CHAPTER 12

IPsec Overview

IP Security, or IPsec, has been in use for a number of years now to protect sensitive data as it flows from one location to another. The evolution of corporate communications has changed the way that private data is exchanged and maintained. Most companies have distributed resources and personnel. It is important that corporate data remains private during transit. IPsec offers a standards-based mechanism to provide such secure data transmission.

Typically, IPsec is associated with Virtual Private Networks (VPN). A VPN creates a private connection, or network, between two endpoints. This is a virtual connection because the physical means of connectivity is indifferent to the safety of the data involved. IPsec adds a layer of protection to the data that travels across the VPN.

Many years ago, wide-area network (WAN) connections between branch offices was accomplished with point-to-point (p2p) circuits. A single port of a router at one site would connect, via a provider, to a single port of a router at a remote site. The introduction of X.25, ATM, and Frame Relay introduced the virtual circuit. With this technology, one router interface could have many virtual circuits, or connections, to many other sites.

Today, practically every site has Internet connectivity. Rather than lease a p2p or virtual circuit between sites across a carrier's network, most sites simply lease access to the Internet. The ability to send data packets from one location to another is simply a matter of knowing the destination IP address.

However, due to the "open" nature of the Internet, it is not considered safe to simply send packets from one site to another. IPsec is used as a means of safeguarding IP data as it travels from one site to another. Note that IPsec can be used on any type of connectivity—not just Internet links. But IPsec is predominantly used on data that traverses insecure or untrusted networks, such as the Internet.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you really need to read the entire chapter. If you already intend to read the entire chapter, you do not necessarily need to answer these questions now.

The 14-question quiz, derived from the major sections in the "Foundation Topics" portion of the chapter, helps you to determine how to spend your limited study time.

Table 12-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 12-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section	Score
IPsec	1–4	
Internet Key Exchange (IKE)	5–8	
Encryption Algorithms	9–12	
PKI	13–14	
Total Score		

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark this question wrong for purposes of self-assessment. Giving yourself credit for an answer that you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which layers of the OSI model can IPsec protect (select all that apply)?
   a. Layer 1—physical
   b. Layer 2—data link
   c. Layer 3—network
   d. Layer 4—transport
   e. Layer 5—session
2. In IPsec, what does data confidentiality mean?
   a. Identity validation of the remote peer
   b. Encryption of the link layer and up
   c. Encryption following the outer IP header
   d. Preventing the ability to replay or resend packets
   e. Ensuring that the packet's contents have not been read during transit

3. Which of the following are IPsec protocols (select all that apply)?
   a. IKE
   b. UDP
   c. AH
   d. ESP
   e. TCP
4. Which of the following are hash algorithms (select all that apply)?
   a. MD5
   b. DES
   c. 3DES
   d. AES
   e. SHA
5. How many phases does IKE consist of?
   a. One required phase and one optional phase
   b. One required phase and two optional phases
   c. Two required phases and one optional phase
   d. Two required phases and two optional phases
   e. Three required phases
6. Which of the following modes occur during IKE phase 1 (select all that apply)?
   a. Quick mode
   b. Fast mode
   c. Main mode
   d. Aggressive mode
   e. Short mode
7. Which of the following functions occur during IKE phase 1 (select all that apply)?
   a. Establish a bidirectional SA
   b. Establish unidirectional SAs
   c. Perform user authentication
   d. Negotiate IKE parameters
   e. Run quick mode

8. For NAT traversal, when are NAT support and NAT existence determined?
   a. NAT support is determined during IKE phase 1, while NAT existence is determined during IKE phase 2.
   b. Both NAT support and NAT existence are determined during IKE phase 1.
   c. NAT existence is determined during IKE phase 1, while NAT support is determined during IKE phase 2.
   d. Both NAT support and NAT existence are determined during IKE phase 2.
   e. NAT support and NAT existence are really the same feature, and their determination occur during IKE phase 2.
9. Which of the following IPsec protocols provide authentication and integrity checks (select all that apply)?
   a. IKE
   b. MD5
   c. AH
   d. ESP
   e. SHA
10. Which HMAC hash algorithm creates a 160-bit output?
   a. IKE
   b. MD5
   c. AH
   d. ESP
   e. SHA
11. Which of the following encrypting algorithms are considered symmetrical (select all that apply)?
   a. DES
   b. 3DES
   c. Diffie-Hellman
   d. RSA
   e. AES

12. Which of the following algorithms uses a public/private structure to generate a shared secret?

    a. DES
    b. 3DES
    c. Diffie-Hellman
    d. MD5
    e. AES

13. Which PKI element contains information to uniquely identify a peer?

    a. CA
    b. Digital certificate
    c. RA
    d. Neighbor
    e. Distribution mechanism

14. What is the first step in the PKI message exchange process?

    a. The CA sends its public key to the end host.
    b. The end host saves the certificate to some nonvolatile storage area.
    c. An end host generates an RSA key pair.
    d. The CA signs the certificate request with its private key.
    e. The end host generates a certificate request.

The answers to the "Do I Know This Already?" quiz are found in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **10 or fewer overall score**—Read the entire chapter. This includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.
- **11 or 12 overall score**—Begin with the "Foundation Summary" section, and then go to the "Q&A" section.
- **13 or more overall score**—If you want more review on these topics, skip to the "Foundation Summary" section, and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

IPsec

IPsec is best thought of as a set of features that protects IP data as it travels from one location to another. The locations involved in the VPN typically define the type of VPN. A location could be an end client (such as a PC), a small remote office, a large branch office, a corporate headquarters, a data center, or even a service provider. The combination of any two of these locations determines the type of VPN in use. For example, a small remote office connecting to a corporate headquarters would be a site-to-site VPN.

It is important to remember that IPsec can protect only the IP layer and up (transport layer and user data). IPsec cannot extend its services to the data link layer. If protection of the data link layer is needed, then some form of link encryption is needed. Such encryption is typically performed within a trusted infrastructure, where the security of the link can be assured. Such encryption is not feasible in the Internet because intermediate links are not controlled by the end users.

Often, the use of encryption is assumed to be a requirement of IPsec. In reality, encryption, or data confidentiality, is an optional (although heavily implemented) feature of IPsec. IPsec consists of the following features, which are further explained later in this chapter:

- Data confidentiality
- Data integrity
- Data origin authentication
- Anti-replay

The features, or services, of IPsec are implemented by a series of standards-based protocols. It is important that the implementation of IPsec is based on open standards to ensure interoperability between vendors. The IPsec protocols do not specify any particular authentication, encryption algorithms, key generation techniques, or security association (SA) mechanisms. The three main protocols that are used by IPsec are as follows:

- Internet Key Exchange (IKE)
- Encapsulating Security Payload (ESP)
- Authentication Header (AH)

These protocols are detailed a bit later in this chapter in the section "IPsec Protocols." It is important to understand that these protocols are based on open standards. IPsec uses the preceding protocols to establish the rules for authentication and encryption, and existing standards-based algorithms provide the actual means of authentication, encryption, and key management.

Remember that IPsec is used to protect the flow of data through a VPN. However, a VPN does not necessarily imply that the contents are protected. A VPN can simply be a tunnel, or link, between two endpoints. As such, a new outer header or tag may be applied, but the internal contents are still available for inspection to anyone between the endpoints. So, an IPsec VPN can be considered safe and protected, while other types of VPNs might not share this luxury.

IPsec Features

As noted earlier, the primary features of IPsec consist of the following:

- Data confidentiality
- Data integrity
- Data origin authentication (peer authentication)
- Anti-replay

It is important to understand the meaning of each of these features. The protocols that implement these features are covered later in this chapter.

Data confidentiality involves keeping the data within the IPsec VPN private between the participants of the VPN. As noted earlier, most VPNs are used across the public Internet. As such, it is possible for data to be intercepted and examined. In reality, any data in transit is subject to examination, so the Internet should not be viewed as the only insecure media.

Data confidentiality involves the use of encryption to scramble the data in transit. Encrypted packets cannot be easily, if ever, understood by anyone other than the intended recipient. The use of encryption involves the selection of an encryption algorithm and a means of distributing encryption keys to those involved. IPsec encryption algorithms are covered later in this chapter.

Data confidentiality, or encryption, is not required for IPsec VPNs. More often than not, packets are encrypted as they pass through the VPN. But data confidentiality is an optional feature for IPsec.

Data integrity is a guarantee that the data was not modified or altered during transit through the IPsec VPN. Data integrity itself does not provide data confidentiality. Data integrity typically uses a hash algorithm to check if data within the packet was modified between endpoints. Packets that are determined to have been changed are not accepted.

Data origin authentication validates the source of the IPsec VPN. This feature is performed by each end of the VPN to ensure that the other end is exactly who you want to be connected to. Note that the use of the data origin authentication feature is dependent upon the data integrity service. Data origin authentication cannot exist on its own.

Anti-replay ensures that no packets are duplicated within the VPN. This is accomplished through the use of sequence numbers in the packets and a sliding window on the receiver. The sequence number is compared to the sliding window and helps detect packets that are late. Such late packets are considered duplicates, and are dropped. Like data confidentiality, anti-replay is considered an optional IPsec feature.

IPsec Protocols

IPsec consists of three primary protocols to help implement the overall IPsec architecture:

- Internet Key Exchange (IKE)
- Encapsulating Security Payload (ESP)
- Authentication Header (AH)

Together, these three protocols offer the various IPsec features mentioned earlier. Every IPsec VPN uses some combination of these protocols to provide the desired features for the VPN.

IKE

Internet Key Exchange (IKE) is a framework for the negotiation and exchange of security parameters and authentication keys. The IPsec security parameters will be examined later in the "Internet Key Exchange (IKE)" section. For now, it is important to understand that there are a variety of possible options between two IPsec VPN endpoints. The secure negotiation of these parameters used to establish the IPsec VPN characteristics is performed by IKE.

IKE also exchanges keys used for the symmetrical encryption algorithms within an IPsec VPN. Compared to other encryption algorithms, symmetrical algorithms tend to be more efficient and easier to implement in hardware. The use of such algorithms requires appropriate key material, and IKE provides the mechanism to exchange the keys.

ESP

Encapsulating Security Payload (ESP) provides the framework for the data confidentiality, data integrity, data origin authentication, and optional anti-replay features of IPsec. While ESP is the only IPsec protocol that provides data encryption, it also can provide all of the IPsec features

mentioned earlier. Because of this, ESP is primarily used in IPsec VPNs today. The following encryption methods are available to IPsec ESP:

- **Data Encryption Standard (DES)**—An older method of encrypting information that has enjoyed widespread use.
- **Triple Data Encryption Standard (3DES)**—A block cipher that uses DES three times.
- **Advanced Encryption Standard (AES)**—One of the most popular symmetric key algorithms used today.

AH

Authentication Header (AH) provides the framework for the data integrity, data origin authentication, and optional anti-replay features of IPsec. Note that data confidentiality is not provided by AH. AH ensures that the data has not been modified or tampered with, but does not hide the data from inquisitive eyes during transit. As such, the use of AH alone in today's networks has faded in favor of ESP. Both AH and ESP use a Hash-based Message Authentication Code (HMAC) as the authentication and integrity check. Table 12-2 shows the HMAC hash algorithms in IPsec.

Table 12-2 *Hash Algorithms*

Hash Algorithm	Input	Output	Used by IPsec
Message Digest 5 (MD5)	Variable	128 bits	128 bits
Secure Hash Algorithm (SHA-1)	Variable	160 bits	First 96 bits

Both MD5 and SHA-1 use a shared secret key for both the calculation and verification of the message authentication values. The cryptographic strength of the HMAC is dependent upon the properties of the underlying hash function. Both MD5 and SHA-1 take variable-length input data and create a fixed-length hash. The difference is the size and strength of the hash created. Although IPsec uses only the first 96 bits of the 160-bit SHA-1 hash, it is considered more secure than MD5 (although SHA-1 is computationally slower than MD5).

IPsec Modes

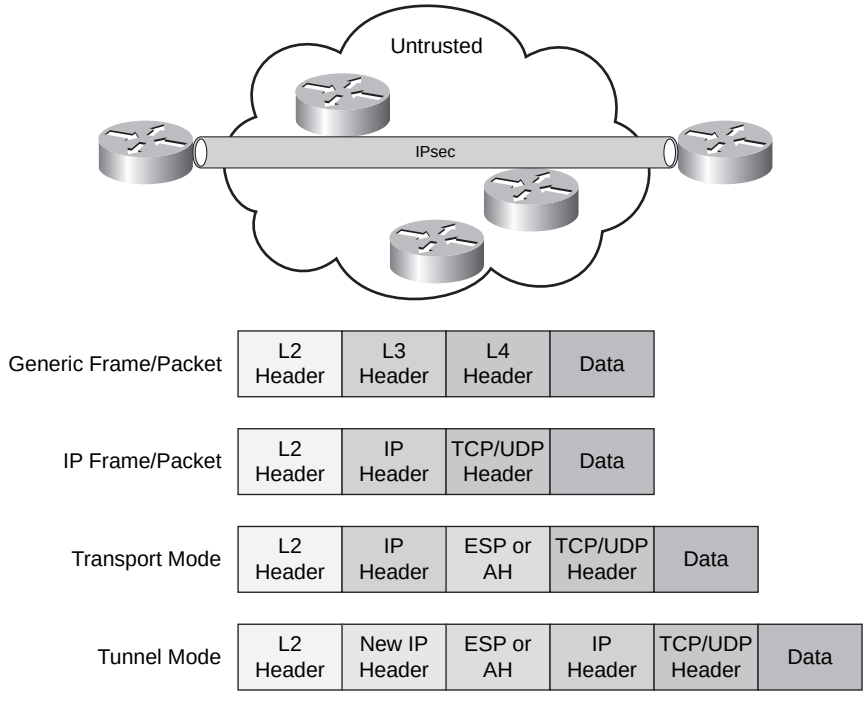
IPsec defines two modes that determine the extent of protection offered to the original IP packet. Remember that the IPsec header follows an IP header, because it is referenced by an IP protocol number. As such, encryption and integrity services can be offered only beyond the IP header. The two IPsec modes are tunnel mode and transport mode.

When IPsec headers are simply inserted in an IP packet (after the IP header), it is called transport mode. In transport mode, the original IP header is exposed and unprotected. Data at the transport

layer and higher layers benefits from the implemented IPsec features. Another way to think of this is that transport mode protects the transport layer and up. As such, when the IPsec packet travels across an untrusted network, all of the data within the packet is safe (based on the IPsec services selected). Devices in the untrusted network can see only the actual IP addresses of the IPsec participants.

IPsec offers a second mode called tunnel mode. In tunnel mode, the actual IP addresses of the original IP header, along with all the data within the packet, are protected. Tunnel mode creates a new external IP header that contains the IP addresses of the tunnel endpoints (such as routers or VPN Concentrators). The exposed IP addresses are the tunnel endpoints, not the device IP addresses that sit behind the tunnel end points. Figure 12-1 shows the two IPsec modes compared to a "normal" IP packet.

Figure 12-1 *IPsec Modes*



As mentioned earlier, the endpoints of the IPsec tunnel can be any device. Figure 12-1 shows routers as endpoints, which might be used for site-to-site VPNs (explained in Chapter 13, "Site-to-Site VPN Operations"). It is also important to remember that the concept of a *VPN tunnel* is used with both VPN modes—transport and tunnel. In transport mode, the packet contents are protected between the VPN endpoints, whereas in tunnel mode, the entire original IP packet is protected.

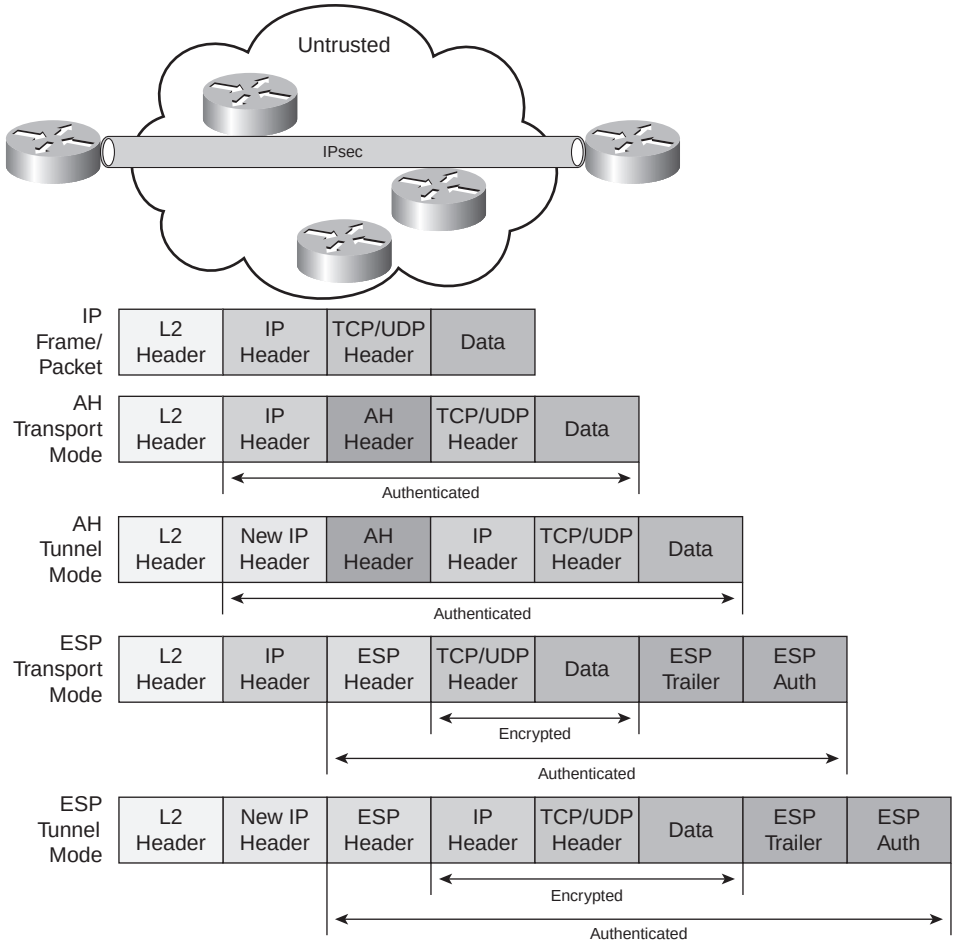
IPsec Headers

Both AH and ESP are implemented by adding headers to the original IP packet. The IPsec VPN uses AH or ESP, or both (but the use of AH along with ESP has no appreciable benefit). Remember that ESP implements all of the IPsec features mentioned earlier, while AH offers all features except data confidentiality. Both AH and ESP are recognized by their particular IP protocol numbers, which makes each a transport layer protocol. AH and ESP are recognized by their respective IP protocol numbers (51 and 50).

The placement of these headers means that the IPsec features that they provide (confidentiality and integrity) can only be for portions of the IP packet that follow the AH or ESP header.

Figure 12-2 shows how the ESP and AH headers are applied to an existing IP packet. Both transport and tunnel modes are shown for comparison.

Figure 12-2 *AH and ESP Headers*



As shown in Figure 12-2, AH authenticates the entire packet after the Layer 2 header. If ESP authentication is used, the outer IP header is not authenticated. Also note that if ESP performs both encryption and authentication, encryption occurs first, and then the encrypted contents along with the ESP headers are authenticated.

Peer Authentication

As described thus far, IPsec has the capability to protect data in transit. It can encrypt the data to prevent those in the middle from seeing it (data confidentiality), and it can ensure that the data has not been modified while in flight (data integrity). However, these functions lose their appeal if one VPN endpoint is not sure of whom the other endpoint truly is. IPsec can secure the data transfer, but before such services are employed, the endpoints of the IPsec VPN must be validated.

The concept of peer authentication certifies that the remote IPsec endpoint is truly who it says it is. There are five different methods to authenticate an IPsec peer:

- **Username and password**—A username and password must be predefined and preconfigured in the IPsec endpoints. As such, they are typically used for long periods of time. They are generally not considered very safe, because if someone guesses or learns the username/password combination, that person can establish an IPsec connection with you.
- **One-time password (OTP)**—An OTP is typically implemented as a personal identification number (PIN) or a transaction authentication number (TAN). Such numbers are good for only one IPsec instantiation. If someone were to learn of an old OTP, it would be useless to establish a new IPsec connection.
- **Biometrics**—Biometric technologies analyze physical human characteristics, such as fingerprints, hand measurements, eye retinas and irises, voice patterns, and facial patterns. Such characteristics are difficult, if not impossible, to duplicate. Any combination of these can be used to authenticate a person, and thus provide assurance of who is at the other end of the IPsec connection.
- **Preshared keys**—Preshared keys are similar to the username/password concept. In this case, a single key (value) is preconfigured in each IPsec peer. Like the username/password, it is important that such manually configured information remain safeguarded. If someone were able to determine the preshared key, they would have the ability to establish an IPsec connection with you.
- **Digital certificates**—Digital certificates are a very popular way to authenticate people and devices. Typically, a digital certificate is issued to a device from a trusted third-party certification authority (CA). This certificate is only good for the machine it was issued to.

When that device needs to authenticate, it presents its certificate, which is then validated against the third-party CA. If another device attempts to use the certificate, the authentication will fail.

Internet Key Exchange (IKE)

A secure IPsec connection between two devices can initially be established by configuring encryption keys in both devices. However, the failure to periodically change these keys makes the network susceptible to brute-force password attacks. The need to manually change the IPsec keys every hour or every day can prove troublesome. If dozens or hundreds of IPsec connections are in use, manual key maintenance can be a nightmare.

IKE Protocols

The IKE protocol, as described earlier, is a means of dynamically exchanging IPsec parameters and keys. IKE makes IPsec scalable by automating the key exchange/update process needed to repel password attacks against the IPsec sessions. IKE helps to automatically establish security associations (SAs) between two IPsec endpoints. An SA is an agreement of IPsec parameters between two peers.

IKE actually uses other protocols to perform peer authentication and key generation:

- **ISAKMP**—The Internet Security Association and Key Management Protocol defines procedures on how to establish, negotiate, modify, and delete SAs. All parameter negotiation is handled through ISAKMP, such as header authentication and payload encapsulation (headers and modes were discussed earlier). ISAKMP performs peer authentication, but it does not involve key exchange.
- **Oakley**—The Oakley protocol uses the Diffie-Hellman algorithm to manage key exchanges across IPsec SAs. Diffie-Hellman is a cryptographic protocol that permits two end points to exchange a shared secret over an insecure channel.

IKE Phases

The IKE protocol/process is broken into two phases, which create a secure communications channel between two IPsec endpoints. Although there are two primary and mandatory IKE phases, there is an optional third phase. The three phases are described here:

- IKE phase 1 is one of the mandatory IKE phases. A bidirectional SA is established between IPsec peers in phase 1. This means that data sent between the end devices uses the same key material. Phase 1 may also perform peer authentication to validate the identity of the IPsec endpoints. There are two IKE modes available for IKE phase 1 to establish the bidirectional

SA: main mode and aggressive mode. IKE modes are described in the next section. Phase 1 consists of parameter negotiation, such as hash methods and transform sets. The two IPsec peers must agree on these parameters or the IPsec connection cannot be established.

- IKE phase 1.5 is an optional IKE phase. Phase 1.5 provides an additional layer of authentication, called Xauth, or Extended Authentication. IPsec authentication provided in Phase 1 authenticates the devices or endpoints used to establish the IPsec connection. However, there is no means of validating the users behind the devices. A preconfigured IPsec device can be used by both friends and foes. Xauth forces the user to authenticate before use of the IPsec connection is granted.
- IKE phase 2 is the second mandatory IKE phase. Phase 2 implements unidirectional SAs between the IPsec endpoints using the parameters agreed upon in Phase 1. The use of unidirectional SAs means that separate keying material is needed for each direction. Phase 2 uses IKE quick mode to establish each of the unidirectional SAs.

IKE Modes

IKE consists of three different modes. As mentioned earlier, IKE phase 1 has a choice of two modes (main or aggressive), while IKE phase 2 always uses the same mode (quick). For one IPsec session between two devices, either main or aggressive mode is used for IKE phase 1, and quick mode is always used for IKE phase 2. The IKE modes are described in the sections that follow. The third optional IKE mode is phase 1.5, which is optionally used for extended authentication.

IKE Main Mode

Main mode consists of six messages exchanged between the IPsec peers. If main mode is selected, aggressive mode is not used. Quick mode always follows main mode. These six messages of main mode are broken into three pairs:

- **IPsec parameters and security policy**—The initiator sends one or more proposals, and the responder selects the appropriate one.
- **Diffie-Hellman public key exchange**—Public keys are sent between the two IPsec endpoints.
- **ISAKMP session authentication**—Each end is authenticated by the other.

IKE Aggressive Mode

Aggressive mode is an abbreviated version of main mode. If aggressive mode is selected, main mode is not used. Quick mode always follows aggressive mode. The six packets of main mode are condensed into three:

- The initiator sends all data, including IPsec parameters, security policies, and Diffie-Hellman public keys.
- The responder authenticates the packet and sends the parameter proposal, key material, and identification back.
- The initiator authenticates the packet.

IKE Quick Mode

Quick mode is used during IKE phase 2. The negotiation of quick mode is protected by the IKE SA negotiated in Phase 1. Such an option is not available during main or aggressive modes, because their function is to establish the first SA. Quick mode negotiates the SAs used for data encryption across the IPsec connection. It also manages the key exchange for those SAs.

Other IKE Functions

Thus far, IKE has been shown as a protocol that exchanges IPsec parameters and keys. However, it does perform other functions that are important to the setup and maintenance of the IPsec connections. These functions include:

- Dead peer detection (DPD)
- NAT traversal
- Mode configuration
- Xauth

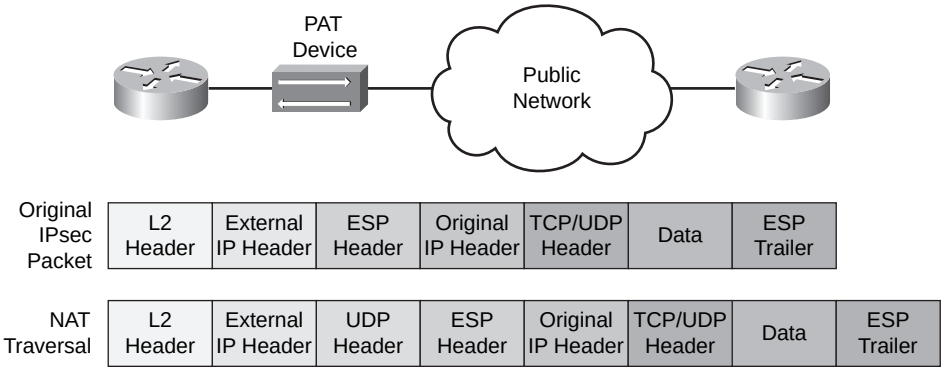
Dead peer detection is accomplished by sending periodic keepalive (or hello) timers between IPsec peers. To be effective, the timer should be fairly repetitive (such as every 10 seconds). That way, the failure of the IPsec connection is quickly recognized by the loss of hello packets. One downside to DPD is the additional traffic that must be sent across the IPsec session.

NAT traversal solves one problem that Network Address Translation/Port Address Translation (NAT/PAT) introduces. Remember that PAT translates both IP addresses and ports typically to permit multiple “inside” devices to share a single or fewer “outside” IP addresses. To translate from one port number to another, the port numbers must be available in the transport layer headers. However, IPsec typically encrypts all data above Layer 3.

NAT traversal is solved using both IKE phase 1 and phase 2. During phase 1 (before quick mode), it is determined whether NAT is supported (NAT support) and whether NAT exists (NAT existence) along the path of the proposed IPsec connection. IKE phase 2 (quick mode) decides whether the IPsec peers will use NAT traversal. The negotiation of NAT traversal occurs via the quick mode SA that is established.

NAT traversal is accomplished by inserting a UDP header before the ESP header in the IPsec packet. This new transport layer header has unencrypted port information that can be stored in PAT tables, and thus the PAT translation process can successfully occur. Figure 12-3 shows a normal IPsec packet compared to one that has been modified for NAT traversal. As mentioned earlier, IPsec end devices can be routers (as shown) or other network devices, such as workstations, servers, or VPN Concentrators.

Figure 12-3 *NAT Traversal*



IKE mode configuration is simply a means of pushing all the IPsec attributes out to the remote IPsec client. Such attributes include the IP address to be used for the IPsec connection, and the DNS and NetBIOS name servers to be used across the IPsec connection. Because these and other attributes can be pushed down to the IPsec client, the required configuration on the client is minimized.

The Cisco Easy VPN solution is an example of such a push model. The server, which runs on Cisco routers, Cisco VPN Concentrators, and Cisco PIX Firewalls, pushes the necessary security policies and parameters out to the remote client, which can be another Cisco router, Cisco VPN Concentrator, Cisco PIX Firewall, or Cisco VPN Client on a workstation.

IKE extended authentication (Xauth), as already mentioned, is a way to authenticate a user of an IPsec connection. Remember that IKE itself provides for device authentication. Xauth adds an additional layer of authentication that a user must validate by means of a username/password combination, Challenge Handshake Authentication Protocol (CHAP), one-time passwords (OTP), or secure key (S/KEY).

Encryption Algorithms

Encryption is simply a mathematical algorithm and a key applied to data to make the contents unreadable to everyone except those who have the ability to decrypt it. Ideally, encrypted data can

be decrypted only with the proper key. Thus, the strength of the cipher text (encrypted data) is based on the complexity of the encryption algorithm, and the size of the key used to encrypt the data. There are two types of encryption algorithms available: symmetric and asymmetric.

Symmetric Encryption

Symmetric encryption algorithms are also called secret key cryptography. As the name implies, there is a single, secret key that is used to both encrypt and decrypt the data. It is very important that the secret key remain a secret. Anyone who manages to get the key can decrypt any messages encrypted with it. This was the only type of encryption available through the mid-1970s. Symmetric algorithms tend to be computationally easier to implement, and are useful for large, bulk encryption requirements.

Today, DES, 3DES, and AES are examples of symmetric encryption algorithms:

- DES, with its 56-bit key, has been broken in less than 24 hours using modern computers.
- 3DES applies three different 56-bit keys (DES encrypt, DES decrypt, DES encrypt) to create the cipher text. It has not yet been broken, but has theoretical flaws.
- AES is considered the symmetric encryption choice today. It originally was called Rijndael. Both AES and Rijndael use the same encryption algorithm and support keys ranging from 128 bits to 256 bits. The difference between the two is that AES uses 64-bit increments, while Rijndael uses multiples of 32. AES is the only public symmetric encryption algorithm adopted by the National Security Agency for use in top-secret networks.

Asymmetric Encryption

Asymmetric encryption algorithms use different keys for encryption and decryption. In fact, the key used to encrypt data cannot be used to decrypt it. The encryption key is called the *public key*, while the decryption key is called the *private key*. It is possible, and expected, to widely distribute the public key. This key can be used only to encrypt messages that will eventually be decrypted with the associated private key.

For digital signatures, the use of the two keys is reversed. The private key is used to sign a hash of the message, while the public key decrypts and validates the signature. In all cases, the private key should be kept secret, similar to the shared secret keys used with symmetric encryption algorithms.

RSA (named after its designers—Rivest, Shamir, and Adleman) is an asymmetric encryption algorithm. It was also the first algorithm that could be used for both signing and encrypting. RSA key lengths start at 1024 bits and get longer (typically by doubling the key length). Full decryption of an RSA key is thought to be impossible due to the difficulty in factoring large prime integers (which is the basic premise of the RSA cryptosystem), although this has not been mathematically

proven. Unlike symmetric algorithms, asymmetric algorithms tend to be computationally expensive to implement, and are not well suited for continuous, bulk encryption jobs.

It was mentioned earlier that symmetric encryption algorithms use the same secret key for encrypting and decrypting. The trick is to keep the secret key covert. Asymmetric encryption algorithms use different keys for encryption and decryption. Asymmetric key exchange algorithms can be used to safely deliver shared secret keys across an insecure network, which can then be use for bulk encryption via symmetric algorithms across that same network.

Diffie-Hellman is the primary asymmetric key exchange algorithm used in IPsec for the exchange of shared secret keys. Table 12-3 outlines the Diffie-Hellman exchange process, which occurs in parallel between two IPsec peers—A and B.

Table 12-3 *The Diffie-Hellman Key Exchange*

Step	What Peer A Does	What Peer A Knows	What Peer B Does	What Peer B Knows
1	Generates a large prime integer → P_A. Sends P_A to peer B. Receives the prime integer generated by peer B → P_B. Generates a primitive root of P_A and P_B → R.	P_A P_B R	Generates a large prime integer → P_B. Sends P_B to peer A. Receives the prime integer generated by peer A→ P_A. Generates a primitive root of P_A and P_B → R.	P_A P_B R
2	Generates its private key→ X_A.	P_A P_B R X_A	Generates its private key → X_B.	P_A P_B R X_B
3	Generates a public key for peer B → $Y_A = R \wedge X_A \bmod P_A$.	P_A P_B R X_A Y_A	Generates a public key for peer A → $Y_B = R \wedge X_B \bmod P_B$.	P_A P_B R X_B Y_B

Table 12-3 *The Diffie-Hellman Key Exchange (Continued)*

Step	What Peer A Does	What Peer A Knows	What Peer B Does	What Peer B Knows
4	Sends Y_A to peer B. Receives the public key from peer B → Y_B.	P_A P_B R X_A Y_A Y_B	Sends Y_B to peer A. Receives the public key from peer A → Y_A.	P_A P_B R X_B Y_A Y_B
5	Generates a shared secret number → Z = Y_B ^ X_A mod P_A.	P_A P_B R X_A Y_A Y_B Z	Generates a shared secret number → Z = Y_A ^ X_B mod P_A.	P_A P_B R X_B Y_A Y_B Z
6	Generates a shared secret key from Z → SS (for DES, 3DES, or AES).	P_A P_B R X_A Y_A Y_B Z SS	Generates a shared secret key from Z → SS (for DES, 3DES, or AES).	P_A P_B R X_B Y_A Y_B Z SS

The large prime number that is used as a seed of the whole process is determined by the Diffie-Hellman group that the two IPsec endpoints agreed upon. Diffie-Hellman consists of seven

different groups (1–7). Each group defines a unique modular exponentiation (MODP) algorithm and key size. The base key is a large prime integer that is used to calculate the public/private key pairs (as shown in Table 12-3).

The mathematical exponentiation in steps 3 and 5 is computationally challenging. The respective public keys are generated in step 3 and exchanged in step 4. As mentioned before, the interception of a public key does not cause any security concerns for an asymmetrical encryption algorithm. Note that the private keys (X_A and X_B) are never exchanged.

Public Key Infrastructure

A public key infrastructure (PKI) is the progression of the key exchange and maintenance concepts discussed throughout this chapter. A PKI provides a hierarchical framework for managing the security attributes of entities who engage in secure communications across a network. Such entities can be all of the IPsec devices mentioned throughout this chapter, as well as the people who use those devices.

The PKI consists of a number of elements, which are also network entities:

- **Peers**—Devices and people who securely communicate across a network. Also known as end hosts.
- **Certification authority (CA)**—Grants and maintains digital certificates. Also known as a trusted entity or a trust point.
- **Digital certificate**—Contains information to uniquely identify a peer, a signed copy of the public encryption key used for secure communications, certificate validity data, and the signature of the CA that issued the certificate. X.509v3 is the current version of digital certificate.
- **Registration authority (RA)**—An optional entity that can handle enrollment requests (obtaining a certificate) for the CA.
- **Distribution mechanism**—A means to distribute certificate revocation lists (CRLs) across the network. LDAP and HTTP are examples.

Through PKI, every network entity who wishes to participate in secure communications receives a digital certificate, which contains a public/private key pair, and has their identity validated by a CA. When peers need to establish a secure communications channel, they exchange certificates.

Certificates can be validated by CAs, and the enclosed keys can be used to secure the channel. Table 12-4 details the PKI message exchange process.

Table 12-4 *The PKI Message Exchange Process*

Step	Action
1	An end host generates an RSA key pair (public/private) and requests the public key of its CA.
2	The CA sends its public key to the end host.
3	The end host generates a certificate request. Depending on the network configuration, either the request is automatically sent to the CA or manual intervention is needed to approve the request. The certificate request is sent to either the CA or the optional RA (if present). The CA or RA receives the certificate request.
4	Once approved, the CA signs the certificate request with its private key. The CA returns the completed certificate to the end host.
5	The end host saves the certificate to some nonvolatile storage area, such as disk, USB smart card (eToken), or NVRAM.
6	The end host uses the validated certificate to establish secure communications with other end hosts that have accomplished these steps.

Foundation Summary

The concept of IPsec often centers on the use of VPN tunnels to encrypt data between endpoints. The use of VPNs is ubiquitous today. The use of IPsec VPNs over the Internet has replaced many of the older point-to-point or virtual circuit–based shared WAN connections. A good understanding of how IPsec operates helps hasten successful deployments.

IPsec offers data confidentiality, data integrity, data origin authentication, and optional anti-replay. Confidentiality is provided through symmetric encryption algorithms such as DES, 3DES, and AES. Data integrity and origin authentication are provided by HMAC algorithms like MD5 and SHA-1.

IPsec can offer integrity and authentication services via AH or add confidentiality to integrity and authentication with ESP. The use of these two protocols can be implemented in either transport mode (only the IP data is protected) or tunnel mode (where the IP header and data are protected). IKE is the third IPsec protocol used to safely exchange keys for symmetric encryption and IPsec security parameters for proper IPsec connection establishment.

Q&A

The questions and scenarios in this book are more difficult than what you will experience on the actual exam. The questions do not attempt to cover more breadth or depth than the exam, but they are designed to make sure that you know the answer. Rather than enabling you to derive the answer from clues hidden inside the question itself, the questions challenge your understanding and recall of the subject.

Hopefully, mastering these questions will help you limit the number of exam questions on which you narrow your choices to two options, and then guess.

The answers to these questions can be found in Appendix A.

1. What are the features of IPsec?
2. What are the three main protocols specified by IPsec?
3. Describe the differences between data confidentiality and data integrity.
4. Which IPsec features are performed by an HMAC?
5. How does IPsec tunnel mode differ from IPsec transport mode?
6. Describe the port or protocol numbers used for AH, ESP, and IKE.
7. Define one-time passwords.
8. Which peer authentication methods require the use of predefined and/or preconfigured information into the IPsec endpoints?
9. What problem does IKE solve for IPsec?
10. Which IKE phase is responsible for extended authentication?
11. IKE creates a number of SAs. What is the purpose of a bidirectional SA?
12. Describe the three IKE modes.
13. What are some of the additional features of IKE?
14. What are the features of symmetric encryption?
15. Which algorithms are considered asymmetric?
16. Which optional PKI component can handle enrollment requests?
17. X.509v3 is considered the current version of which security mechanism?
18. Within the PKI, what are LDAP and HTTP examples of?

Exam Topic List

This chapter covers the following topics that you need to master for the CCNP ISCW exam:

- **Site-to-Site VPN Overview**—Describes how a single VPN between sites permits various devices to have secure communications.
- **Creating a Site-to-Site IPsec VPN**—Describes what is needed to create a site-to-site VPN.
- **Site-to-Site IPsec Configuration Steps**—Covers the steps needed to create a site-to-site VPN.
- **Security Device Manager Features and Interface**—Describes how SDM is used to configure a Cisco IOS device.
- **Configuring a Site-to-Site VPN in SDM**—Explains the specific steps within SDM to create a site-to-site VPN.
- **Monitoring the IPsec VPN Tunnel**—Describes how to examine and monitor the VPN tunnel after it has been created.

CHAPTER 13

Site-to-Site VPN Operations

The growth of the Internet has spawned the use of site-to-site VPNs. Prior to widespread adoption of the Internet, remote sites were connected to each other or back to a central location via point-to-point connections or virtual circuits. Because virtually every location has an Internet connection today, connectivity to virtually anywhere is possible. Secure connectivity is achieved through the use of IPsec VPNs.

Site-to-site VPNs are typically used to connect a remote office back to the central facility. Typically, more than one end device at one site needs to securely communicate with more than one end device at the other location. If only a single device is connecting to a network, then a VPN client on the workstation is sufficient.

A site-to-site VPN eliminates the need for each device to establish its own secure path to the remote location. A single IPsec VPN is used to securely carry all packets between sites.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you really need to read the entire chapter. If you already intend to read the entire chapter, you do not necessarily need to answer these questions now.

The 24-question quiz, derived from the major sections in the "Foundation Topics" portion of the chapter, helps you to determine how to spend your limited study time.

Table 13-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 13-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section	Score
Creating a Site-to-Site IPsec VPN	1–6	
Site-to-Site IPsec Configuration Steps	7–13	
Security Device Manager Features and Interface	14	
Configuring a Site-to-Site VPN in SDM	15–22	
Monitoring the IPsec VPN Tunnel	23-24	
Total Score		

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark this question wrong for purposes of self-assessment. Giving yourself credit for an answer that you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. In IPsec, what does interesting traffic refer to?
   a. Traffic that creates but does not travel through an IPsec tunnel
   b. Traffic that does not create but travels through an IPsec tunnel
   c. Traffic that both creates and travels through an IPsec tunnel
   d. Traffic that causes an IPsec tunnel to be torn down
   e. Traffic that causes a new set of IPsec keys to be exchanged
2. What are the two databases that are used to track IPsec SAs (select two)?
   a. Security Association Policy Database (SAPD)
   b. Security Association Database (SAD)
   c. Security Policy Database (SPD)
   d. Security Association Security Database (SASD)
   e. Security Association Security Database (SAS)
3. How are IKE transform sets used (select all that apply)?
   a. There is one transform set for each IKE parameter.
   b. There is one transform set for each IKE neighbor.
   c. There is one transform set for each unique group of IKE parameters.
   d. There may be multiple transform sets that are used for a single IKE neighbor.
   e. One transform set may be used for multiple IKE neighbors.

4. How many secure tunnels are created for a typical IPsec connection?
   a. One bidirectional IKE tunnel and two unidirectional IPsec SAs
   b. Two unidirectional IKE tunnels and one bidirectional IPsec SA
   c. One bidirectional IKE tunnel and one bidirectional IPsec SA
   d. Two unidirectional IKE tunnels and two bidirectional IPsec SAs
   e. One bidirectional tunnel for both IKE and IPsec traffic
5. What is the SA lifetime used for?
   a. Determines at what time an IPsec SA must be created
   b. Determines at what time an IPsec SA must be torn down
   c. Determines at what time an IKE SA must be created
   d. Defines the conditions when an IKE SA must be torn down
   e. Defines how long an IPsec SA can operate before it must be torn down
6. Which of the seven different Diffie-Hellman versions are supported by Cisco (select all that apply)?
   a. 1
   b. 2
   c. 4
   d. 5
   e. 7
7. The *configure ISAKMP policy* IPsec configuration step maps to which generic IPsec step?
   a. Specify interesting traffic
   b. IKE phase 1
   c. IKE phase 2
   d. Secure data transfer
   e. IPsec tunnel termination
8. The *configure IPsec transform sets* IPsec configuration step maps to which generic IPsec step?
   a. Specify interesting traffic
   b. IKE phase 1
   c. IKE phase 2
   d. Secure data transfer
   e. IPsec tunnel termination

9. Which of the following IKE parameters are configured within the **crypto isakmp policy** command (select all that apply)?

   a. Encryption algorithm

   b. Hash algorithm

   c. Authentication method

   d. Diffie-Hellman group

   e. IKE tunnel lifetime

10. Which of the following transform types are configured with the **crypto ipsec transform-set** command (select all that apply)?

   a. AH transform

   b. AH-ESP transform

   c. ESP encryption transform

   d. ESP authentication transform

   e. AH authentication transform

11. When configuring the ESP encryption transform, which key lengths are available for AES (select all that apply)?

   a. 64 bits

   b. 128 bits

   c. 192 bits

   d. 256 bits

   e. 512 bits

12. Which of the following is the correct interface command to apply the crypto map "test"?

   a. **crypto map test in**

   b. **crypto-map test in**

   c. **crypto map test out**

   d. **crypto-map test out**

   e. **crypto map test**

13. Which protocols/ports must be permitted so that IPsec VPNs can be created (select all that apply)?

    a. Protocol AHP
    b. Protocol ESP
    c. Protocol ISAKMP
    d. UDP port ESP
    e. UDP port AHP

14. Which SDM page is used to access the Site-to-Site VPN Wizard?

    a. Home
    b. Configure
    c. Monitor
    d. Refresh
    e. Save

15. Which options are offered at the start of the Site-to-Site VPN Wizard (select all that apply)?

    a. Create a Site to Site GRE Tunnel
    b. Create a Secure GRE Tunnel
    c. Create a Site to Site VPN
    d. Create a Secure VPN Tunnel
    e. Create an IPsec VPN Tunnel

16. The first step of the Site-to-Site VPN Wizard is to select a configuration option. Which of the following are available choices (select all that apply)?

    a. Quick Setup
    b. Instant Setup
    c. Step by Step Setup
    d. Step by Step Wizard
    e. Manual Setup

17. In the Quick Setup portion of the Site-to-Site VPN Wizard, what configuration options are possible (select all that apply)?

    a. Source interface
    b. IPsec peer IP address
    c. IKE policy
    d. IPsec transform set
    e. Destination subnet for the interesting traffic

18. Which window in the step-by-step setup of the Site-to-Site VPN Wizard is used to configure the tunnel mode?

    a. Connection Settings
    b. IKE Proposals
    c. IPSec Transform Sets
    d. Traffic to Protect
    e. Summary

19. Which IKE lifetime options are available in SDM (select all that apply)?

    a. Hours
    b. Minutes
    c. Seconds
    d. Bytes
    e. Kilobytes

20. On the IPsec Transform Sets screen, how many IPsec transform sets can be displayed at a time?

    a. All transform sets
    b. Only the active transform sets
    c. Only the transform sets applied to this IPsec VPN
    d. Only the transform set displayed in the pull-down menu
    e. Only the transform sets that are selected in the pull-down menu

21. When defining interesting traffic in the Quick Setup window, which options are available (select all that apply)?

    a. Source IP address
    b. Source IP subnet
    c. Destination IP address
    d. Destination IP subnet
    e. ACLs for multiple subnets

22. When completing the configuration of the site-to-site VPN tunnel in the Summary window, which options are available (select all that apply)?

    a. Return to the configuration with the **<Back** button
    b. Advance to the next summary screen with the **Next>** button
    c. Complete the configuration with the Finish button
    d. Edit the configuration with the Edit button
    e. Abort the configuration with the Cancel button.

23. Which SDM page allows you to view the status of various VPN configurations?

    a. Home page
    b. Configure page
    c. Monitor page
    d. VPN page
    e. Security page

24. In the IOS, what command displays the results of successful IKE phase II negotiations?

    a. **show crypto isakmp sa**
    b. **show crypto ipsec sa**
    c. **show crypto ipsec established**
    d. **show crypto ike negotiated**
    e. **show crypto isakmp established**

The answers to the "Do I Know This Already?" quiz are found in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

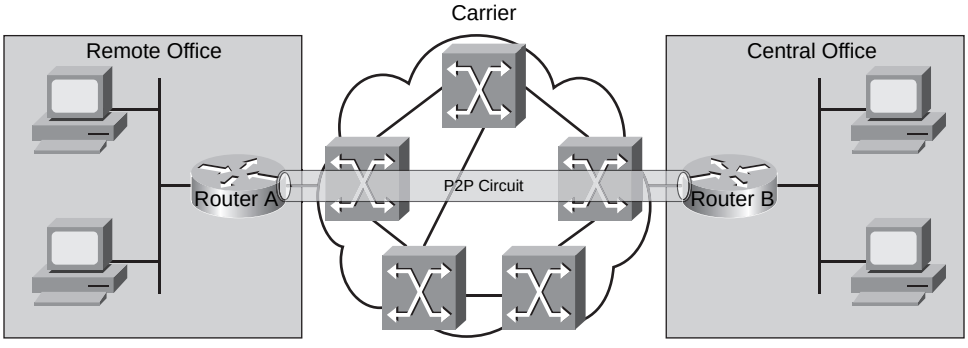
- **16 or fewer overall score**—Read the entire chapter. This includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.
- **18 or 20 overall score**—Begin with the "Foundation Summary" section, and then go to the "Q&A" section.
- **21 or more overall score**—If you want more review on these topics, skip to the "Foundation Summary" section, and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

Site-to-Site VPN Overview

Even before the remarkable growth of the Internet, corporations had deployed remote offices, disbursed data centers, and establish global operations. Before the Internet was embraced as a trusted conduit to fulfill such corporate communications requirements, however, carriers were called upon to provide local, regional, national, and international conduits between locations. Figure 13-1 shows two corporate sites connected "the old way."

Figure 13-1 *Carrier-Provided Circuits*



Before the Internet became the ubiquitous means of global connectivity that it is today, various carriers created enormous networks and provided connectivity services for a fee. Corporations often tried to use a single carrier to provide connections between the various remote offices. This is depicted in Figure 13-1. However, the use of a single carrier was often not possible due to the location of remote offices outside the carrier presence.

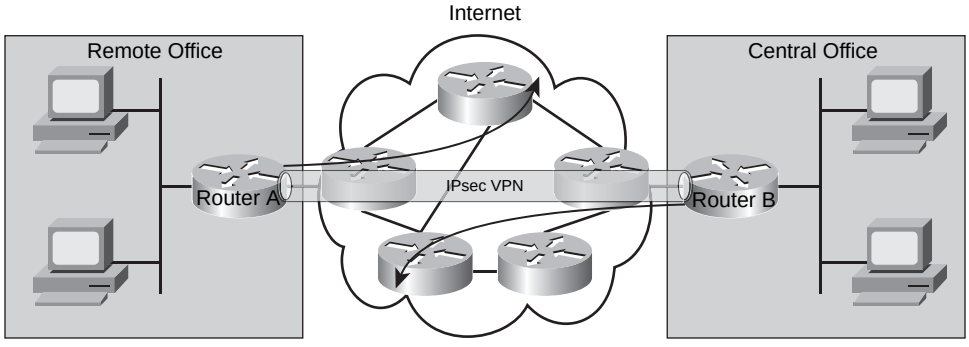
The circuit-based connections provided by the carriers can be thought of as the first site-to-site VPNs. They were indeed private connections between endpoints. Whether they were "nailed-up" permanent virtual circuits (PVC) or "create as needed" switched virtual circuits (SVC), the carriers ensured that the data was delivered as promised between the sites. PVCs tended to offer fixed-sized pipes across the carrier's network, while SVCs had fixed minimum data rates with burst capabilities.

When the Internet grew beyond its academic beginnings, corporations started to experiment with using it to transport data. Soon, the same carriers who offered VC services became Internet service providers (ISP) and offered Internet connectivity. The difference was that instead of providing

end-to-end connections, they simply provided access—access to the entire Internet. It is difficult to provide throughput guarantees across the Internet due to its open and shared nature.

The need to create private, secure communications channels between sites saw the rise of site-to-site IPsec VPNs. Figure 13-2 shows such a connection.

Figure 13-2 *Site-to-Site IPsec VPN*



The networks depicted in both Figure 13-1 and Figure 13-2 are similar, and for a reason. The corporate sites shown have not changed all that much from the days of the carriers. Back then, a remote site had connectivity only back to the main campus or to some other central location. In today's networks, a remote site can use its generic Internet connectivity to get anywhere in the Internet (as depicted by the arrows to the great beyond) and use its IPsec VPN to securely communicate with the main campus.

Creating a Site-to-Site IPsec VPN

There are five generic steps in the lifecycle of any IPsec VPN. The steps described here are applied specifically to site-to-site VPNs, but these steps are true whenever any two endpoints wish to establish an IPsec VPN between them. The five steps in the life of an IPsec VPN are as follows:

Step 1 Specify interesting traffic.

Step 2 IKE phase 1.

Step 3 IKE phase 2.

Step 4 Secure data transfer.

Step 5 IPsec tunnel termination.

Each of these steps is detailed in the following sections. Some of these steps should be familiar from Chapter 12, "IPsec Overview," where IKE was a primary ingredient. In this chapter, IKE is moved from the explanation to the implementation.

The name "VPN tunnel" is somewhat of a misnomer to some. There is no tunnel that the packets are locked inside of as they transit the Internet (or some insecure network). All the IPsec VPN packets are subject to interception and capture at any point during their travels. Data integrity ensures that the data was not modified during any unscheduled stop, while data confidentiality guarantees that the contents of the packets cannot be deciphered by any unwanted inspectors.

Step 1: Specify Interesting Traffic

Interesting traffic is better thought of as traffic that must be protected by the IPsec VPN. When an IPsec VPN tunnel exists between two sites, traffic that is considered "interesting" is sent securely through the VPN to the remote location. Once inside the VPN, the data is safe until it reaches the other end of the tunnel. The traffic cannot be modified without detection, nor can it be read by anyone in the middle (if ESP is employed).

In fact, such traffic can only travel to the other end of the VPN tunnel. It cannot "escape" from the VPN tunnel and travel to some unintended destination. Only the predetermined VPN endpoint has the capability to validate and decrypt such packets.

This concept of interesting traffic also implies that packets that are not interesting do not enjoy the benefits of the IPsec VPN. They are not encrypted or protected in any way. They may travel to any destination, including the remote destination where the VPN tunnel terminates.

An extended access control list (ACL) is used to specify interesting traffic. Traffic that is permitted by this ACL has the appropriate security policy applied to it and the packets then enter the IPsec VPN tunnel. However, if the tunnel does not yet exist, then the arrival of the first interesting packet triggers the events needed to create the tunnel.

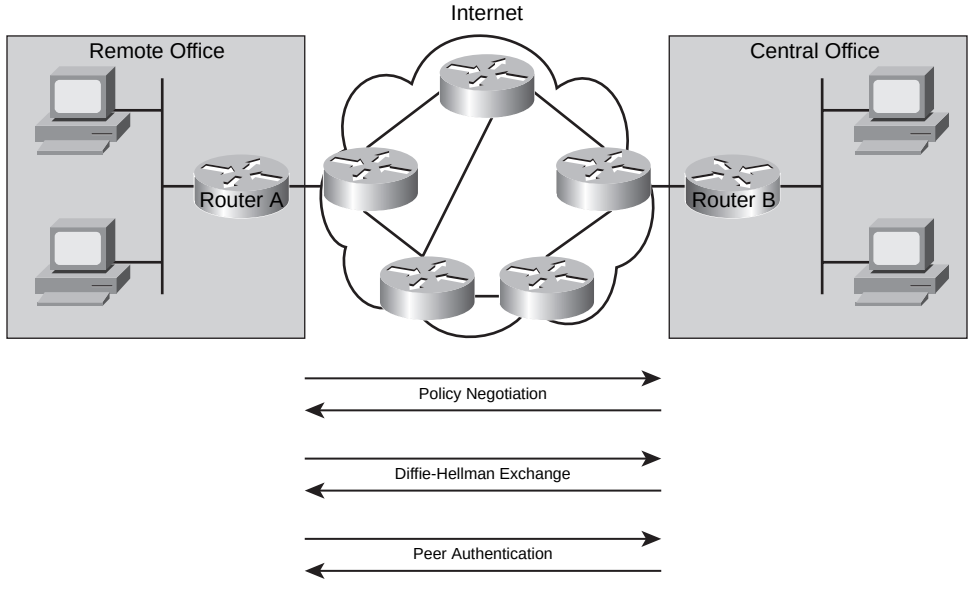
The five steps in the lifecycle of an IPsec VPN (explained here) assume that the tunnel does not yet exist and must be built upon the receipt of interesting traffic. It takes only one interesting packet to trigger the IPsec VPN tunnel process. If the IPsec tunnel already exists, then the traffic that is considered interesting (Step 1) is sent through the tunnel (Step 4).

Step 2: IKE Phase 1

Once the first packet deemed interesting arrives, the process of creating the site-to-site IPsec VPN tunnel commences. As already discussed in Chapter 12, IKE exchanges the security parameters and symmetric encryption keys used to create the IPsec tunnels that the data will eventually flow in. The second step in an IPsec VPN is the first phase of IKE.

Remember that IKE phase 1 has two possible modes: main mode or aggressive mode. The basic purpose of either mode is identical, but the number of messages exchanged is greatly reduced in aggressive mode. Figure 13-3 graphically shows IKE phase 1 main mode.

Figure 13-3 *IKE Phase 1, Main Mode*



In main mode, the first two exchanges negotiate the security parameters used to establish the IKE tunnel. The two endpoints exchange proposals in the form of transform sets. The use of transform sets is explained later in this chapter.

The second pair of packets exchanges the Diffie-Hellman public keys needed to create the secure IKE tunnel. This tunnel is used later for the exchange of keys for the IPsec security associations (SA).

The final pair of packets performs peer authentication. Remember that a hash function is used to confirm identity and ensure that no rogue devices are permitted to establish a secure communications channel to your site.

Aggressive mode reduces the IKE phase 1 exchange to three packets:

- The first packet goes from the initiator to the receiver. It sends security policy proposals, the Diffie-Hellman public key, a nonce (which is signed and returned for identity validation), and a means to perform authentication.

- The second packet goes from the receiver back to the initiator. It contains the accepted security policy proposal, its Diffie-Hellman public key, and the signed nonce for authentication.
- The final packet is a confirmation from the initiator to the receiver.

IKE Transform Sets

In IKE, numerous individual parameters must be coordinated. Instead of trying to negotiate each one individually, different combinations of security parameters are grouped into transform sets, also known as IKE policies. Administrators typically create these policies on IPsec endpoints.

Anytime two IPsec endpoints negotiate security parameters, they exchange IKE policies. If the pair of devices have a common policy (a common set of security parameters), then the setup of the IPsec VPN can continue. If there are no common parameter sets between the two devices, then the overall IPsec VPN process fails.

There are five parameters that must be coordinated during IKE phase 1:

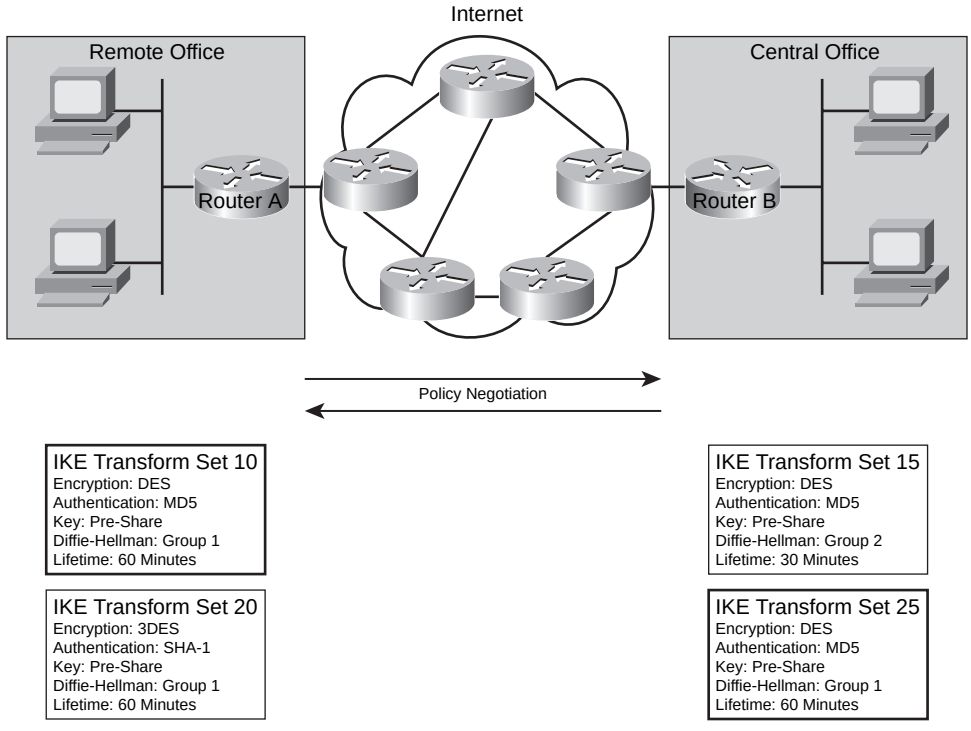
- IKE encryption algorithm (DES, 3DES, or AES)
- IKE authentication algorithm (MD5 or SHA-1)
- IKE key (preshare, RSA signatures, nonces)
- Diffie-Hellman version (1, 2, or 5)
- IKE tunnel lifetime (time and/or byte count)

Figure 13-4 shows how the two IPsec endpoints use IKE transform sets to coordinate the IKE tunnel.

In Figure 13-4, Router A and Router B are attempting to negotiate an IKE tunnel. Assume that Router A starts the IKE negotiation process. Router A sends its two IKE policies, 10 and 20, to Router B. The change of a single parameter makes an entirely new IKE policy. It is possible to use the same IKE policy for multiple sites. However, different policies and parameters may dictate that unique IKE policies be used for each site.

When Router B receives the two transform sets, it compares the contents of each to any transform sets that it has. This comparison is done in sequence of the local IKE policies. The first match found becomes the policy that is used (which implies that there could be multiple policies with identical parameters). The policy number merely determines the comparison priority (sequence) and is not one of the parameters.

Figure 13-4 *IKE Transform Sets*



In this example, the contents of IKE policy 10 from Router A match those in IKE policy 25 in Router B. Router B responds to Router A that it accepts policy 10 and the IKE SA is created. If Router B could not find any exact parameter matches between the transform sets, then the IKE tunnel would not be constructed and the IPsec process would fail. Router A and Router B have found a common IKE policy, however, so an IKE SA can be established.

A remote site that creates only a single IPsec connection to one remote location needs only one IKE transform set. Multiple transform sets are needed if one location establishes many IPsec connections to different destinations and each uses different IKE parameters. It is possible to use a single transform set for multiple IKE connections, as long as each site uses the same security parameters.

Diffie-Hellman Key Exchange

After the IKE policies have been agreed to, the DH protocol is used to exchange the key material that will be used in Phase 1. Remember that DH allows two parties to share a secret key over an insecure channel. Because this key forms the basis of the rest of the VPN, it is essential that the key be kept secret.

Although there are seven different Diffie-Hellman groups (1–7), Cisco VPN devices support only Diffie-Hellman groups 1, 2, and 5, which use 768-bit, 1024-bit, and 1536-bit prime numbers, respectively. The larger the prime number, the longer it takes to generate the keys, but the more secure the keys are. Both IPsec devices must agree on the Diffie-Hellman group in the transform sets. It is generally recommended to avoid the use of Diffie-Hellman group 1 today, although groups 2 and 5 are computationally more expensive.

After the Diffie-Hellman keys are exchanged and the shared secret is established, the SA for phase 1 is created. This phase 1 SA is used to exchange key material for phase 2.

Peer Authentication

The final IKE phase 1 responsibility is to authenticate the remote peer. This is an important step to prevent rogue devices from establishing secure tunnels into your network. If this authentication phase fails, then the IPsec process halts and the IPsec tunnels are never created.

There are three typical methods used for peer authentication:

- Preshared keys
- RSA signatures
- RSA-encrypted nonces

A preshared key is manually entered into each peer. These keys are exchanged in the IKE policies. If the key received does not match the configured key, then the authentication fails.

RSA signatures use digital certificates to authenticate peers. Each peer is issued a certificate, and this certificate is passed in the transform set. The IPsec endpoint ensures that the certificate has been signed/validated by a known CA. If so, the peer is authenticated. RSA signatures are an instantiation of PKI.

A nonce is a number that is used only once. Think of it as a form of one-time password (OTP). A nonce is a "nonsense" random number generated by each peer, encrypted and sent to the other.

Step 3: IKE Phase 2

The actual IPsec tunnels are established in IKE phase 2. IKE phase 1 creates a very secure communications channel (its own SAs) so that the IPsec tunnels (SAs) can be created for data encryption and transport. IPsec parameters are negotiated via the IKE SAs.

The following functions are performed in IKE phase 2:

- Negotiation of IPsec security parameters via IPsec transform sets
- Establishment of IPsec SAs (unidirectional IPsec tunnels)

- Periodic renegotiation of IPsec SAs to ensure security
- An additional Diffie-Hellman exchange (optional)

Remember that IKE phase 2 has a single mode, called quick mode. Assuming phase 1 is successful (main or aggressive mode), quick mode is used in phase 2. Quick mode encompasses the entire process that occurs in IKE phase 2.

First, each IPsec peer must negotiate the IPsec parameters that are used to create the IPsec tunnels. Similar to IKE phase 1 (which uses IKE policies), IPsec transform sets are used during this process.

Once the IPsec parameters are agreed upon (discussed in the next section), the IPsec SAs can be created. IPsec SAs are unidirectional. Thus, two SAs are needed to have secure, bidirectional communication between two peers. Quick mode uses nonces to generate new key material for the shared secrets and to prevent replay attacks. Because a nonce is used only one time, the reuse of one would indicate a bogus SA attempt.

Quick mode also monitors the expiration of SAs and establishes new ones when needed. An SA should never stay up indefinitely, to prevent the encryption keys from ultimately being determined and compromised. When an SA nears expiration, a new one is created so that there is no loss of protected data flow.

Quick mode can also optionally perform additional Diffie-Hellman exchanges. Such exchanges would generate new public/private keys between the IPsec peers. This happens when the Diffie-Hellman keys expire, due to exceeding time or data allocations.

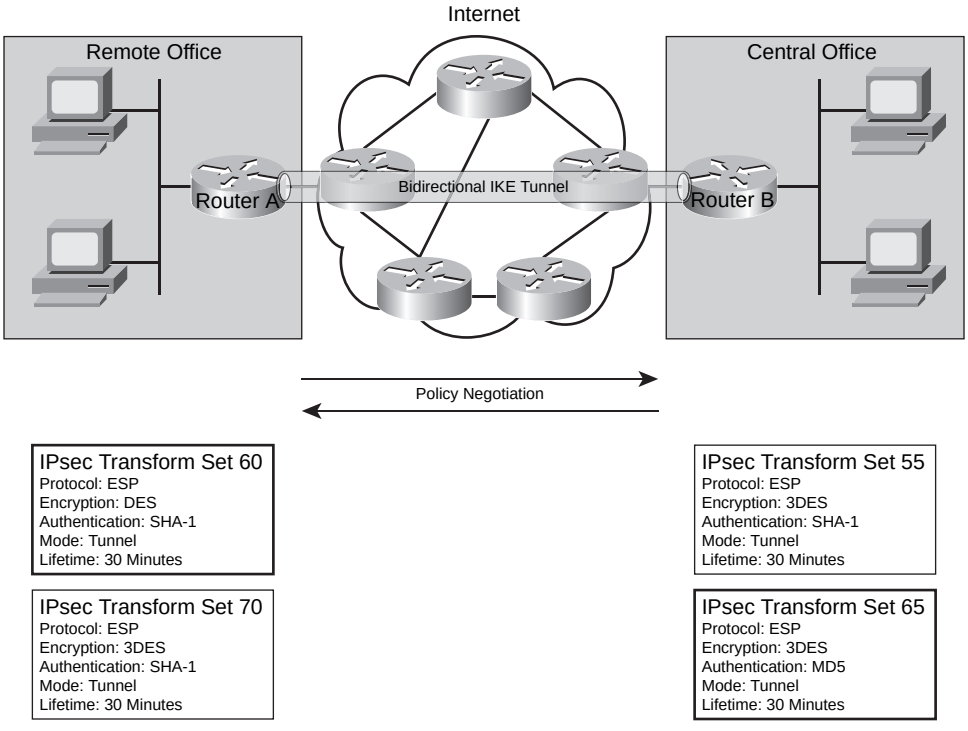
IPsec Transform Sets

A transform set, as described in the context of IKE policies, is a group of attributes that are exchanged together, which eliminates the need to coordinate and negotiate individual parameters. The difference between an IKE policy and an IPsec transform set are the attributes that are exchanged. Five parameters must be coordinated during quick mode between IPsec peers:

- IPsec protocol (ESP or AH)
- IPsec encryption type (DES, 3DES, or AES)
- IPsec authentication (MD5 or SHA-1)
- IPsec mode (tunnel or transport)
- IPsec SA lifetime (seconds or kilobytes)

Figure 13-5 shows how the two IPsec endpoints use IPsec transform sets to coordinate the IPsec SAs.

Figure 13-5 *IPsec Transform Sets*



In Figure 13-5, Router A and Router B are attempting to negotiate parameters for IPsec SAs. Assume that Router A starts the IKE phase 2 negotiation process. Router A sends to Router B its two IPsec transform sets, 60 and 70. A single variation in any parameter makes the entire transform set different. The same IPsec transform set can be used for SAs to many destinations, so there is no need to create an identical transform set for each IPsec endpoint.

When Router B receives the two IPsec transform sets, it sequentially compares the contents of each to any transform sets that it has. The local IPsec transform set numbers determine the comparison priority or sequence. These numbers are not actual parameters in the transform set. The values of the security parameters are the important parts.

In this example, the contents of IPsec transform set 70 from Router A match those in IPsec transform set 55 in Router B. Router B responds to Router A that it accepts IPsec transform set 70 and the IPsec SAs are built. If Router B could not find any exact parameter matches between the IPsec transform sets, then the IPsec SAs would not be constructed and the IPsec process would fail.

A remote site that creates only a single IPsec connection to one location needs only one IPsec transform set. Multiple IPsec transform sets may be needed if one location establishes many IPsec connections to different destinations. It is possible to use a single IPsec transform set for SAs to multiple locations. Multiple IPsec transform sets would be needed if each IPsec connection used different security parameters.

Security Associations

A security association (SA) is a group of security services (parameters) agreed upon between two IPsec peers. As discussed earlier, these security parameters are exchanged during IKE phase 2 in transform sets. Once each IPsec endpoint agrees upon the common services to use, the IPsec SAs are constructed.

Each IPsec SA is a one-way connection between two IPsec peers. In most cases, effective network communications requires bidirectional traffic flow. Thus, a complete IPsec connection between two endpoints consists of two IPsec SAs—one incoming and one outgoing. Each of these SAs uses the same security parameters agreed upon in the IPsec transform sets. However, each SA is tracked and maintained separately.

Each SA is referenced by a Security Parameter Index (SPI). The SPI travels with each IPsec packet and is used to reference and confirm the security parameters upon arrival at the far end. The use of the SPI eliminates the need to send the security parameters with each IPsec packet.

Each IPsec client uses an SA Database (SAD) to track each of the SAs that the client participates in. Remember that for any remote client, there will be two SAs. The SAD contains the following information about each IPsec connection (SA):

- Destination IP address
- SPI number
- IPsec protocol (ESP or AH)

A second database, the Security Policy Database (SPD), contains the security parameters that were agreed upon for each SA (in the transform sets). For each SA, this database contains:

- Encryption algorithm (DES, 3DES, or AES)
- Authentication algorithm (MD5 or SHA-1)
- IPsec mode (tunnel or transport)
- Key lifetime (seconds or kilobytes)

The use of both the SAD and the SPD allows any IPsec client to quickly track IPsec attributes for any incoming or outgoing packets to any remote client.

SA Lifetime

One of the security parameters that must be agreed upon in the IPsec transform sets is the key lifetime. The IPsec tunnel must not use the same key indefinitely, due to the possibility of compromise. IPsec forces the keys to expire either after a predetermined amount of time (measured in seconds) or after a predetermined amount of data has been transferred (measured in kilobytes).

If data continues to flow through the IPsec connection as the key expiration approaches, new keys are exchanged, new tunnels are built, and the data stream is switched over to the new SAs. All of this typically occurs without any loss of data through the IPsec connection and without knowledge of the users involved.

The lifetime values must not be too excessive, to ensure that the security of the tunnel is not exposed or compromised. On the other hand, short lifetime values cause the two IPsec endpoints to continually generate and exchange new keys. Configuration of these values is described in the "Configure the IPsec Transform Sets" section later in this chapter.

Step 4: Secure Data Transfer

After the IPsec transform sets have been agreed upon by the two endpoints and the SAD and SPD have been updated at each end (which implies that the SAs have been built), traffic can flow through the IPsec tunnel. Remember that not all traffic is permitted through the tunnel. Only the interesting traffic that caused the tunnel to be created is permitted to use the tunnel. All other traffic continues to flow through the interface, but not through the IPsec VPN tunnel.

Step 5: IPsec Tunnel Termination

There are two events that can cause an IPsec tunnel to be terminated. As mentioned earlier, if the SA lifetime expires (time and/or byte count), then the tunnel must be torn down. However, if secure transfer is still needed between the two endpoints, then a new pair of SAs is normally created before the old set is retired.

It is also possible to manually delete an IPsec tunnel. This is typically done by an administrator at either end of the IPsec connection. In most cases, the automatic termination of the tunnel (due to excessive time or kilobyte usage) is sufficient and an administrator never needs to get involved.

Upon tunnel termination, all information about an SA is removed from both the SAD and SPD, regardless of the cause. The security parameters may be copied to a new SPI as the secure data exchange continues, but the actual entries in the database are deleted.