Chapter 59: Virtual Private Networks

Jim Harmening Cybersecurity & Risk Management, Illinois Commerce Commission, Chicago, IL, United States

Abstract

A VPN is a virtual network, built on top of existing physical networks, that can provide a secure communications mechanism for data and other information transmitted between two endpoints. Secure Sockets Layer (SSL) virtual private networks (VPN) provide secure remote access to an organization's resources. This chapter discusses the fundamental technologies and features of VPNs. It describes SSL and how it fits within the context of layered network security. Zero Trust VPNs (ZTNAs) have become more prevalent and should be considered for all new VPN deployments. It presents a phased approach to VPN planning and implementation that can help in achieving successful VPN deployments. It also compares the VPN technology with Internet Protocol Security (IPsec) VPNs and other VPN solutions. This information is particularly valuable for helping organizations to determine how best to deploy VPNs within their specific network environments. Because a VPN can be used over existing networks such as the Internet, it can facilitate the secure transfer of sensitive data across public networks. An SSL VPN consists of one or more VPN devices to which users connect using their web browsers. The traffic between the web browser and the VPN device is encrypted with the SSL protocol or its successor, the Transport Layer Security (TLS) protocol. This type of VPN may be referred to as either an SSL VPN or a TLS VPN. This chapter uses the term SSL VPN. SSL VPNs provide remote users with access to Web applications and client/server applications, and connectivity to internal networks. Despite the popularity of SSL VPNs, they are not intended to replace IPsec VPNs. The two VPN technologies are complementary and address separate network architectures and business needs. VPNs offer versatility and ease of use because they use the SSL protocol, which is included with all standard web browsers, so the client usually

does not require configuration by the user. VPNs also offer granular control for a range of users on a variety of computers, accessing resources from many locations.

Keywords

Integrated services digital network; Internet protocol; Internet protocol security; Leased lines; Local area networks; Private branch exchange; Public networks; Secure sockets layer; Transport layer security; Virtual private networks; Zero Trust VPNs; ZTNA

1. Introduction

With the incredible advance of the Internet, it has become more and more popular to set up virtual private networks (VPNs) within organizations. Several types of VPNs are typically employed. The first will connect two separate local area networks (LANs), in different locations, to each other; while the second is a single remote computer connecting through the Internet, back to the home network. VPNs have been around for many years and have branched out into more and more varieties (see [**Fig. 59.1**] for a high-level view of a VPN.) Once only the largest of organizations would utilize VPN technology to connect multiple networks over the Internet's “public networks,” but now VPNs are being used by many small businesses and individuals as a way to allow remote users access to their business networks from home or while traveling. Apple has VPN on by default for it's latest iPhones. Zero trust VPNs, also known as ZTNAs, have become more popular with the idea that we no longer trust a connection all the time. Many vendors including Cisco, Fortinet, Palo Alto, Zscaler, and CheckPoint have ZTNA solutions.

Authentication in network to network zero trust VPNs happens on a consistent basis and is accomplished through a device certificate. These device certificates should have a short life, under 1 year for most connections, but for more security conscience network managers every 3–6 months may be better, in order to protect against digital certificate theft. You should choose a reputable organization for purchasing your certificates. A few trusted certificate vendors are Entrust, DigiCert, and Trustwave. For individual users the authentication can be done through a

username and password combination or add multifactor authentication for a more secure connection. Using an authenticator app is the better way, but many people still use a text or email message. Although the authenticator app is the most secure form of multifactor authentication, any second factor is more secure than just a password. It is imperative to secure your digital certificates and monitor them for unauthorized access.

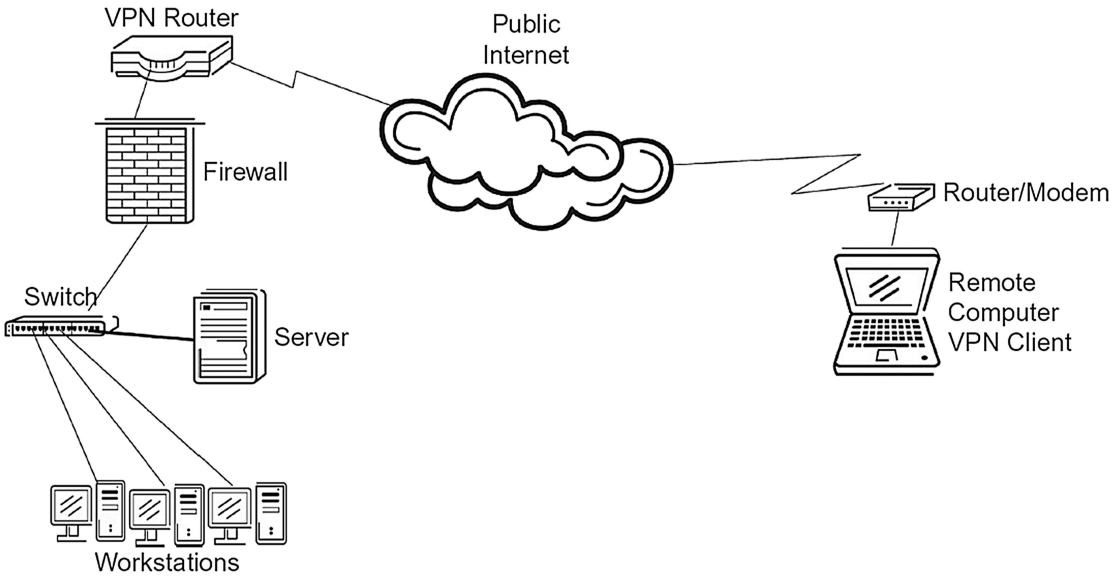

FIGURE 59.1 A high-level view of a virtual private network (VPN).

Consultants have changed their recommendations from dial-in systems and leased lines to VPNs for several reasons. Security concerns were once insurmountable, forcing the consultants to set up direct dial-in lines. Not that the public telephone system was much more secure but it gave the feeling of security and with the right setup, dial-in systems can approach very secure settings. Sometimes the dial-in systems utilized automatic callback options and had their own encryption methods. Now, with advanced security, including random-number generator logins, a network administrator is far more likely to allow access to their network via a VPN. High-speed Internet access is now the rule instead of the exception. In 2023, the FCC was working on getting even more of rural America connected to high-speed internet [1]. Costs have plummeted for the hardware and software to make the VPN connection as well. The proliferation of vendors, standardization of Internet Protocol (IP) networks, and ease of setup all played a role in the increasingly wide use and acceptance of VPNs.

The key to this VPN technology is the ability to route communications over a public network to allow access to office servers, printers, or data warehouses in an inexpensive manner. As high-speed Internet connections have grown and become prevalent throughout the world, VPNs over the public Internet have become common. Even inexpensive hotels are offering free Internet access to their customers. This is usually done through Wi-Fi connections, thus causing some concern for privacy, but the connections are available. Moreover, the iPhone, Android, Windows, Blackberry, and other multifunction web-enabled phones are giving mobile users access to the Internet via their phones. Some of the best ways to access the Internet are via a USB or wireless Hotspot from the major phone companies. These dedicated modem cards allow users to surf the Internet as long as they are in contact with the cell towers of their subscribing company.

Getting two computers to work together over the Internet is a difficult feat, but making two different computer networks be securely connected together via the public Internet is pure genius. By connecting different locations over the Internet, many companies cut out the cost of dedicated circuits from the phone companies. Some companies have saved thousands of dollars by getting rid of their Integrated Services Digital Network (ISDN) lines, too. Once thought of as the high-speed (128,000 bits per second, or 128 kb) Holy Grail, it is now a relic of the early 21st century. The ISDN lines are often referred to as glorified fast dial-up connections. Some companies utilize multiple ISDN connections to get dedicated higher-quality voice or video between two points, but similar to dial-up, you can dial into many different ISDN numbers and connect.

Not all VPNs had security in the early days. Packets of information were transmitted as clear text and could be easily seen. To keep the network systems secure, the information must be encrypted. Throughout the past 25 years, different encryption techniques have gained and lost favor. Some are too easy to break with the advanced speed of current computers; others require too much processing power at the router level, thus making their implementation expensive. This is one of those areas where an early technology seemed too expensive, but through time and technological advancements, the hardware processing power has caught up with requirements of the software. Encryption that seems secure in our

current environments is often insecure as time passes. With supercomputers doing trillions of computations a second, we are required to make sure that the technology employed in our networks is up to the task. There are many different types of encryption, as discussed later in this chapter.

Early in the VPN life-cycle, the goal for organizations was to connect different places or offices to remote computer systems. This was usually done with a dedicated piece of hardware at each site. This "point-to-point" setup allowed for a secure transmission between two sites, allowing users access to computer resources, data, and communications systems. Many of these sites were too expensive to access, so the advent of the point-to-point systems allowed access where none existed. Now multinational companies set up VPNs to access their manufacturing plants all over the world.

Accounting, order entry, and personnel databases were the big driving forces for disparate locations to be connected. Our desire to have more and more information and faster and faster access to information has driven this trend. Now individuals at home or on their cell phones are connecting into the corporate network either through VPN connections or Secure Sockets Layer (SSL)-VPN web connections. This proliferation is pushing vendors to increase security, especially in unsecure or minimally secure environments. Giving remote access to some users, unfortunately, makes for a target to hackers and crackers.

2. History

Like many innovations in the network arena, the telephone companies first created VPNs. AT&T, with its familiar "Bell logo" (see [**Fig. 59.2**]), was one of the leading providers of Centrex systems. The goal was to take advantage of different telephone enhancements for conferencing and dialing extensions within a company to connect to employees. Many people are familiar with the Centrex systems that the phone companies offered for many years.

FIGURE 59.2 AT&T logo; the company was often referred to as Ma Bell.

With Centrex the phone company did not require you to have a costly private branch exchange (PBX) switching computer system onsite. These PBXs were big, needed power, and cost a bundle of money. By eliminating the PBX and using the Centrex system, an organization could keep costs down yet have enhanced service and flexibility of the advanced phone services through the telephone company PBX.

The primary business of the phone companies was to provide voice service, but they also wanted to provide data services. Lines from the phone company from one company location to another (called leased lines) offered remote data access from one part of a company to another.

Many companies started utilizing different types of software to better utilize their leased lines. In the early days, the main equipment was located centrally, and all the offices connected to the "hub" (see [Fig. 59.3]). This

was a good system and many companies still prefer this network topography, but times are changing. The phone company usually charged for their circuits taking into consideration the distances between locations. With this in mind, instead of having a hub-and-spoke design, some companies opted to daisy-chain their organization together, thus trying to limit the distance they would have to pay for their leased lines. So, a company would have a leased line from New York to Washington, DC, another from DC to Atlanta, and a third from Atlanta to Miami. This would cut costs over the typical hub-and-spoke system of having all the lines go through one central location (see [**Fig. 59.4**]).

With the proliferation of the Internet and additional costs for Internet connections and leased-line connections, the companies pushed the software vendors to make cheap connections via the Internet. VPNs solved their problems and had a great return on investment (ROI). Within a year, the cost of the VPN equipment paid for itself through eliminating the leased lines. Though this technology has been around for years, some organizations still rely on leased lines due to a lack of high-speed Internet in remote areas.

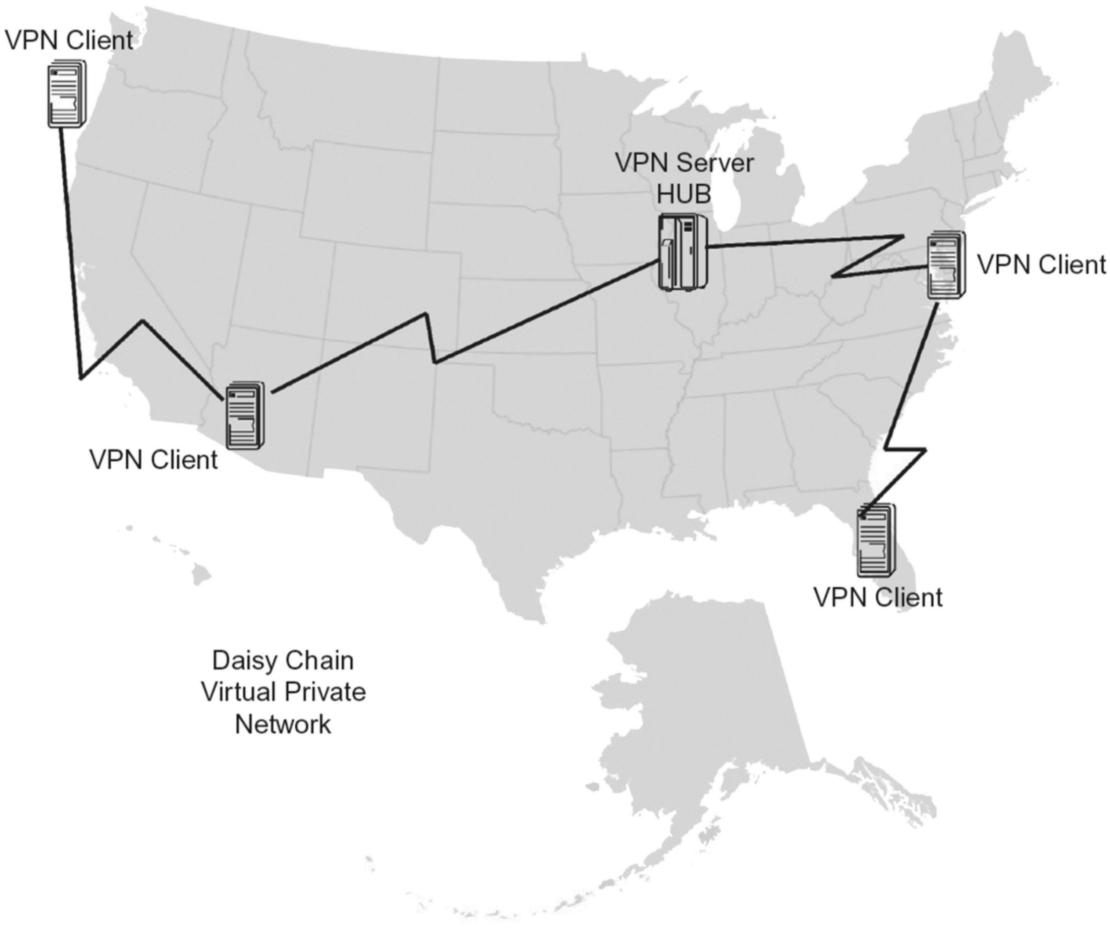

FIGURE 59.3 The hub in the early days.*VPN*, virtual private network.

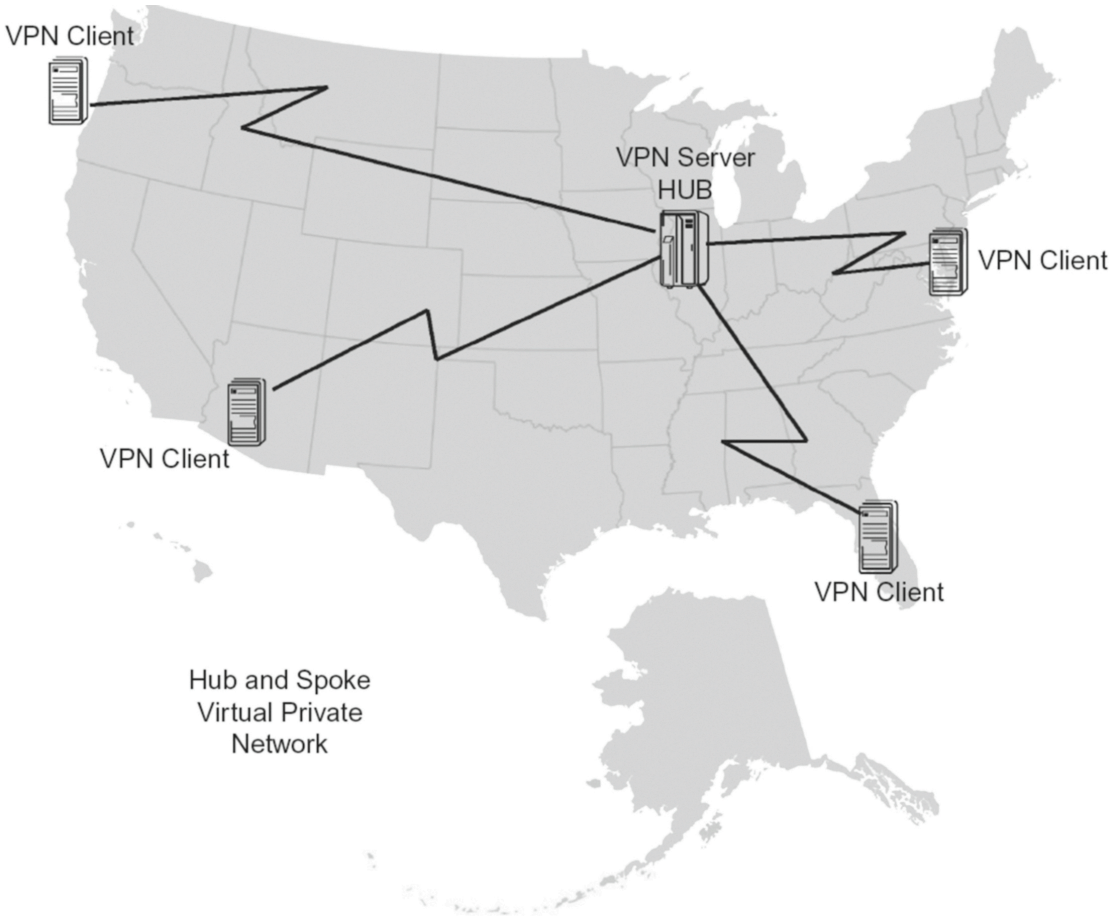

FIGURE 59.4 One central location for the hub-and-spoke system. *VPN*, virtual private network.

In 1995, Internet Protocol Security (IPsec) was one of the first attempts at bringing encryption to the VPN arena. One of the early downfalls of this technology was its complexity and requirement for fast processors on the routers to keep up with the high bandwidths. Fortunately, Moore's Law has been at work for decades, and today our processing speeds are high enough to get IPsec working on even phones and small routers. Moore's Law is named after Intel cofounder Gordon Moore, who wrote in 1965: “the number of transistors on a chip will double about every 2 years” [2]. This doubling of chip capacity allows for more and more computing to be done.

Another issue with early IPsec is that it is fairly inflexible, with differing IP addresses. Many home and home office computers utilize dynamic IP addresses. You may get a different IP address each time you turn on your computer and connect to the Internet. The IPsec connection will have to be reestablished and may cause a hiccup in your transmissions or the re-quirement that a password be reentered.

Another difficulty is the use of Network Address Translation (NAT) for some networks. Each computer on the network has the same IP address as far as the greater VPN Client Internet is concerned. This is in part because of the shortage of legal IP addresses available in the IPv4 address space. As we move closer and closer to the IPv6 or higher address space model, some of these issues will be moot. Soon, every device we own, including our refrigerators, radios, and heating systems, will have a static IP address. Maybe even our kitchen sinks will. Big Brother is coming, but won't it be cool to see what your refrigerator is up to? Want that ice cold beer a bit cooler, get on your smartphone and tell the refrigerator you are on your way!

In the late 1990s, Linux began to take shape as a great test environment for networking. A technology called tun, short for tunnel, allows data to be siphoned through the data stream to create virtual hardware. From the operating system perspective it looks like point-to-point network hardware, even though it is virtual hardware. Another technology, called tap, looks like Ethernet traffic and also uses virtual hardware to fool the operating system into thinking it is real hardware.

These technologies utilize a program running in the user area of the operating system software in order to look like a file. They can read and write IP packets directly to and from this virtual hardware, even though the systems are connected via the public Internet and could be on the other side of the world. Security is an issue with the tun/tap method. One way to build in security is to utilize the Secure Shell protocol (SSH) and transport the data via a User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) packet sent over the network.

It is important to remember that IP is an unreliable protocol. There are collisions on all IP networks; high traffic times give high collisions and lost packets, but the protocol is good at resending the packets so that eventually all the data will get to its destination. On the other hand, TCP is a reliable protocol. So, like military and intelligence, we have the added problem of a reliable transportation protocol (TCP) using an unreliable transportation (IP) method.

So, how does it work if it is unreliable? Well, eventually all the packets get there; TCP makes sure of that, and they are put in order and delivered to the other side. Some may have to be retransmitted, but most won't and the system should work relatively quickly.

One way that we can gain some throughput and added security is by utilizing encapsulation protocols. Encapsulation allows you to stuff one kind of protocol inside another type of protocol. The idea is to encapsulate a TCP packet inside a UDP packet. This forces the application to worry about dropped packets and reliability instead of the TCP network layer, since UDP packets are not a reliable packet protocol. This really increases speed, especially during peak network usage times. So, follow this logic: The IP packets are encrypted, then encapsulated and stored for transport via UDP over the Internet. On the receiving end the host system receives, decrypts, and authenticates the packets and then sends them to the tap or tun virtual adapter at the other end, thus giving a secure connection between the two sides, with the operating system not really knowing or caring about the encryption or transport methods. From the OS point of view, it is like a data file being transmitted; the OS doesn't have to know that the hardware is virtual. It is just as happy thinking that the virtual data file is real—and it processes it just like it processes a physical file locally stored on a hard drive.

OpenVPN is just one of many Open Source VPNs in use today. Use your favorite Internet search engine and you will see a great example of a VPN system that employs IPsec. IPsec is another way to ensure security on your VPN connection. IPsec took the approach that it needed to replace the IP stack and do it securely. IPsec looks to do its work in the background, without utilizing operating system CPU cycles. This is wonderful for its nonimpact on servers, but it then relies heavily on the hardware.

A faster-growing encryption scheme involves SSL VPN; we will talk about it later in this chapter. This scheme gives the user access to resources like a VPN but through a web browser. The end user only needs to install the browser plug-ins to get this type of VPN up and working, for remote access on the fly. One example of this SSL type of VPN is LogMeIn Rescue [3]. It sets up a remote control session within the SSL layer of the

browser. It can also extend resources out to the remote user without initiating a remote-control session.

Finally, the future for standardizing Transport Layer Security (TLS)-based, user-space VPNs is here to stay. With the ability to prevent eavesdropping before the transmissions begin, future VPN sessions will be even more secure. The current version is 1.3 and was released in 2018. With all these different schemes, we should take a look at who is in charge of helping to standardize the hardware and software requirements of the VPN world.

3. Who is in Charge?

For all this interconnectivity to actually work, there are several organizations that publish standards and work for cooperation among vendors in the sea of computer networking change. In addition to these public groups, there are also private companies that are working toward new protocols to improve speed and efficiency in the VPN arena.

The two biggest public groups are the Internet Engineering Task Force (**www.ietf.org**; see [**Fig. 59.5**]) and the Institute of Electrical and Electronic Engineers (**www.IEEE.org**; see [**Fig. 59.6**]). Each group has its own way of doing business and publishes its recommendations and standards.

As the IEEE website proclaims, the group's “core purpose is to foster technological innovation and excellence for the benefit of humanity” [**4**]. This is a wonderful and noble purpose. Sometimes they get it right and sometimes input and interference from vendors get in the way of moving technology forward—or worse yet, vendors go out and put up systems that come out before the specifications get published, leaving humanity with different standards. This has happened several times in the wireless networking standards group. Companies release their implementation of a standard prior to final agreement by the standards boards.

FIGURE 59.5 Logo for the Internet Engineering Task Force (IETF).

FIGURE 59.6 Logo for the Institute of Electrical and Electronics Engineers (IEEE).

The group's vision is stated thus: “IEEE will be essential to the global technical community and to technical professionals everywhere, and be universally recognized for the contributions of technology and of technical professionals in improving global conditions” [5].

The Internet Engineering Task Force (IETF) is a large, open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The IETF Mission Statement is documented in RFC 3935. According to the group's mission statement, “The goal of the IETF is to make the Internet work better” [6].

Finally, we can't get away from acronyms as we include the United States Government. An organization called the American National Standards Institute (ANSI; **www.ansi.org**) an over 90-year-old organization with responsibilities that include writing voluntary standards for the market-

place to have somewhere to turn for standardizing efforts to improve efficiencies and interoperability(see [**Fig. 59.7**]).

There are many standards for many physical things, such as the size of a light bulb socket or the size of an outlet on your wall. All of these groups help set standards for networking as well. Two international groups that are represented by ANSI are the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).

These organizations have ongoing workgroups and projects that are tackling the various standards that will be in use in the future releases of the VPN standard. They also have the standards written for current interoperability. However, this does **not** require a vendor to follow the standards. Each vendor can and will implement parts and pieces of standards, but unless they meet all the requirements of a specification, they will not get to call their system compatible.

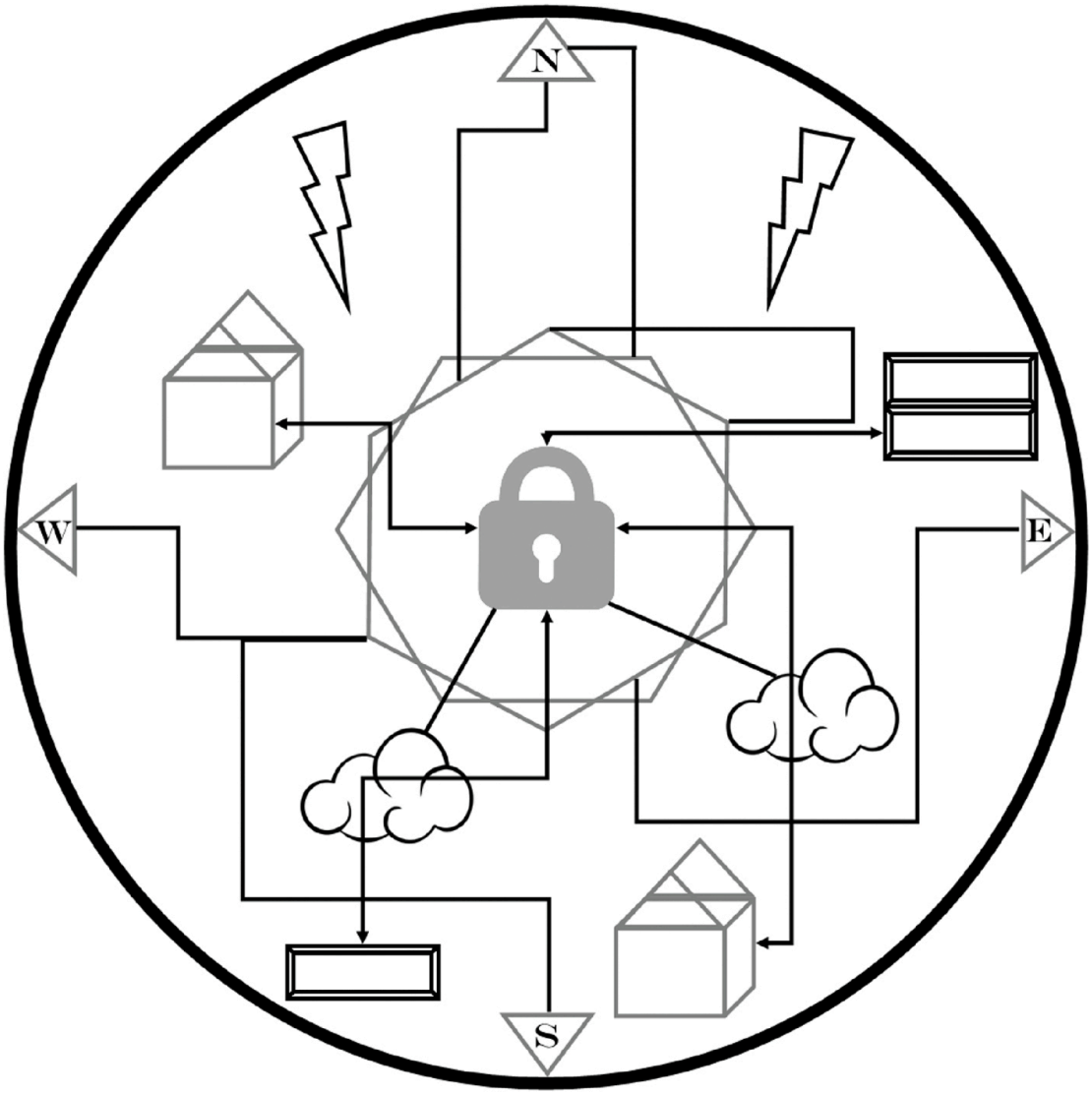

FIGURE 59.7 Interoperability.

There are several Institute of Electrical and Electronics Engineers (IEEE) projects relating to networking and the advancement of interconnectivity. If you are interested in networking, the 802 family of workgroups is your best bet. Check out **www.ieee802.org**.

4. Virtual Private Network Types

There are many different types of VPNs that rely on different transport protocols and different encryption standards. As our world continues to change and we have more and more cloud-based services, we will see VPNs as a default on devices from tablets to cell phones. When choosing a VPN, you should consider security, speed, and reliability. What type of data will be coming over your VPN? Are you using audio only? Or are you sending video too? Do you have large data files or are you doing remote

printing? Knowing the type of data you will be transporting is critical in picking the correct VPN type.

Internet Protocol Security

As we talked about earlier, this encryption standard for VPN access is heavy on the hardware for processing the encryption and decrypting the packets. This protocol operates at the Layer 3 level of the Open Systems Interconnection (OSI) model. The OSI model dates to 1982 by ISO [7]. IPsec is still used by many vendors for their VPN hardware.

One of the weaknesses of VPNs we mentioned earlier is also their strength. Because the majority of the processing work is done by the interconnecting hardware, the application doesn't have to worry about knowing anything about IPsec at all.

There are two modes for IPsec. First, the transport mode secures the information all the way to each device trying to make the connection. The second mode is the tunnel mode, which is used for network-to-network communications. The latest standard for IPsec came out in 2005. One of the downsides to IPsec is its complexity at the kernel level. With one buffer overflow, you can wreak havoc on the transmitted data.

Layer 2 Tunneling Protocol

Layer Tunneling Protocol was released in 1999; then to improve the reliability and security of Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) was created. It really is a layer 5 protocol because it uses the session layer in the OSI model. This was more cumbersome than PPTP and forced the users at each end to have authentication with one another. It also has weak security; thus, most implementations of the L2TP protocol utilize IPsec to enhance security.

There is a 32-bit header for each packet that includes flags, versions, Tunnel ID, and Session IDs. There is also a space for the packet size. Because this is a very weak protocol, some vendors combined it with IPsec to form L2TP/IPsec. In this implementation you take the strong, secure nature of IPsec as the secure channel, and the L2TP will act as the tunnel.

This protocol is a server/user setup. One part of the software acts as the server and waits for the user side of the software to make contact. Because this protocol can handle many users or clients at a time, some Asymmetric Digital Subscriber Line (ADSL) providers use this L2TP protocol and share the resources at the telephone central office. Their modem/routers utilize L2TP to phone home to the central office and share a higher capacity line out to the Internet.

For more information, see the **IETF.org** publication RFC8229. You can delve deeper into the failover mode of L2TP or get far more detail on the standard.

L2TPv3 or Higher

This is the draft advancement of the L2TP for large carrier-level information transmissions. In 2005, the draft protocol was released; it provides additional security features, improved encapsulation, and the ability to carry data links other than simply PPP over an IP network (Frame Relay, Ethernet, ATM). The L2TPv3 tunnel is established between two L2TP access concentrators (LACs). The LACs encapsulate Ethernet frames in L2TPv3 packets and send them over the IP network. The L2TP Network Server (LNS) expands the L2TPv3 packets and sends the Ethernet frames to the destination host. The L2TPv3 tunnel is established using the following steps:

1. The LACs exchange HELLO messages to negotiate the parameters of the tunnel.
2. The LACs exchange CONNECT messages to authenticate each other and establish the tunnel.
3. The LACs exchange ACK messages to acknowledge the establishment of the tunnel.
- Once the tunnel is established, the LACs can encapsulate and expand Ethernet frames as needed.

Layer 2 Forwarding

Cisco's Layer 2 Forwarding protocol is used for tunneling the link layer (layer 2 in the OSI model). This protocol allows for virtual dial-up that al-

lows for the sharing of modems, ISDN routers, servers, and other hardware.

This protocol was popular in the mid-to-late 1990s and was utilized by Shiva's products to share a bank of modems to a network of personal computers. This was a fantastic cost savings for network administrators wanting to share a small number of modems and modem lines to a large user group. Instead of having 50 modems hooked up to individual PCs, you could have a bank of eight modems that could be used during the day to dial out and connect to external resources, becoming available at night for workers to dial back into the computer system for remote access to corporate data resources.

For those long-distance calls to remote computer systems, an employee could dial into the office network. For security and billing reasons, the office computer system would dial back to the home user. The home user would access a second modem line to dial out to a long-distance computer system. This would eliminate all charges for the home user except for the initial call to get connected. RFC4301 on **IETF.org** gives you the detailed standard.

Point-to-Point Tunneling Protocol Virtual Private Network

PPTP was created in the 1990s by Microsoft, Ascend, 3COM, and a few other vendors, in order to try and serve the user community. This VPN protocol allowed for easy implementation with Windows machines because it was included in Windows. It made for fairly secure transmissions, though not as secure as IPsec. Although Microsoft has a great deal of influence in the computing arena, the IPsec and L2TP protocols are the standards-based protocols that most vendors use for VPNs.

Under PPTP, Microsoft has implemented Microsoft Point-to-Point Encryption (MPPE) Protocol, which allows encryption keys of 40–128 bits. The latest updates were done in 2003 to strengthen the security of this protocol. A great excerpt from Microsoft TechNet for Windows NT 4.0 or higher Server explains the process of PPTP extremely well; check out **http://technet.microsoft.com/en-us/library/cc768084.aspx** for more information.

Multiprotocol Label Switching

Multiprotocol Label Switching (MPLS) is another system for large telephone companies or huge enterprises to get great response times for VPN with huge amounts of data. This protocol operates between layer 2 and layer 3 of the OSI model we have mentioned before. The IETF web page with the specifications for the label switching architecture can be found RFC3031.

This protocol has big advantages over Asynchronous Transfer Mode (ATM) and Frame Relay communication protocols. The overhead is lower and with the ability to have variable length data packets, audio and video will be transmitted much more efficiently. Another big advantage over ATM is the ATM requirement that the two endpoints have to handshake and make a connection before any data is ever transmitted.

The name MPLS came from the underlying way in which the endpoints find each other. The switches using this technology find their destination through the lookup of a label instead of the lookup of an IP address. Label Edge Routers are the beginning and ending points of an MPLS network. The big competitor for future network expansion is L2TPv3 or higher.

Multipath Virtual Private Network

Ragula Systems Development Company created Multipath Virtual Private Network (MPVPN) to enhance the quality of service of VPNs. The basic concept is to allow multiple connections to the Internet at both endpoints and use the combination of connections to create a faster connection. So, if you have a T1 line and a DS3 at your office, you can aggregate both lines through the MPVPN device to increase your response times. The data traffic will be load balanced and will increase your throughput.

For a large network MPVPN is ideal, but other factors must be considered when deploying this architecture versus MPLS and L2TPv3. At the network layer only L2TP is Layer 2, while the others are Layer 3. MPLS and MPVPN are more scalable and reliable. All have good security and quality of service (QoS), while L2TPv3 is the easiest to deploy and manage.

Secure Shell Protocol

This protocol lets network traffic run over a secured channel between devices. SSH uses public-key cryptography. Tatu Ylőnen from Finland created the first version of SSH in 1995 to thwart password thieves at his university network. The company he created is called SSH Communications Security and can be reached at **www.ssh.com** (see [**Fig. 59.8**]).

Utilizing public-key cryptography is a double-edged sword. If an inside user authenticates an attacker's public key, you have just let them into the system, where they can deploy man-in-the-middle hacks. Also, the intent for this security system was to keep out the bad guys at the gate. Once a person is authenticated, she is in and a regular user and can deploy software that would allow a remote VPN to be set up through the SSH protocol. Future versions of SSH may prevent these abuses.

FIGURE 59.8 Secure Shell (SSH) communications security logo.

Secure Socket Layer Virtual Private Network

SSL VPN isn't really VPN at all. It's more of an interface that gives users the services that look like VPN through their web browsers. There are many remote-control applications that take advantage of this layer in the web browser to gain access to users' resources. It is sometimes referred to as a Hybrid VPN. This type of VPN is usually the most expensive to implement because it allows for many different types of clients and servers to be connected together.

Transport Layer Security

TLS, the successor to SSL, is used to prevent eavesdropping on information being sent between computers. When using strong encryption algorithms, the security of your transmission is almost guaranteed. The latest

version is 1.3 released in August of 2018. TLS 1.4 is being worked on as of 2023.

Both SSL and TLS work very much the same way. First, the sessions at each endpoint contact each other for information about what encryption method is going to be employed. Second, the keys are exchanged. These could be (Ron Rivest, Adi Shamir, and Leonard Adleman) RSA, elliptic curve Diffie–Hellman (ECDH), security rollup package (SRP), or preshared key.

Finally, the messages are encrypted and authenticated, sometimes using Certificate of Authorities Public Key list. When you utilize SSL and TLS you may run into a situation where the server certificate does not match the information held in the Certificate of Authorities Public Key list. If this is the case, the user may override the error message or may choose not to trust the site and end the connection.

The whole public key/private key encryption is able to take place behind the scenes for a few reasons. During the beginning phase of the connection, the server, and requesting computer generate a random number. Random numbers are combined and encrypted using the private keys. Only the owner of the public key can unencrypt the random number that is sent using their private key.

TLS is growing every year. One of the limiting factors is the size of the hash value in the final message is truncated to 96 bits. So even though it could be using a 256 bit hash, the transmission cuts it to 96 bits. In the future we may see something that addresses this.

Datagram Transport Layer Security

Datagram Transport Layer Security is an implementation of TLS that allows for tunneling over UDP. It is used in OpenConnect VPN and Cisco's now unsupported AnyConnect VPN. OpenConnect was created in order to interface with Cisco's AnyConnect VPNs. Cisco has dropped its offering so the OpenConnect community developed an application that integrates into several routers; with a firmware upgrade the device can now route network traffic using the VPN protocol. It is also used in many other ap-

plications including gaming, video conferencing, file sharing, and voice over Internet Protocol (VOIP). The largest companies in the world use this including Amazon, Google, Microsoft, Apple, and Facebook.

5. Authentication Methods

Currently, usernames and passwords are the most common authentication method employed in the VPN arena. There is increasing pressure to include digital certificates and multifactor authentication to ensure a more secure login. We may transport the data through an SSL channel or via a secured and encrypted transport model, but when it comes to gaining access to the system resources, most often you will have to log into the VPN with a simple username and password.

As we talked about earlier, there are some edge-based systems that require a dongle, and a random number is generated on gaining access to the login screen. These tiered layers of security can be a great addition that will thwart a hacker's attempt to gain access to your network system in favor of going after easier targets. Not all authentication methods are the same. We will talk about a few different types of protection schemes and point out weaknesses and strengths. With each type of encryption, we are concerned with its veracity along with concerns over the verification and authentication of the data being sent. Transmission speeds and overhead in encrypting and decrypting data are another consideration, but as mentioned earlier, Moore's Law has helped a great deal.

Hashing

Using a computer algorithm to mix up the characters in your encryption is fairly common. If you have a secret and want another person to know the answer, but you are fearful that it will be discovered, you can mix up the letters.

Hash Message Authentication Code

Keyed Hash Message Authentication Code (HMAC) is a type of encryption that uses an algorithm in conjunction with a key. The algorithm is only as

strong as the complexity of the key and the size of the output. For HMAC either 128 or 160 bits are used.

This type of Message Authentication Code (MAC) can be defeated. One way is by using the birthday attack. To ensure that your data is not deciphered, choose a strong key; use upper- and lowercase letters, numbers, and special characters. Also use 160 bits when possible.

Message Digest 5 (MD5)

Message Digest 5 is one of the best file integrity checks available today. It is also used in some encryption schemes, though the veracity of its encryption strength is being challenged.

The method uses a 128-bit hash value. It is represented as a 32-digit hexadecimal number. A file can be "hashed" down to a single 32-digit hex number. The likelihood of two files with the same hash is 2128 but with the use of rainbow tables and collision theory, there have been a few successes in cracking this encryption. As Tim Callan points out in his January 5, 2009 blog post, "Considering that it took the original researchers four tries over at least a month to successfully accomplish their attack against the RapidSSL brand, we're fully confident that no malicious organization had the opportunity to use this information against RapidSSL, or any other certificate authority authorized by VeriSign."

Secure Hash Algorithm

Secure Hash Algorithm was designed by the US National Security Agency (NSA). There is also SHA-224, SHA-256, SHA-384, and SHA-512. The number of bits in SHA-1 is 160. The others have the number of bits following the SHA. SHA-2 and SHAA-3 have up to 512 bits, while SHA-3 is much stronger and resistant to quantum computing algorithms. SHA-1 is compromised. The basic premise is the same as the MD5 hash: The data is encrypted utilizing a message digest. This method is the basis for several common applications including SSL, PGP, SSH, S/MIME, and IPsec.

NIST announced Keccak as the winner of the SHA-3 Cryptographic Hash Algorithm Competition on October 2, 2012 Check the NIST website [8] at

http://csrc.nist.gov/groups/ST/hash/sha-3/index.html for details about the 5-year competition. SHA-3 is described by some as a sponge. Data gets absorbed into the sponge on the sending end and then ringed out on the other end. For those who are interested in encryption you can check the NIST site for more information.

6. Symmetric Encryption

Symmetric encryption requires that both the sender and receiver have the same key and each computes a common key that is subsequently used. Two of the most common symmetric encryption standards are known as Data Encryption Standard (DES) and Advanced Encryption Standard (AES). Once AES was released, DES was withdrawn as a standard and replaced with 3-DES, often referred to as Triple DES and TDES.

3DES takes DES and repeats it two more times. So, it is hashed with the 56-bit algorithm and password, and then done twice more. This prevents more brute-force attacks, assuming a strong key is used. Some VPN software is based on these symmetric keys, as we have discussed before.

Finally, a system of shared secrets allows encryption and decryption of data. This can either be done as a preshared password, which is known by both ends prior to communication, or some kind of key agreement protocol where the key is calculated from each end using a common identifier or public key.

7. Asymmetric Cryptography

The biggest example of asymmetric cryptography for VPNs is in the RSA protocol. Three professors at MIT, Ron Rivest, Adi Shamir, and Leonard Adelman (thus RSA), came up with the RSA encryption algorithm, which is an implementation of public/private key cryptography. The RSA protocol is one of the coolest and most secure means of transmitting data. Not only is it used for transmission of data but a person can also digitally sign a document with the use of RSA secure systems.

Although these systems have been around for a while, they are becoming more and more prevalent. For example, some states will allow accoun-

tants who sign up with them to transmit income tax forms electronically as long as they digitally sign the returns. The federal government also allows electronic signatures and passed the E-SIGN Act, Public Law No. 106–229 in June of 2000.

The RSA algorithm uses two large random prime numbers. Prime number searching has been a pastime for many mathematical scientists. As the prime number gets larger and larger, its use for privacy and security systems is increased. Thus, many search for larger prime numbers. Through the use of these numbers and a key, the data is secured from prying eyes. Key sizes are growing and 4096 bit keys are becoming common in 2023. Quantum resistant algorithms are already being deployed in RSA as well. A big improvement in efficiency has allowed even video streaming services to utilize large keys and very secure communications.

When you are in a public system and don't have the luxury of knowing the keys in advance, there are ways to create a key that will work. This system is very interesting and is known as the exponential key exchange because it uses exponential numbers in the initial key exchange to come to an agreed-on cipher.

8. Edge Devices

As with any system, having two locked doors is better than one. With the advent of many remote computing systems, a new type of external security has come into favor. For instance, the setting up of an edge device allows for a unique username and password, or better yet, a unique username and a random password that only the user and the computer system knows.

FIGURE 59.9 Example of a QR code.

These edge systems often employ authentication schemes in conjunction with a key fob that displays a different random number every 30–60 s. The server knows what the random number should be based on the time and only authenticates the person into the edge of the network if the username and password match. Once into the edge network, the user is prompted for a more traditional username and password to gain access to data, email, or applications under his username.

Another popular implementation of a two-step encryption system is Google Authenticator. Based upon IETF RFC6238, the application utilizes HMAC-SHA-1 (HOTP algorithm) along with a time difference (TOTP algorithm) and HMAC-SHA-256 or HMAC-SHA-512 in order to get a six-digit number as a secondary key to gain access in the two-step passwords. The Time difference is unique and only known by the originating application and thus ensuring a random number. We all know that the SHA-256 is 64

digits long and SHA-512 is 128 digits long. The algorithm only takes six digits in order to make it reasonable for a person to enter.

After logging into the Edge device for the first time, a picture of a three-dimensional QR code (see [**Fig. 59.9**]) is displayed on the screen, using the Google Authenticator application, you scan the code and get your six-digit number for your one-time use password. You can download the application to your phone or computer in order to set up a system for a secondary single-use password for online applications that utilize a secondary one-use password. Examples of sites utilizing Authenticator include **Salesforce.com**, **Microsoft.com**, Barracuda SSL VPN, and Amazon Web Services.

9. Passwords

Your system and data are often only as good as the strength of your password. The weakest of passwords entails a single word or name. An attacker using common dictionary attacks will often break a weak password. For example, using the word password is usually broken very quickly.

Using multiple words or mixing spelling and upper and lowercase will make your weak password a bit stronger. PasswOrd would be better than password. Adding numbers increases your passwords veracity. P2ssw9rd decreases your chance of getting hacked. Add in a few special characters and your password gets even more secure, as with P2#$w9rd.

But to get even stronger you need to use a password over 12 characters made up of upper and lowercase letters, numbers, and special characters: P2#$w9rd.34HHlz. Stay away from acronyms. There are even some systems that don't allow any word from the English language to be used in any part of the password. To organize your passwords, it is always good to use a password manager. One very good password protects your vault of passwords. The password manager can assign random passwords to your websites that are very long and very strong.

Another way to keep your VPNs secure is to only allow access from fixed IP addresses. If the IP address isn't on the allowable list, you don't allow

the computer in, no matter what. There is a unique MAC address for each network card. This is another fixed ID that can be used to allow or disallow computers onto your VPN. The problem with this method is that both IP and MACs can be spoofed. So, if a person gets his hands on a valid MAC ID, he can get around this bit of security.

Some VPN systems will allow you to log in with a username and password, and then it will connect to a predefined IP address. So even if your passwords are stolen, unless the person knows the predefined IP address of the callback, they can't get into your system. This idea is a throwback to the dial-in networks that would allow a person to dial in, connect with their username and password, and then promptly disconnect and call the person's computer system back. It was an extra 2 min on the front end, but a great added level of security.

Finally, biometrics are playing a role in authentication systems. For example, instead of a password, your fingerprint may be used. Some systems use voiceprint, hand geometry, retinal eye scan, or facial geometry. I am not a fan of biometrics as once they are stolen, you can't get them back or change them. Also, high-definition cameras can capture fingerprints from a distance. I can foresee the day when a DNA reader uses your DNA as your password. Like a bloodhound who is able to follow you by the scent of the dead skin falling off your body, a sniffer device may be employed to analyze the DNA falling off your body. Homeland Security already has a commercial Rapid DNA product that can test DNA samples in 90 min.

10. Security Tips for VPN Systems

One of the inherent problems with remote access is security. Some good ways to prevent hackers and crackers from getting into your system are to enable the best security levels that your hardware has to offer. If you can utilize 2048 or 512-bit encryption methods, then use them. If you can afford a random-number generated edge security system, then use it.

Have your users change their VPN passwords regularly, 6 months or less, especially if they are utilizing public Internet portals. Long passwords are better than short. Don't expect your local library or Starbucks to have the security that you desire. If you access your VPN from an insecure public

Internet hotspot, then make sure you change your VPN password afterward. Don't give out your VPN password for other people to use. This can cause you great difficulties if something sinister happens to the network and the connection is traced back to your account.

Another way to secure your network is to deactivate accounts that have not been used for 30 days. Yes, this can be a pain, but if a person is not regularly accessing the system, then maybe they don't need access in the first place.

Finally, remove stale VPN accounts from the system. One of the biggest problems with unauthorized VPN access is the employee who has retired but their account never got disabled. Maybe their logon and email were removed, but IT didn't remove their VPN account. Put in checks and balances on accounts.

11. Mobile Virtual Private Networks

We have become a mobile computing society. We have smartphones, iPads, Android Tablets, netbooks, laptops, and cars, just to name a few of the things we carry that can connect to the Internet. With this connectivity comes challenges to the VPN world. Having a policeman or fireman connected back to the station's computers while on the road can cause subnets to change, cell towers to change, phone carriers to change. Not only the speed of your transmission but also the protocol for the telecommunications service. Imagine having to deal with this, all while keeping a secure data connection to the office. Some vehicles are even equipped with radios that can transmit data through their own private network. Or the health professional who does well-care or sick care visits throughout the community and needs to enter information about their visit as they go. How does the VPN keep the connection alive, let alone keep it secure?

Host Identity Protocol (HIP) is the technology now being employed to keep us connected on our mobile devices. IETF standard RFC7401 for Host Identity Protocol version 2 (HIPv2) will guide you to the details of this protocol. Each vendor uses this technology a little bit differently. But the market has pushed them to better conform.

The basic premise is to have the tunnel bound to an IP address that is static on the mobile device, that static IP is used even though the tunnels change and go through different subnets and even different carriers. The VPN software does all the security and handshaking when the changes occur, thus leaving the user free to think they have a steady connection no matter where they are traveling.

Think of some of the security risks as well as the speed problems. This harkens back to the days where an application had to be written with transmission speeds in mind—think more text, less graphics. Think reusable graphics on different form pages, so the browser doesn't have to download them each time a page is changed. Now we have people flying at 400-plus miles an hour in an airplane with full access to the internet. Some airlines are planning free offerings in 2024.

Finally, let's briefly look at VPN deployments. Organizations planning VPN deployments should identify and define requirements and evaluate several products to determine their fit into the organization.

12. Virtual Private Network Deployments

VPN products vary in functionality, including protocol and application support. They also vary in breadth, depth, and completeness of features and security services. Some recommendations and considerations are included the following checklist: “An Agenda For Action For VPN Deployments.”

An Agenda for Action for Virtual Private Network Deployments

Some of the cryptographic requirements, including allowable hash functions and certificate key lengths, have changed. Therefore, organizations who want to provide VPN services must ensure that their systems are upgradeable to the cipher suites and key lengths, and that their SSL VPN vendors guarantee that such upgrades will be available early enough for testing and deployment in the field. Thus, the following set of VPN deployments activities must be adhered to (check all tasks completed):

- 1. VPN manageability features such as status reporting, logging, and auditing should provide adequate capabilities for the organization to effectively operate and manage the SSL VPN and to extract detailed usage information.
- 2. The SSL VPN high availability and scalability features should support the organization's requirements for failover, load balancing, and throughput.
- 3. State and information sharing is recommended to keep the failover process transparent to the user.
- 4. VPN portal customization should allow the organization to control the look and feel of the portal and to customize the portal to support various devices such as personal digital assistants (PDA) and smartphones.
- 5. SSL VPN authentication should provide the necessary support for the organization's current and future authentication methods and leverage existing authentication databases.
- 6. VPN authentication should also be tested to ensure interoperability with existing authentication methods.
- 7. The strongest possible cryptographic algorithms and key lengths that are considered secure for current practice should be used for encryption and integrity protection unless they are incompatible with interoperability, performance, and export constraints.
- 8. SSL VPNs should be evaluated to ensure they provide the level of granularity needed for access controls.
- 9. Access controls should be capable of applying permissions to users, groups, and resources, as well as integrating with endpoint security controls.
- 10. Implementation of endpoint security controls is often the most diverse service among VPN products.
- 11. Endpoint security should be evaluated to ensure it provides the necessary host integrity checking and security protection mechanisms required for the organization.
- 12. Not all SSL VPNs have integrated intrusion prevention capabilities. Those that do should be evaluated to ensure they do not introduce an unacceptable amount of latency into the network traffic.

13. Summary

This chapter assisted organizations in understanding VPN technologies and in designing, implementing, configuring, securing, monitoring, deploying, and maintaining SSL VPN solutions. This chapter also provided a phased approach to VPN planning and implementation that can help in achieving successful SSL VPN deployments. It also provided a comparison with other similar technologies such as IPsec VPNs and other VPN technology solutions. Utilizing standard organization like IEEE, IETF, ANSI, and ISO will help you dig into the details of any VPN deployment.

Finally, let's move on to the real interactive part of this chapter: review questions/exercises, hands-on projects, case projects, and optional team case project. The answers and/or solutions by chapter can be found in **Appendix G**.

Chapter Review Questions/Exercises

True/False

1. True or False? All VPNs had security in the early days.
2. True or False? ATT, with its familiar “Bell logo,” was one of the leading providers of Centrex systems.
3. True or False? In the early days, the main equipment was located locally, and all the offices connected to the “hub.”
4. True or False? The encryption standard for VPN access is heavy on the hardware for processing the encryption and decrypting the packets.
5. True or False? Secure Socket Layer (SSL) VPN is really VPN.

Multiple Choice

1. What is another system for large telephone companies or huge enterprises to get great response times for VPNs with huge amounts of data?

- A. PPTP VPN
- B. L2F
- C. MPLS
- D. L2TPv3
- E. L2TP

2. What allows multiple connections to the Internet at both endpoints and use the combination of connections to create a faster connection?
   - A. MPLS
   - B. SSH
   - C. MPVPN
   - D. SSL-VPN
   - E. TLS
3. What is used to prevent eavesdropping on information being sent between computers?
   - A. SSL
   - B. TLS
   - C. RSA
   - D. ECDH
   - E. SRP
4. What are two of the most common authentication methods employed in the VPN arena?
   - A. Usernames
   - B. Encryption
   - C. Random numbers
   - D. Decryption
   - E. Passwords
5. What is a type of encryption that uses an algorithm in conjunction with a key?
   - A. MAC
   - B. HMAC
   - C. MD5
   - D. SHA-1
   - E. DES

Exercise

Problem

The problem described in this exercise is how do you connect remote users to a single main office. A medium-sized organization has a large population of users that work from remote locations once to several days each week. The organization is research-oriented, and many of these users require access to a broad range of internal IT resources to conduct

their research. These resources include email, calendar, file sharing services, and secure shell access on a variety of hosts. The organization already offers remote access services in the form of a host-to-gateway IPsec solution. This works successfully, but has required significant IT labor resources to install and support the client software on user machines. The current solution also does not provide remote access for users based in public locations such as hotels and kiosks. How does the organization implement a complementary remote access architecture?

Hands-on Projects

Project

A health care company formed from the merger of two large health care companies started to experience a succession of network stability issues. This was a big concern for the company. Strong network availability is a crucial business requirement for the company, as it predominantly operates in a moderate client environment. If users cannot connect to the central server, they cannot access either the applications or the data that are essential for them to do their jobs. After a competitive evaluation of multiple telecommunications services, what did the company decide to do with regards to replacing its existing point-to-point connections with a Virtual Private Network (VPN)?

Case Projects

Problem

This case study illustrates how a leading building construction company needed a highly scalable and flexible telecommunications solution. So, how would the company go about meeting all of its telecommunications requirements and ensure business continuity in order to back up its vital systems in the event of an unforeseen disaster?

Optional Team Case Project

Problem

An engineering company developed a site-to-site virtual private network (VPN). How was the company's VPN solution able to cut networking costs dramatically by integrating security applications with other platform components to create a tightly-integrated, multi-layer security perimeter?

References

1. *Federal Communications Commission (FCC)*. August 27, 2023. **https://www.fcc.gov/rbap**.
2. Intel Corporation. 2200 Mission College Blvd. RNB 4-148. Santa Clara, CA 95054, USA. **https://www.intel.com/content/www/us/en/history/virtual-vault/articles/moores-law.html?wapkw=moore%27s%20law**.
3. *LogMeIn a GoTo Company*. LogMeIn.com; August 27, 2023.
4. *Institute of Electrical and Electronics Engineers*. August 27, 2023. **https://www.ieee.org**.
5. *Institute of Electrical and Electronics Engineers*. August 27, 2023. **https://www.ieee.org/about/vision-mission.html**.
6. *Internet Engineering Task Force*. August 27, 2023.
7. ISO/IEC standard 7498-1:1994, Copyright 1994, **http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip**.
8. National Institutes of Science and Technology, August 27, 2023, **http://csrc.nist.gov/groups/ST/hash/sha-3/index.html**.