Lesson Proper for Week 13

VPN CONCEPTS

Understanding VPN Concepts

A virtual private network (VPN) provides a way for two computers or computer networks to communicate securely by using the same public communication channels available on the Internet, where millions of computers and networks exchange data.

The Internet is the most common network used for VPNs, but you can create a VPN on any network, large or small.

To understand what VPNs are, consider how regular mail works. Because you want your letter kept private, you place it in a sealed envelope (encapsulation). If you are concerned about the possibility of your letter being intercepted and read by someone else, you could write it in code (encryption), but you would need a way to let the receiver decrypt it, which could be considered a “key exchange.”

You need to tell the mail carrier where to deliver the envelope and who should receive it, so you include a name and address (the destination address information). In case your envelope cannot be delivered, you put a return address on it (the source address) so that the mail carrier can bring it back to you. As on the public Internet, your message can take several paths to its destination. This is the “virtual” part of a VPN.

Finally, the mail is processed through many different sorting centers, air and ground transportation systems, and post offices in the postal service “network,” just as the Internet is a con- glomeration of private LANs, public transmission lines, and other systems that form a giant mesh network.

Specified computers, users, or network gateways are identified as endpoints of the VPN connection, which is called a tunnel; only those designated computers, users, or gateways can participate in the VPN (see Figure 11-1). A VPN is a network because it connects computers and extends an organization's network beyond its current boundaries. A VPN, then, is a virtual network that uses the Internet to establish a secure connection. VPNs enable computers to exchange private encrypted messages that others cannot decipher

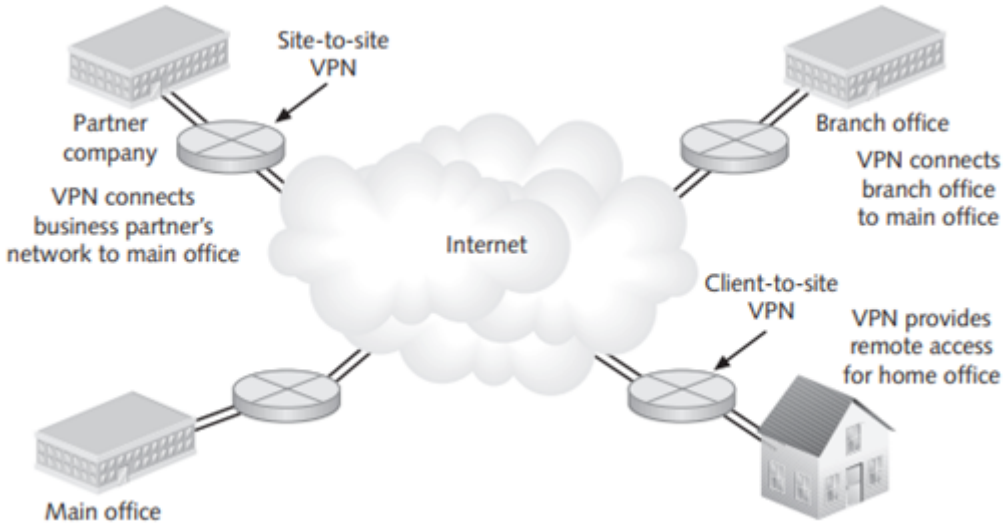

Figure 11-1 Establishing connections with a VPN

VPN endpoints represent extensions of participating networks. If these endpoints are not secured by a firewall, they could give intruders a way to access the network. Unless your VPN client software incorporates its own firewall, you need to make sure any remote computers that connect to your organization's VPN are equipped with desktop firewalls.

VPN Components

VPNs can be assembled using a variety of components. However, all VPNs contain some essential elements that enable data to be transmitted securely from one point to another:

- VPN server or host—A VPN server is configured to accept connections from clients who connect via dial-up or broadband.
- VPN client or guest—A VPN client can be a router that serves as the endpoint of a site-to-site VPN connection, which uses hardware to connect two networks. It can also be an operating system (OS) configured to function as an endpoint in a VPN.
- Tunnel—The connection through which data is sent.
- VPN protocols—VPN protocols are groups of standardized communication settings that software and hardware use to encrypt data sent along the VPN. They include Internet Protocol Security (IPsec), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and Secure Sockets Tunneling Protocol (SSTP).

The number of components in a VPN depends on the number of networks in its configuration. For instance, if a VPN contains four networks, it has at least four separate servers and four tunnels; clients from each endpoint can participate in any of the VPN tunnels they have permission and credentials to access.

In general, you can set up two different types of VPNs. The first type links two or more net- works and is called a site-to-site VPN (or a gateway-to-gateway VPN). The second type makes a network accessible to users who need remote access, and is called a client-to-site VPN (or a remote access VPN).

Some companies that maintain VPNs with partner organizations benefit by using the same ISP as their partners for an Internet connection. Positioning participants in the VPN on the same part of the Internet backbone can make the VPN run more smoothly and reliably.

Types of VPNs

Hardware VPNs

The components you choose to establish a VPN depend on whether you want to use existing hardware or software. Creating a VPN with new components increases costs but has the benefit of reducing the load on other network security components, such as firewalls.

Hardware-based VPNs connect one gateway to another to create a gateway-to-gateway VPN. Typically, the VPN hardware is a router at each network gateway that encrypts outbound packets and decrypts inbound packets. Another hardware option involves a VPN appliance, a hardware device designed to serve as the VPN endpoint and join LANs (see Figure 11-2).

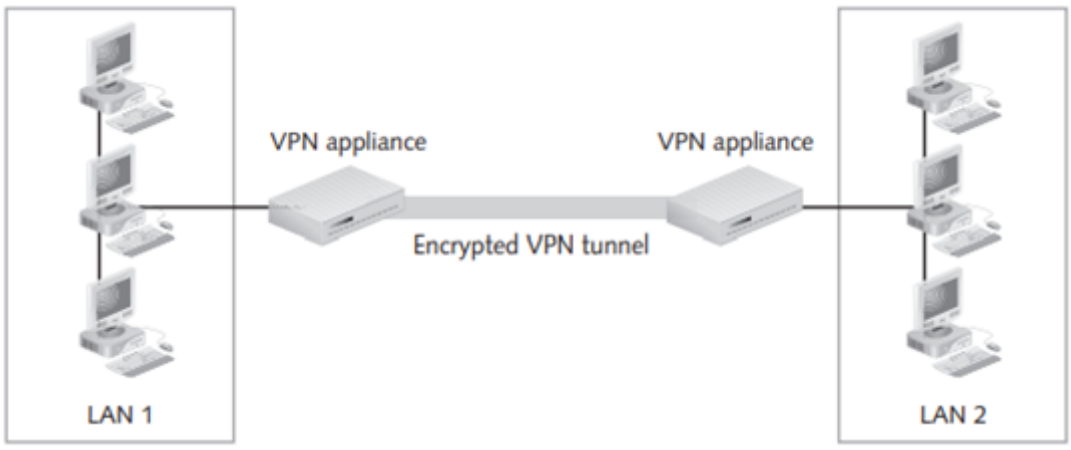

Figure 11-2 VPN appliance creates secure connections between two or more LANs

Software VPNs

Most software-based VPNs are integrated with firewalls and are more cost-effective than hardware VPN devices. Software-based VPNs also increase network security because they are integrated with functions that a firewall already performs, such as packet filtering and Network Address Translation (NAT). Software-based VPNs are appropriate when participating networks use different routers and firewalls or when the endpoints are controlled by different organizations and network administrators.

The main reason for using software VPNs to link networks is the flexibility they offer. They can be configured to enable traffic based on domain name, protocol, or IP address. These restrictions prove useful when some, but not all, of the traffic passing through the VPN is meant to be encrypted and sent through the tunnel. However, because software VPNs often rely on the OS on which they are installed, configuring and using them are complex tasks.

Evaluating Business Needs for VPNs

Planning a VPN deployment requires assessing an organization's goals. For example, the need to keep business transactions private has prompted more organizations to adopt VPNs. The popularity of e-commerce is an incentive as well, and government and military agencies need to share information to provide effective homeland security.

A VPN is an excellent solution for an organization that needs to follow a budget while maintaining security. Budgetary considerations have always made VPNs an attractive business proposition. When you use a VPN, you are essentially spreading the cost of its operation over many users, which makes it cost effective.

In addition, many companies employ remote contractors who need to access the corporate network from their homes or offices. Employees who travel for business reasons need to check e-mail and exchange files with colleagues in the central office. Secure remote access is an essential requirement for many businesses and is an important reason for establishing a VPN. Another reason is the need for a secure means of connection for partners, suppliers, contractors, and others outside the company who need real-time data access to support just-in-time processes, inventory management, and shipment status information.

You should review the company security policy for guidance on existing security goals and procedures, and as a basis for planning VPN deployment. Also, you should consider the type of business an organization runs, along with its number of employees and existing infra-structure, as well as security and throughput rates required for data. With this information, you can integrate a VPN with minimal disruptions and avoid unexpected and undesirable outcomes.

VPNs are as diverse as the needs they support. When you have a clear picture of the organization and its users, you can begin planning the VPN's configuration, testing, and deployment. A secure VPN design should address the following factors:

- Secure connectivity
- Encryption
- Availability
- Authentication
- Secure management
- Reliability

- Scalability
- Performance

Advantages and Disadvantages of VPNs

VPNs have advantages and disadvantages. They offer a high level of security, provided that network administrators address inherent challenges. For instance, if a VPN device is configured incorrectly or remote users at a VPN endpoint disable their firewalls by mistake and let in an attacker, the VPN's protections can be circumvented. In addition, VPNs can be complex to configure, and the necessary hardware and software can represent a substantial investment. Table 11-1 summarizes some of the main advantages and disadvantages.

Advantages	Disadvantages
Far less expensive than leased lines	Can be complex to configure
Many elements working together provide strong security	Can result in slower data transfer rates than a leased line
Standards and protocols used in VPNs are well developed and widely used	Depends on the often unpredictable Internet; if your ISP or other parts of the Internet go down, your VPN goes down
Can result in less overall complexity in an organization's network	Requires administrators to install VPN client software on remote computers
Can make use of a company's existing broadband connection	VPN hardware and software from different vendors might prove incompatible because they use different protocols

Table 11-1 Advantages and disadvantages of VPNs

By focusing on Internet-based technologies, VPNs simplify a network. You have only one Internet connection to manage instead of managing an Internet connection plus leased lines. In addition, running a VPN means you have even more ways to maximize network uptime. Downtime is expensive; in addition to the cost of repairs, it adds administrative time in troubleshooting and repairing problems and affects users' productivity.

The Three VPN Core Activities

Encapsulation

VPNs can use unsecure, public Internet connections and still provide a high level of security because they perform a core set of activities: encapsulation, encryption, and authentication. Together, these activities tunnel data from one network to another using the infrastructure of the Internet.

First, VPNs perform encapsulation of data: They enclose a packet within another packet that has different IP source and destination information for a high degree of protection.

Encapsulation protects the integrity of data sent through the VPN by hiding the data packets' source and destination information. The VPN encapsulates data packets in packets that use the VPN gateway's source and destination addresses, as shown in Figure 11-3. The gateway could be a router that uses IPsec, a VPN appliance, or a firewall that functions as a VPN and has a gateway setup.

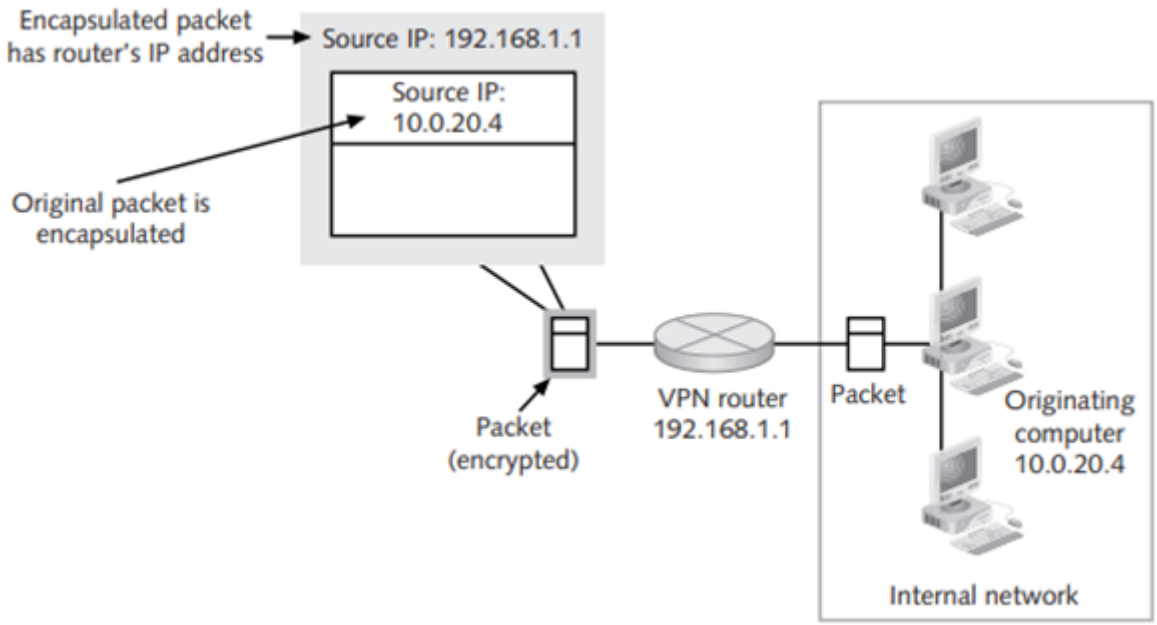

Figure 11-3 Encapsulating data to conceal source and destination information

When a VPN tunnel is in place, the source and destination IP addresses of the encapsulated data packets can be in private reserved blocks that are not routable over the Internet, such as the 10.0.0.0/8 addresses or the 192.168.0.0/16 reserved network blocks.

Encryption

As you learned in Chapter 5, encryption is the process of rendering information unreadable by all but the intended recipient. The encryption process is carried out by means of an algorithm that generates an encoded block of data called a key. The key is part of an electronic document called a digital certificate, which is obtained from a certification authority (CA), a trusted organization that issues keys. The key is then used to encrypt data at the originating endpoint of the VPN and to decrypt it at the destination endpoint (see Figure 11-7).

To perform encryption at both endpoints of the VPN, the keys must be exchanged by participants who have an SA. The exchange can be performed by using a variety of encryption methods. In symmetric cryptography, the same key is exchanged by sender and recipient. In asymmetric cryptography, two different keys are used—a public key and a private key. When a person or an organization obtains a digital certificate from a CA, an encryption algorithm is used to generate a private key. This key is never exchanged but is maintained securely by the certificate holder. The private key is used to generate a public key, which can be exchanged freely among VPN participants.

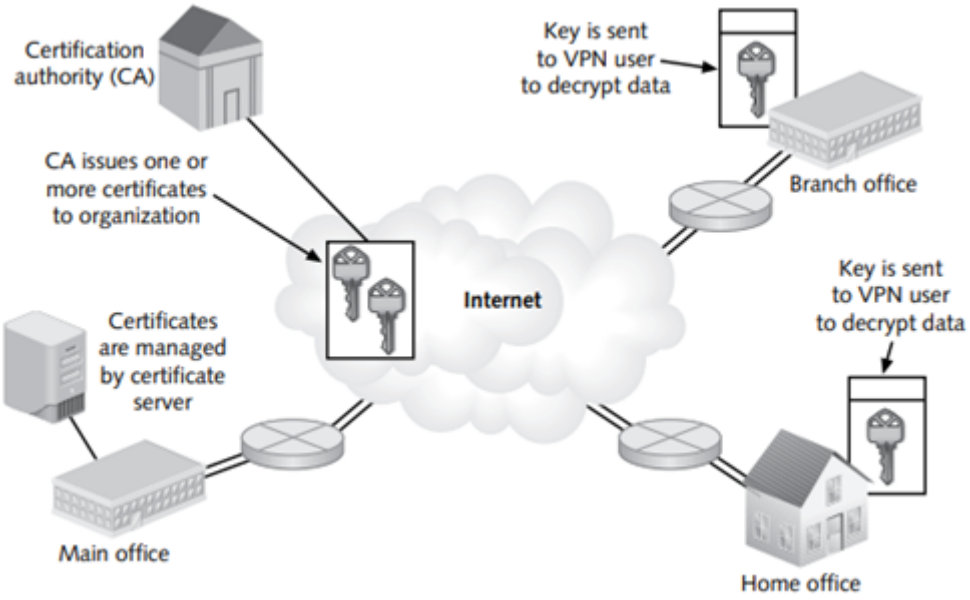

Figure 11-7 VPN endpoints encrypt and decrypt data by exchanging keys

Another key exchange method, IKE, uses tunnel method encryption to encrypt the header and data components of a packet and to encapsulate the packet within a new packet that has a different header. IKE is increasingly popular because it provides a high level of security, which outweighs the decrease in network performance caused by complex encryption.

Authentication

Authentication is the third core activity that VPNs perform to ensure the security of tunneled communication. Authentication is essential because network hosts that receive VPN communications need to know that the originator of the communication is an approved user of the VPN.

The type of authentication used in a VPN depends on the tunneling protocol. Many networks use IPsec to authenticate users; VPN participants establish an SA and exchange keys to authenticate one another. PPTP, which is used for dial-up access to a remote server, uses MS-CHAP, in which both computers exchange authentication packets. TLS/SSL uses certificate-based authentication. RADIUS is also commonly used for authentication services in VPN architecture.

VPNs use digital certificates to authenticate users and encryption to ensure that communications cannot be read even if they are intercepted in transit. Figure 11-9 illustrates the VPN's core activities of encapsulation, encryption, and authentication.

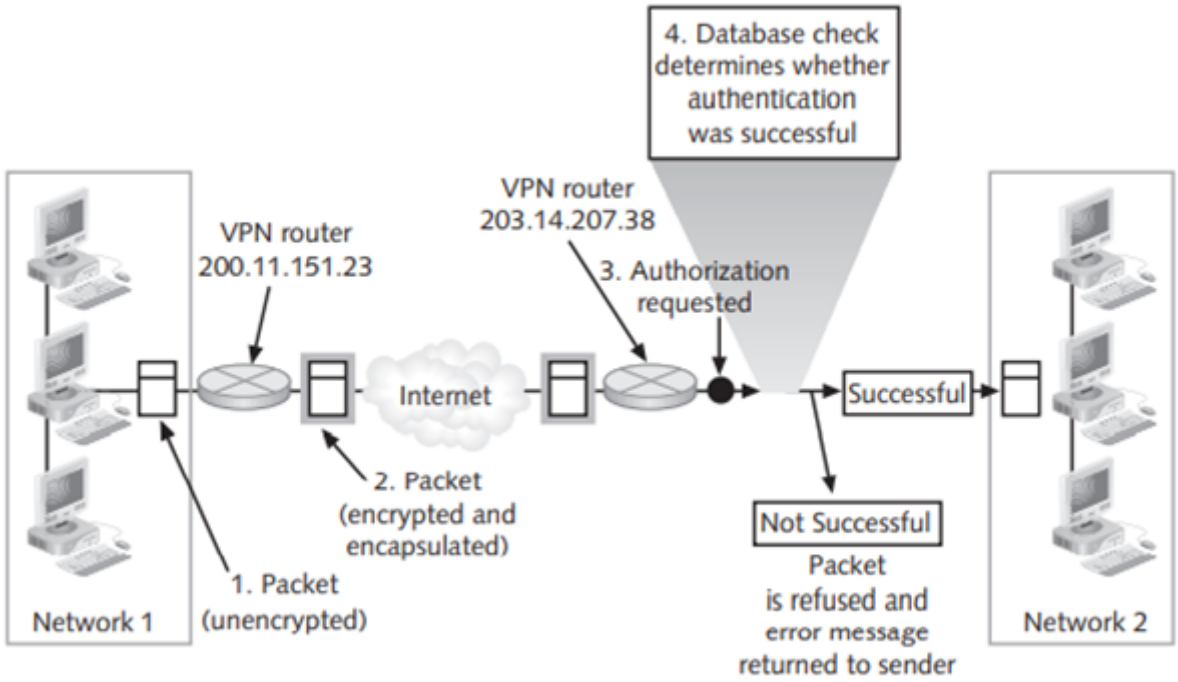

Figure 11-9 VPN core activities

In Figure 11-9, the following steps are basic to the authentication process:

1. The source computer transmits the unencrypted packet on internal network 1.

2. After the VPN router at 200.11.151.23 encrypts and encapsulates the packet, the packet passes through the gateway into the Internet.

3. The VPN router at internal network 2 requests authentication.

4. A database check determines whether authentication is successful. If it is, the packet is allowed to reach its destination. Otherwise, an error message is returned.

Examining VPN Design and Architecture

A VPN's topology—the way components in a network are connected—determines how gate- ways, networks, and clients are related to each other. As you will learn in the following sections, VPN topologies correspond to a basic network's physical and logical topologies. The three basic topologies are mesh, star, and hybrid VPNs.

Mesh Topology

In a mesh configuration, all participants in the VPN have Security Associations with one another. Two types of mesh arrangements are possible:

· Full mesh—Every subnetwork is connected to all other subnets in the VPN (see Figure 11-11). This topology is complex to manage and is best used with small VPNs.

· Partial mesh—Any subnet in the VPN may or may not be connected to the other subnets. This configuration offers more flexibility than a full-mesh arrangement.

The advantage of a mesh configuration is that each participant can establish VPN communications with all other participants. However, if a new LAN is added to the VPN, all other VPN devices have to be updated to include information about new users. The problem with mesh VPNs is the difficulty of expanding the network and updating every VPN device whenever a host is added.

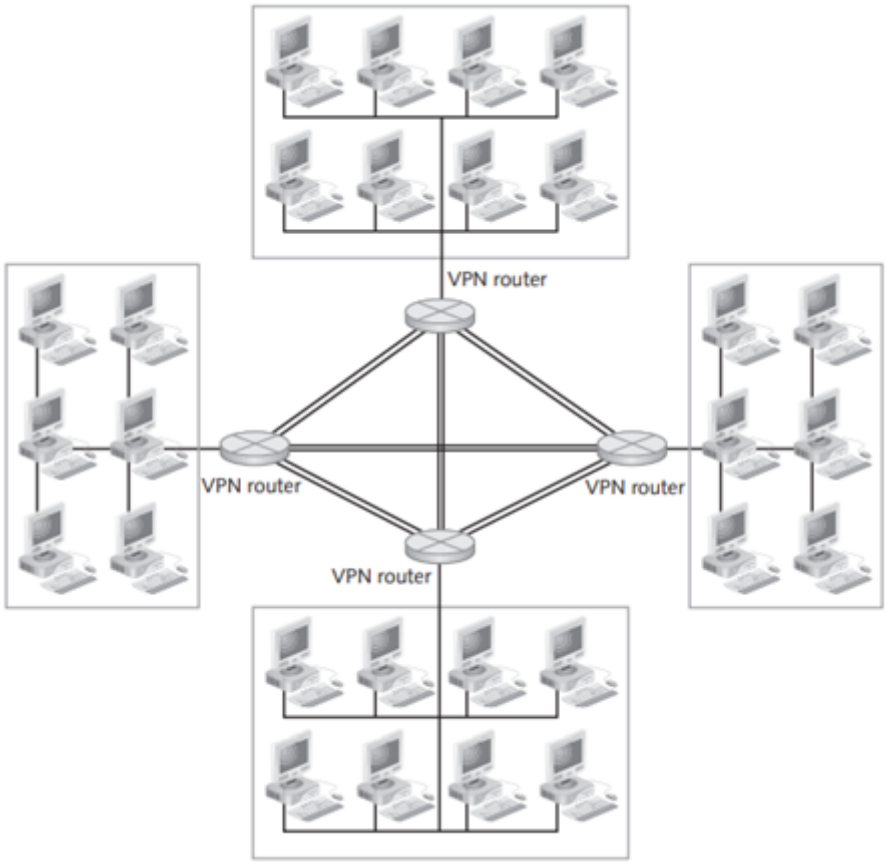

Figure 11-11 A full-mesh VPN configuration

Star Topology

In a star configuration (also known as a hub-and-spoke configuration), the VPN gateway is the hub, and other networks participating in the VPN are called rim subnetworks (see Figure 11-12).

In this configuration, separate SAs are made between the hubs of each rim subnetwork. The central VPN router is at the organization's central office because most star VPNs have communications go through the office where the main IT staff is located. Any networks or computers that want to participate in the VPN need to connect only to the central server, not to any other systems in the VPN. This setup makes it easy to increase the VPN's size when more branch offices or computers are added. On the other hand, in star configurations, all communications flow in and out of a central router. This setup creates a single point of failure at the central router and can slow communication, especially if branch offices are far apart. One solution is to use two or more routers at the central office. They can be configured for load balancing to improve performance and function as failover devices.

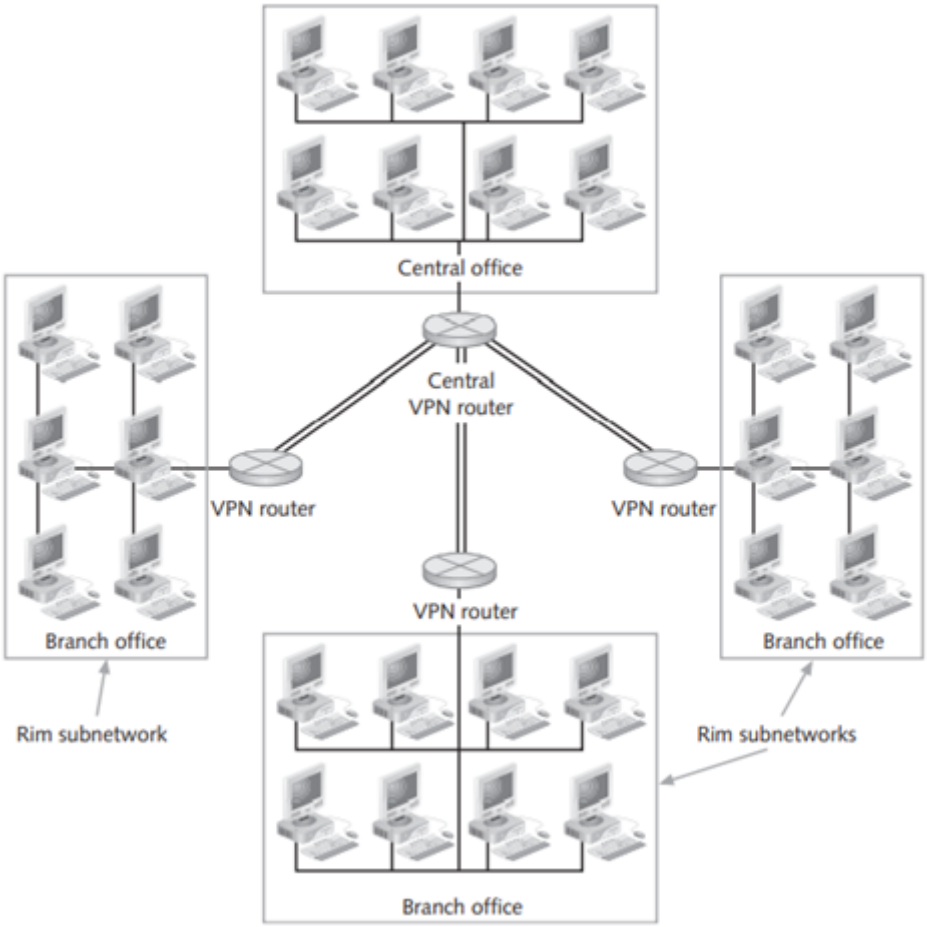

Figure 11-12 A star VPN configuration

Hybrid Topology

As organizations with VPNs grow to include new computers and branch offices, they naturally evolve from a mesh or star configuration into a hybrid configuration that combines network topologies (see Figure 11-13). Because mesh configurations tend to operate more efficiently, the central core that links the network's most important branches should probably be a mesh configuration to provide fault tolerance. However, branch offices can be added as spokes that connect to a VPN router at the central office. A hybrid setup that combines these two configurations benefits from the star configuration's scalability and the mesh configuration's speed.

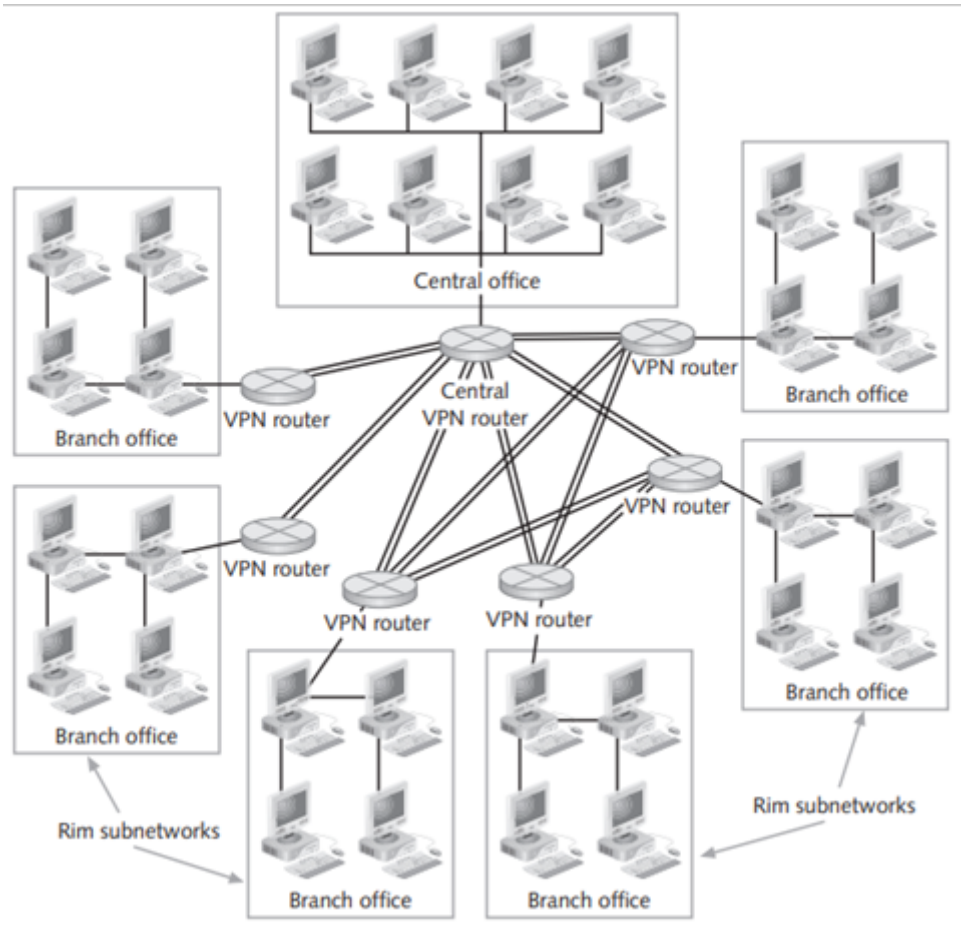

Figure 11-13 A hybrid VPN configuration

VPN Domains

To set up a VPN, you need to define a VPN domain: a set of one or more computers that VPN hardware and software handle as a single entity. The computers in a VPN domain use the VPN to communicate with another domain. With a firewall, a domain might be a set of networked computers grouped under a name, such as Office Network.

Single and Multiple Entry Point Configurations The decision whether to have single or multiple entry points depends on whether your network has a site-to-site or client- to-site VPN configuration. Small networks that use VPNs typically have only site-to-site connections and often have single entry point configurations: All traffic to and from the net- work passes through a single gateway, such as a router or firewall (or both). In a single entry point configuration, the gateway must be a member of the VPN domain. In the configuration shown in Figure 11-14, the VPN domain includes a group of computers in the internal network as well as the gateway.

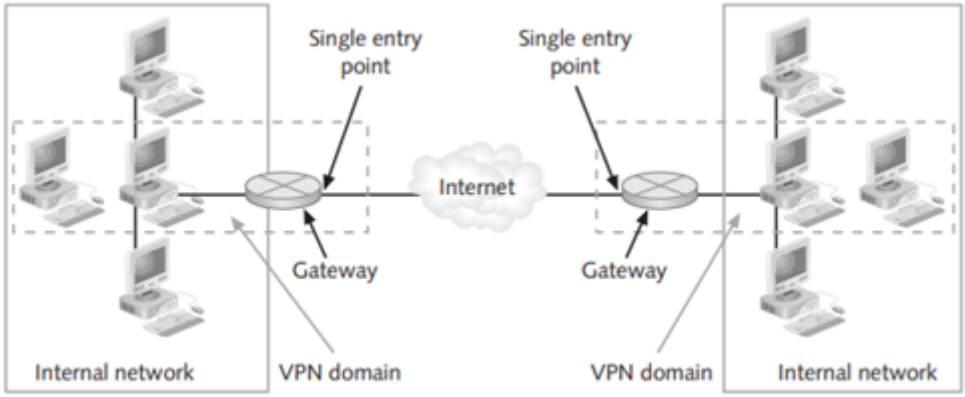

Figure 11-14 A single entry point configuration

In contrast, many large organizations have networks with several client-to-site connections. These connections require multiple entry point configurations in which multiple gateways are used, each with a VPN tunnel connecting a different location (see Figure 11-15). In a multiple entry point configuration, excluding the gateway from the VPN domain is important. If you do not exclude the gateway, all traffic to and from each gateway in the internal network is encrypted. This encryption reduces performance unnecessarily because you need to encrypt only the traffic from gateway to gateway.

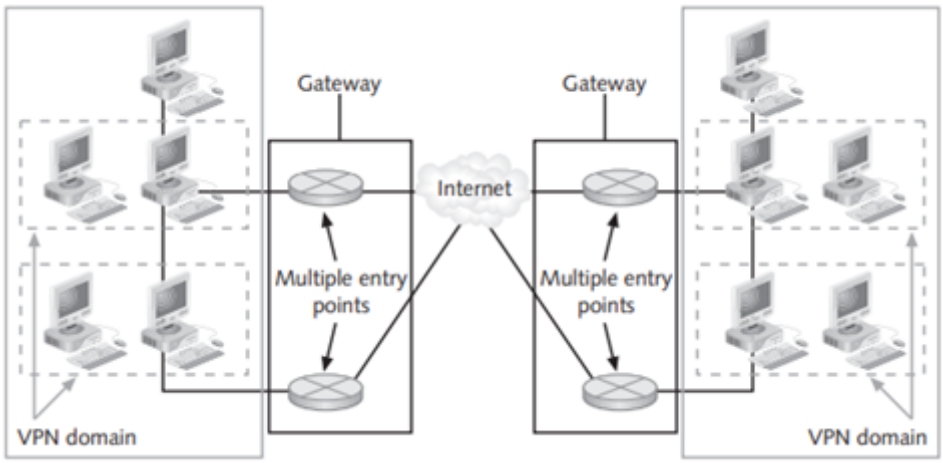

Figure 11-15 A multiple entry point configuration

Preventing VPN domains from overlapping is also important; having multiple routes in routing tables could cause some traffic to be routed incorrectly or not at all because of duplicate IP addresses. If a router has multiple paths for directing packets, it might not respond correctly. This problem can be fixed easily by configuring routing tables correctly.

Using VPNs with Firewalls

Having a VPN does not reduce the need for a correctly configured firewall. You should always use a firewall as part of your VPN security design. Using a VPN with a firewall, how- ever, requires careful planning and configuration? Several different configurations are possible, and each option has advantages and disadvantages, as you learn in this section.

One option is to install VPN software on the firewall. Several commercial firewalls include VPN components as an added option. As you can see in Figure 11-16, this configuration has a single point of entry into the network:

- The firewall allows outbound access to the Internet.
- The firewall prevents inbound access from the Internet.
- The VPN service encrypts traffic to remote clients or networks.

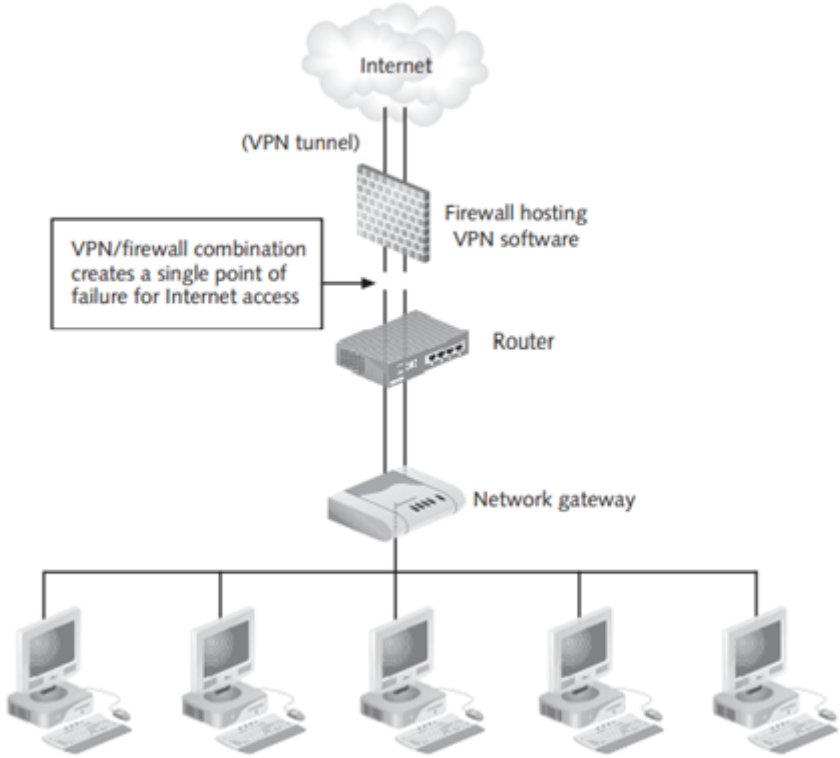

Figure 11-16 The VPN server on a firewall

Putting the VPN on a firewall has the following advantages:

- You can control all network access security from one server.
- You have fewer computers to manage, meaning less chance of configuration mistakes.
- You can create and manage rules that apply to your VPN traffic with the same tools you already use to manage your firewall.

Installing the VPN on a firewall carries disadvantages as well:

- You have one server controlling all network access security. Any errors in configuring the VPN or firewall could leave your network open to attack.
- You must make sure to configure routes carefully so that traffic goes through the correct interfaces.
- Incorrect configuration of the firewall or VPN rules could allow traffic from the Internet to get past your security.
- Internet access and VPN traffic compete for resources on the server, so a more powerful computer might be necessary.

Another option, shown in Figure 11-17, is to set up the VPN parallel to your firewall inside the demilitarized zone (DMZ). Internal clients continue to point to the firewall as their default gateway and are unaware of the VPN connection. The firewall has a route to any net- works accessible via the VPN server and instructs clients to send packets to the VPN server when appropriate.

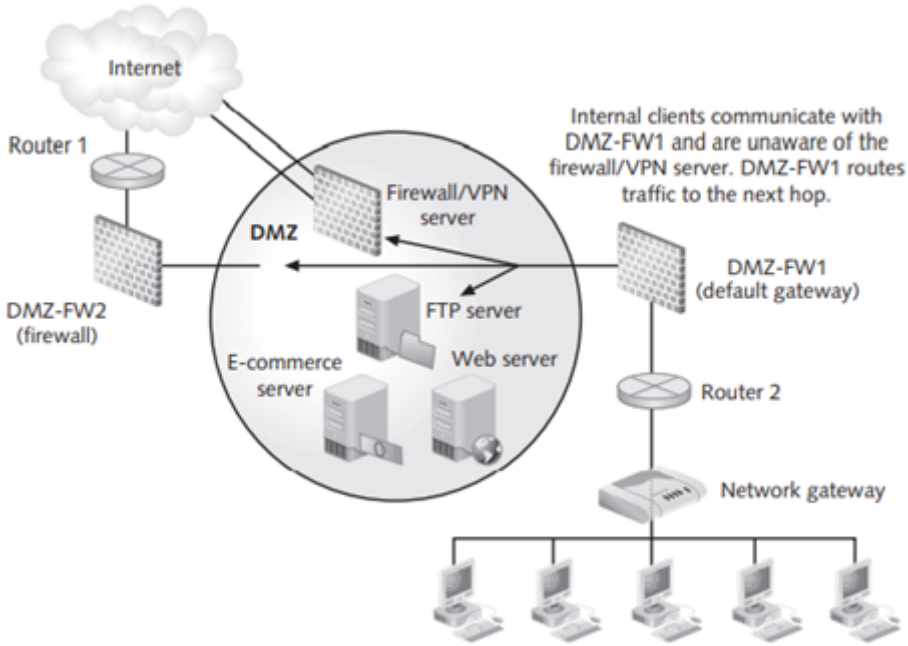

Figure 11-17 The VPN server parallel to a firewall

A DMZ can also be called a screened subnet or a perimeter network. If it is used for sharing files and access to company data with a business partner, a perimeter network is often referred to as an extranet.

Placing the VPN server parallel to the firewall has the following advantages:

- VPN traffic is not going through the firewall, so there is no need to modify firewall settings to support VPN traffic.
- This configuration can be scaled more easily. New VPN servers can be added without having to reconfigure the firewall.
- If the VPN server becomes too congested, you can add another server and distribute the load.

Placing a VPN server parallel to a firewall also includes the following disadvantages:

- The VPN server is connected directly to the Internet, making it an ideal target for attackers.
- If the VPN server becomes compromised, the attacker will have direct access to your internal network.
- The cost of supporting a VPN increases with the addition of new servers and extra support staff.

Another location for the VPN server is behind the firewall connected to the internal network. As shown in Figure 11-18, the VPN server is not accessible from the Internet. All packets must go through the firewall to reach the VPN server. As with the parallel configuration, you need to add a route to the firewall that redirects VPN traffic from internal clients to the VPN server. You also need to configure the firewall to pass encrypted VPN traffic directly to

Putting the VPN server behind the firewall has some advantages:

- The VPN server is completely protected from the Internet by the firewall.
- The firewall is the only device controlling access to and from the Internet.
- Network restrictions for VPN traffic are configured only on the VPN server, making it easier to create rule sets.

On the other hand, putting the VPN server behind the firewall has the following disadvantages:

- All VPN traffic must travel through the firewall, which increases congestion and latency.
- The firewall must handle VPN traffic from the Internet to the VPN server. Getting the firewall to pass encrypted VPN traffic to the VPN server could require advanced configuration.
- The firewall might not know what to do with IP protocols other than ICMP, TCP, and UDP. Supporting VPNs that use IP protocols, such as ESP packets for IPsec or GRE packets for PPTP, could be challenging.

If you terminate the VPN connection in front of the firewall, VPN traffic will be on the unprotected external network for a brief period before passing through the firewall.

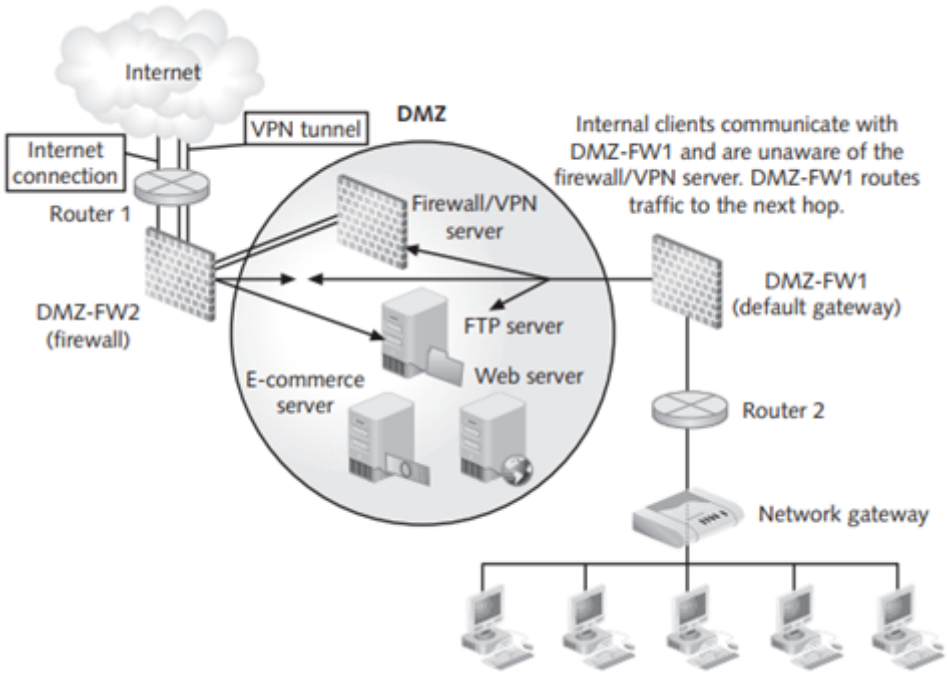

Figure 11-18 The VPN server behind a firewall

Ensuring Client Security

Another critical aspect of deployment is enforcing security on the client side of the VPN tunnel. If a remote user's computer is compromised, the internal network is at risk. Client- side issues include whether to require clients to use a firewall and intrusion detection and prevention system (IDPS), and whether policies should be enforced on client computers before allowing remote users to authenticate to the internal network.

Remember that a VPN extends the corporate network by using public communication channels. When it is set up and configured correctly, a VPN can supply inexpensive, secure access; when set up incorrectly, a VPN is a tremendous security liability that can give intruders full access to your network. Failing to secure access to a remote network has legal implications, too. If your VPN connects to partner or vendor networks, and an intruder gains access to their network through your poorly configured VPN, your company could face litigation for damages resulting from the security breach. This situation isn't likely, but it is possible. The point is that you must consider the security implications of any extension of your network.

There are several ways to increase VPN client security, from network configuration settings to third-party software solutions. For example, when a Windows client connects to a VPN server, administrators can configure the remote system to use the corporate network's default gateway for further Internet access. This option prevents split tunneling by the client, which results in multiple paths. One path goes to the VPN server and is secured, but an unauthorized and unsecured path permits users to connect to the Internet or another network while still connected to the corporate VPN (see Figure 11-19). Split tunneling leaves the VPN server and internal network vulnerable to attack.

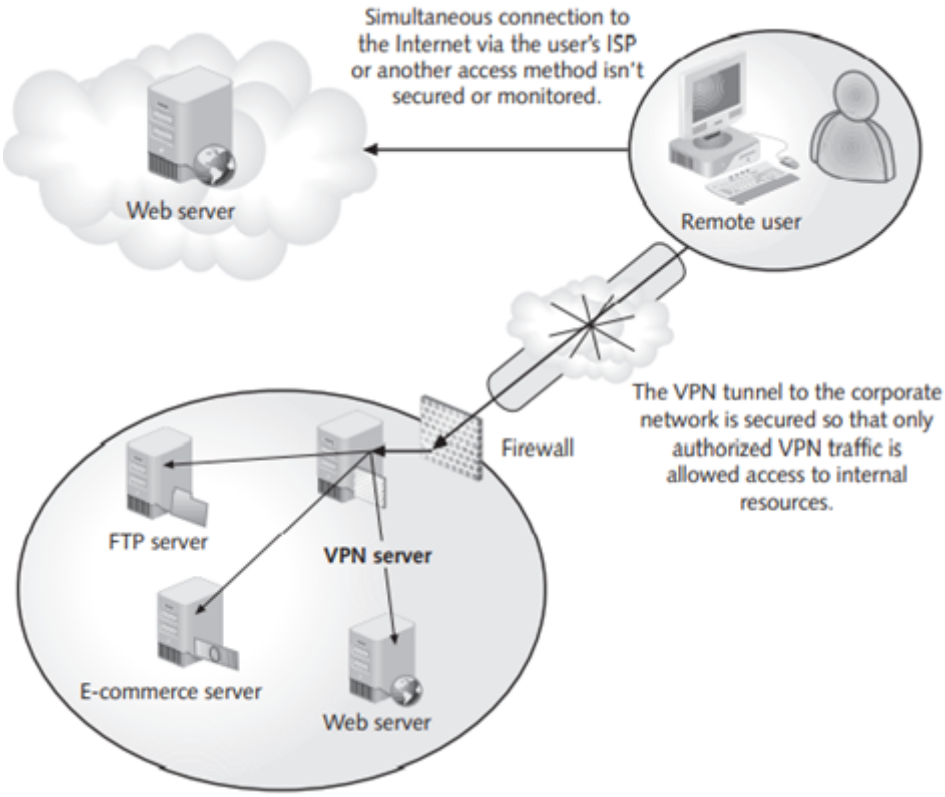

Figure 11-19 Split tunneling introduces a vulnerability

Small organizations that do not have the resources to enforce total control over clients should at least require users to sign an acceptable use agreement. Remote users should be required to maintain an Internet firewall and current virus protection to secure the computer against unauthorized use, and should be prevented from enabling split tunneling while connected to the network.

Auditing VPNs and Setting VPN Policies

VPN endpoints are vulnerable to many of the same viruses, Trojan programs, and spyware as internal network computers, and an infected remote computer can spread viruses or malicious code to computers on the internal network. Because remote clients are outside an administrator's realm of control, the responsibility for remote client security falls mostly on end users. You can take measures to mitigate these risks, however, such as including VPN policies in your overall security policy, using VPN quarantine procedures, logging VPN connections, and auditing remote access activity logs. These measures are discussed in the following sections.

Using VPN Quarantine

A quarantine network is a segment of the network with limited access to resources, especially internal resources. Quarantine networks are logical topology structures that are used for untrusted clients, such as business partners, vendors, and consultants, as well as remote access/VPN clients. Quarantined clients can be checked for policy compliance and then granted access to resources after compliance is verified, or a connection can be maintained in quarantine state for the duration of a session, depending on the client's access permissions and the nature of the connection (for example, a remote access/VPN client or a limited access consultant).

VPN quarantine was created to address the problem of remote clients not meeting an organization's security standards. Although a VPN provides encryption and encapsulation to secure access, it cannot check to make sure that clients have the latest updates or check for malicious software. A computer that connects to a network via a VPN can introduce malware; if the operating system or the antivirus software is not updated, it might contain software vulnerabilities that can be exploited. VPN quarantine provides a method to address these vulnerabilities by placing clients in virtual solitary confinement while they are checked for policy compliance.

Clients are subjected to preconnection and postconnection checks with custom scripts or a third-party add-on utility. The checks can examine the service pack version, software update status, and whether an approved antivirus program and personal firewall are running and updated on the client. Other requirements can be specified in the scripts. While these checks are running to verify compliance with the remote access policy, computers that attempt to connect are placed in a quarantine network. After computers are examined and pass the checks, the quarantine is lifted, and clients are allowed access to network resources. VPN quarantine is not a cure-all for security vulnerabilities, but it can help prevent computers with unsafe configurations from connecting to the internal network.

Quarantine is not used solely for remote access. It can be used to mitigate other threats, such as e-mail, which is a primary source of malware infections. Many corporate e-mail systems use an approach similar to quarantine for screening suspicious e-mails or e-mails with attachments. If an e-mail contains viruses or does not comply with policies, it is dropped, and the recipient might get an e-mail that explains the problem.

To use VPN quarantine, you must have quarantine-compatible remote access clients and servers, resources for a quarantine network, an accounts database, and a quarantine remote access policy. VPN quarantine can use Windows authentication or a RADIUS server, but RADIUS is the preferred method.

Windows Server 2008 R2 and Threat Management Gateway 2010 support VPN quarantine scripts, and most other modern OSs can be configured to support quarantine procedures. Because VPN quarantine uses scripts and integrates with RADIUS servers, you can implement it on varied platforms easily. Refer to vendor instructions for procedures.

Logging VPN Activity

In a Microsoft network, the Routing and Remote Access Services (RRAS) server can log local machine events and record them in the server's System, Security, and Application logs. You can see these events in Event Viewer. Typically, the logs are used to notify administrators of unusual events or for troubleshooting. Event logs provide limited information about remote access, but specific logs give you more useful data about remote clients.

The RRAS server that hosts VPN services has additional logging capabilities beyond standard Event Viewer logs. It can also perform local authentication and accounting logging, which track remote access authentication attempts and use. The name of the applicable remote access policy is included with each connection attempt, making these logs useful for troubleshooting problems with remote access policies. You might need to enable Windows Authentication and Windows Accounting before you can configure what to log or where to store the logs.

Windows also provides support for RADIUS-based authentication and accounting logging. The RADIUS server stores logs in a separate file, which can be used for tracking remote access and use. You must enable RADIUS accounting and authentication before you can con- figure logging.

You must make sure that log files cannot be tampered with, maintain a reasonable retention policy, and ensure that log data is reviewed regularly. Storing a backup copy of log files on a separate computer is a good idea for sensitive data, and including log files in backups is a sensible precaution. Using a database with third-party log-file analysis tools can help you keep up with log file reviews. Using an integrated database that stores your remote access, firewall, and intrusion detection logs helps you compare logged events from all devices to get a clear picture of an event.

Auditing Compliance with VPN Policies

An organization's VPN or remote access policy defines standards for connecting to the network from any host or remote system. These policies must be integrated with an organization's overall security policies. Policies should be defined for different levels of restriction, such as what time of day access is allowed. You might also want to define tighter controls for business partners than you do for company employees working from home. Controls for administrators might be less restrictive; however, administrators should be required to have more secure passwords and to change them more often.

You should audit these policies to confirm that they are being enforced and that all users are complying with them. Enforcing these policies can be difficult with remote users, however. Having strict policies for client-side OSs, configuration, and VPN client software makes this task easier, but configuring remote computers often requires long phone calls with the help of tech support, which can be frustrating and time consuming. One solution is to standardize the VPN client for remote users. That way, tech support staff need to learn how to support only one application, so there is less chance of errors.

In addition, test each client that will connect to the network to ensure smooth operation and help prevent security threats. After bugs are worked out and remote users can access the net- work, verify that everything is working according to the organization's policies and procedures. Remote user connections should be monitored for performance and capability to connect. Is the connection maintained during file transfers? How long does a normal file transfer take? Is an idle connection terminated after a specified time? You should work with a knowledgeable remote user to help determine a baseline for future auditing, testing, and troubleshooting.

Guidelines for VPN Policies

Incorporate the following best practices into your remote access and VPN policy:

- Plan the most secure deployment possible, and keep careful records of all changes.
- Use strong authentication methods.
- Require adequate password strength, length, and complexity, and require passwords to be changed frequently. Make sure that the password history setting is long enough to prevent the reuse of passwords.
- Have the remote access server use DHCP to assign addresses to remote clients or con- figure a static range of IP addresses on the VPN server so that it can assign addresses dynamically to remote clients.
- Log remote connections and use a centralized database or server for storing log files, if possible.
- Use VPN quarantine procedures, if available, to ensure policy compliance.
- Disable public peer-to-peer (P2P) file-sharing programs. If these programs are necessary for productivity, provide approved programs and ban all others.
- Preventing users from downloading and installing software is usually the safest route.
- Make sure that user accounts do not have full administrative access to their systems.
- Ensure strong encryption for data, especially passwords.

- Disable split tunneling.
- Require remote clients to be configured automatically to limit or eliminate user intervention. In general, you should prevent users from making security decisions.
- Disable or remove vulnerable protocols, such as Telnet, FTP, and rlogin.
- Use extra caution when configuring connectivity methods, especially wireless. Configure automatic disabling of wireless connectivity when users are connected directly or using another method of access.
- Prevent the use of removable storage devices, such as thumb drives or external hard drives, anywhere on the network.
- Install personal firewall and antivirus programs on remote devices and configure them for automatic updates.
- Make sure that remote clients are self-defending, which means remote users cannot disable or bypass security measures. Whenever possible, measures should take place automatically without user intervention.
- Manage user audit information so that remote users receive policy updates and transmit their audit data before connecting.
- Conduct regular user training on security topics.

Try to strike the best balance between productivity and security in remote access and VPN policies. It is easy to err on the side of caution and lock a network down too tightly, which erases all the benefits of mobility. It is equally easy to err on the side of productivity and leave the network open to attack. Try to provide the best possible security within the guide- lines of your security policy, yet give remote users enough freedom to be productive. Remember that overly stringent or complex policies are likely to be bypassed or ignored.

◀ Preliminary Activity for Week 13

Jump to...

Analysis, Application, and Exploration for Week 13 ▶

Navigation

Home
Dashboard
Site pages
My courses
Capstone Project 2
Network Defense and Remote Access Configuration
Participants
General
12 - Midterm Examination
13 [Enter Module Title Here]
Preliminary Activity for Week 13
Lesson Proper for Week 13

- Analysis, Application, and Exploration for Week 13
- Generalization for Week 13
- Evaluation for Week 13
- Assignment for Week 13

OJT/Practicum 2

Seminars and Tours

Courses

Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission***.

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

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

Activities

- Assignments
- Forums
- Quizzes
- Resources