Basic Network Security Defense Tools

Defense against these kinds of risks begins with some basic hardware and software tools, such as firewalls, virtual private networks (VPNs), and network admission control.

Firewalls

A **firewall** controls the flow of traffic by preventing unauthorized network traffic from entering or leaving a particular segment of a network. You can place a firewall between an internal network and the outside world or within internal subnetworks to control access to particular corporate assets by only authorized users. Firewalls are critical elements of networking security, but they are just that, elements; they will not solve all security problems, but they do add a much-needed deterrent.

FIGURE 5-8 shows the role of a firewall in a network, which is to separate private networks from the Internet as well as to separate different private networks from each other. This section covers the different types of firewalls and the roles they play in the network topology.

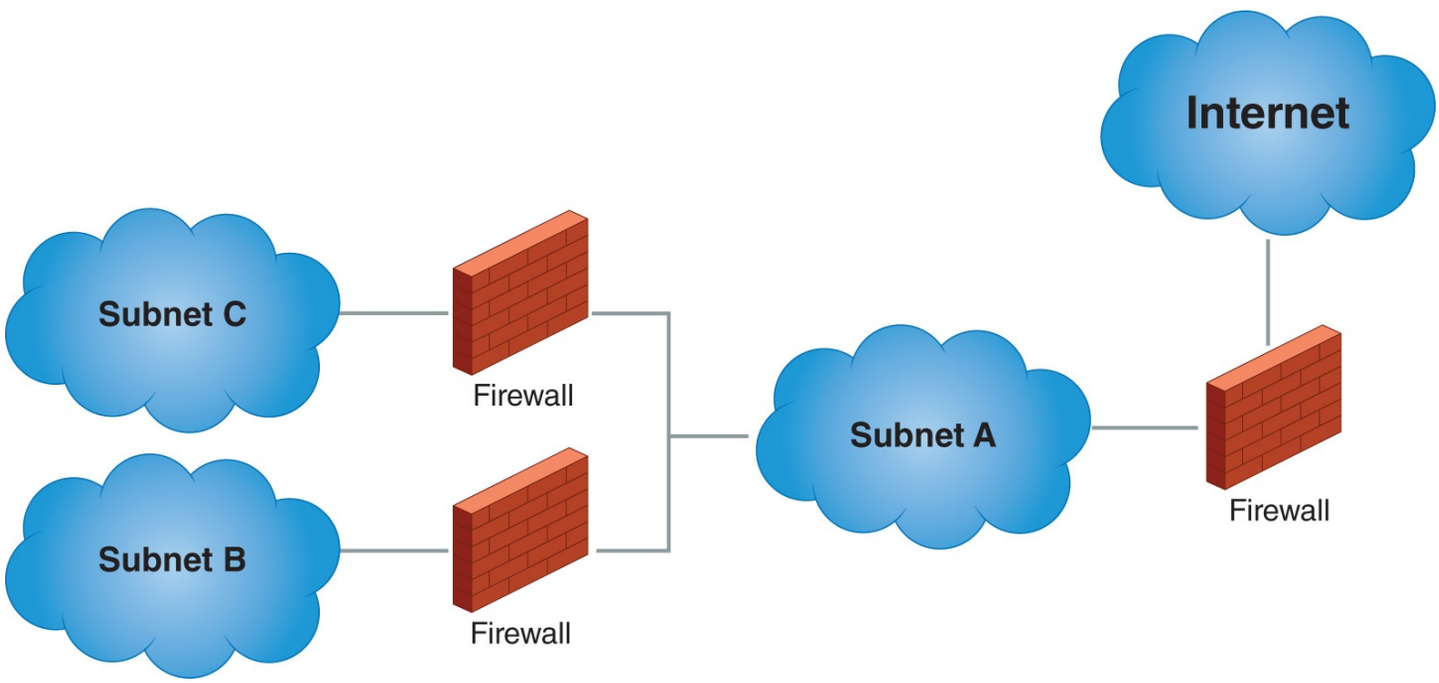

FIGURE 5-8 Firewalls.

Firewalls can be very powerful tools in securing networks. Because each firewall is configured using rules, it provides the most common way to implement rule-based management, which means simply managing the security of a network by defining rules of what network traffic is and is not acceptable. Firewall rules are filters,

defined in a firewall's configuration, that make it easy to implement many of these security requirements. Different types of firewalls use different types of rules, but even the simplest firewalls support access control lists (ACLs), which define rules for handling traffic from one or more hosts using a specific protocol and one or more ports. In addition to securing a host, firewalls can also filter traffic based on ports, often called port security. ACLs can contain very specific rules for a single host, protocol, and port or may contain ranges of hosts and ports with multiple protocols. Each rule tells the firewall how to handle certain types of messages, with the most common actions being allowing and denying. To create the most secure network, configure the firewall to deny all messages except the ones that are explicitly allowed, an approach called implicit deny. This approach can be very secure, but it requires more effort on the part of network administrators to open ports as needed.

Firewalls can help secure networks in several ways, a few of which have already been covered. In addition to these filtering features, they can also provide the following:

- **Flood guard**—Rules can limit traffic bandwidth from hosts, thus reducing the ability for any one host to flood a network.
- **Loop protection**—Firewalls can look at message addresses to determine whether a message is being sent around an unending loop, which can be another form of flooding.
- **Network segmentation**—Filtering rules enforce divisions, or separations, between networks, thus keeping traffic from moving from one network to another.

Firewall Types

The basic function of a firewall is quite simple—to block any traffic that is not explicitly allowed. Firewalls contain rules that define the types of traffic that can come and go through a network, and, each time the firewall receives a network message, it checks the message against its rules. If the message matches a rule, the firewall allows it to pass, whereas, if the message does not match a rule, the firewall blocks it.

Going beyond this basic functionality, firewall technology includes three main types:

- **Packet filtering**—A **packet-filtering firewall** is very basic. It compares received traffic with a set of rules that define which traffic it will permit to pass through the firewall. It makes this decision for each packet that reaches the

firewall and has no memory of packets it has encountered in the past.

- **Stateful inspection**—Unlike the packet-filtering firewall, a **stateful inspection firewall** remembers information about the status of a network communication. Once the firewall receives the first packet in a communication, the firewall remembers that communication session until it is closed. This type of firewall needs to check rules only when a new communication session starts, not each time it receives a packet.
- **Application proxy**—An **application proxy firewall** goes even further than a stateful inspection firewall in that it does not actually allow packets to travel directly between systems on opposite sides of the firewall. Instead, it opens separate connections with each of the two communicating systems and then acts as a broker (or proxy) between the two, which allows for an added degree of protection because the firewall can analyze information about the application in use when making the decision to allow or deny traffic.

Firewalls are not simply preventive controls; instead, they also operate as detective controls and can log as much information as can be analyzed. A structured log analysis process can help identify reconnaissance activity or even attacks that have already occurred. You should regularly monitor all firewall logs to identify potential problems. Because log files from firewalls and other network devices can become very large, using automated log monitors and analysis tools helps to efficiently sort through the log data.

The type of firewall chosen for a network will depend on many factors. If you're placing a simple firewall at the border of a large network, you may want to use a basic packet filter. On the other hand, if you're protecting a highly secure data center that hosts web applications, an application proxy might be more appropriate.

Firewall Deployment Techniques

You can deploy firewalls in several ways on a network. This section will cover three of the most common firewall deployment techniques—border firewalls, screened subnet (or DMZ) firewalls, and multilayered firewalls. Depending on an organization's security needs, one or more of these approaches may be a good fit.

Border Firewall.

The **border firewall** is the most basic approach. These firewalls simply separate the

protected network from the Internet, as shown in **FIGURE 5-9**; they normally sit behind the router and receive all communications passing from the router into the private network as well as all communications passing from the private network to the Internet. Border firewalls normally use either packet filtering or stateful inspection.

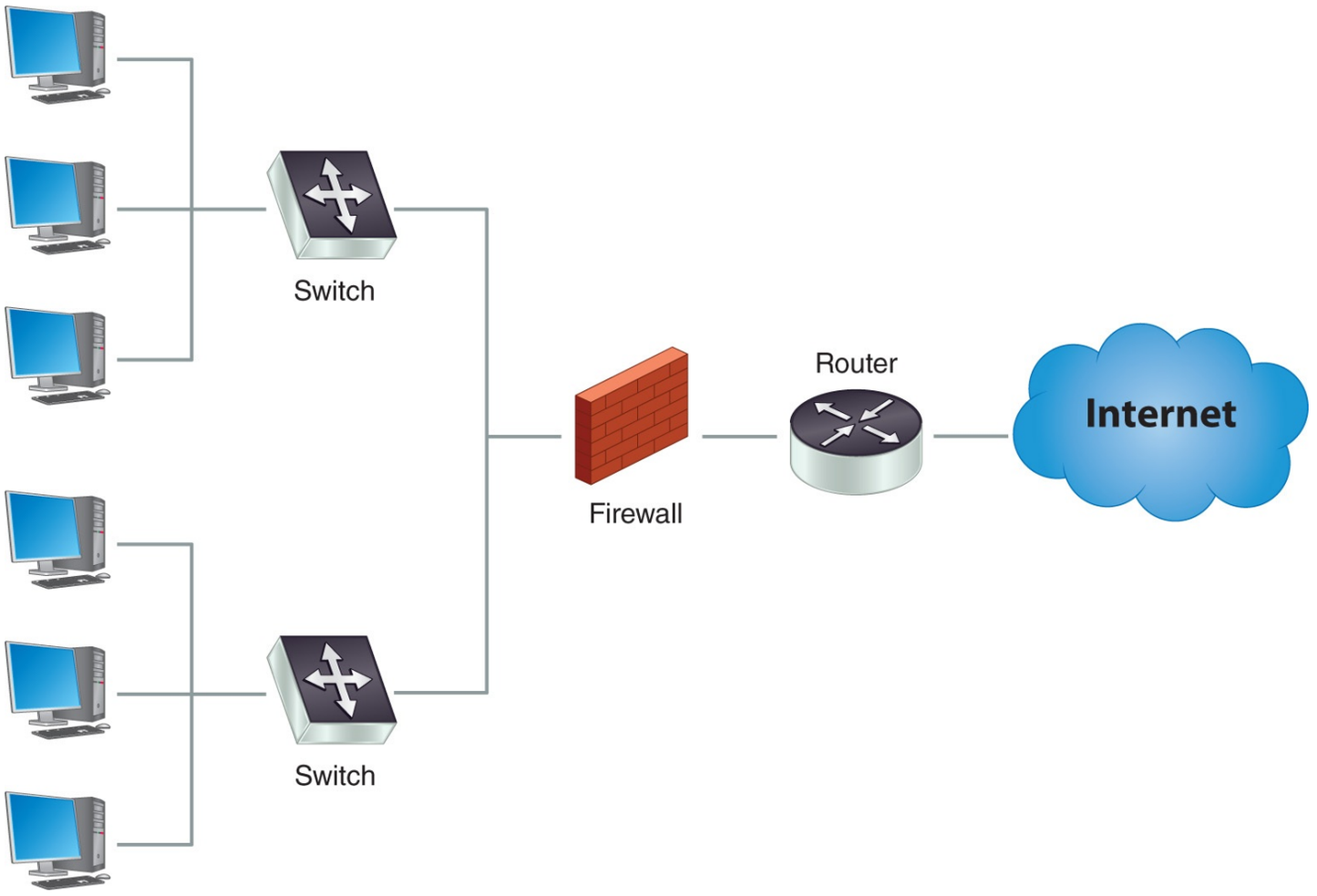

FIGURE 5-9 A border firewall.

Border firewalls are most common for organizations that do not host public services. If an organization outsources its website and email and does not provide any Internet-facing services, it might not need to allow the public access to the network at all. In this case, simply blocking most (or sometimes all) inbound traffic is all that is necessary, and a border firewall excels in this scenario.

Screened Subnet.

Often, it's not possible to block all traffic into a network, such as when an organization hosts a public website or its own email server, thus making it necessary to allow inbound connections on a limited basis. The screened subnet firewall topology, shown in **FIGURE 5-10**, is the best approach for this type of requirement. This firewall has three network interfaces. Two are set up identically to a border

firewall, with one of them connected to the Internet and the other connected to the private network. The third interface connects to a special network known as the screened subnet, or **demilitarized zone (DMZ)**.

NOTE

The screened subnet is the most common firewall topology in use today.

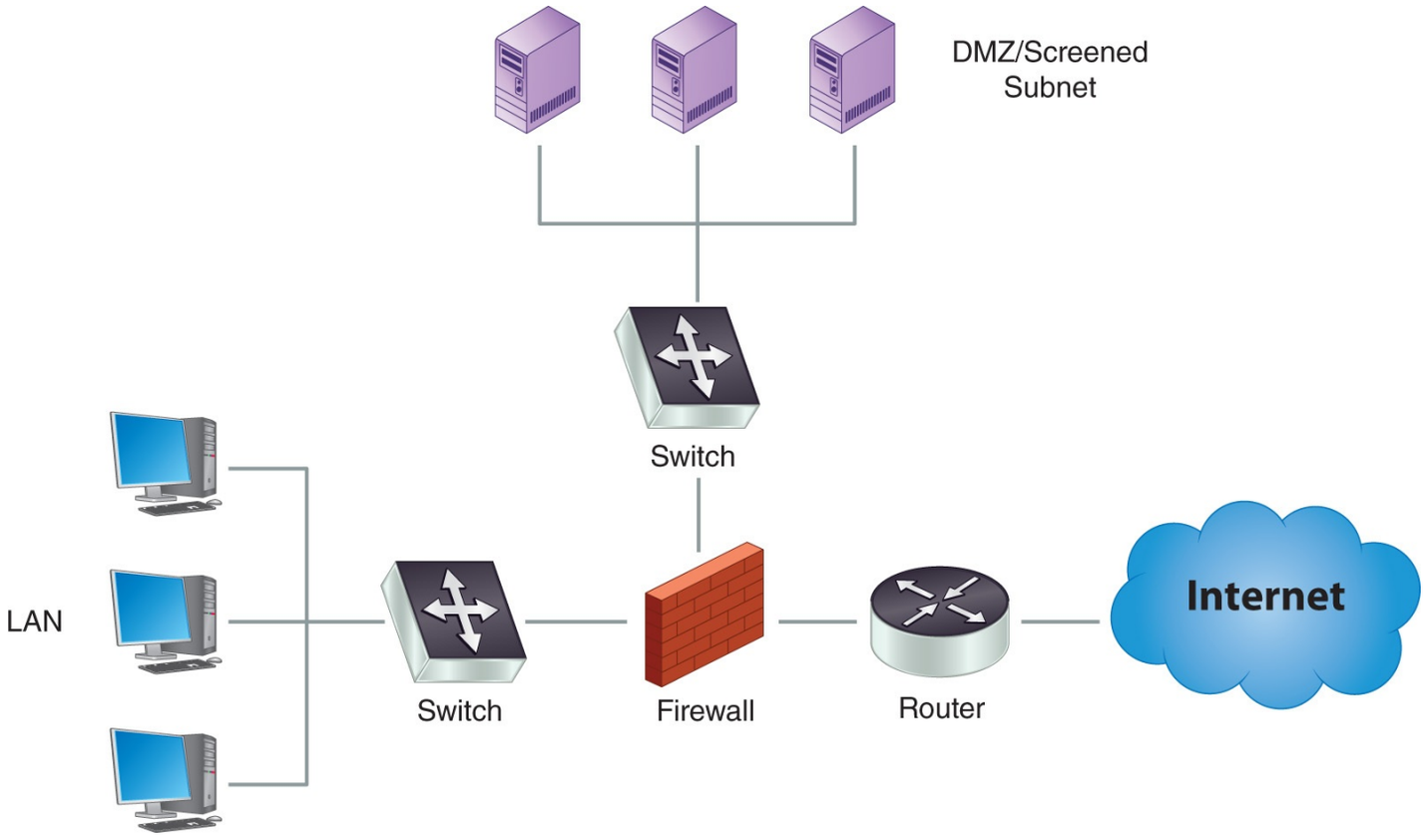

FIGURE 5-10 A screened subnet firewall.

The DMZ is a semiprivate network used to host services that the public can access. Thus, users are allowed limited access from the Internet to systems in the DMZ but are blocked from gaining direct access from the Internet to the private network by a secure network.

This approach recognizes that systems accessed from the Internet pose a special risk because they are more likely to be targets of attacks and, therefore, more likely to suffer successful ones. If these machines are confined to the DMZ, then the only other systems they can jeopardize are those also in the DMZ. Therefore, an attacker who gains access to a DMZ system will not be able to use that system to directly access systems on the private network.

Multilayered Firewalls.

In large and/or highly secure environments, organizations often use multiple firewalls to segment their network into pieces. This is the case illustrated in Figure 5-8, which shows that one firewall acts as the border firewall, protecting subnets A, B, and C from the Internet, and the other two firewalls separate subnets B and C from each other and from subnet A.

Multilayered firewalls are useful when networks have different security levels. For example, referring to Figure 5-8, general users may connect to subnet A, users working on a secret research project might connect to subnet B, and executives might connect to subnet C. This structure provides the secret project and the executives with protection from the general user community.

Unified Threat Management.

Firewalls are so important to network security that they have matured into devices that do far more than just inspect packets. In fact, multipurpose firewalls are more commonly referred to as unified threat management (UTM) devices. These devices do provide filtering as well as many other security services, some of which follow:

- **URL filter**—This feature filters web traffic by examining the Uniform Resource Locator (URL) as opposed to the IP address.
- **Content inspection**—The device looks at some or all network packet content to determine whether the packet should be allowed to pass. This type of inspection can help identify malicious content from trusted sources, which could happen if a trusted source is compromised.
- **Malware inspection**—Providing a specialized form of content inspection, the device looks at packet content for signs of malware.

These unified services make it possible to reduce the number of devices that must analyze network packets. Fewer UTM devices can provide the same level of security as many older devices. However, even with fewer devices inspecting packets, introducing UTM devices can slow down a network because of the sheer amount of work the devices must accomplish. It takes time to inspect and analyze each network packet at multiple layers of the network stack. For this reason, some organizations have elected a “middle-of-the-road” approach, such as implementing a web security gateway, which performs URL filtering but does not examine the content of the packets and therefore accomplishes some of what a UTM device does but without all the overhead.

NOTE

Another useful feature of firewalls is that they can be configured as load balancers, which can dynamically route network traffic to different network segments to avoid congestion. They do this by monitoring known network segments and directing traffic onto a segment that is appropriate for the destination host and has the necessary bandwidth, a process that can keep networks from slowing down when the demand is high.

Virtual Private Networks and Remote Access

With the advent of telecommuting, remote access has become a common part of many corporate networks. When the COVID-19 pandemic hit, the migration toward support for a remote workforce had already begun, and the pandemic simply accelerated support for remote and distributed workers to keep business functions from completely stopping. Today, many companies have employees who rarely if ever come into the corporate office, instead working at home or on the road. Even so, they still need access to corporate resources, which means opening access to more corporate resources from the Internet than IT professionals are comfortable with. The trick is to allow corporate personnel the access they need but to keep attackers out of these potentially open doors.

Virtual private networks (VPNs) are an effective way to increase the security level of data that is transmitted across a public data network by using encryption to protect all the data sent between a user and the organization's network. The cost difference between using a VPN and paying for a dedicated connection between two sites is significant. Therefore, using a VPN for remote access not only provides security but is also cost effective. **FIGURE 5-11** shows an example of VPN access to a network.

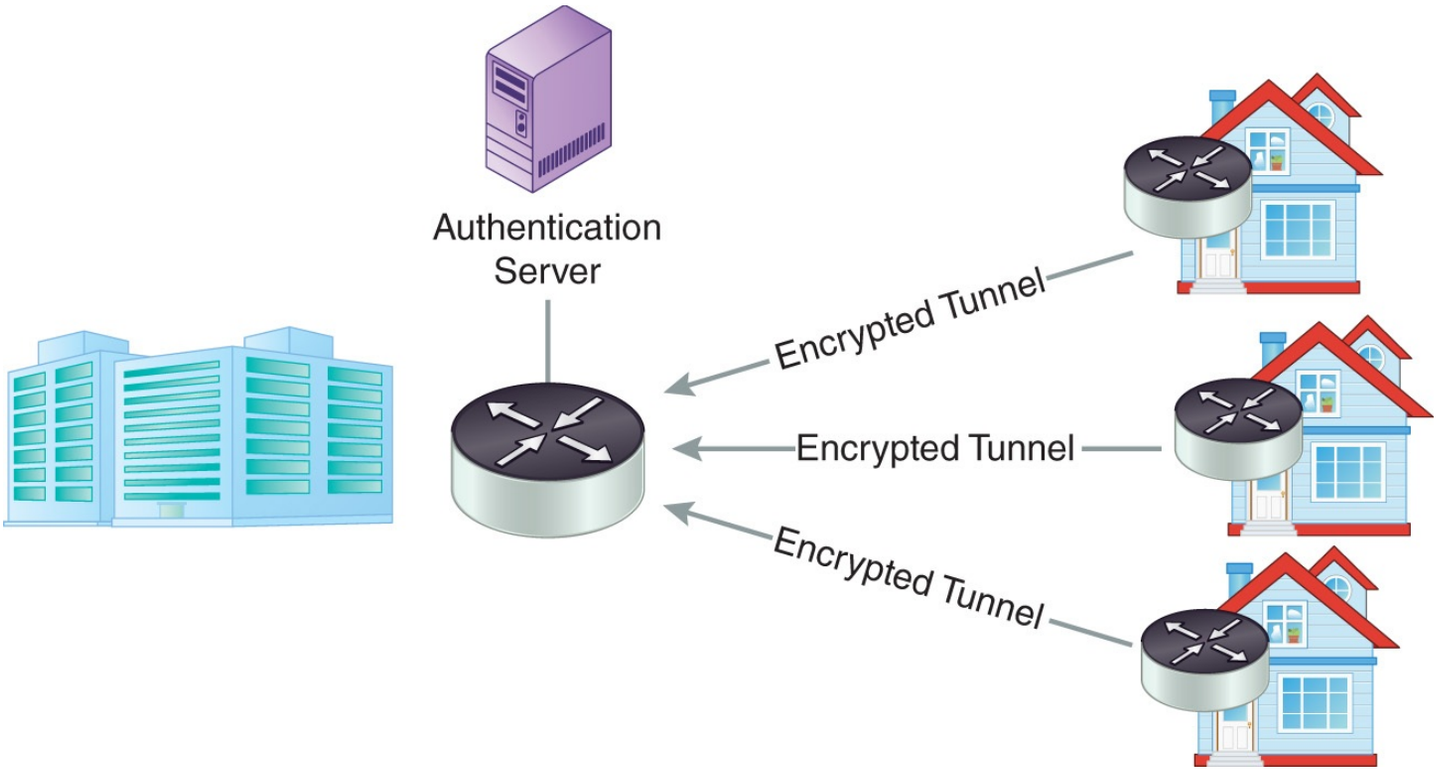

FIGURE 5-11 VPN access.

VPNs require gateway equipment with high processing power to handle the encryption algorithms. You can offload this processing power to another device by using a dedicated VPN concentrator rather than having the router or firewall terminate the VPN.

In deploying a VPN, the security of the end users' computers must be considered because, once users connect to the corporate network, their computers could be open portals into those resources for an attacker who gains access to them. For this reason, many organizations require that employees install security software on their home computers as well as limiting VPN access to laptop computers that the organization owns and manages.

Following are the major VPN technologies in use today:

- **Point-to-Point Tunneling Protocol (PPTP)**—The PPTP was once the predominant VPN protocol and almost all VPNs used it. It is easy to set up on client computers because most operating systems include PPTP support.
- **Secure Sockets Layer (SSL)/Transport Layer Security (TLS)**—The **Secure Sockets Layer (SSL)/Transport Layer Security (TLS)** protocol encrypts web communications, and many VPNs use it. Users connect to an SSL/TLS-protected webpage and log on. Their web browser then downloads software that connects them to the VPN. This setup requires no advance configuration of the

system. For this reason, SSL/TLS VPNs are quickly growing in popularity.

- **Secure Socket Tunneling Protocol (SSTP)**—Microsoft's SSTP is available only for the Windows operating system. This protocol is a more modern approach to VPNs that route traffic over SSL, which makes it easy to set up VPN connections that can go through firewalls and proxy servers.
- **Internet Protocol Security (IPSec)**—**Internet Protocol Security (IPSec)** is a suite of protocols designed to securely connect sites. Although some IPSec VPNs are available for end users, they often require the installation of third-party software on the user's system and, therefore, are not popular. The required IPSec VPN functionality is built into many routers and firewalls, allowing for easy configuration.
- **OpenVPN**—OpenVPN is an open source VPN protocol that is available for most current operating systems. It uses SSL/TLS for its preshared key exchange process and then sets up a tunnel for communication. Two versions are available, OpenVPN TCP and OpenVPN UDP, to support the two most common transport protocols.

VPNs provide clear benefits to an organization by offering an inexpensive, secure replacement for dedicated connections between sites and enabling users to connect securely to the organization's network from remote locations. Being able to securely connect from remote locations promises increased productivity because workers can easily get to resources they need while on the road.

Network Access Control

Network access control (NAC) systems enable you to add more security requirements before allowing a device to connect to a network. These systems perform two major tasks—authentication and posture checking—and work on both wired and wireless networks. Although NAC is a new technology, it is growing in popularity, and many organizations now deploy NAC for both internal users and guests using their network.

The IEEE 802.1x, commonly referred to as simply 802.1x or 1x, standard governs how clients, through the authentication component of NAC, may interact with a NAC device to gain entry to the network. The authentication process involves software on users' computers that prompts them to log on to the network. After verifying the users' credentials, the NAC device then instructs the switch (for a wired network) or access point (for a wireless network) to grant the user access to the network.

Posture checking is an optional second use of NAC technology. When posture checking is used, the NAC device checks the configuration of the user's computer to ensure that it meets security standards before allowing it access to the network. Following are some things commonly checked:

- Up-to-date antivirus software
- Host firewall enabled
- Operating system supported
- Operating system patched

If a user attempts to connect a noncompliant system to a network, the NAC device offers two options: either the administrator can decide to block such systems from the network until they are fixed, or the system can connect to a special quarantine network where it can be fixed before gaining access to the main network. One of the most common protocols that NAC devices use to authenticate devices is the **Extensible Authentication Protocol (EAP)**. EAP is an authentication framework, not a specific protocol implementation, that defines the transport of keys and authentication credentials used by other protocols, such as wireless network authentication, and exists in several variations. Such variations include EAP Flexible Authentication via Secure Tunneling (EAP-FAST), which is an EAP extension that sets up a secure tunnel to protect the authentication process; EAP Transport Layer Security (EAP-TLS), which uses TLS to secure authentication credentials; EAP Tunneled Transport Layer Security (EAP-TTLS), which extends TLS to create a tunnel for authentication; and the Protected Extensible Authentication Protocol (PEAP), which is basically EAP running in a TLS tunnel but providing more security than EAP for authentication exchanges.

Voice and Video in an IP Network

Historically, homes and businesses communicated with the rest of the world using telephone lines, the endpoints of which could be standard telephones, fax machines, modems to support computer communications, and voice/video devices for multimedia communication. Regardless of the endpoint device being used, the device would connect to the public switched telephone network to communicate with some remote endpoint. Security primarily consisted of stopping attackers from making calls without paying for them or severing connections. Because all telephone line connections were leased from a communication company, attackers making unauthorized calls could cost an organization large amounts of money.

As LANs and the Internet became more commonplace, organizations began to replace traditional phone systems with devices that use IP networks to

communicate. Many of today's businesses use their IP networks for voice and video calls, the cost of which can be reduced by replacing traditional phone lines with Voice over IP (VoIP) software and services. Though VoIP is not free, it can be far less costly than leasing traditional phone lines.

The Session Initiation Protocol (SIP) establishes and manages connections between endpoints by setting the stage for a connection that VoIP or other media-related protocols can use to support audio and video calls. Although using an existing network for SIP/VoIP traffic can reduce phone line costs, doing so has several drawbacks: increases in traffic, service costs, and risk. Adding voice and video to an existing network increases that network's usage and can cause performance problems if the available bandwidth is insufficient to handle the traffic; implementing SIP/VoIP likely requires software and agreements with external service providers to carry the content outside the local environment and interface with the traditional telephone system; and, finally, SIP/VoIP traffic is subject to the same network attacks as any other network traffic.

Securing voice and video communications is essentially just like securing any other network traffic. However, there are a few steps that each organization should take to keep SIP/VoIP communications secure. Following are some of the best practices for securing SIP/VoIP:

- Patch all SIP/VoIP software and network component firmware.
- Use VLANs to separate voice and video from other network use (i.e., workstations and printers).
- Enforce encrypted VPN use for all remote access (including SIP/VoIP).
- Require end-to-end encryption for all voice or video calls using TLS or Secure Real-Time Transport Protocol (SRTP).
- Enforce strong authentication for all network users.
- Use firewalls to protect all SIP/VoIP devices and services.
- Harden all SIP/VoIP devices and software.