unless you have explicitly defined a resource, an SSL VPN user cannot access it, which offers security benefits. However, in a complex environment, this could add significant overhead to your VPN support.
- **Fewer firewall rules are required:** In order to access an IPsec gateway across a firewall, you need to open several ports to support the individual protocols for authentication and the tunnel. With an SSL VPN, you only need to open port 443, which is generally easy to do due to the prevalence of the HTTPS protocol.

EXAMINING SECURE SHELL (SSH)

Secure Shell (SSH) is a protocol for secure remote login and other secure network services over a network. SSH can be used for a number of applications across multiple platforms, including UNIX, Microsoft Windows, Apple Mac, and Linux. Some of the applications supported with SSH include the following:

- Secure logins
- Secure remote command executions
- Secure file transfers
- Secure backups, copying, and mirroring of files

- Creating VPN connections (when used in conjunction with the OpenSSH server and client)

The SSH protocol consists of three major components:

- **Transport layer protocol:** This provides server authentication, confidentiality, and integrity with perfect forward secrecy.
- **User authentication protocol:** This provides authentication of the client to the server.
- **Connection protocol:** This multiplexes the encrypted tunnel into several logical channels.

Now that we've looked at some of the protocols you can use to secure traffic across a network, and usually across public networks like the Internet, let's look at a technique for providing additional security on your internal network.

Looking at Server and Domain Isolation

Security professionals are constantly being asked by businesses to allow greater resource access to facilitate business requirements. Although wider and easier access to resources can increase the production of a business, it also presents significant security challenges. The risks of virus attack, rogue users and devices, and unauthorized access to sensitive information associated with unauthorized or unmanaged devices are enough to keep any information security professional awake at night.

One example of this might be a developer's workstation. Many developers feel they have unique requirements in order to do their job, and as a result, they may run custom configurations, unsupported operating systems, and/or open source applications, and they may not participate in the corporate patch and configuration management programs. Since these computers will have to be connected to an organization's network to access internal resources, and these workstations may give you additional security challenges, server and domain isolation gives you some additional security options.

> **TAKE NOTE***
> If you want to leverage isolation in your environment, be sure to take the time to plan appropriately. This can be a complex implementation, and you must understand your needs before you start enabling protocols.

Server and domain isolation is a solution based on IPsec and Microsoft Active Directory that enables administrators to dynamically segment their Windows environment into more secure and isolated logical networks. These logical networks are segmented based on policy and can be accomplished without needing to deploy firewalls, implement VLANs, or make other changes on the network. Internal servers and domains can be secured through the use of authentication and encryption. This creates an additional layer of policy-driven protection, and it provides another alternative to the security controls previously discussed in this lesson.

Server and domain isolation should not be confused with Network Access Protection (NAP). NAP focuses on ensuring that the clients that attach to the network are configured appropriately and authorized. In comparison, server and domain isolation creates logical security zones within the network and controls who can access them. Both are viable security solutions, but they have very different goals and use very different technologies to secure the environment. In a high-security setting, you may want to deploy both technologies to ensure the protection of your network and data.

Figure 4-6 provides an example of server and domain isolation in which the isolated network can only be accessed by computers with the appropriate IPsec and Active Directory configuration.

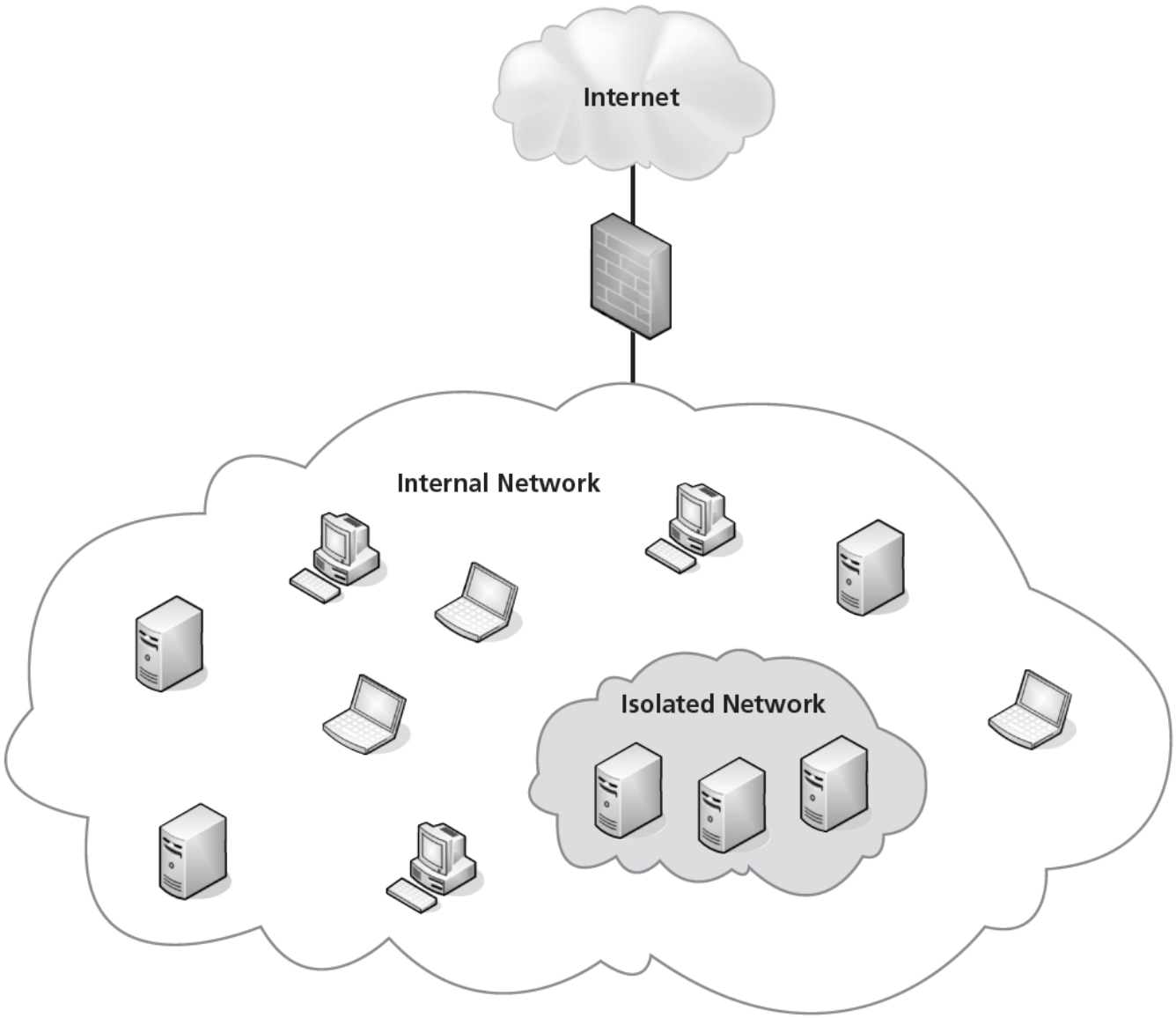

Figure 4-6 Server and domain isolation How does the isolation process work? In short, authentication to the isolated environment is based on a computer's machine credentials. The machine credentials can be an Active Directory-issued Kerberos ticket, or it can be an X.509 certificate automatically distributed to the computer by a Group Policy. Once the machine has authenticated, the associated isolation policies are enforced by the built-in IPsec functionality in Windows.

Here, it's important to recall that IPsec supports two modes. Tunnel mode is the most frequently used mode, because it supports the widely used remote access and site-to-site VPN solutions that are becoming ubiquitous in the corporate world. Transport mode is used for server and domain isolation because it is the mode that supports secure host-to-host communications.

Protecting Data with Protocol Security

THE BOTTOM LINE

In this lesson, we have discussed a number of security protocols, such as IPsec, SSL/TLS, and SSH. In this section, we are going to look at several additional protocols that can be used to secure your data. This includes an examination of protocol spoofing, network sniffing, and some other common attack methods you might encounter when working to secure a corporate computing environment.

One of the more challenging topics for any information security professional to tackle is the idea of protocol security. This has long been the area of networking professionals, and although there is an obvious overlap between networking and information security, understanding protocol security can be a real challenge for information security professionals both new and old. In order to develop an appreciation of exactly how network protocols can impact security, we need to start our discussion with a look at tunneling.

CERTIFICATION READY

What protocol can be used to protect confidential data that is sent between servers?
3.4

Understanding Tunneling

Tunneling is defined as the encapsulation of one network protocol within another. Tunneling can be used to route an unsupported protocol across a network, or to securely route traffic across an insecure network. VPNs employ a form of tunneling when data is encapsulated in the IPsec protocol.

One example of tunneling that is used to move unsupported traffic across a network is the Generic Routing Encapsulation (GRE) protocol. GRE is an IP-based protocol frequently used to carry packets from unroutable IP addresses across an IP network.

In order to understand why the GRE protocol is used, we need to discuss IPv4 addressing. One component of the IPv4 addressing scheme is a set of addresses known as either private or reserved address ranges. These ranges include 10.0.0.0 through 10.255.255.255, 172.16.0.0 through 176.31.255.255, and 192.168.0.0 through 192.168.255.255. These ranges were assigned to help delay the exhaustion of all available IPv4 IP addresses, and they are typically used for both home and office networks where there is not a requirement for the addresses to be routed across a public network like the Internet. These networks generally use NAT to permit Internet access.

Another area where these addresses are used is for lab/development networks in an enterprise environment. Sometimes there is a requirement to route traffic from one lab/development network to another, but because these networks use private addresses, they may not be routable across the enterprise network. This is when GRE becomes useful. Traffic between the labs can be encapsulated in a GRE tunnel, which can be routed over the enterprise network without requiring readdressing.

PPTP (Point-to-Point Tunneling Protocol) is a proprietary VPN protocol originally developed by the PPTP Forum, a group of vendors that included Ascend Communications, Microsoft Corporation, 3Com, ECI Telematics, and U.S. Robotics. PPTP was designed as an extension of the Point-to-Point Protocol (PPP) to allow PPP to be tunneled through an IP network.

TAKE NOTE*

What is PPP? PPP, the Point-to-Point Protocol, was a protocol defined in the late 1990s that provided a standard transport mechanism for point-to-point data connections.

> This protocol was mainly used in conjunction with modem connections and has largely been phased out as modem connections have been replaced by high-speed Internet connections.

At one time, PPTP was the most widely used VPN protocol, but the release of IPSec had a significant effect on PPTP's use.

Another tunneling protocol that was once widely used is L2TP (Layer 2 Tunneling Protocol), which combined the best features of PPTP and the L2F (Layer Two Forwarding) protocol, which was an early competing protocol for PPTP developed by Cisco Systems. Like PPTP, L2TP was designed as an extension of PPP to allow PPP to be tunneled through an IP network. L2TP support was first included in a Microsoft server product with the release of Windows Server 2000. Prior to Windows Server 2000, PPTP was the only supported protocol. A number of hardware VPN vendors, including Cisco, also supported the L2TP protocol.

Using DNS Security Extensions (DNSSEC)

If you have ever connected to a website by name, you have used the Domain Name System (DNS). DNS is a service used on the Internet for resolving fully qualified domain names (FQDN) to their actual Internet Protocol (IP) addresses using a distributed network of name servers. Here, you enter a server name (such as **www.espn.com),** and DNS ensures your connection is directed to the proper servers. Although this service is largely invisible to end users, DNS is a critical element of how the Internet functions.

Let's say you want to check the scores from your favorite sport using ESPN's website. Before DNS, when you asked, "What's the address of ESPN's website?" the answer might be 199.181.132.250. If you are like most people, you'd remember that number for less than 30 seconds, so you would probably never find those sports scores. In contrast, with DNS, you can simply tell your computer to go to **www.espn.com,** and the DNS infrastructure of the Internet will translate this name to the correct address. In other words, DNA is much like a phone book: You put in a name, and it gives you the correct number.

However, DNS was developed during the early years of the Internet, when functionality was the goal, not security. As a result, DNS was built without security. In recent years, this lack of security has been exploited with forged DNS data, which, among other things, redirects connections to malicious websites. Say you type in the address of your bank, and shortly thereafter, it appears you have reached your destination. You enter your user ID and password to access your account, but you can't log in. Now, say that one month later, you find out your account has been emptied. What happened was that your initial connection was the result of a bad DNS entry. Instead of connecting to your bank's website, you connected to a clever duplicate that captured your login information and let the bad guys steal your savings.

Thankfully, ***DNS Security Extensions (DNSSEC)*** adds security provisions to DNS so that computers can verify they have been directed to proper servers. This new standard was published in March 2005 and is slowly being adopted across the Internet. DNSSEC provides authentication and integrity checking on DNS lookups, ensuring that outgoing Internet traffic is always sent to the correct server. This removes the issue of forged DNS data because there is no way to forge the appropriate authentication. This not only addresses the problem of website redirection, but it also reduces some of the challenges associated with spam and use of faked mail domains.

DNSSEC provides authentication and integrity checking through the use of public key encryption. The domain name structure provides a hierarchy of authenticated keys, creating a chain of trust from the root of the DNS hierarchy to the domain being queried. DNSSEC addresses many of the most problematic security issues associated with the Internet's core infrastructure, but it comes at a significant cost. As with any large-scale public key implementation,

rolling DNSSEC out to the entire Internet will be an enormously complex, resource-intensive project. There are also challenges associated with maintaining the web of trust created by using public keys on a scale this large.

Looking at Protocol Spoofing

Another area of concern with respect to protocols is the concept of protocol ***spoofing***. The word “spoof” can be used to refer to a hoax. Accordingly, protocol spoofing is the misuse of a network protocol to perpetrate a hoax on a host or a network device. Some common forms of protocol spoofing are as follows:

- **ARP spoofing:** ARP (Address Resolution Protocol) spoofing (also called ARP poisoning) is an attack on the protocol used to determine a device’s hardware address (MAC address) on the network when you have its IP address. This is critical for proper delivery of network data once the data has reached the proper LAN segment. An ARP spoofing attack occurs when an attacker modifies the network’s ARP caches and takes over the IP address of the victim host. This permits the attacker to receive any data intended for the original host.
- ***DNS spoofing:*** DNS spoofing occurs when an attacker is able to intercept a DNS request and respond to the request before the DNS server is able to. As a result, the victim host is directed to the wrong website, where additional malicious activities can take place. This attack is frequently used in conjunction with network sniffing, which is discussed in the next section.
- **IP address spoofing:** In an IP address spoofing attack, the attacker creates IP packets with a forged source IP address to either conceal the identity of the attacking host or impersonate the identity of a victim host. This type of attack was very popular in the early days of packet analysis firewalls. Here an attacker would spoof an internal IP address from outside a firewall, and if not configured correctly, the firewall would permit the attacker access to the internal network.

It is important to note that the term “protocol spoofing” also has another definition within the computing arena. In particular, the term is sometimes used to represent a technique associated with data compression and employed to improve network throughput and performance. Although a valuable tool in the appropriate circumstances, this form of protocol spoofing does not have any information security implications.

Utilizing Network Sniffing

Network sniffing is a type of network analysis that is useful for administrators responsible for maintaining networks and identifying network issues. It involves connecting a device to a network with the appropriate software to allow access to the details of the packets that are traversing the network. Figure 4-7 shows an example of Wireshark, a commonly used open source network sniffing tool.

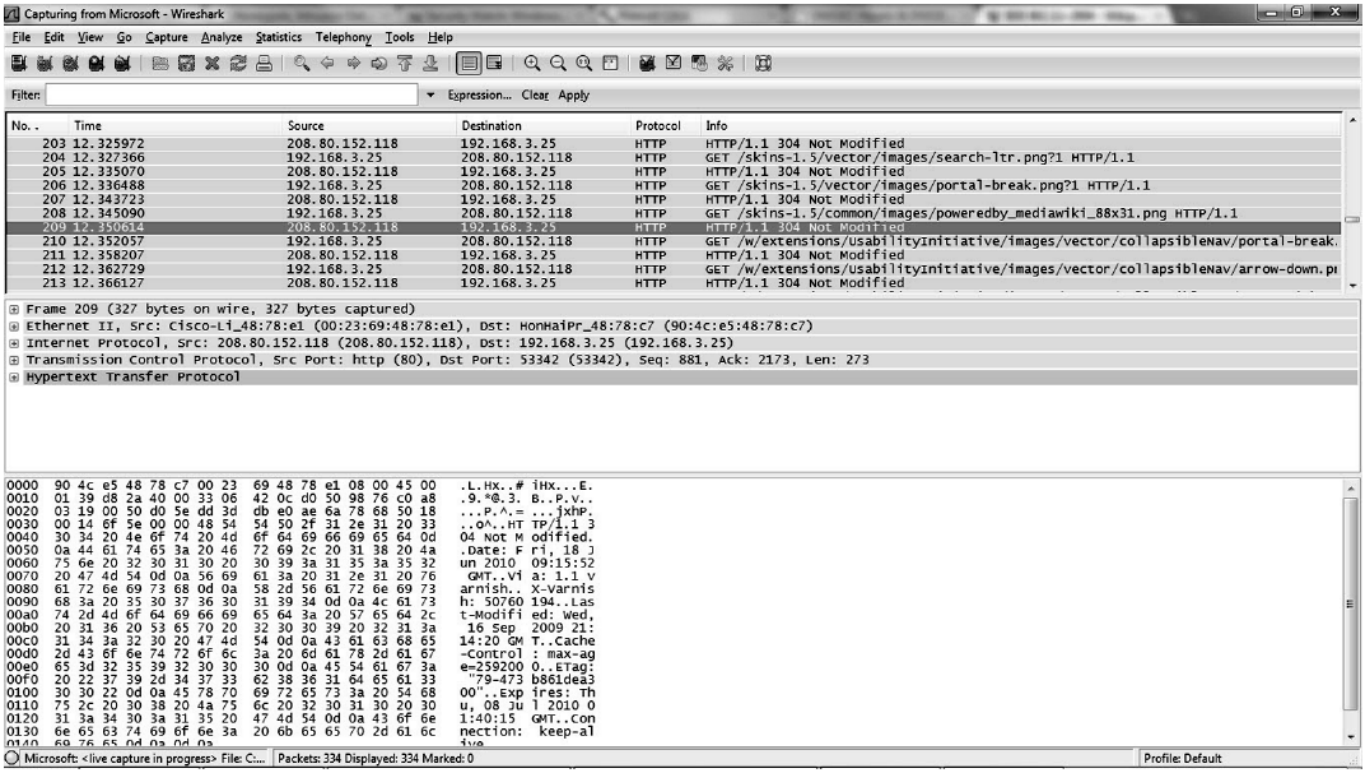

Figure 4-7 Wireshark

As you can see in the figure, this tool reveals a significant amount of information about the packet being analyzed. To a network administrator with an in-depth understanding of networking, this information can be used to identify application issues, network latency, and a variety of other network errors. Unfortunately, to an attacker with similar skills, the information offered by network sniffing provides equally valuable data that can be used for attack purposes. For example, any data sent in clear text (i.e., not encrypted) can generally be read directly from the network. In the early days of the Internet, this was a significant amount of traffic. Back then, reading passwords from data packets was a trivial exercise. Today, however, with the widespread use of encryption through secure websites and the use of VPNs for remote access, the risks presented by network sniffing are slightly mitigated because attackers can no longer read the data contents of a packet. Nonetheless, attackers can still obtain important information about data packets that can be useful in attacks.

It is important to be aware that a network sniffer can only see traffic that crosses the port that it is connected to. Therefore, a sniffer placed on the LAN in a branch office cannot capture traffic from the headquarters network. And, in a switched environment that leverages VLANs, the amount of traffic passing any one port can be limited. The ports that offer the most information are the ingress/egress points to the network, where all the traffic from the subnet is concentrated. This means an attacker cannot directly capture traffic from your network, but that doesn't mean you're safe. For instance, a system on your internal network that is infected by a virus can end up running a network sniffer and providing the captured traffic to a remote host.

Another security challenge associated with network sniffers is that they are passive devices. Unless an attacker has made modifications to a network to access more information, it is almost impossible to detect a network sniffer. In fact, there could be a network sniffer on a network node beyond your internal network that could be capturing packets about your Internet access. In this circumstance, you don't even have access to the network infrastructure to look for changes.

You also need to be aware that wireless networks are particularly susceptible to network sniffing attacks, due to the lack of a port requirement. Once connected to a wireless network, an attacker has access to all the traffic on that

network. That's why it's an excellent idea to only use encrypted connections for anything you do on a wireless network beyond general web browsing.

Understanding Common NETWORK Attack Methods

We have covered the information security challenges associated with computer networking throughout this lesson. The final piece of the network security puzzle is understanding the types of attacks you can expect to see as you work to protect computer networks. Although no list of attack methods can ever be complete, if only because attackers are constantly coming up with new types of attacks, this list covers the most common categories:

- **Denial of service/distributed denial of service (DoS/DDoS) attacks:** The goal of a denial of service attack is to flood the network that is being attacked with overwhelming amounts of traffic, thereby shutting down network infrastructure like a router or firewall. Because the attacker isn't interested in receiving responses to his or her attack packets, DoS attacks are ideal opportunities for using spoofed addresses. Spoofed addresses are more difficult to filter because each spoofed packet appears to come from a different address, thus hiding the true source of the attack. This makes backtracking the attack extremely difficult. The new wrinkle to the DoS is the distributed DoS, which leverages botnets to generate DoS attacks from multiple sources. Not only does this make the attack more difficult to defend against, as multiple computers can generate significantly more traffic than a single computer, but it also makes it much more difficult to track down the source of the attack.

> **TAKE NOTE***
> A botnet is a distributed network of computers that have been compromised by malicious software and are under the control of an attacker.

- **IP spoofing to bypass network security:** As previously discussed, IP spoofing is the modification of data packets so that data packets from an attacking computer appear to be from a trusted computer. By appearing as a trusted computer, the attacker is able to bypass network security measures, like packet filters or other solutions that rely on IP addresses for authentication. Using this method of attack on a remote system can be extremely difficult, because the attacker must modify thousands of packets in order to successfully complete the attack. This type of attack generally works best when there are trust relationships between machines. For example, it is not uncommon in some environments to have UNIX hosts on a corporate network that trust each other. In such instances, once a user successfully authenticates to one host, he or she is automatically trusted on the other hosts and does not need a user ID or password to get into the system. If an attacker can successfully spoof a connection from a trusted machine, he or she may be able to access the target machine without an authentication. Identifying the trusted machine is frequently accomplished via network sniffing.

- **Man in the middle attacks:** A man in the middle attack is a type of attack in which the attacker breaks into the communication between the endpoints of a network connection. Once the attacker has broken into the communication stream, he or she can intercept the data being transferred or even inject false information into the data stream. These types of attacks are frequently used to intercept both HTTP and HTTPS connections. Systems that are connected to a wireless network are especially susceptible to this form of attack.

- **Back door attack:** Back door attacks are attacks against an opening left in a functional piece of software that allows access into a system or software application without the owner's knowledge. Many times, these back doors were left by the application developers, but current code testing has dramatically reduced the number of back doors found in commercial software. A more common version of this attack occurs when system administrators create system accounts that they can use in the event they are asked to leave a company. Thus, as an information security professional, one of your goals should be to validate all system accounts belonging to employees at least once a year.

- ***DNS poisoning:*** A DNS poisoning attack is an attack against the cached information on your DNS server. When a DNS request is made, the result of the request is cached on the DNS server so that subsequent requests for the same server can be returned more quickly, without requiring lookup by an external DNS server. Unfortunately, these cache files are not particularly secure, and attackers can target these files to insert a bogus IP address for a specific server entry into a cache. When this occurs, any host making a request for that site from the poisoned DNS server will be directed to the wrong site. The bogus entry in the cache will remain until the cache expires and is refreshed.

- **Replay attack:** A replay attack occurs when an attacker is able to capture an intact data stream from a network using a network sniffer, modify certain components of the data stream, and then replay the traffic back to the network to complete the attack. For example, an attacker could capture a session in which a purchase is being made, modify the delivery address, and replay the traffic to place an order that would be delivered to his or her address.

- **Weak encryption keys:** An attack against weak encryption keys successfully occurs when the keys have a value that permits encryption to be broken. Once this happens, the attacker is able to access the data that is supposed to be encrypted. Probably the most high-profile example of this attack was the weakness exploited in the Wired Equivalent Privacy (WEP) security standard used in conjunction with wireless networks. Intended to be used to secure wireless networks, WEP keys were found to be weak, and they could be broken if 5 to 10 MB of wireless traffic could be captured. This traffic could then be run through one of many tools published by the hacker community, and the result would be the WEP key, which permits an attacker to read the information protected with WEP. This is another example of an attack that relies on a network sniffer to be successful.

- **Social engineering:** Social engineering attacks occur when an attacker contacts an employee of an organization and tries to extract useful information from that person. This information may later be used to help pull off a different attack. With social engineering, the attacker usually tries to appear as harmless or respectful as possible. Generally, he or she will ask a number of questions in an attempt to identify possible avenues to exploit during an attack. If an attacker does not receive sufficient information from one employee, he or she may reach out to several others until he or she has sufficient information for the next phase of an attack.

- **Software vulnerability attack:** This category of attack exploits a known or unknown vulnerability in an operating system or application to perform malicious activities. This is probably one of the most common avenues for attack, and it is used frequently by viruses and worms. A solid patch management practice is the best defense against this type of attack, especially if coupled with a vulnerability management program.

- **Buffer overflow attack:** A buffer overflow attack exploits poorly written code by injecting data into variable fields and leveraging the response to access information in the application. This attack is made possible when the application developer doesn't limit or check the size of the data being entered in an application field. When data that is too long for the field is entered, it creates an error that can be exploited by the attacker to perform malicious actions against the application.

- **Remote code execution attack:** Remote code execution attacks are commonly run against web applications. When an application is improperly coded, an attacker is able to run arbitrary, system-level code through the application and use the results to access data or perform other unintended actions against the application or application server.

- **SQL injection attack:** SQL injection attacks are one of the oldest attacks against web applications using the SQL Server database application. In this type of attack, control characters are entered into the web application, and depending on the configuration of the database server, the attack results can range from retrieval of information from the web server's database to allowing the execution of code or even full access to the server. This attack relies on database weaknesses as well as coding weaknesses.

- **Cross-site scripting attack (sometimes abbreviated as an XSS attack):** Cross-site scripting attacks are by far the most common and potentially the most dangerous current attack method employed against web users. These attacks allow hackers to bypass the security mechanisms provided by a web browser. By injecting malicious scripts into web pages and getting users to execute them, an attacker can gain elevated access privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser.

Other attack methods include the password cracking, dictionary attack and brute force attacks, which were covered in Lesson 3.

The final component of network security you must be familiar with is wireless security.

Securing Wireless Networks

THE BOTTOM LINE

Wireless LANs have become one of the most popular forms of network access, rapidly spreading through homes, to business, to public access wireless hotspots like the ones you find in a Starbucks or McDonald's. Wireless networks offer a great deal of convenience, but this convenience must be balanced against the security implications of a network that is not contained by the walls of your building. In this section, we discuss those implications and describe some of the techniques you can use to secure a wireless network, including encryption keys, SSID, and MAC address filters.

A wireless LAN (WLAN) allows users to connect to a network while remaining mobile. Although this gives users easy access to a network from areas like conference rooms, offices, lunch rooms, and other areas where wired connections don't exist, it also gives potential attackers similarly easy access to the network. Many corporate wireless networks can actually be accessed by anyone with a laptop and wireless card. If you have ever used a wireless connection in a neighborhood, you may have noticed that your computer sees wireless networks other than the one you are connecting to. Businesses have the same issues as your neighbors: They are broadcasting their network to anyone within range. In fact, with specialized antennas, wireless networks can be accessed from surprisingly long distances, and if you're not careful, that access may occur without your knowledge.

CERTIFICATION READY

What methods can you use to secure a wireless network?
1.4

In the early days of wireless networks, implementing this technology was easy, but securing it was not. As a result, there were battles between users who wanted the ease of access and increased mobility that wireless promised and security personnel who were acutely aware of the risks that wireless networking introduced. As a result, most corporations had strict policies prohibiting the use of wireless to directly access internal networks, frequently requiring users to use VPNs to connect from the production wireless network to the internal network. As a result, some users would install wireless access points under their desks and hope that no one from security would notice. Attackers would then drive around office parks looking for these unsecured access points so that they could breach the perimeters of corporate networks and attack unprotected internal networks. Corporate security organizations would also perform similar exercises in the hopes of finding rogue wireless connections before attackers did. Today, however, with some of the new security capabilities available with wireless networks, it is now possible to securely offer wireless access to internal networks, reducing both the frequency of rogue access points, as well as the number of resources needed to find and shut down those access points.

Another capability sometimes discussed when deploying wireless networks is ensuring the wireless access point radio strength is tuned appropriately. Although there is some ability to tune a wireless signal to reduce the risk of unauthorized users, it is not a good idea to rely on this method as your first line of defense when trying to keep your network secure. Frequently, what you will find is that you negatively impact usability far more than you improve security.

Using Service Set Identifier (SSID)

The most basic component of a wireless network is the Service Set Identifier (SSID). An SSID is defined in the IEE 802.11 standard as a name for the WLAN. It does not provide any inherent security capabilities, although specifying the SSID of the WLAN you want to connect to will ensure that you connect to the correct WLAN.

Although there aren't any specific security capabilities associated with an SSID, there are definitely some security considerations you should take into account:

- **Choose your own SSID:** The first thing you need to do when setting up a WLAN is to choose a unique SSID. Each WLAN access point comes with a default SSID set. If you use the default, there is a risk that one of your neighbors will also use the default, causing confusion and conflicts. Therefore, be sure to select your own unique yet easy to remember SSID.
- **Naming conventions:** Now that you have chosen an SSID, there are some measures you can take to make it a little more challenging for an attacker to identify the owner of your WLAN. It is generally not a good idea for corporations to broadcast the fact that they are the owner of a particular wireless network. Selecting SSIDs based on company name, company product lines, or anything else that might allow an attacker to confirm who owns the WLAN should thus be avoided. Instead, select an SSID that your employees can remember but that doesn't invite attacks. Things like city names, sports, mythological characters, or other generic SSID names are generally safe choices.
- **Turn off your SSID:** Your SSID is used to identify your WLAN and permit computers to connect to it. If you broadcast this information, then client systems can search for available wireless networks, and the name of your WLAN will appear in the list. With just a few clicks, you can connect to the WLAN. Although extremely convenient for authorized users, broadcasting an SSID makes it equally easy for attackers to connect in the same way. To prevent this from happening, you can turn off the SSID broadcast for your network, rendering it essentially invisible to casual wireless network browsers. The problem with doing this is twofold, however. First, it makes it more difficult for authorized users to connect to the network, and second, any attacker who is trying to get in through your wireless network will most likely have a wireless sniffer, which will show him or her the SSID of your WLAN whether it's broadcast or not, because this information is in the wireless packets. In this case, it's generally wise to select ease of use over hiding your SSID (i.e., security through obscurity).

Now, let's look at some techniques for securing a WLAN.

Understanding Keys

The best available mechanism for securing a WLAN is to use authentication and encryption. WLANs offer three key-based security mechanisms for this purpose.

EXAMINING WIRED EQUIVALENCY PRIVACY (WEP)

The very first security capability available to WLAN users was WEP (Wired Equivalency Privacy). WEP was included as part of the original IEEE 802.11 standard and intended to provide privacy. Widely recommended in the early days of WLAN use, WEP rapidly fell out of favor when a flaw with the encryption mechanism was discovered. This flaw makes it relatively easy for an attacker to crack the encryption and access the wireless network, so WEP is generally only used if no other solution is available or if the WLAN is being used with older devices or devices (like PDAs or handheld games) that require WEP.

One of the other challenges associated with WEP was the confusing mix of keys used by vendors. Some vendors implemented the keys in HEX, some used ASCII characters, and some just used passphrases. Depending on the version of WEP, the length of the keys could also vary. This was particularly problematic for home users who wanted to use equipment from multiple vendors. Consumers often ended up with equipment that wouldn't support WEP in the same way.

EXAMINING WI-FI PROTECTED ACCESS (WPA) AND WI-FI PROTECTED ACCESS VERSION 2 (WPA2)

Wi-Fi Protected Access (WPA) was designed as the interim successor to WEP. The WPA protocol implements the majority of the IEEE 802.11i standard, which was included in the updated WLAN standard. WPA features a new security protocol, Temporal Key Integrity Protocol (TKIP), which although related to WEP to ensure backwards compatibility, adds new features to help address the issues associated with WEP. Unfortunately, because TKIP uses the same underlying mechanism as WEP, it is also vulnerable to a number of similar attacks—although the possibility of attack is significantly less than with WEP.

Wi-Fi Protected Access Version 2 (WPA2) is the standards-based version of WPA, except WPA2 implements all of the IEEE 802.11i standards.

WPA/WPA2 functions in two modes:

- **Shared-key WPA:** In shared-key WPA, a passphrase is configured and entered on both the client and the wireless network. This is similar to how WEP works, but the protection of the WPA passphrase is much more secure due to the use of strong encryption with automatic rekeying. This mode is generally meant for home users.
- **IEEE 802.1x:** In 802.1x mode, WPA/WPA2 uses an external authentication server coupled with the EAP (Extensible Authentication Protocol) standard to enable strong authentication for connection to the WLAN. A typical authentication process includes the following steps:
  1. **Initialization:** Upon detection of a host, the port on the switch is enabled and set to the "unauthorized" state. Only 802.1x traffic is allowed while the port is in this state.
  2. **Initiation:** The host that is trying to connect to the WLAN next transmits EAP-Request Identity frames to a special layer 2 address on the local network segment. This is known

as the authenticator. The authenticator then forwards the packets to a RADIUS authentication server.

3. **Negotiation:** The authentication server sends a reply to the authenticator. The authenticator then transmits the packets to the connecting host. These packets are used to negotiate the EAP authentication method.

4. **Authentication:** If the authentication server and connecting host agree on the EAP authentication method, then the connecting host is authenticated. If authentication is successful, the authenticator sets the port to the “authorized” state and normal traffic is allowed. If it is unsuccessful, the port remains in the “unauthorized” state and the host is not able to connect.

Use of 802.1x authentication to secure a WLAN is generally reserved for large corporate environments where there are sufficient resources to support the additional servers and support required by this mode of operation. IEEE 802.1x authentication, particularly when used in conjunction with a token-based authentication solution, permits a very secure WLAN implementation.

Utilizing MAC Filters

As discussed earlier in this lesson, a MAC address is the unique hardware address of a network adapter. This information can be used to control what systems are able to connect to a WLAN through the use of MAC filters. By turning MAC filtering on, you can limit network access to only permitted systems by entering the MAC address information into the MAC filters. The table of permitted MAC addresses is maintained by the wireless access points.

Considering Pros and Cons of Specific Security Types

Now that we have discussed the different security mechanisms available when working with WLANs, let’s consider some of the advantages and disadvantages of each:

- **WEP:** WEP is a solution that, although better than no security at all, is not particularly secure. The vulnerabilities within the WEP encryption scheme make it very easy to crack. WEP will keep your neighbors from connecting to your home WLAN, but it will not slow a determined attacker.

- **WPA/WPA2:** WPA/WPA2 is the best security method for both home and corporate WLAN security. In pre-shared key mode, WPA/WPA2 can secure a WLAN with a passcode that is shared by the clients and wireless access points. As long as a secure passcode is selected, this is a very secure solution for small networks. For corporate networks, where additional authentication infrastructure can be purchased, the 802.1x security available within WPA/WPA2 permits a more secure WLAN implementation. The downside to this approach is that it is more expensive and significantly more complex that the other solution. This method also requires significantly higher support because user accounts need to be maintained,

additional servers need to be supported, and troubleshooting is more challenging. Nonetheless, these challenges can be overcome with a well designed, redundant architecture for the WLAN.

- **MAC address filtering:** MAC address filtering is a good solution for a home or small office environment, but it has significant challenges as the number of permitted devices grows. Manually maintaining a table of MAC addresses becomes a significant challenge when you get above 10 to 20 devices, especially in dynamic environments where systems are being purchased and decommissioned regularly. Any changes to the list of permitted devices requires updating the MAC address filtering table, which is generally a manual process. Another issue with MAC address filtering is that MAC addresses can be “spoofed” by someone with sufficient knowledge or the ability to perform an Internet search for a tool to change a MAC address. If hackers are able to get the MAC address of an authorized system, they can reset their MAC address to that address and thus gain access to a WLAN. MAC address filters are a good solution for small, static environments like a home or a small office. Although they will not stop a determined attacker, they are one more impediment to ensure that only a truly motivated attacker will attempt to bypass them.

The good news when reviewing available security mechanisms for wireless networks is that there are solutions available for just about any situation. In the early days of wireless, WLANs offered great convenience for users but no security for protecting a company’s network. Deploying wireless access was as easy as buying an inexpensive wireless access point and plugging it into the network. As a result, security departments were forced to dedicate resources to tracking down rogue wireless access points. Fortunately, there are now multiple tools that you can use to identify rogue access points. So, while the issue certainly still exists, it is not as prevalent as it was in years past.

SKILL SUMMARY

IN THIS LESSON YOU LEARNED:

- A firewall is a system that is designed to protect a computer or a computer network from network-based attacks. A firewall does this by filtering the data packets that are traversing the network.
- Firewalls that are based on packet filtering inspect data packets as they attempt to traverse the firewall. Based on rudimentary rules, these firewalls permit all outbound traffic while denying all inbound traffic or blocking specific protocols, like telnet or ftp, from passing through the router.
- Instead of analyzing each individual packet, a circuit-level firewall monitors TCP/IP sessions by monitoring the TCP handshaking between packets to validate a session.

- Application-level firewalls (also known as proxy servers) work by performing a deep inspection of application data as it traverses the firewall. Rules are set by analyzing client requests and application responses, and correct application behavior is then enforced.

- Stateful multilevel firewalls are designed to provide the best features of both packet filtering and application-level firewalls.

- Network Access Protection (NAP) gives administrators a more powerful way to control access to network resources. NAP controls are based on a client computer's identity and whether the computer complies with the configured network governance policies.

- Virtual LANs (VLANs) were developed as an alternate solution to deploying multiple routers. VLANs are logical network segments used to create separate broadcast domains while still allowing the devices on the VLANs to communicate at layer 2 without a router.

- An intrusion detection system (IDS) is a solution designed to detect unauthorized user activities, attacks, and network compromises.

- An intrusion prevention system (IPS) is similar to an IDS, except that in addition to detecting and alerting, an IPS can also take action to prevent a breach from occurring.

- Honeypots, honey nets, and padded cells are complementary technologies to IDS/IPS deployments. A honeypot is a trap for hackers.

- A DMZ is a firewall configuration used to secure hosts on a network segment. In most DMZs, the hosts on the DMZ are connected behind a firewall that is connected to a public network like the Internet.

- Network Address Translation (NAT) is a technique used to modify the network address information of a host while traffic is traversing a router or firewall. This technique hides the network information of a private network while allowing traffic to be transferred across a public network like the Internet.

- DNS Security Extensions (DNSSEC) adds security provisions to DNS so that computers can verify that they have been directed to the proper servers.

- Protocol spoofing is the misuse of a network protocol to perpetrate a hoax on a host or a network device.
- A denial of service (DoS) attack floods the target network with overwhelming amounts of traffic, shutting down network infrastructure like routers or firewalls.
- A man in the middle attack occurs when an attacker breaks into the communication between the endpoints of a network connection. Once the attacker has broken into the communication stream, he or she can intercept the data being transferred or even inject false information into the data stream.
- Back door attacks are attacks against an opening left in a functional piece of software that allows access into a system or software application without the owner's knowledge.
- A DNS poisoning attack is an attack against the cached information on a DNS server.
- A replay attack occurs when an attacker is able to capture an intact data stream from a network using a network sniffer, modify certain components of the data stream, and then replay the traffic back to the network to complete the attack.
- A buffer overflow attack exploits poorly written code by injecting data into variable fields and leveraging the response to access information in the application.
- SQL injection attacks are one of the oldest types of attacks against web applications using the SQL Server database application.
- A wireless LAN (WLAN) allows users to connect to a network while mobile.
- The Service Set Identifier (SSID) is the name for a WLAN. A connecting host must know a WLAN's SSID to connect.
- Wired Equivalency Privacy (WEP) is an older wireless encryption protocol that rapidly fell out of favor when a flaw with its encryption mechanism was found.
- Wi-Fi Protected Access (WPA) was designed as the interim successor to WEP.
- Wi-Fi Protected Access Version 2 (WPA2) is the standards-based version of WPA.

Unlike WPA, WPA2 implements all of the IEEE 802.11i standards.

- A MAC address is the unique hardware address of a network adapter.
- By turning MAC filtering on, you can limit network access to only permitted systems by entering the MAC address information into the MAC filters.

Knowledge Assessment

Multiple Choice

Circle the letter or letters that correspond to the best answer or answers.

1. Which of the following elements and issues should be considered when deciding whether to use a software or hardware firewall? (Choose all that apply.)

a. Host operating system

b. Application conflicts

c. Operating system version

d. Firewall service efficiency

e. Stability

2. Which of the following are layers of the OSI model? (Choose all that apply.)

a. Physical

b. Control

c. Application

d. Network

e. Encryption

3. At which layer of the OSI model does routing occur?

a. Physical

b. Data link

c. Transport

d. Session

e. Network

4. Which of the following are valid firewall types? (Choose the best answer.)

a. Virtual

b. Network

c. Packet filtering

d. IPsec

e. Application

5. Which of the following pieces of information are typically examined by a stateful inspection firewall?

a. IP address of the sending host

b. IP address of the receiving host

c. IP address of the router

d. Data packet type

e. Data packet size

6. What is the purpose of NAP? (Choose the best answer.)

a. NAP translates private IP addresses to Internet-routable IP addresses.

b. NAP permits a firewall to perform deep inspection on packets.

c. NAP provides a mechanism to perform network analysis on captured packets.

d. NAP controls what systems are permitted to connect to a network.

7. An attack that relies on having a user execute a malicious script embedded in a web page is which kind of attack? (Choose the best answer.)

a. Man in the middle

b. Brute force

c. Cross-site scripting

d. SQL injection

8. You have just purchased a new wireless access point for your small computer services company, and you want to ensure that only your systems are able to connect to the wireless network. To that end, you enable MAC address filtering and put the MAC addresses of all your computers in the permitted table. At what layer of the OSI model does this filtering occur?

a. Physical

b. Data link

c. Network

d. Transport

e. Session

9. You are the Information Security Officer for a medium-sized manufacturing company, and your sales team has just deployed a new e-commerce application to allow for the direct sale of your products to your customers. To secure this application, you are deploying an application firewall. At what layer of the OSI model does this filtering occur? (Select all answers that apply.)

a. Physical

b. Data link

c. Network

d. Presentation

e. Application

10. Which of the following are components of Network Access Protection? (Choose all that apply.)

a. MAC address compliance

b. Health policy compliance

c. Limited access mode

d. IP address mode

e. Health state validation

11. Which of the following are password-based attacks? (Choose all that apply.)

a. Replay attacks

b. Network sniffer attacks

c. Brute force attacks

d. Man in the middle attacks

e. Dictionary attacks

12. What type of attack relies on the attacker tricking the sending host into thinking his or her system is the receiving host, and the receiving host into thinking his or her system is the sending host? (Choose the best answer.)

a. Replay attack

b. Brute force attack

c. Man in the middle attack

d. Cross-site scripting attack

e. SQL injection attack

13. Which of the following systems cannot participate in a NAP implementation? (Choose all that apply.)

a. Windows 7 Home

b. Windows 7 Home Premium

c. Windows XP Service Pack 2

d. Windows Vista Ultimate

e. Windows 7 Professional

14. Which of the following are common uses for a VPN?

a. Remote access

b. Server isolation

c. Intrusion detection

d. Extranet connections

e. Domain isolation

15. Which of the following are common types of routing protocols? (Choose all that apply.)

a. Link vector

b. Dynamic link

c. Distance link

d. Distance vector

e. Link state

Fill in the Blank

1. You are a network administrator, and you have just been put in charge of registering your company's domain name and setting up the DNS so that people on the Internet can get to your website. Here, _____ can be used to ensure that your DNS entries are not poisoned by an attacker.

2. The two most common protocols you can use to create a VPN are _____ and _____.

3. The three common types of protocol spoofing are _____, _____, and _____.

4. The type of attack that relies on a weakness in an operating system or an application is known as a(n) _____.

5. An attack that relies on access to a physical LAN segment is known as a(n) _____ attack.

6. An attack that records a stream of data, modifies it, and then resends it is known as a(n) _____ attack.

7. The two common types of Network Address Translation are _____ and _____.

8. If you are setting up a WLAN in a corporate environment and you want to use 802.1x and a RADIUS server to secure the connections, you need to use _____ keys.

9. The four mechanisms used by NAP to restrict network access and enforce policies are _____, _____, _____, and _____.

10. A(n) _____ can be deployed to distract an attacker from the critical systems on your network.

Competency Assessment

Scenario 4-1: Using Windows Firewall

You work for the ABC Corporation. You need to tell a user how to open the Windows Firewall console on a computer running Windows 7 and create a Windows Firewall inbound rule that allows Internet Explorer to communicate over ports 80 and 443. What steps must this user follow?

Scenario 4-2: Looking at a Routing Table

You work for the Contoso Corporation, where you have a computer running Windows 7. Execute the commands necessary to display the current routes. Now, add a route to the 10.24.57.0 network using the 192.168.50.1 gateway, and display the routes to confirm it has been added. Finally, delete the new route.

Proficiency Assessment

Scenario 4-3: Sniffing Packets

You've decided that you want to develop a better understanding of packets and how they operate. Therefore, you choose to use a protocol sniffer provided by Microsoft called Network Monitor to analyze these packets. When you look at the packets, you want to identify the four main parts that make up most of them. What steps would you take to do this?

Scenario 4-4: Looking at Ports

You are talking with the CIO of your company. One of the programs she needs access to is on a server that is on the DMZ using the following protocols:

Secure Shell (SSH) Network News Transfer Protocol Simple Network Management Protocol NetBIOS Session Service Network Time Protocol

The CIO wants to know what a port is and what ports are involved with these protocols. What should you tell her?

Workplace Ready

Defense in Depth

Recall from Lesson 1 that the concept of defense in depth involves providing multiple layers of security to defend your assets. This ensures that if an attacker breaches one layer of your defenses, you still have additional layers to keep him or her out of the critical areas of your environment. To use access control, you must establish physical security that prevents individuals from getting direct access to your servers without going through the network. You should also have firewalls and routers that limit access over the network. You can then use host firewalls, User Account Control, and other components to protect the server itself.

Besides looking at access control, keep in mind the need for authentication, authorization, and accounting. To protect network resources, you still need to establish a system that allows access based on authentication and

authorization. And to ensure that a security breach has not occurred, you must also have established accounting measures that are reviewed regularly.