CHAPTER 15

Virtual Private Networks

A company with one main site and ten remote sites could buy ten T1 lines, one each from the central site to each remote office. A more cost-effective solution would be to use Frame Relay. However, especially because the remote sites often need access to the Internet, it is even more cost effective to simply connect each office to the Internet, and send traffic between sites over the Internet, using the Internet as a WAN.

Unfortunately, the Internet is not nearly as secure as leased lines and Frame Relay. For example, for an attacker to steal a copy of data frames passing over a leased line, the attacker would have to physically tap into the cable, oftentimes inside a secure building, under the street, or at the telco central office (CO); all of these actions can result in a jail sentence. With the Internet, an attacker can find less intrusive ways to get copies of packets, without even having to leave his home computer, and with a much smaller risk of getting carted off to jail.

Virtual private networks (VPN) solve the security problems associated with using the Internet as a WAN service. This chapter explains the concepts and terminology related to VPNs.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows you to assess whether you should read the entire chapter. If you miss no more than one of these six self-assessment questions, you might want to move ahead to the section "Exam Preparation Tasks." Table 15-1 lists the major headings in this chapter and the "Do I Know This Already?" quiz questions covering the material in those headings so that you can assess your knowledge of these specific areas. The answers to the "Do I Know This Already?" quiz appear in Appendix A.

Table 15-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions
VPN Fundamentals	1–2
IPsec VPNs	3–5
SSL VPNs	6

1. Which of the following terms refers to a VPN that uses the Internet to connect the sites of a single company, rather than using leased lines or Frame Relay?

    a. Intranet VPN

    b. Extranet VPN

    c. Access VPN

    d. Enterprise VPN

2. Which of the following are not considered to be desirable security goals for a site-to-site VPN?

    a. Message integrity checks

    b. Privacy (encryption)

    c. Antivirus

    d. Authentication

3. Which of the following functions could be performed by the IPsec IP Authentication Header?

    a. Authentication

    b. Encryption

    c. Message integrity checks

    d. Anti-reply

4. Which of the following is considered to be the best encryption protocol for providing privacy in an IPsec VPN as compared to the other answers?
   a. AES
   b. HMAC-MD5
   c. HMAC-SHA-1
   d. DES
   e. 3DES

5. Which three of the following options would be the most commonly used options for newly purchased and installed VPN components today?
   a. ASA
   b. PIX firewall
   c. VPN concentrator
   d. Cisco router
   e. Cisco VPN client

6. When using the Cisco Web VPN solution, with the client using a normal web browser without any special client software, which of the following are true?
   a. The user creates a TCP connection to a Web VPN server using SSL.
   b. If the user connects to a normal web server inside the enterprise, and that server only supports HTTP and not SSL, those packets pass over the Internet unencrypted.
   c. The Web VPN server connects to internal web servers on behalf of the Web VPN client, translating between HTTP and SSL as need be.
   d. The web VPN client cannot connect without at least thin-client SSL software installed on the client.

Foundation Topics

This chapter has three main sections. The first section introduces the basic concept of a VPN. The second (and largest) section examines some of the details of building VPNs using the rules defined in the IP Security (IPsec) RFCs. The last section explains the basics of an alternative VPN technology called SSL.

VPN Fundamentals

Leased lines have some wonderful security features. The router on one ends knows with confidence the identity of the device on the other end of the link. The receiving router also has good reason to believe that no attackers saw the data in transit, or even changed the data to cause some harm.

Virtual private networks (VPN) try to provide these same secure features as a leased line. In particular, they provide the following:

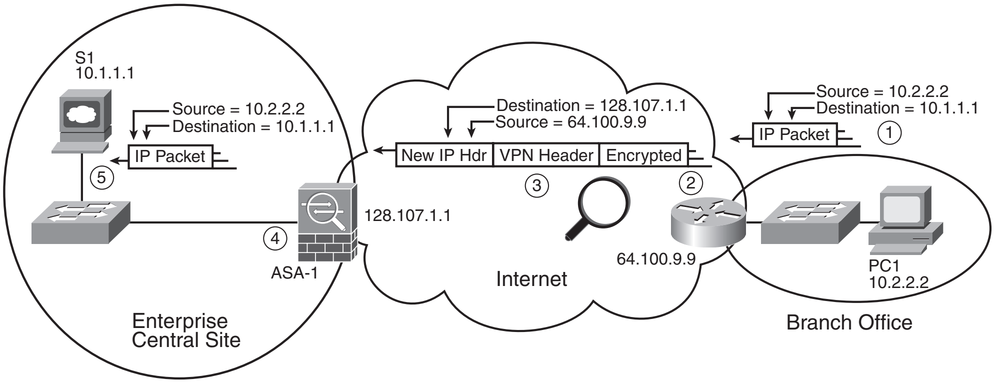
Key Topic

- **Privacy:** Preventing anyone in the middle of the Internet (man in the middle) who copies the packet in the Internet from being able to read the data
- **Authentication:** Verifying that the sender of the VPN packet is a legitimate device and not a device used by an attacker
- **Data integrity:** Verifying that the packet was not changed as the packet transited the Internet
- **Antireplay:** Preventing a man in the middle from copying packets sent by a legitimate user, and then later resending the packets to appear to be a legitimate user

To accomplish these goals, two devices near the edge of the Internet create a VPN, sometimes called a *VPN tunnel*. These devices add headers to the original packet, with these headers including fields that allow the VPN devices to perform all the functions. The VPN devices also encrypt the original IP packet, meaning that the original packet's contents are undecipherable to anyone who happens to see a copy of the packet as it traverses the Internet.

Figure 15-1 shows the general idea of what typically occurs with a VPN tunnel. The figure shows a VPN created between a branch office router and a Cisco Adaptive Security Appliance (ASA). In this case, the VPN is called a site-to-site VPN, because it connects two sites of a company, in particular. This VPN is also called site-to-site *intranet* VPN, because it connects sites that belong inside a single company.

Figure 15-1 *VPN Tunnel Concepts for a Site-to-Site Intranet VPN*



The figure shows the following steps, which explain the overall flow in the figure:

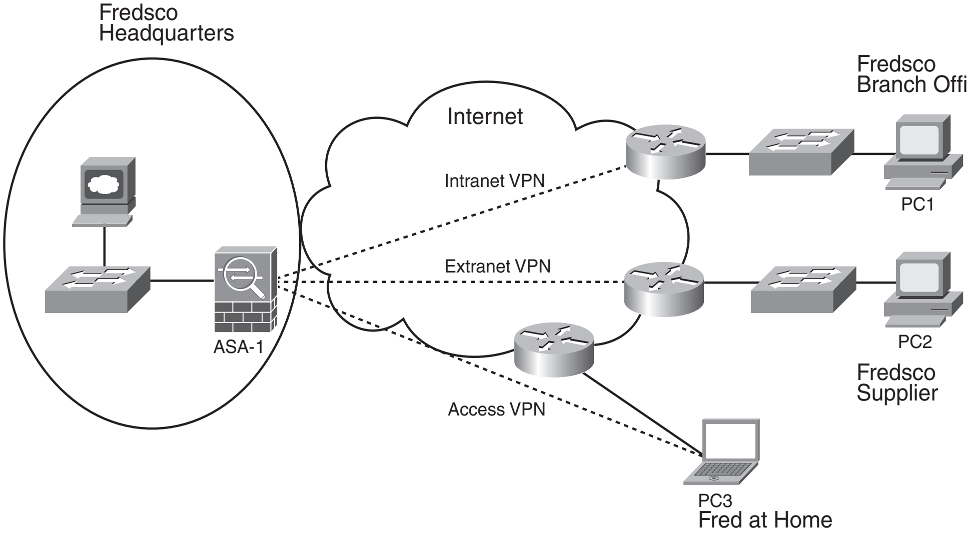
1. Host PC1 (10.2.2.2) on the right sends a packet to the web server (10.1.1.1), just as it would without a VPN.
2. The router encrypts the packet, adds some VPN headers, adds another IP header (with public IP addresses), and forwards the packet.
3. A man in the middle copies the packet but cannot change the packet without being noticed, and cannot read the contents of the packet.
4. ASA-1 receives the packet, confirms the authenticity of the sender, confirms that the packet has not been changed, and then decrypts the original packet.
5. Server S1 receives the unencrypted packet.

The benefits of using an Internet-based VPN as shown in Figure 15-1 are many. The cost of a high-speed Internet connection is typically much less than that of either a leased line or a Frame Relay WAN. The Internet is seemingly everywhere, making this kind of solution available worldwide. And by using VPN technology and protocols, the communications are secure.

NOTE The term *tunnel* generically refers to any protocol's packet that is sent by encapsulating the packet inside another packet. The term *VPN tunnel* implies that the encapsulated packet has been encrypted, whereas the term *tunnel* does not imply whether the packet has been encrypted.

VPNs can be built with a variety of devices and for a variety of purposes. Figure 15-2 shows an example of three of the primary reasons for building an Internet VPN today.

Figure 15-2 *Intranet, Extranet, and Access VPNs*



In the top part of the figure, the central site and a remote branch office of a fictitious company (Fredsco) are connected with an intranet VPN. The middle of the figure shows Fredsco connecting to another company that supplies parts to Fredsco, making that VPN an extranet VPN. Finally, when Fred brings his laptop home at the end of the day and connects to the Internet, the secure VPN connection from the laptop back into the Fredsco network is called a remote access VPN, or simply an access VPN. In this case, the laptop itself is the end of the VPN tunnel, rather than the Internet access router. Table 15-2 summarizes the key points about these three types of VPNs.

Key Topic

Table 15-2 *Types of VPNs*

Type	Typical Purpose
Intranet	Connects all the computers at two sites of the same organization, typically using one VPN device at each site
Extranet	Connects all the computers at two sites of different but partnering organizations, typically using one VPN device at each site
Access	Connects individual Internet users to the enterprise network

To build a VPN, one device at each site needs to have hardware and/or software that understand a chosen set of VPN security standards and protocols. The devices include the following:

- **Routers:** In addition to packet forwarding, the router can provide VPN functions as well. The router can have specialized add-on cards that help the router perform the encryption more quickly.
- **Adaptive Security Appliances (ASA):** The Cisco leading security appliance that can be configured for many security functions, including VPNs.
- **PIX firewalls:** The older product line of Cisco firewall products that can perform VPN functions in addition to working as a firewall. New installations today would instead use an ASA.
- **VPN concentrators:** An older product line from Cisco, these devices provide a hardware platform to specifically act as the endpoint of a VPN tunnel. New installations today would instead use an ASA.
- **VPN client:** For access VPNs, the PC might need to do the VPN functions; the laptop needs software to do those functions, with that software being called a *VPN client*.

Next, the text examines the use of a set of protocols called IPsec to create VPNs.

IPsec VPNs

IPsec is an architecture or framework for security services for IP networks. The name itself is not an acronym, but rather a shortened version of the title of the RFC that defines it (RFC 4301, *Security Architecture for the Internet Protocol*), more generally called IP Security, or IPsec.

IPsec defines a set of functions, for example, authentication and encryption, and some rules regarding each of those functions. However, like the TCP/IP protocol architecture defines many protocols, some of which are alternatives to each other, IPsec allows the use of several different protocol options for each VPN feature. One of IPsec's strengths is that its role as an architecture allows it to be added to and changed over time as improvements to security protocols are made.

The following sections examine the components of IPsec, beginning with encryption, followed by key exchange, message integrity, and authentication.

IPsec Encryption

If you ignore the math—and thankfully, you can—IPsec encryption is not too difficult to understand. IPsec encryption uses a pair of encryption algorithms, which are essentially math formulas, that meet a couple of requirements. First, the two math formulas are a matched set:

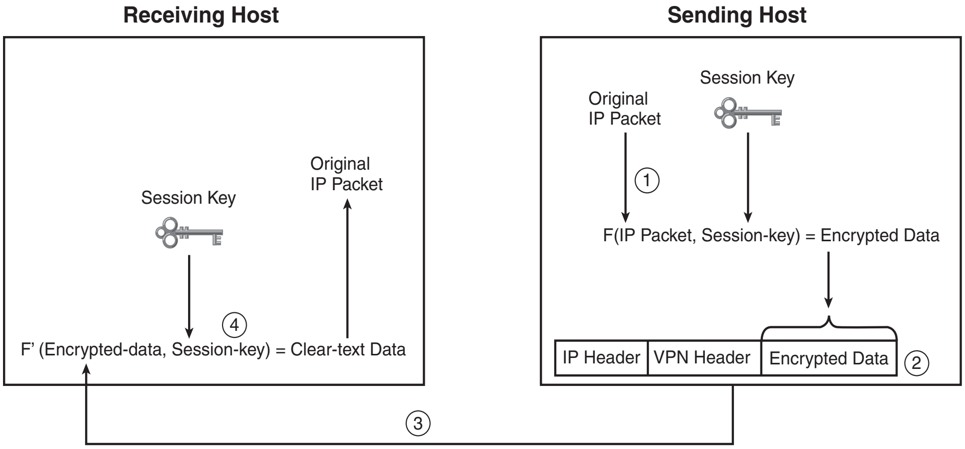
- One to hide (encrypt) the data
- Another to re-create (decrypt) the original data from the encrypted data

Besides those somewhat obvious functions, the two math formulas were chosen so that if you intercept the encrypted text, but do not have the secret password (called an encryption key), decrypting that one packet would be difficult. Additionally, the formulas are also chosen so that if an attacker did happen to decrypt one packet, that information would not give the attacker any advantages in decrypting the other packets.

The process for encrypting data for an IPsec VPN works generally as shown in Figure 15-3. Note that the encryption key is also known as the session key, shared key, or shared session key.

Key Topic

Figure 15-3 *Basic IPsec Encryption Process*



The four steps highlighted in the figure are as follows:

1. The sending VPN device (like the remote office router in Figure 15-1) feeds the original packet and the session key into the encryption formula, calculating the encrypted data.

2. The sending device encapsulates the encrypted data into a packet, which includes the new IP header and VPN header.
3. The sending device sends this new packet to the destination VPN device (ASA-1 back in Figure 15-1).
4. The receiving VPN device runs the corresponding decryption formula, using the encrypted data and session key—the same value as was used on the sending VPN device—to decrypt the data.

IPsec supports several variations on the encryption algorithms, some of which are simply more recently developed and better, while some have other trade-offs. In particular, the length of the keys has some impact on both the difficulty for attackers to decrypt the data, with longer keys making it more difficult, but with the negative result of generally requiring more processing power. Table 15-3 summarizes several of these options and the lengths of the keys.

Table 15-3 *Comparing VPN Encryption Algorithms*

Key Topic

Encryption Algorithm	Key Length (Bits)	Comments
Data Encryption Standard (DES)	56	Older and less secure than the other options listed here
Triple DES (3DES)	56 x 3	Applies three different 56-bit DES keys in succession, improving the encryption strength versus DES
Advanced Encryption Standard (AES)	128 and 256	Considered the current best practice, with strong encryption and less computation than 3DES

IPsec Key Exchange

The use of a shared common key value (also called symmetric keys) for encryption causes a bit of chicken-and-egg problem: If both devices need to know the same key value before they can encrypt/decrypt the data, how can the two devices send the key values to each over the network without having to send the keys as clear text, open to being stolen by an attacker?

The problem related to *key distribution* has existed since the idea of encryption was first created. One simple but problematic option is to use Pre-Shared Keys (PSK), a fancy term for the idea that you manually configure the values on both devices. With PSKs, you might just exchange keys by calling the engineer at the remote site, or sending a letter, or (don't do this at home) sending an unsecure e-mail with the key value.

The problem with PSKs is that even if no one steals the shared encryption key, it is only human nature that the PSKs will almost never change. It's like changing your password on a website that never requires you to change your password: You might never think about it, no one makes you change it, and you do not want to have to remember a new password. However, for better security, the keys need to be changed occasionally because even though the encryption algorithms make it difficult to decrypt the data, it is technically possible for an attacker to break a key, and then be able to decrypt the packet. Dynamic key exchange protocols allow frequent changes to encryption keys, significantly reducing the amount of lost data if an attacker compromises an encryption key.

IPsec, as a security architecture, calls for the use of *dynamic key exchange* through a process defined by RFC 4306 and called Internet Key Exchange (IKE). IKE (RFC 4306) calls for the use of a specific process called Diffie-Hellman (DH) key exchange, named after the inventors of the process. DH key exchange overcomes the chicken-and-egg problem with an algorithm that allows the devices to make up and exchange keys securely, preventing anyone who can see the messages from deriving the key value.

The primary configuration option for DH key exchange is the length of the keys used by the DH key exchange process to encrypt the key exchange messages. The longer the encryption key that needs to be exchanged, the longer the DH key needs to be. Table 15-4 summarizes the main three options.

Key Topic

Table 15-4 *DH Options*

Option	Key Length
DH-1	768-bit
DH-2	1024-bit
DH-5	1536-bit

IPsec Authentication and Message Integrity

IPsec has several options for the authentication and message integrity process as well. Authentication generally refers to the process by which a receiving VPN device can confirm that a received packet was really sent by a trusted VPN peer. Message integrity, sometimes referred to as message authentication, allows the receiver to confirm that the message was not changed in transit.

IPsec authentication and message integrity checks use some of the same general concepts as does the encryption and key exchange process, so this text does not go into a lot of detail. However, it is useful to understand the basics.

Message integrity checks can be performed by the IPsec Authentication Header (AH) protocol using a shared (symmetric) key concept, like the encryption process, but using a hash function rather than an encryption function. The hash works similarly to the frame check sequence (FCS) concept in the trailer of most data-link protocols, but in a much more secure manner. The hash (a type of math function), with the formal name of Hashed-based Message Authentication Code (HMAC), results in a small number that can then be stored in one of the VPN headers. The sender calculates the hash and sends the results in the VPN header. The receiver recomputes the hash, using a shared key (same key value on both ends), and compares the computed value with the value listed in the VPN header. If the two values match, it means that the data fed into the formula by the sender matches what was fed into the formula by the receiver, so the receiver knows that the message did not change in transit.

These integrity check functions with HMAC typically use a secret key that needs to be at least twice as long as the encryption key that encrypts the message. As a result, several HMAC options have been created over the years. For example, the long-supported message digest algorithm 5 (MD5) standard uses a 128-bit key, allowing it to support VPNs that use the 56-bit DES encryption key length.

NOTE If the VPN uses ESP to encrypt the packets, the HMAC message integrity function is not needed, because the attacker would have had to break the encryption key before she could have possibly altered the contents of the message.

The authentication process uses a public/private key concept similar to DH key exchange, relying on the idea that a value encrypted with the sender's private key can be decrypted with the sender's public key. Like the message integrity check, the sender calculates a value and puts it in the VPN header, but this time using the sender's private key. The receiver uses the sender's public key to decrypt the transmitted value, comparing it to the value listed in the header. If the values match, the receiver knows that the sender is authentic.

Table 15-5 summarizes a few of the specific protocols and tools available for IPsec authentication and message integrity.

Table 15-5 *IPsec Authentication and Message Integrity Options*

Function	Method	Description
Message integrity	HMAC-MD5	HMAC-MD5 uses a 128-bit shared key, generating a 128-bit hash value.
Message integrity	HMAC-SHA	HMAC–Secure Hash Algorithm defines different key sizes (for example, SHA-1 [160], SHA-256 [256], and SHA-512 [512]) to support different encryption key sizes. Considered better than MD5 but with more compute time required.
Authentication	Pre-Shared Keys	Both VPN devices must be preconfigured with the same secret key.
Authentication	Digital signatures	Also called Rivest, Shamir, and Adelman (RSA) signatures. The sender encrypts a value with its private key; the receiver decrypts with the sender's public key and compares with the value listed by the sender in the header.

The ESP and AH Security Protocols

To perform the VPN functions described in this chapter, IPsec defines two security protocols, with each protocol defining a header. These headers are shown in generic form back in Figure 15-1 as the VPN header. These headers simply provide a place to store information that is needed for the various VPN functions. For example, the message integrity process requires that the sender place the results of the hash function into a header and transmit the header (as part of the entire message) to the receiving VPN device, which then uses the value stored in that header to complete the message integrity check.

Two of the protocols defined by IPsec are the Encapsulating Security Payload (ESP) and the IP Authentication Header (AH). ESP defines rules for performing the main four functions for VPNs, as mentioned throughout this chapter and as summarized in Table 15-6. AH supports two features, namely, authentication and message integrity. A particular IPsec VPN might only use one of the two headers, or both. For example, AH could provide authentication and message integrity, with ESP providing data privacy (encryption).

Table 15-6 *Summary of Functions Supported by ESP and AH*

Key Topic

Feature	Supported by ESP?	Supported by AH?
Authentication	Yes (weak)	Yes (strong)
Message integrity	Yes	Yes
Encryption	Yes	No
Antireplay	Yes	No

IPsec Implementation Considerations

IPsec VPNs provide a secure connection through the unsecure Internet so that hosts can behave as if they are connected directly to the corporate network. For site-to-site VPNs, the end-user hosts have no idea that a VPN even exists, just as would be the case with a leased line or Frame Relay WAN. The user can use any application, just as if he were connected to the LAN at the main office.

IPsec remote access VPN users enjoy the same functions as do site-to-site VPN users, providing the user access to any and all allowed applications. However, remote access VPNs do require some additional effort in that each host needs to use the Cisco VPN client software. This software implements the IPsec standards on the PC, rather than requiring VPN support on a separate device. The installation is not difficult, but it is an additional bit of work for each host, whereas compared to a site-to-site VPN implemented with an already installed Cisco router, the only requirement might be an upgrade of the Cisco IOS.

To ease the installation and configuration of VPNs, Cisco provides a framework and a set of functions called *Easy VPN*. The problem solved by Easy VPN can be easily understood by considering the following example. A company has 200 remote sites with which it wants to create an intranet VPN using the Internet. Additionally, this company wants extranet site-to-site VPN connections to a dozen partners. Finally, 2000 employees own laptops, and they all at least occasionally bring home their laptops and connect to the enterprise network through the Internet. And, IPsec has many options for each function, requiring configuration at each site.

Easy VPN helps solve the administration headaches in such an environment by allowing a Cisco Easy VPN server, typically the central site VPN device (for example, an ASA), to dynamically inform the remote site devices as to their IPsec VPN configurations. The remote devices—routers, ASAs, laptops with Cisco VPN client software, and so on—act as Easy VPN clients, connecting to the Easy VPN server and downloading the configuration settings.

Next, the final section of this chapter briefly examines an alternative VPN technology called SSL.

SSL VPNs

Today's commonly used web browsers all support a protocol called *Secure Socket Layer (SSL).* These same browsers also typically support a follow-on but less-well-known standard called *Transport Layer Security (TLS).* This section explains how SSL can be used to create access VPNs.

NOTE Rather than refer to both SSL and TLS throughout this section, the text uses the more popular SSL term alone. SSL and TLS are not truly equivalent protocols, but they perform the same functions, and they are equal to the level of depth described in this chapter.

Web browsers use HTTP to connect to web servers. However, when the communications with the web server need to be secure, the browser switches to use SSL. SSL uses well-known port 443, encrypting data sent between the browser and the server, and authenticating the user. Then, the HTTP messages flow over the SSL connection.

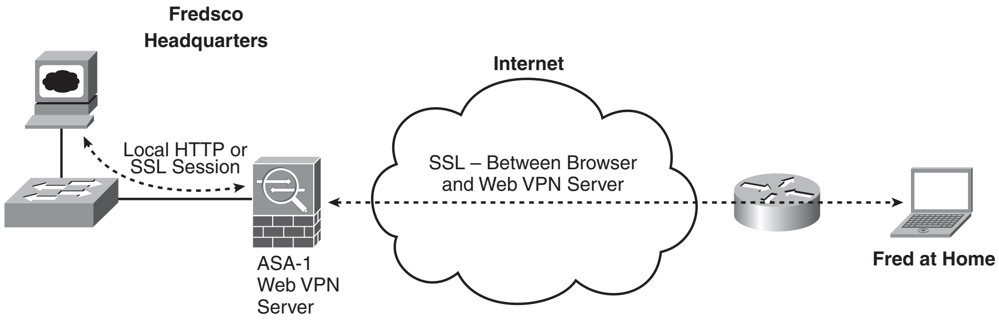
Most people have used SSL, oftentimes without knowing it. If you have ever used a website on the Internet, and needed to supply some credit card information or other personal information, the browser probably switched to using SSL. Most browsers show an icon that looks like a padlock, with the padlock open when not using SSL and the padlock closed (locked) when using SSL.

Web servers can choose when and how to implement SSL. Because SSL requires more work, many web servers just use HTTP for supplying general information, switching to use SSL only when the user needs to supply sensitive information, such as login credentials and financial information. However, when an enterprise's internal web servers need to send data to a home user on the other side of the Internet, rather than a user on the enterprise's local LAN, the server might need to secure all communications to the client to prevent the loss of data.

Cisco solves some of the problems associated with internal web access for Internet-based users with a feature called Web VPN. Unlike IPsec VPNs, Web VPN typically only allows web traffic, as opposed to all traffic. However, a large majority of enterprise applications today happen to be web-enabled. For example, most end users need access to internal applications, which run from internal web servers and possibly to an e-mail server. If a user can check her e-mail from a web browser, most if not all the functions needed by that user can be performed from a web browser, and Web VPN can provide a reasonable solution.

Web VPN secures an enterprise home user's connection to the enterprise network by using SSL between the end user and a special Web VPN server. Figure 15-4 shows the general idea.

Figure 15-4 *Web VPN Using SSL*


Fredsco Headquarters
Internet
Local HTTP or SSL Session
SSL – Between Browser and Web VPN Server
ASA-1 Web VPN Server
Fred at Home

To use Web VPN, the Internet-based user opens any web browser and connects to a Cisco Web VPN server. The Web VPN server can be implemented by many devices, including an ASA. This connection uses SSL for all communications, using the built-in SSL capabilities in the web browser, so that all communications between the client and the Web VPN server are secure.

The Web VPN server acts as a web server, presenting a web page back to the client. The web page lists the enterprise applications available to the client. For example, it might list all the typical enterprise web-based applications, the e-mail server's web-based server, and other web-based services. When the user selects an option, the Web VPN server connects to that service, using either HTTP or SSL, as required by the server. The Web VPN server then passes the HTTP/SSL traffic to and from the real server over the SSL-only connection back to the Internet-based client. As a result, all communications over the Internet are secured with SSL.

The strength of this Web VPN solution is that it requires no software or special effort from the client. Employees can even use their home computer, someone else's computer, or any Internet-connected computer, and connect to the host name of the Web VPN server.

The negative with Web VPN is that it only allows the use of a web browser. If you need to use an application that cannot be accessed using a browser, you have a couple of options. First, you could implement IPsec VPNs, as already discussed. Alternately, you could use a variation on Web VPN in which the client computer loads an SSL-based thin client, much in concept like the IPsec-based Cisco VPN client used with IPsec VPNs. The client computer could then connect to the Web VPN server using the thin client, and the Web VPN server would simply pass the traffic from the PC through to the local LAN, allowing access as if the client were connected to the main enterprise network.

Exam Preparation Tasks

Review All the Key Topics

Key Topic

Review the most important topics from this chapter, noted with the Key Topics icon in the outer margin of the page. Table 15-7 lists a reference of these key topics and the page numbers on which each is found.

Table 15-7 *Key Topics for Chapter 15*

Key Topic Element	Description	Page Number
List	Desired security features for VPNs	528
Table 15-2	Three types of VPNs and their typical purpose	530
Figure 15-3	Significant parts of the VPN encryption process	532
Table 15-3	Facts about the three IPsec VPN encryption algorithms for encrypting the entire packet	533
Table 15-4	Three DH key exchange options and key lengths	534
Table 15-6	Summary of functions supported by the IPsec ESP and AH protocols	537

Complete the Tables and Lists from Memory

Print a copy of Appendix J, "Memory Tables," (found on the CD) or at least the section for this chapter, and complete the tables and lists from memory. Appendix K, "Memory Tables Answer Key," also on the CD, includes completed tables and lists to check your work.

Definitions of Key Terms

Define the following key terms from this chapter, and check your answers in the glossary:

Diffie-Hellman key exchange, IPsec, shared key, SSL, VPN, VPN client, Web VPN