CCNA 3 v7.0 Curriculum: Module 8 – VPN and IPsec Concepts

itexamanswers.net/ccna-3-v7-0-curriculum-module-8-vpn-and-ipsec-concepts.html

April 11, 2020

8.0. Introduction

8.0.1. Why should I take this module?

Welcome to VPN and IPsec Concepts!

Have you, or someone you know, ever been hacked while using public WiFi? It's surprisingly easy to do. But there is a solution to this problem: Virtual Private Networks (VPNs) and the additional protection of IP Security (IPsec). VPNs are commonly used by remote workers around the globe. There are also personal VPNs that you can use when you are on public WiFi. In fact, there are many different kinds of VPNs using IPsec to protect and authenticate IP packets between their source and destination. Want to know more? Click Next!

8.0.2. What will I learn in this module?

Module Title: VPN and IPsec Concepts

Module Objective: Explain how VPNs and IPsec are used to secure site-to-site and remote access connectivity.

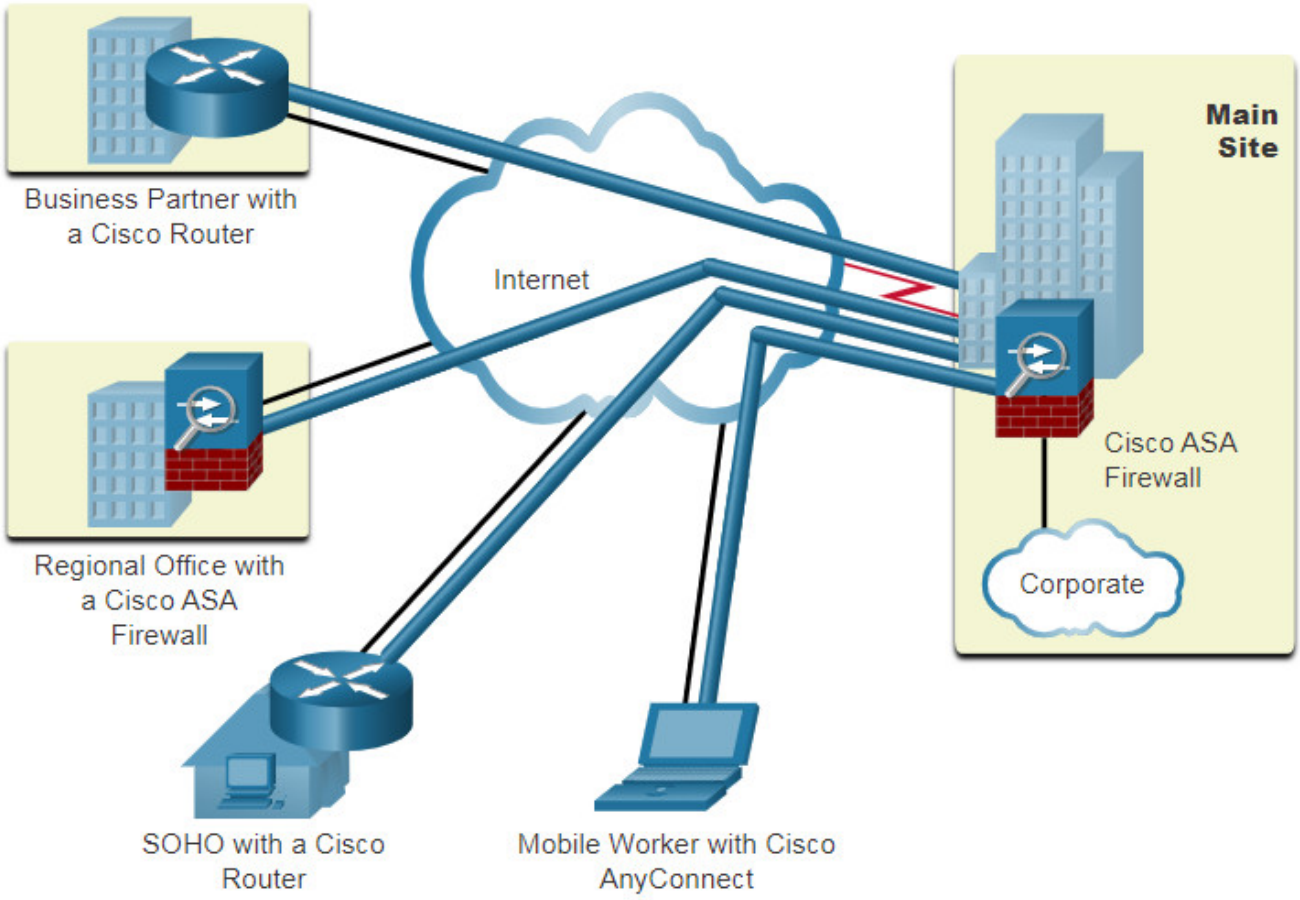
Topic Title	Topic Objective
VPN Technology	Describe benefits of VPN technology.
Types of VPNs	Describe different types of VPNs.
IPsec	Explain how the IPsec framework is used to secure network traffic.

8.1. VPN Technology

8.1.1. Virtual Private Networks

To secure network traffic between sites and users, organizations use virtual private networks (VPNs) to create end-to-end private network connections. A VPN is virtual in that it carries information within a private network, but that information is actually transported over a public network. A VPN is private in that the traffic is encrypted to keep the data confidential while it is transported across the public network.

The figure shows a collection of various types of VPNs managed by an enterprise's main site. The tunnel enables remote sites and users to access main site's network resources securely.



- A Cisco Adaptive Security Appliance (ASA) firewall helps organizations provide secure, high performance connectivity including VPNs and always-on access for remote branches and mobile users.
- SOHO stands for small office home office where a VPN-enabled router can provide VPN connectivity back to the corporate main site.
- Cisco AnyConnect is software that remote workers can use to establish client-based VPN connection with the main site.

The first types of VPNs were strictly IP tunnels that did not include authentication or encryption of the data. For example, Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco and which does not include encryption services. It is used to encapsulate IPv4 and IPv6 traffic inside an IP tunnel to create a virtual point-to-point link.

8.1.2. VPN Benefits

Modern VPNs now support encryption features, such as Internet Protocol Security (IPsec) and Secure Sockets Layer (SSL) VPNs to secure network traffic between sites.

Major benefits of VPNs are shown in the table.

Benefit	Description
Cost Savings	With the advent of cost-effective, high-bandwidth technologies, organizations can use VPNs to reduce their connectivity costs while simultaneously increasing remote connection bandwidth.
Security	VPNs provide the highest level of security available, by using advanced encryption and authentication protocols that protect data from unauthorized access.
Scalability	VPNs allow organizations to use the internet, making it easy to add new users without adding significant infrastructure.
Compatibility	VPNs can be implemented across a wide variety of WAN link options including all the popular broadband technologies. Remote workers can take advantage of these high-speed connections to gain secure access to their corporate networks.

8.1.3. Site-to-Site and Remote-Access VPNs

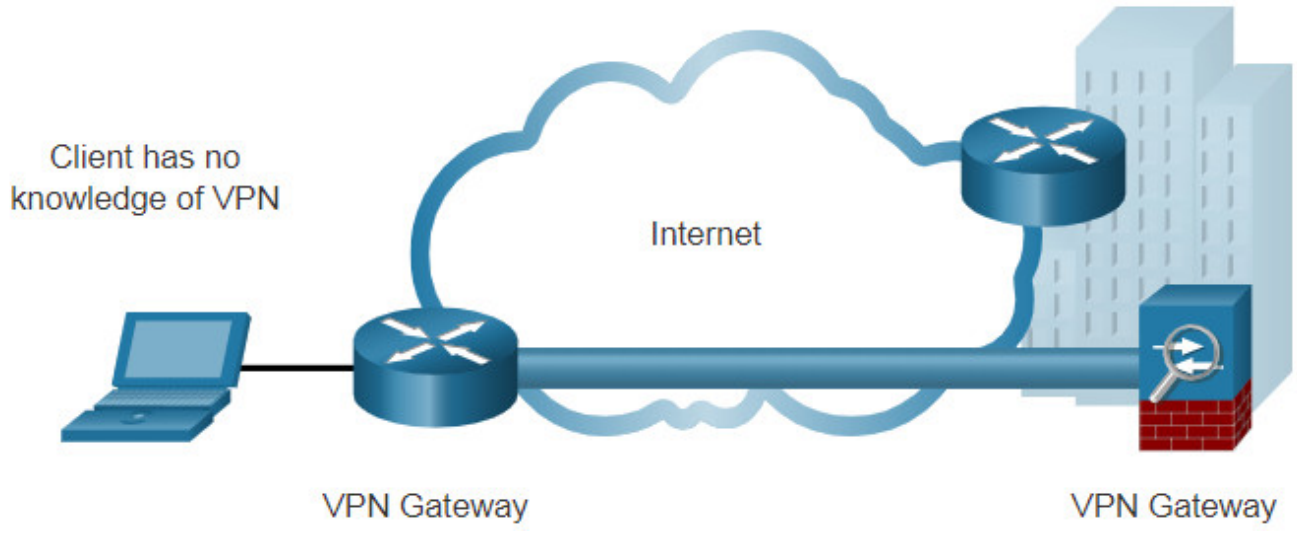
VPNs are commonly deployed in one of the following configurations: site-to-site or remote-access.

Click each for VPN type for more information.

- Site-to-Site VPN
- Remote-Access VPN

Site-to-Site VPN

A site-to-site VPN is created when VPN terminating devices, also called VPN gateways, are preconfigured with information to establish a secure tunnel. VPN traffic is only encrypted between these devices. Internal hosts have no knowledge that a VPN is being used.



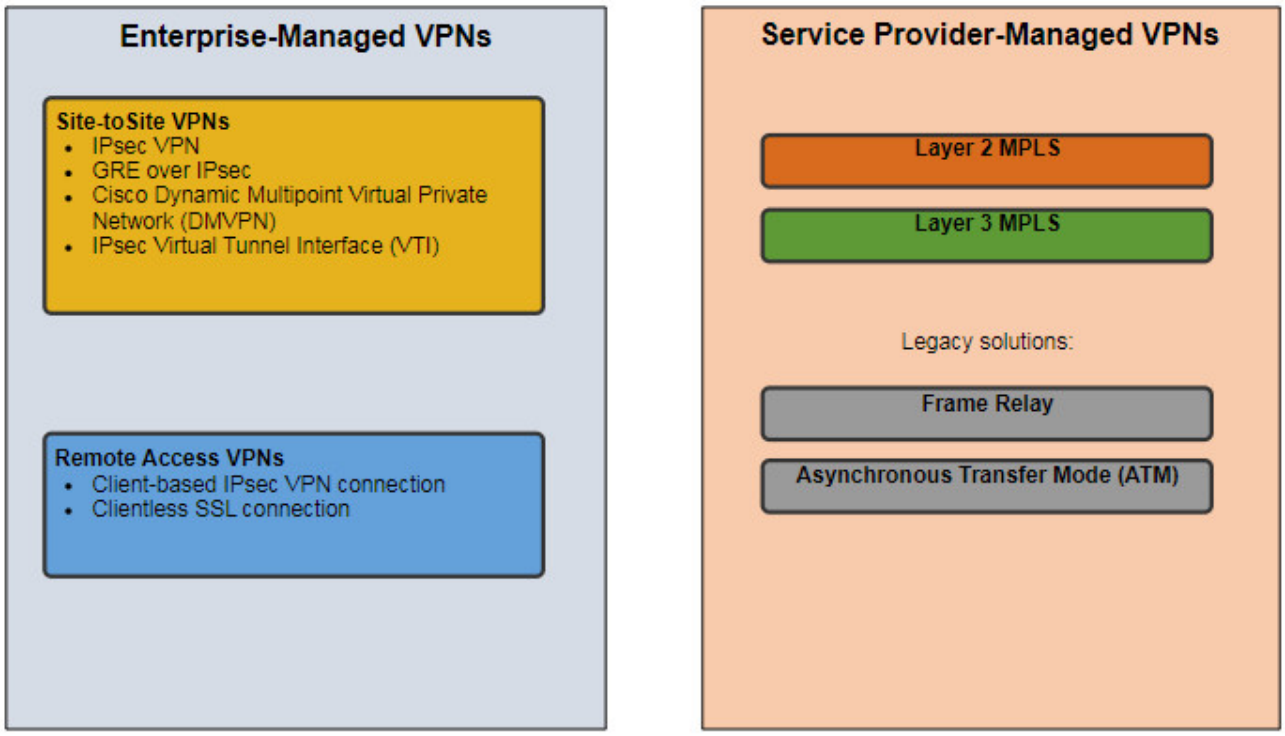
8.1.4. Enterprise and Service Provider VPNs

There are many options available to secure enterprise traffic. These solutions vary depending on who is managing the VPN.

VPNs can be managed and deployed as:

- **Enterprise VPNs** – Enterprise-managed VPNs are a common solution for securing enterprise traffic across the internet. Site-to-site and remote access VPNs are created and managed by the enterprise using both IPsec and SSL VPNs.
- **Service Provider VPNs** – Service provider-managed VPNs are created and managed over the provider network. The provider uses Multiprotocol Label Switching (MPLS) at Layer 2 or Layer 3 to create secure channels between an enterprise's sites. MPLS is a routing technology the provider uses to create virtual paths between sites. This effectively segregates the traffic from other customer traffic. Other legacy solutions include Frame Relay and Asynchronous Transfer Mode (ATM) VPNs.

The figure lists the different types of enterprise-managed and service provider-managed VPN deployments that will be discussed in more detail in this module.



8.2. Types of VPNs

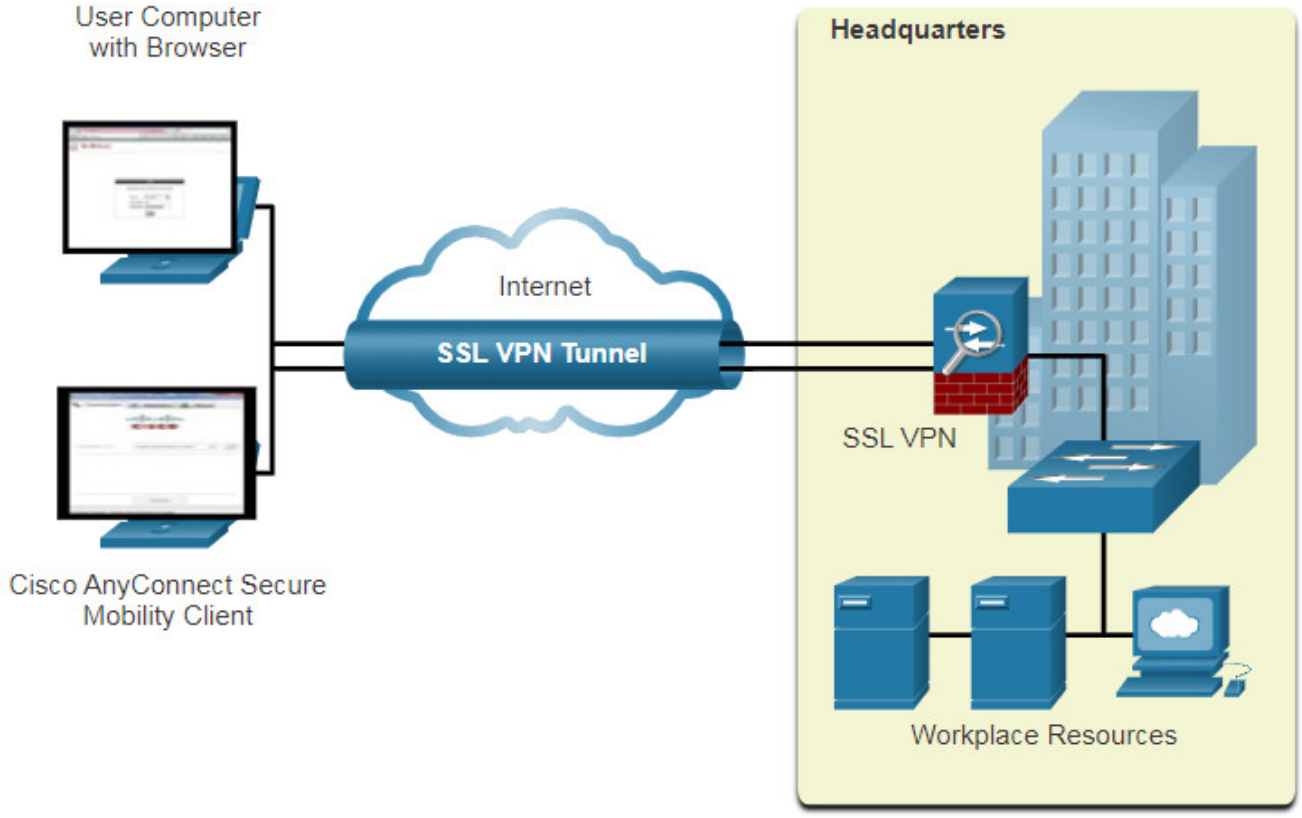
8.2.1. Remote-Access VPNs

In the previous topic you learned about the basics of a VPN. Here you will learn about the types of VPNs.

VPNs have become the logical solution for remote-access connectivity for many reasons. As shown in the figure, remote-access VPNs let remote and mobile users securely connect to the enterprise by creating an encrypted tunnel. Remote users can securely replicate their enterprise security access including email and network applications. Remote-access VPNs also allow contractors and partners to have limited access to the specific servers, web pages, or files as required. This means that these users can contribute to business productivity without compromising network security.

Remote-access VPNs are typically enabled dynamically by the user when required. Remote access VPNs can be created using either IPsec or SSL. As shown in the figure, a remote user must initiate a remote access VPN connection.

The figure displays two ways that a remote user can initiate a remote access VPN connection: clientless VPN and client-based VPN.



- **Clientless VPN connection** -The connection is secured using a web browser SSL connection. SSL is mostly used to protect HTTP traffic (HTTPS), and email protocols such as IMAP and POP3. For example, HTTPS is actually HTTP using an SSL tunnel. The SSL connection is first established, and then HTTP data is exchanged over the connection.

- **Client-based VPN connection** – VPN client software such as Cisco AnyConnect Secure Mobility Client must be installed on the remote user's end device. Users must initiate the VPN connection using the VPN client and then authenticate to the destination VPN gateway. When remote users are authenticated, they have access to corporate files and applications. The VPN client software encrypts the traffic using IPsec or SSL and forwards it over the internet to the destination VPN gateway.

8.2.2. SSL VPNs

When a client negotiates an SSL VPN connection with the VPN gateway, it actually connects using Transport Layer Security (TLS). TLS is the newer version of SSL and is sometimes expressed as SSL/TLS. However, both terms are often used interchangeably.

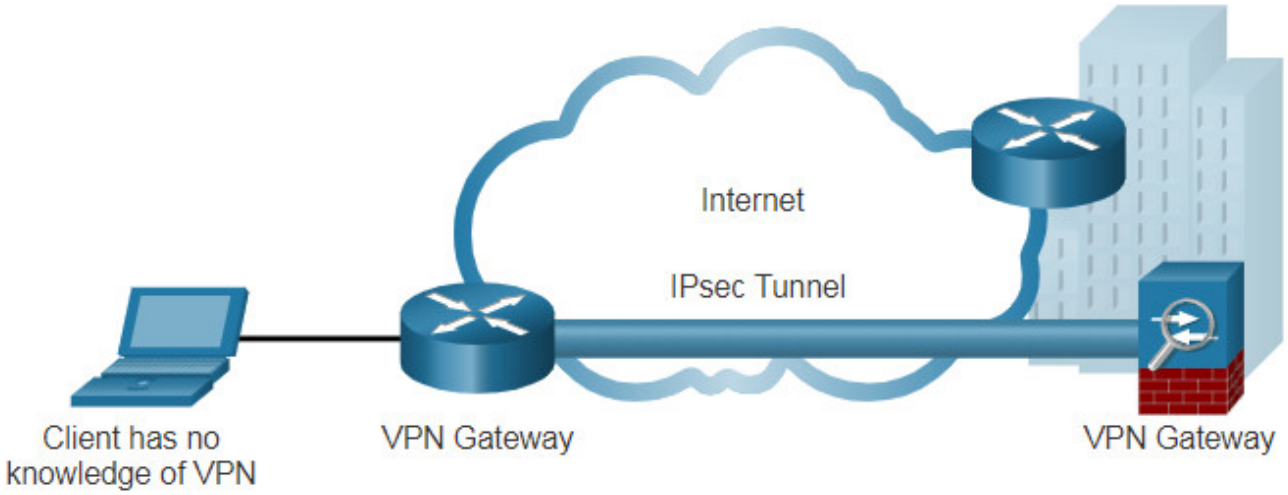
SSL uses the public key infrastructure and digital certificates to authenticate peers. Both IPsec and SSL VPN technologies offer access to virtually any network application or resource. However, when security is an issue, IPsec is the superior choice. If support and ease of deployment are the primary issues, consider SSL. The type of VPN method implemented is based on the access requirements of the users and the organization's IT processes. The table compares IPsec and SSL remote access deployments.

Feature	IPsec	SSL
Applications supported	**Extensive** – All IP-based applications are supported.	**Limited** – Only web-based applications and file sharing are supported.
Authentication strength	**Strong** – Uses two-way authentication with shared keys or digital certificates.	**Moderate** – Using one-way or two-way authentication.
Encryption strength	**Strong** – Uses key lengths from 56 bits to 256 bits.	**Moderate to strong** – With key lengths from 40 bits to 256 bits.
Connection complexity	**Medium** – Because it requires a VPN client pre-installed on a host.	**Low** – It only requires a web browser on a host.
Connection option	**Limited** – Only specific devices with specific configurations can connect.	**Extensive** – Any device with a web browser can connect.

It is important to understand that IPsec and SSL VPNs are not mutually exclusive. Instead, they are complementary; both technologies solve different problems, and an organization may implement IPsec, SSL, or both, depending on the needs of its telecommuters.

8.2.3. Site-to-Site IPsec VPNs

Site-to-site VPNs are used to connect networks across another untrusted network such as the internet. In a site-to-site VPN, end hosts send and receive normal unencrypted TCP/IP traffic through a VPN terminating device. The VPN terminating is typically called a VPN gateway. A VPN gateway device could be a router or a firewall, as shown in the figure. For example, the Cisco Adaptive Security Appliance (ASA) shown on the right side of the figure is a standalone firewall device that combines firewall, VPN concentrator, and intrusion prevention functionality into one software image.



The VPN gateway encapsulates and encrypts outbound traffic for all traffic from a particular site. It then sends the traffic through a VPN tunnel over the internet to a VPN gateway at the target site. Upon receipt, the receiving VPN gateway strips the headers, decrypts the content, and relays the packet toward the target host inside its private network.

Site-to-site VPNs are typically created and secured using IP security (IPsec).

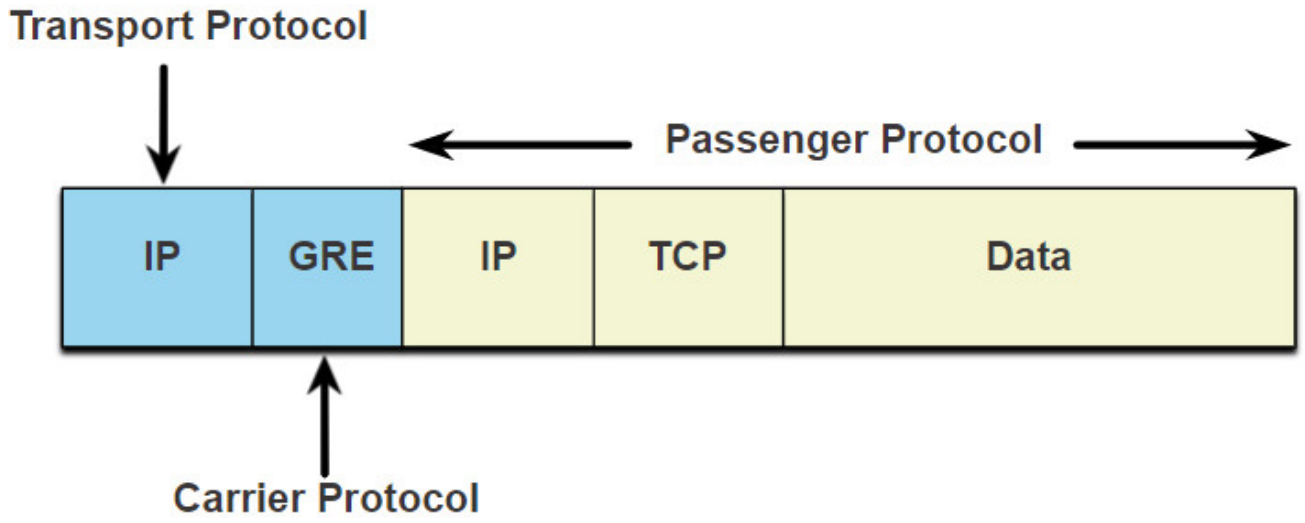
8.2.4. GRE over IPsec

Generic Routing Encapsulation (GRE) is a non-secure site-to-site VPN tunneling protocol. It can encapsulate various network layer protocols. It also supports multicast and broadcast traffic which may be necessary if the organization requires routing protocols to operate over a VPN. However, GRE does not by default support encryption; and therefore, it does not provide a secure VPN tunnel.

A standard IPsec VPN (non-GRE) can only create secure tunnels for unicast traffic. Therefore, routing protocols will not exchange routing information over an IPsec VPN.

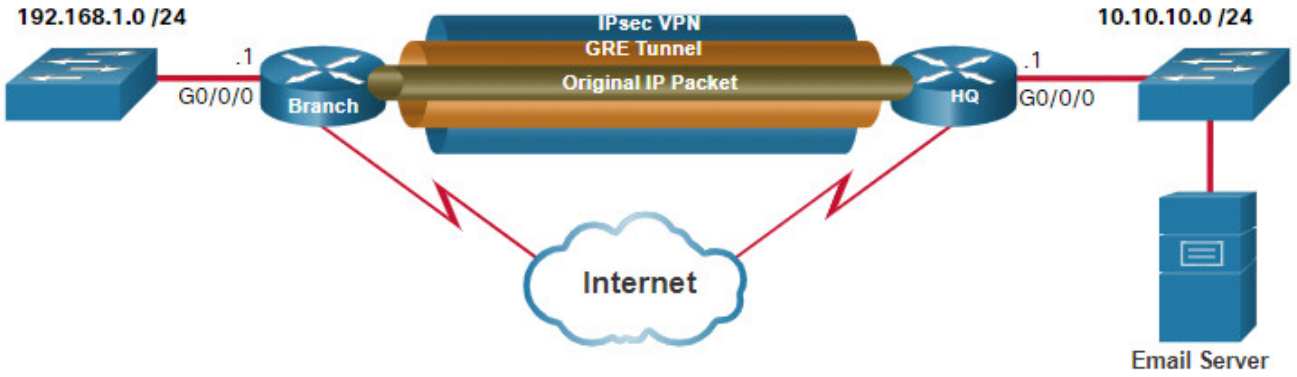
To solve this problem, we can encapsulate routing protocol traffic using a GRE packet, and then encapsulate the GRE packet into an IPsec packet to forward it securely to the destination VPN gateway.

The terms used to describe the encapsulation of GRE over IPsec tunnel are passenger protocol, carrier protocol, and transport protocol, as shown in the figure.



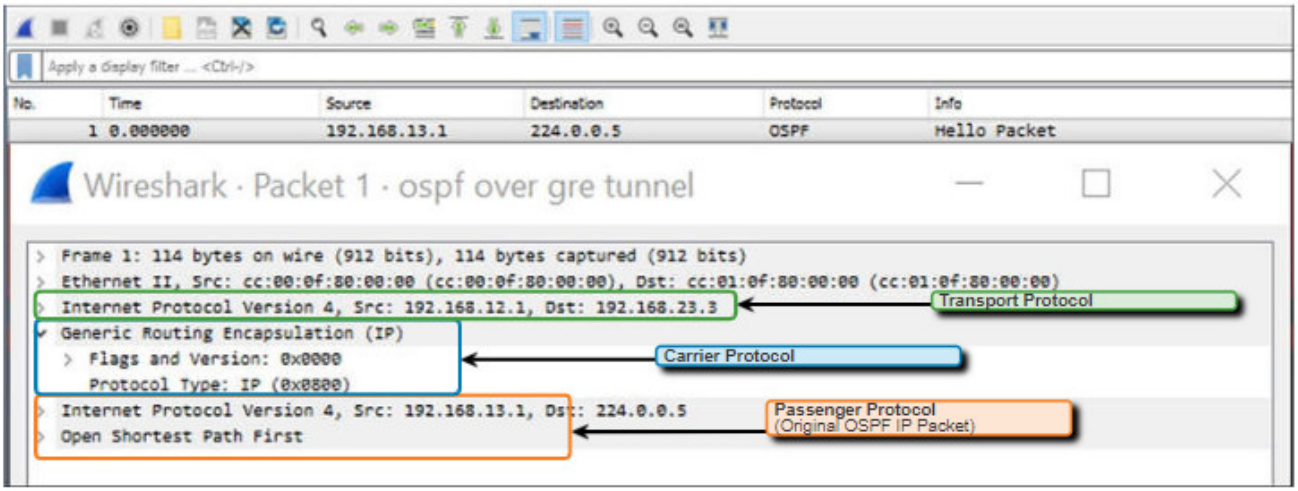
- **Passenger protocol** – This is the original packet that is to be encapsulated by GRE. It could be an IPv4 or IPv6 packet, a routing update, and more.
- **Carrier protocol** – GRE is the carrier protocol that encapsulates the original passenger packet.
- **Transport protocol** – This is the protocol that will actually be used to forward the packet. This could be IPv4 or IPv6.

For example, in the figure displaying a topology, Branch and HQ would like to exchange OSPF routing information over an IPsec VPN. However, IPsec does not support multicast traffic. Therefore, GRE over IPsec is used to support the routing protocol traffic over the IPsec VPN. Specifically, the OSPF packets (i.e., passenger protocol) would be encapsulated by GRE (i.e., carrier protocol) and subsequently encapsulated in an IPsec VPN tunnel.



The Wireshark screen capture in the figure displays an OSPF Hello packet that was sent using GRE over IPsec. In the example, the original OSPF Hello multicast packet (i.e., passenger protocol) was encapsulated with a GRE header (i.e., carrier protocol), which is

subsequently encapsulated by another IP header (i.e., transport protocol). This IP header would then be forwarded over an IPsec tunnel.



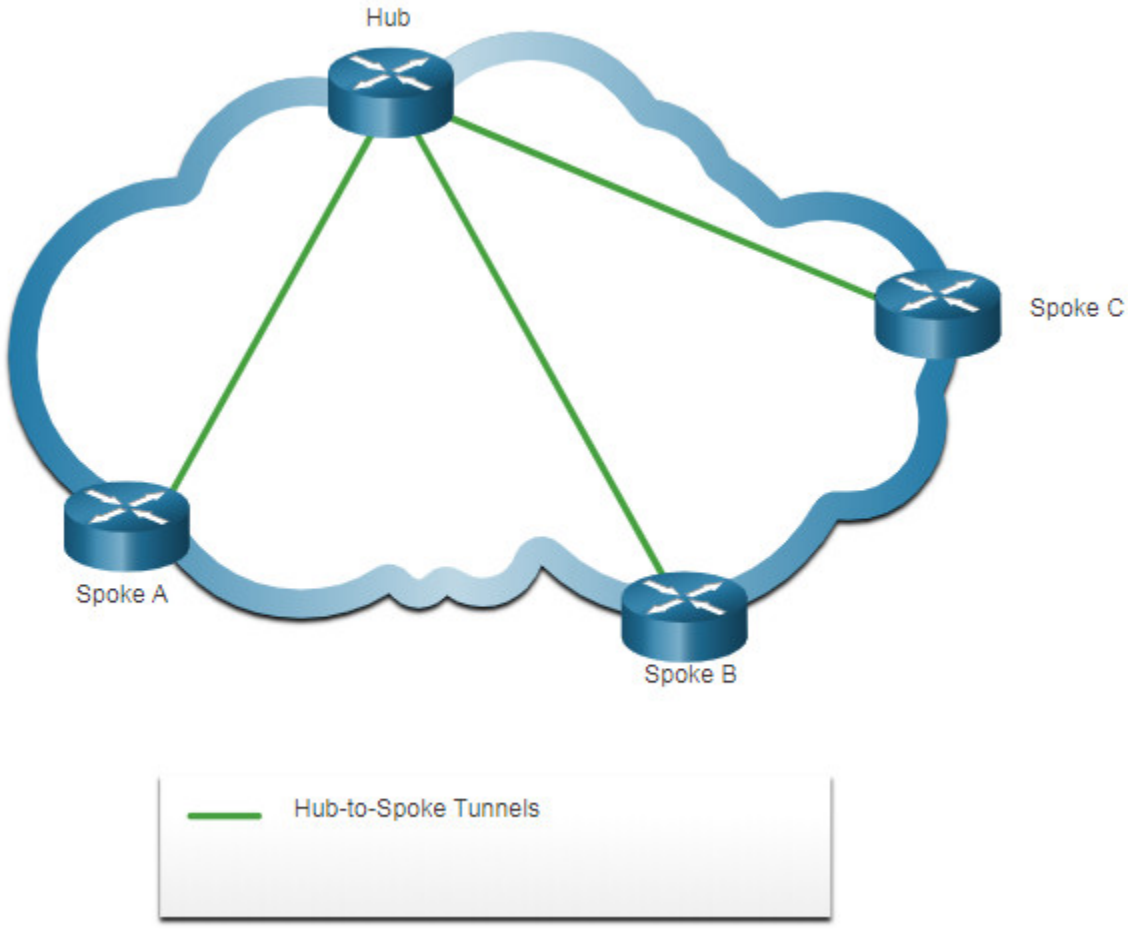
8.2.5. Dynamic Multipoint VPNs

Site-to-site IPsec VPNs and GRE over IPsec are adequate to use when there are only a few sites to securely interconnect. However, they are not sufficient when the enterprise adds many more sites. This is because each site would require static configurations to all other sites, or to a central site.

Dynamic Multipoint VPN (DMVPN) is a Cisco software solution for building multiple VPNs in an easy, dynamic, and scalable manner. Like other VPN types, DMVPN relies on IPsec to provide secure transport over public networks, such as the internet.

DMVPN simplifies the VPN tunnel configuration and provides a flexible option to connect a central site with branch sites. It uses a hub-and-spoke configuration to establish a full mesh topology. Spoke sites establish secure VPN tunnels with the hub site, as shown in the figure.

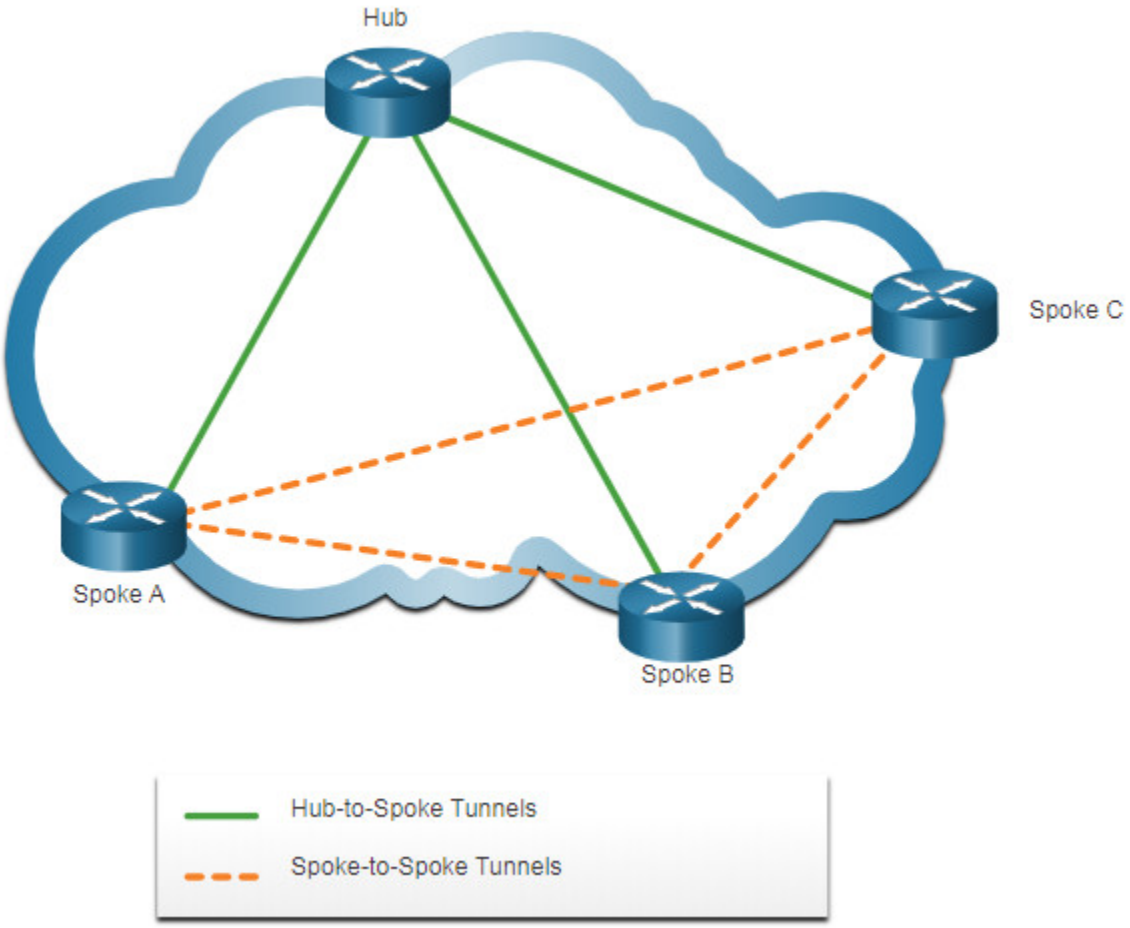
DMVPN Hub-to-Spoke Tunnels



Each site is configured using Multipoint Generic Routing Encapsulation (mGRE). The mGRE tunnel interface allows a single GRE interface to dynamically support multiple IPsec tunnels. Therefore, when a new site requires a secure connection, the same configuration on the hub site would support the tunnel. No additional configuration would be required.

Spoke sites could also obtain information about remote sites from the central site. They can use this information to establish direct VPN tunnels, as shown in the figure.

DMVPN Hub-to-Spoke and Spoke-to-Spoke Tunnels

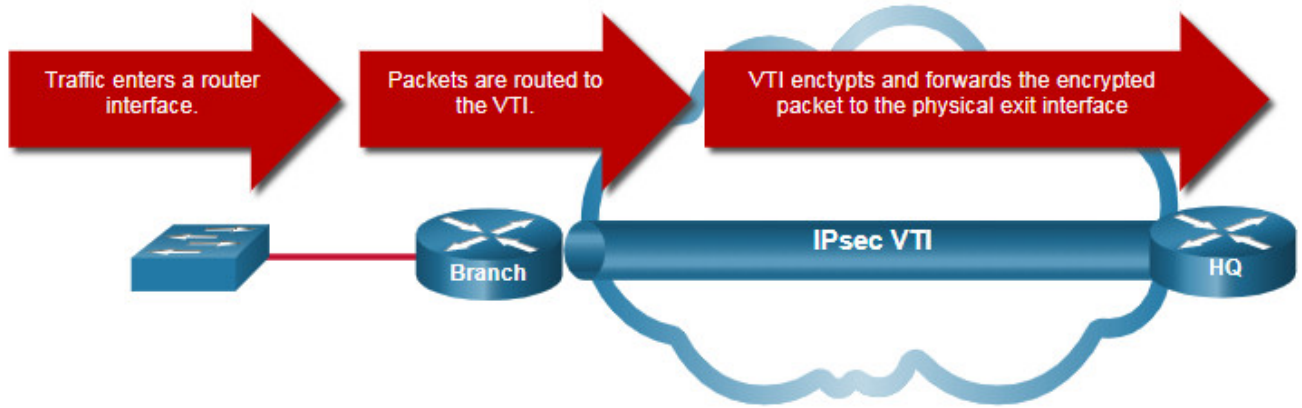


8.2.6. IPsec Virtual Tunnel Interface

Like DMVPNs, IPsec Virtual Tunnel Interface (VTI) simplifies the configuration process required to support multiple sites and remote access. IPsec VTI configurations are applied to a virtual interface instead of static mapping the IPsec sessions to a physical interface.

IPsec VTI is capable of sending and receiving both IP unicast and multicast encrypted traffic. Therefore, routing protocols are automatically supported without having to configure GRE tunnels.

IPsec VTI can be configured between sites or in a hub-and-spoke topology.



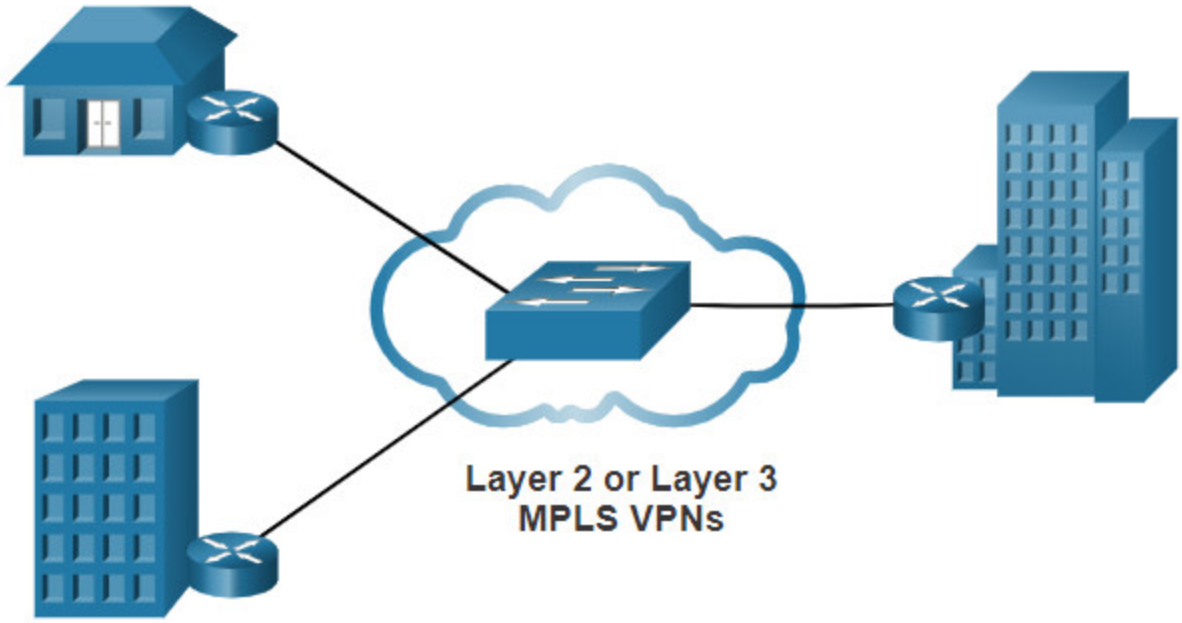
8.2.7. Service Provider MPLS VPNs

Traditional service provider WAN solutions such as leased lines, Frame Relay, and ATM connections were inherently secure in their design. Today, service providers use MPLS in their core network. Traffic is forwarded through the MPLS backbone using labels that are previously distributed among the core routers. Like legacy WAN connections, traffic is secure because service provider customers cannot see each other's traffic.

MPLS can provide clients with managed VPN solutions; therefore, securing traffic between client sites is the responsibility of the service provider. There are two types of MPLS VPN solutions supported by service providers:

- **Layer 3 MPLS VPN** – The service provider participates in customer routing by establishing a peering between the customer's routers and the provider's routers. Then customer routes that are received by the provider's router are then redistributed through the MPLS network to the customer's remote locations.
- **Layer 2 MPLS VPN** – The service provider is not involved in the customer routing. Instead, the provider deploys a Virtual Private LAN Service (VPLS) to emulate an Ethernet multiaccess LAN segment over the MPLS network. No routing is involved. The customer's routers effectively belong to the same multiaccess network.

The figure shows a service provider that offers both Layer 2 and Layer 3 MPLS VPNs.



8.3. IPsec

8.3.1. Video – IPsec Concepts

In the previous topic you learned about types of VPNs. It is important to understand how IPsec works with a VPN.

Click Play in the figure for a video about IPsec.

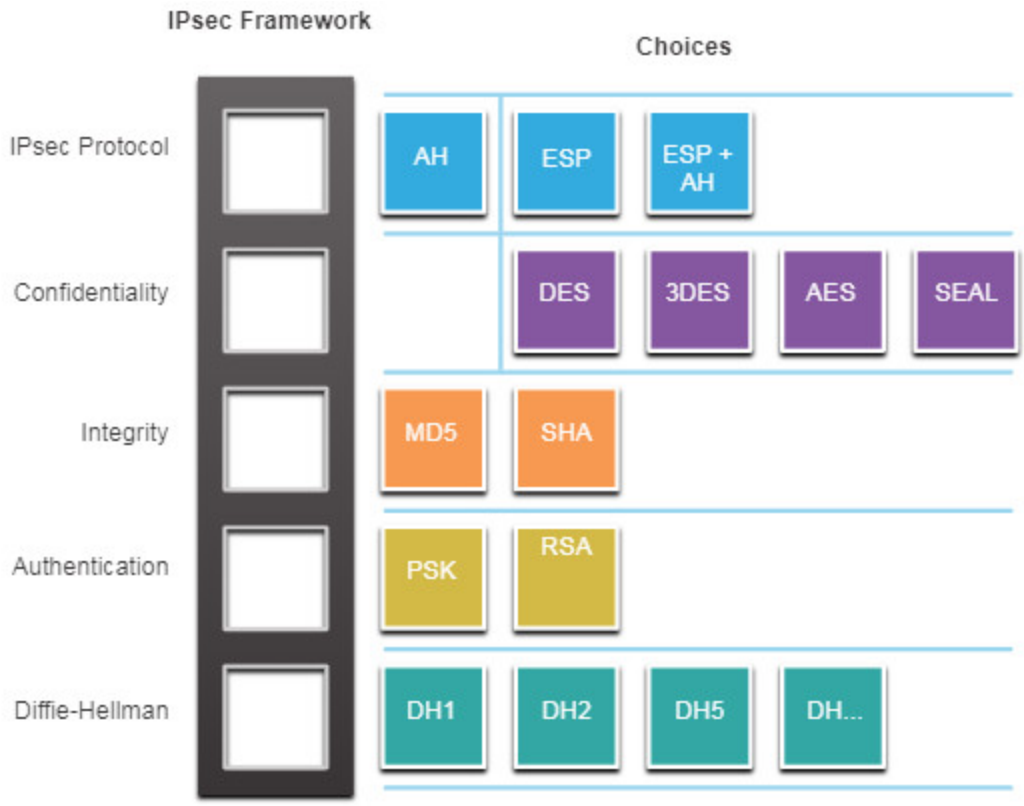
8.3.2. IPsec Technologies

IPsec is an IETF standard (RFC 2401-2412) that defines how a VPN can be secured across IP networks. IPsec protects and authenticates IP packets between source and destination. IPsec can protect traffic from Layer 4 through Layer 7.

Using the IPsec framework, IPsec provides these essential security functions:

- **Confidentiality** – IPsec uses encryption algorithms to prevent cybercriminals from reading the packet contents.
- **Integrity** – IPsec uses hashing algorithms to ensure that packets have not been altered between source and destination.
- **Origin authentication** – IPsec uses the Internet Key Exchange (IKE) protocol authenticate source and destination. Methods of authentication including using pre-shared keys (passwords), digital certificates, or RSA certificates.
- **Diffie-Hellman** – Secure key exchange typically various groups of the DH algorithm.

IPsec is not bound to any specific rules for secure communications. This flexibility of the framework allows IPsec to easily integrate new security technologies without updating the existing IPsec standards. The currently available technologies are aligned to their specific security function. The open slots shown in the IPsec framework in the figure can be filled with any of the choices that are available for that IPsec function to create a unique security association (SA).



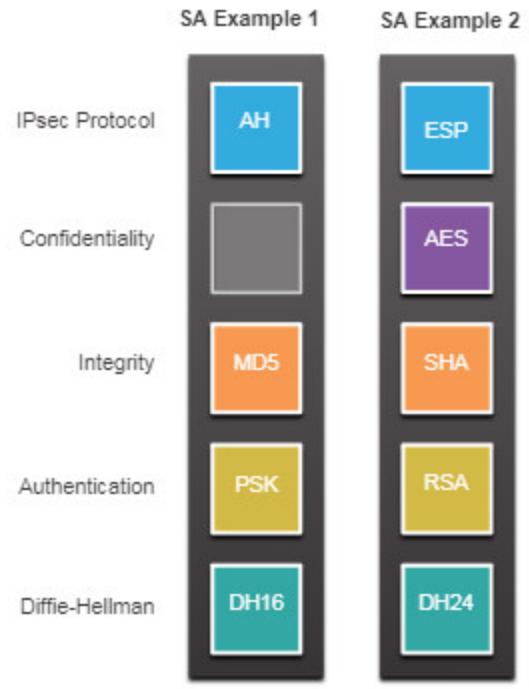
The security functions are list in the table.

IPsec Function	Description
IPsec Protocol	The choices for IPsec Protocol include Authentication Header (AH) or Encapsulation Security Protocol (ESP). AH authenticates the Layer 3 packet. ESP encrypts the Layer 3 packet. **Note**: ESP+AH is rarely used as this combination will not successfully traverse a NAT device.
Confidentiality	Encryption ensures confidentiality of the Layer 3 packet. Choices include Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES), or Software-Optimized Encryption Algorithm (SEAL). No encryption is also an option.
Integrity	Ensures that data arrives unchanged at the destination using a hash algorithm, such as message-digest 5 (MD5) or Secure Hash Algorithm (SHA).

IPsec Function	Description
Authentication	IPsec uses Internet Key Exchange (IKE) to authenticate users and devices that can carry out communication independently. IKE uses several types of authentication, including username and password, one-time password, biometrics, pre-shared keys (PSKs), and digital certificates using the Rivest, Shamir, and Adleman (RSA) algorithm.
Diffie-Hellman	IPsec uses the DH algorithm to provide a public key exchange method for two peers to establish a shared secret key. There are several different groups to choose from including DH14, 15, 16 and DH 19, 20, 21 and 24. DH1, 2 and 5 are no longer recommended.

The figure shows examples of SAs for two different implementations. An SA is the basic building block of IPsec. When establishing a VPN link, the peers must share the same SA to negotiate key exchange parameters, establish a shared key, authenticate each other, and negotiate the encryption parameters. Notice that SA Example 1 is using no encryption.

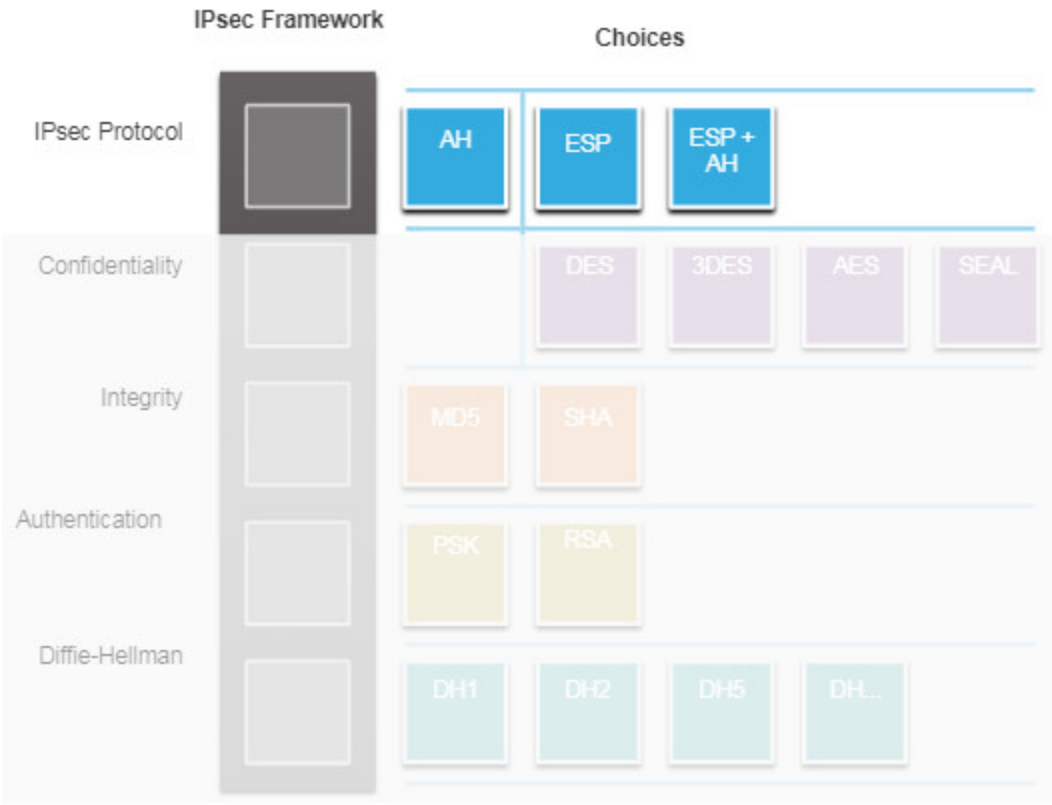
IPsec Security Association Examples



8.3.3. IPsec Protocol Encapsulation

Choosing the IPsec protocol encapsulation is the first building block of the framework. IPsec encapsulates packets using Authentication Header (AH) or Encapsulation Security Protocol (ESP).

The choice of AH or ESP establishes which other building blocks are available. Click each IPsec protocol in the figure for more information.

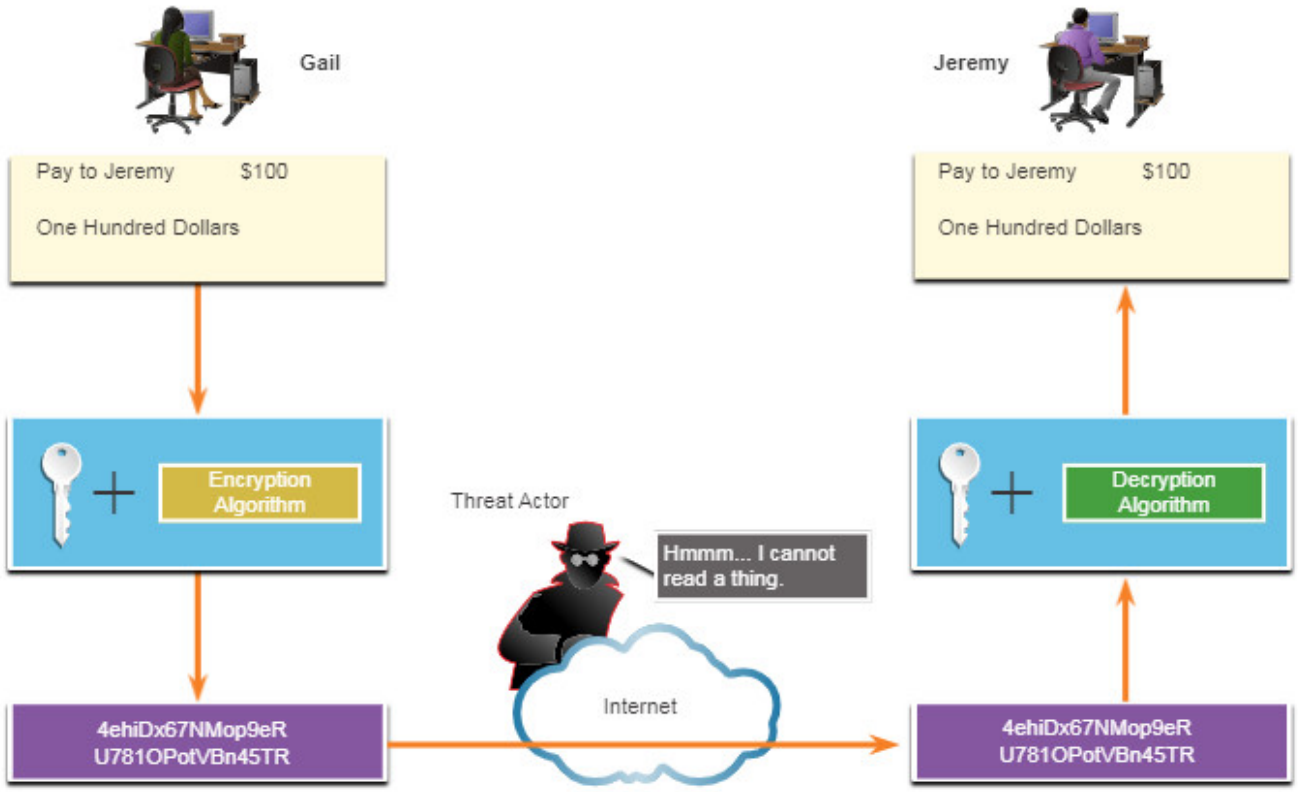


AH is appropriate only when confidentiality is not required or permitted. It provides data authentication and integrity, but it does not provide data confidentiality (encryption). All text is transported unencrypted.

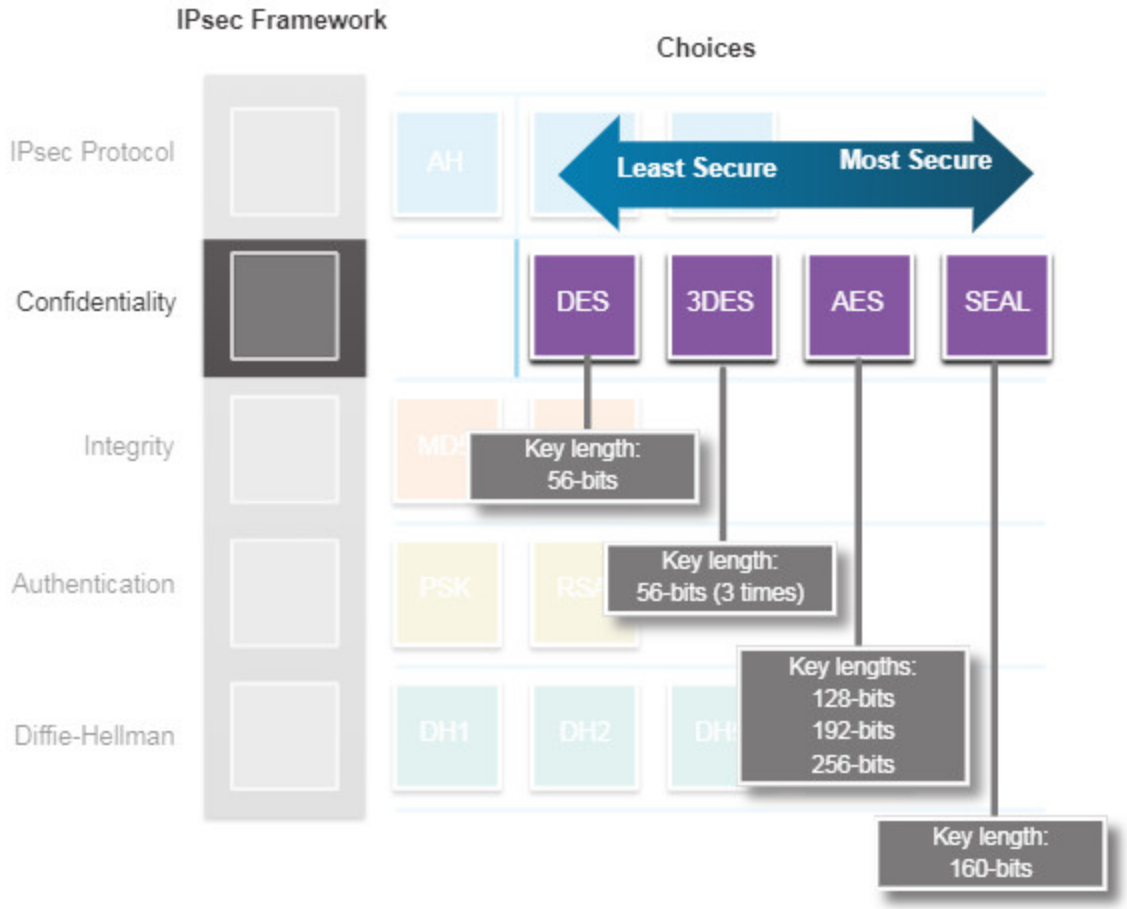
ESP provides both confidentiality and authentication. It provides confidentiality by performing encryption on the IP packet. ESP provides authentication for the inner IP packet and ESP header. Authentication provides data origin authentication and data integrity. Although both encryption and authentication are optional in ESP, at a minimum, one of them must be selected.

8.3.4. Confidentiality

Confidentiality is achieved by encrypting the data, as shown in the figure. The degree of confidentiality depends on the encryption algorithm and the length of the key used in the encryption algorithm. If someone tries to hack the key through a brute-force attack, the number of possibilities to try is a function of the length of the key. The time to process all the possibilities is a function of the computer power of the attacking device. The shorter the key, the easier it is to break. A 64-bit key can take approximately one year to break with a relatively sophisticated computer. A 128-bit key with the same machine can take roughly 1019 or 10 quintillion years to decrypt.



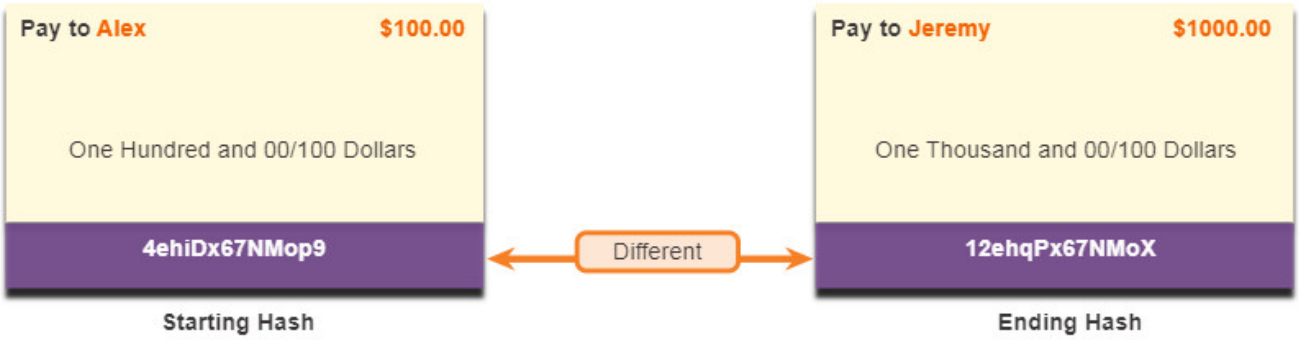
The encryption algorithms highlighted in the figure are all symmetric key cryptosystems.



- DES uses a 56-bit key.
- 3DES is a variant of the 56-bit DES. It uses three independent 56-bit encryption keys per 64-bit block, which provides significantly stronger encryption strength over DES.
- AES provides stronger security than DES and is computationally more efficient than 3DES. AES offers three different key lengths: 128 bits, 192 bits, and 256 bits.
- SEAL is a stream cipher, which means it encrypts data continuously rather than encrypting blocks of data. SEAL uses a 160-bit key.

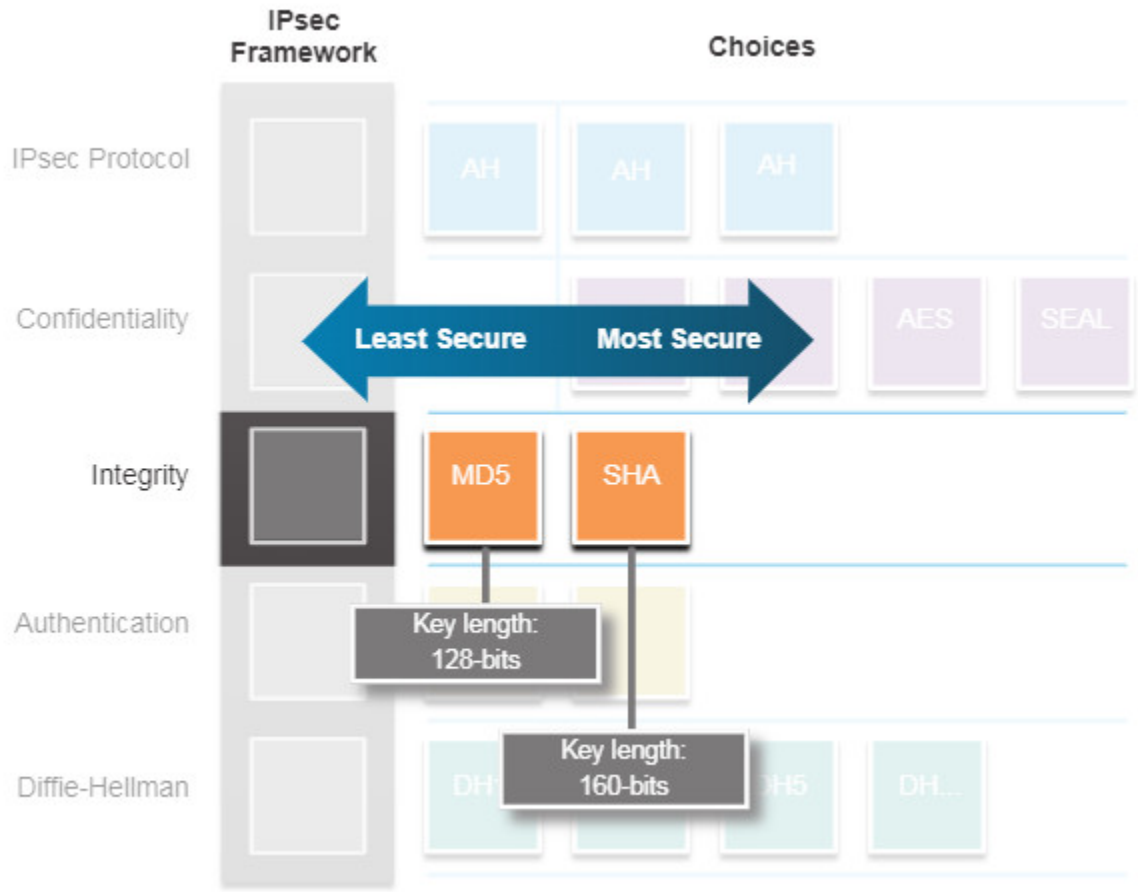
8.3.5. Integrity

Data integrity means that the data that is received is exactly the same data that was sent. Potentially, data could be intercepted and modified. For example, in the figure, assume that a check for $100 is written to Alex. The check is then mailed to Alex, but it is intercepted by a threat actor. The threat actor changes the name on the check to Jeremy and the amount on the check to $1,000 and attempts to cash it. Depending on the quality of the forgery in the altered check, the attacker could be successful.



Because VPN data is transported over the public internet, a method of proving data integrity is required to guarantee that the content has not been altered. The Hashed Message Authentication Code (HMAC) is a data integrity algorithm that guarantees the integrity of the message using a hash value. The figure highlights the two most common HMAC algorithms. Click each algorithm for more information.

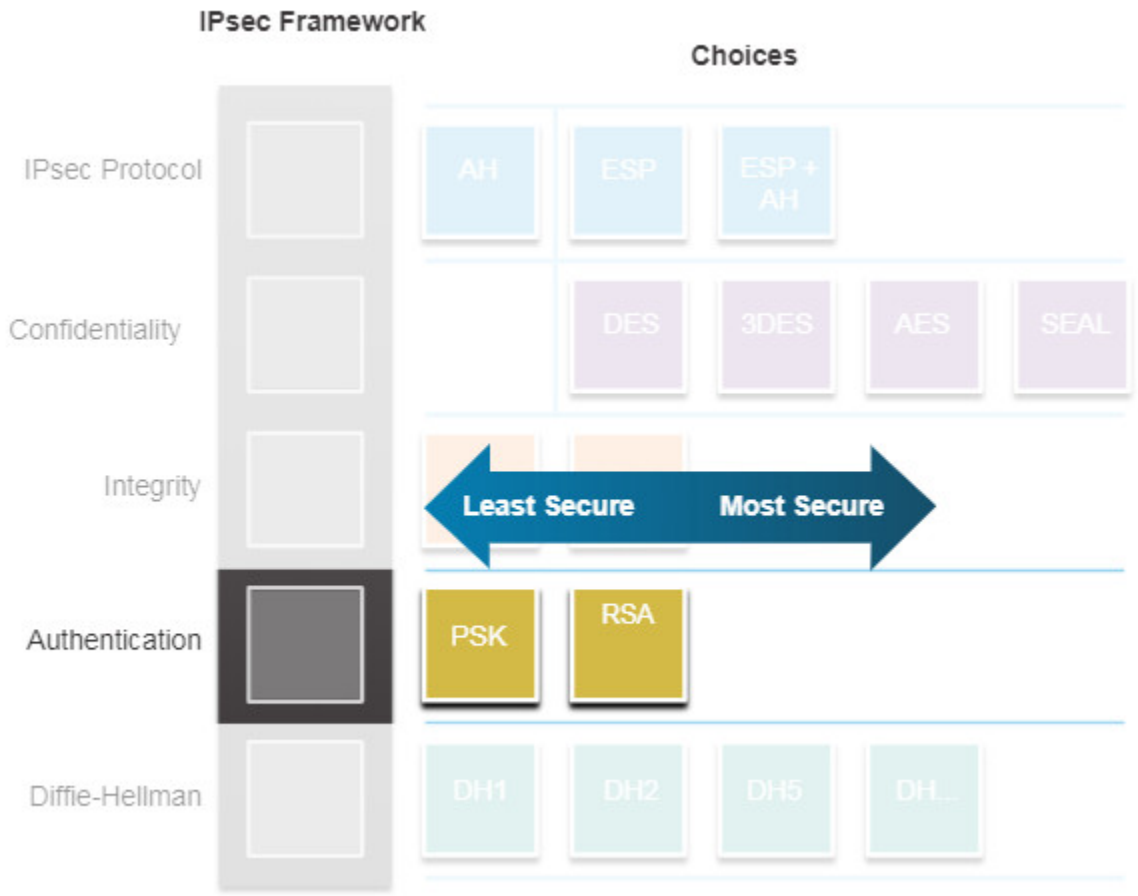
Note: Cisco now rates SHA-1 as legacy and recommends at least SHA-256 for integrity.



- Message-Digest 5 (MD5) uses a 128-bit shared-secret key. The variable-length message and 128-bit shared secret key are combined and run through the HMAC-MD5 hash algorithm. The output is a 128-bit hash.
- The Secure Hash Algorithm (SHA) uses a 160-bit secret key. The variable-length message and the 160-bit shared secret key are combined and run through the HMAC-SHA-1 algorithm. The output is a 160-bit hash.

8.3.6. Authentication

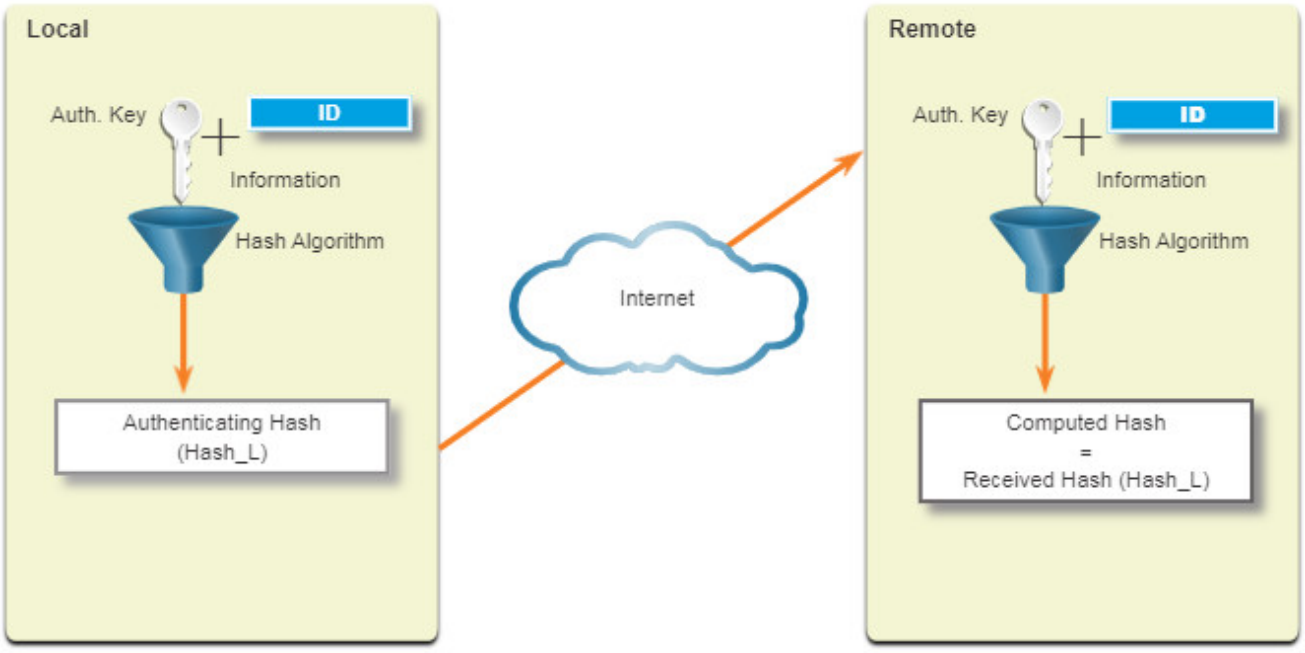
When conducting business long distance, you must know who is at the other end of the phone, email, or fax. The same is true of VPN networks. The device on the other end of the VPN tunnel must be authenticated before the communication path is considered secure. The figure highlights the two peer authentication methods.



- A pre-shared secret key (PSK) value is entered into each peer manually. The PSK is combined with other information to form the authentication key. PSKs are easy to configure manually, but do not scale well, because each IPsec peer must be configured with the PSK of every other peer with which it communicates.
- Rivest, Shamir, and Adleman (RSA) authentication uses digital certificates to authenticate the peers. The local device derives a hash and encrypts it with its private key. The encrypted hash is attached to the message and is forwarded to the remote end and acts like a signature. At the remote end, the encrypted hash is decrypted using the public key of the local end. If the decrypted hash matches the recomputed hash, the signature is genuine. Each peer must authenticate its opposite peer before the tunnel is considered secure.

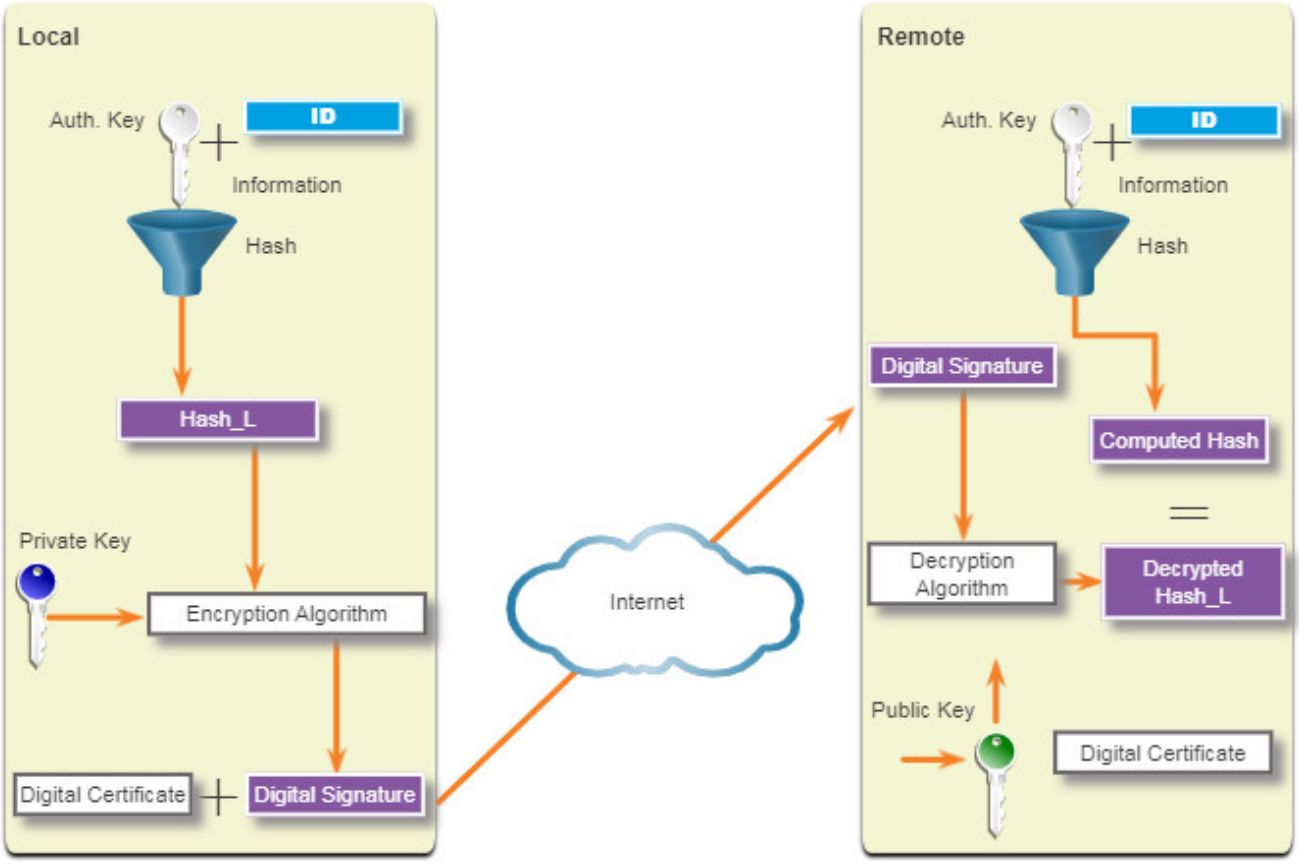
The figure shows an example of PSK authentication. At the local device, the authentication key and the identity information are sent through a hash algorithm to form the hash for the local peer (Hash_L). One-way authentication is established by sending Hash_L to the remote device. If the remote device can independently create the same hash, the local device is authenticated. After the remote device authenticates the local device, the authentication process begins in the opposite direction, and all steps are repeated from the remote device to the local device.

PSK Authentication



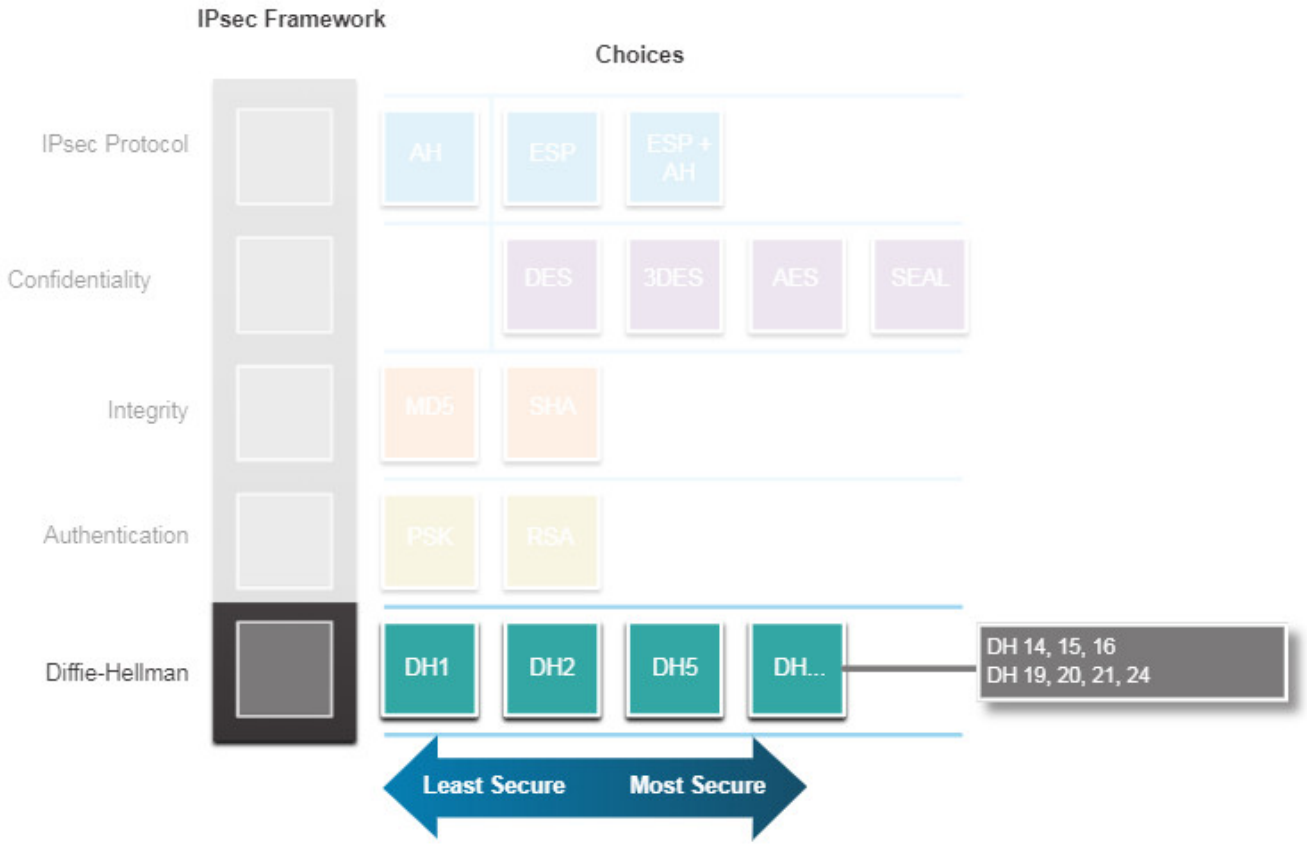
The figure shows an example of RSA authentication. At the local device, the authentication key and identity information are sent through the hash algorithm to form the hash for the local peer (Hash_L). Then the Hash_L is encrypted using the local device's private encryption key. This creates a digital signature. The digital signature and a digital certificate are forwarded to the remote device. The public encryption key for decrypting the signature is included in the digital certificate. The remote device verifies the digital signature by decrypting it using the public encryption key. The result is Hash_L. Next, the remote device independently creates Hash_L from stored information. If the calculated Hash_L equals the decrypted Hash_L, the local device is authenticated. After the remote device authenticates the local device, the authentication process begins in the opposite direction and all steps are repeated from the remote device to the local device.

PSK Authentication



8.3.7. Secure Key Exchange with Diffie-Hellman

Encryption algorithms require a symmetric, shared secret key to perform encryption and decryption. How do the encrypting and decrypting devices get the shared secret key? The easiest key exchange method is to use a public key exchange method, such as Diffie-Hellman (DH), as shown in the figure.



DH provides a way for two peers to establish a shared secret key that only they know, even though they are communicating over an insecure channel. Variations of the DH key exchange are specified as DH groups:

- DH groups 1, 2, and 5 should no longer be used. These groups support a key size of 768 bits, 1024 bits, and 1536 bits, respectively.
- DH groups 14, 15, and 16 use larger key sizes with 2048 bits, 3072 bits, and 4096 bits, respectively, and are recommended for use until 2030.
- DH groups 19, 20, 21 and 24 with respective key sizes of 256 bits, 384 bits, 521 bits, and 2048 bits support Elliptical Curve Cryptography (ECC), which reduces the time needed to generate keys. DH group 24 is the preferred next generation encryption.

The DH group you choose must be strong enough, or have enough bits, to protect the IPsec keys during negotiation. For example, DH group 1 is strong enough to support DES and 3DES encryption, but not AES. For example, if the encryption or authentication algorithms use a 128-bit key, use group 14, 19, 20 or 24. However, if the encryption or authentication algorithms use a 256-bit key or higher, use group 21 or 24.

8.3.8. Video – IPsec Transport and Tunnel Mode

Click Play in the figure for a video about IPsec transport and tunnel modes.

8.4. Module Practice and Quiz

8.4.1. What did I learn in this module?

A VPN is virtual in that it carries information within a private network, but that information is actually transported over a public network. A VPN is private in that the traffic is encrypted to keep the data confidential while it is transported across the public network. Benefits of VPNs are cost savings, security, scalability, and compatibility. VPNs are commonly deployed in one of the following configurations: site-to-site or remote-access. VPNs can be managed and deployed as enterprise VPNs and service provider VPNs.

Remote-access VPNs let remote and mobile users securely connect to the enterprise by creating an encrypted tunnel. Remote access VPNs can be created using either IPsec or SSL. When a client negotiates an SSL VPN connection with the VPN gateway, it actually connects using TLS. SSL uses the public key infrastructure and digital certificates to authenticate peers. Site-to-site VPNs are used to connect networks across an untrusted network such as the internet. In a site-to-site VPN, end hosts send and receive normal unencrypted TCP/IP traffic through a VPN terminating device. The VPN terminating device is typically called a VPN gateway. A VPN gateway could be a router or a firewall. GRE is a non-secure site-to-site VPN tunneling protocol. DMVPN is a Cisco software solution for easily building multiple, dynamic, scalable VPNs. Like DMVPNs, IPsec VTI simplifies the configuration process required to support multiple sites and remote access. IPsec VTI configurations are applied to a virtual interface instead of static mapping the IPsec sessions to a physical interface. IPsec VTI can send and receive both IP unicast and multicast encrypted traffic. MPLS can provide clients with managed VPN solutions; therefore, securing traffic between client sites is the responsibility of the service provider. There are two types of MPLS VPN solutions supported by service providers, Layer 3 MPLS VPN and Layer 2 MPLS VPN.

IPsec protects and authenticates IP packets between source and destination. IPsec can protect traffic from Layer 4 through Layer 7. Using the IPsec framework, IPsec provides confidentiality, integrity, origin authentication, and Diffie-Hellman. Choosing the IPsec protocol encapsulation is the first building block of the framework. IPsec encapsulates packets using AH or ESP. The degree of confidentiality depends on the encryption algorithm and the length of the key used in the encryption algorithm. The HMAC is an algorithm that guarantees the integrity of the message using a hash value. The device on the other end of the VPN tunnel must be authenticated before the communication path is considered secure. A PSK value is entered into each peer manually. The PSK is combined with other information to form the authentication key. RSA authentication uses digital certificates to authenticate the peers. The local device derives a hash and encrypts it with its private key. The encrypted hash is attached to the message and is forwarded to the remote end and acts like a signature. DH provides a way for two peers to establish a shared secret key that only they know, even though they are communicating over an insecure channel.

8.4.2 Module Quiz – VPN and IPsec Concepts

Download Slide Powerpoint (PPT)

CCNA 3 v7.0 Curriculum: Module 8 - VPN and IPsec Concepts.pptx

1 file(s) 1.71 MB

Download

Tags:ccna 3 v7 modules