Chapters 5/6

VPN and IPsec Concepts

Master 1 IS , Guelma University, 2024-2025

Chapter Objectives

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

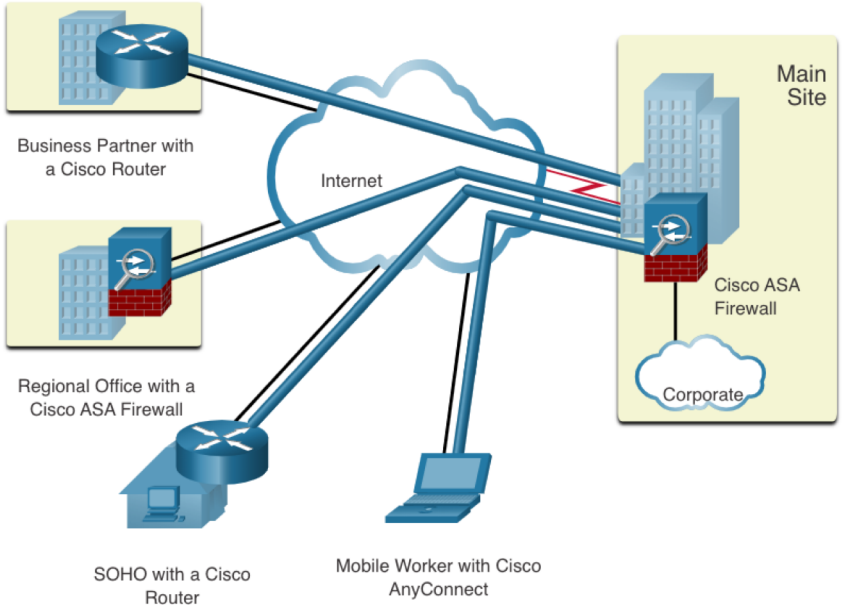
Topic Title	Topic Objective
VPN Technology	Describe the benefits of VPN technology.
Types of VPNs	Describe different types of VPNs.
IPsec	Explain how the IPsec framework is used to secure network traffic.

VPN Technology

VPN Technology

Virtual Private Networks

- 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.
- Cisco ASA stands for Adaptive Security Appliance. It is a series of network security devices that combine firewall capabilities with additional features such as VPN (Virtual Private Network) support, intrusion prevention, and advanced threat protection.



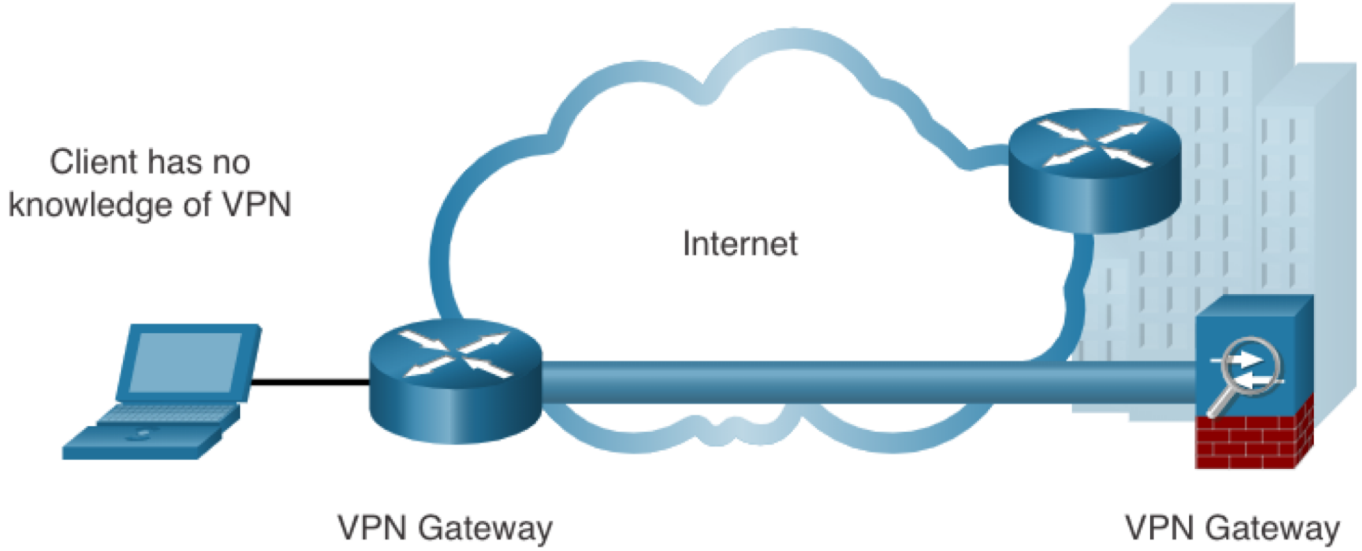
VPN Benefits

- 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	Organizations can use VPNs to reduce their connectivity costs while simultaneously increasing remote connection bandwidth.
Security	Encryption and authentication protocols 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 broadband technologies. Remote workers can use these high-speed connections to gain secure access to corporate networks.

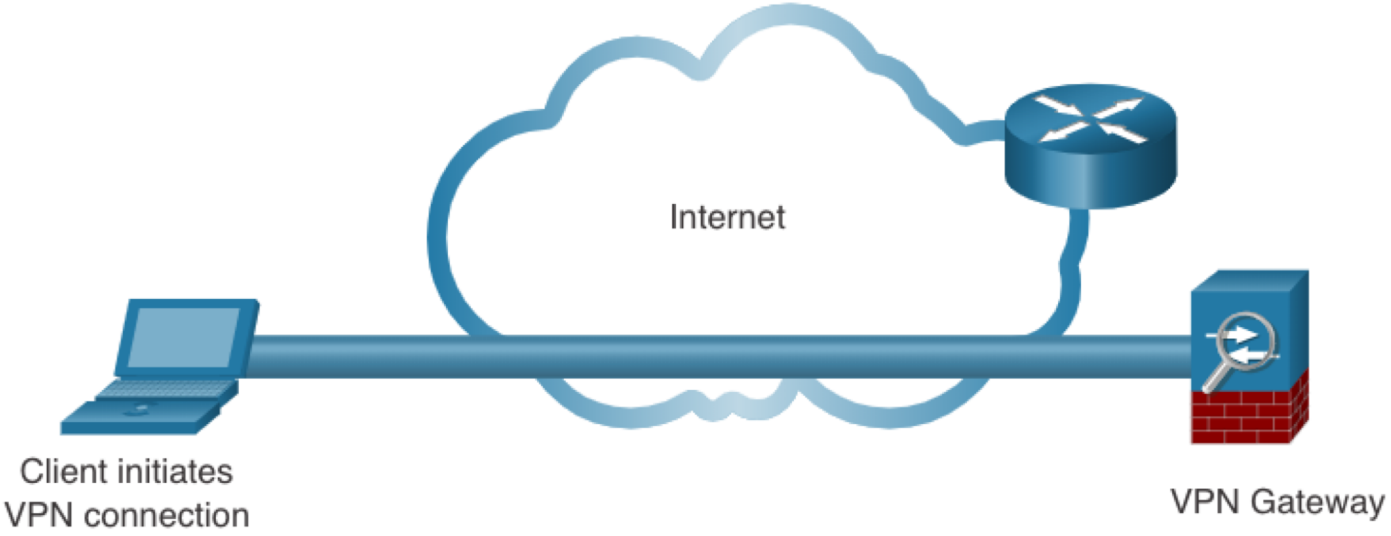
Site-to-Site and Remote Access VPNs

A site-to-site VPN is terminated on VPN gateways. VPN traffic is only encrypted between the gateways. Internal hosts have no knowledge that a VPN is being used.



Site-to-Site and Remote Access VPNs (Cont.)

A remote-access VPN is dynamically created to establish a secure connection between a client and a VPN terminating device.

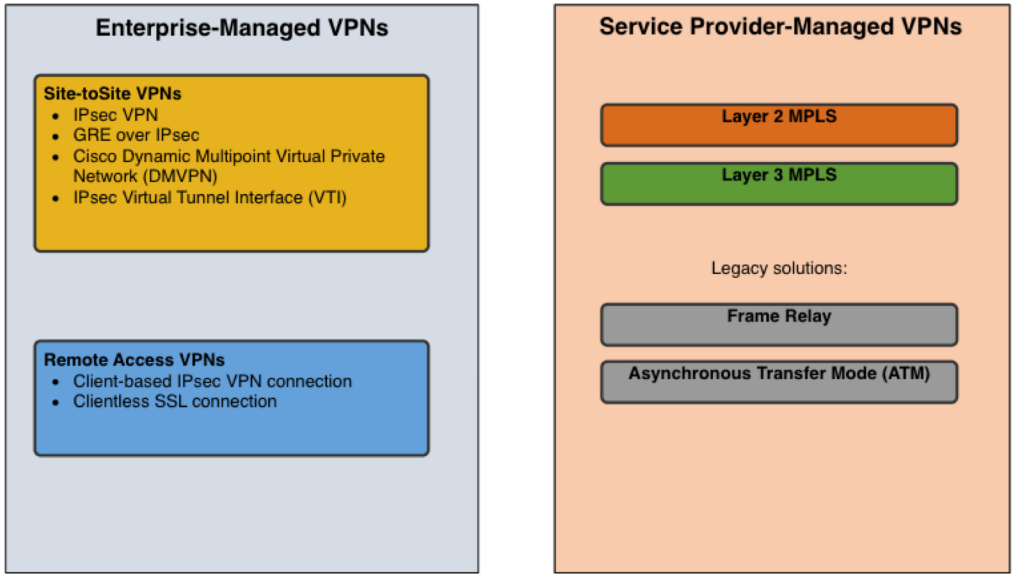


Enterprise and Service Provider VPNs

"GRE over IPSec" refers to a network tunneling configuration that combines two protocols—GRE (Generic Routing Encapsulation) and IPSec (Internet Protocol Security)—to provide both flexibility in encapsulating various types of traffic and strong encryption for secure data transmission.

VPNs can be managed and deployed as:

- **Enterprise VPNs** - common solution for securing enterprise traffic across the internet. Site-to-site and remote access VPNs are created and managed by the enterprise using IPsec and SSL VPNs.
- **Service Provider VPNs** - created and managed by 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, effectively segregating the traffic from other customer traffic.

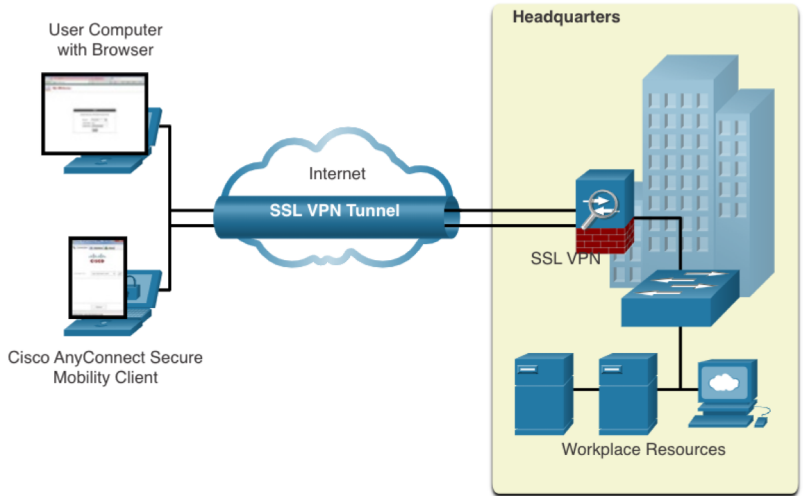


Layer 2 – Data Link Layer
Layer 3 – Network Layer

Types of VPNs

Remote-Access VPNs

- Remote-access VPNs let remote and mobile users securely connect to the enterprise.
- Remote-access VPNs are typically enabled dynamically by the user when required and can be created using either IPsec or SSL.
  - **Clientless VPN connection** -The connection is secured using a web browser SSL 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.



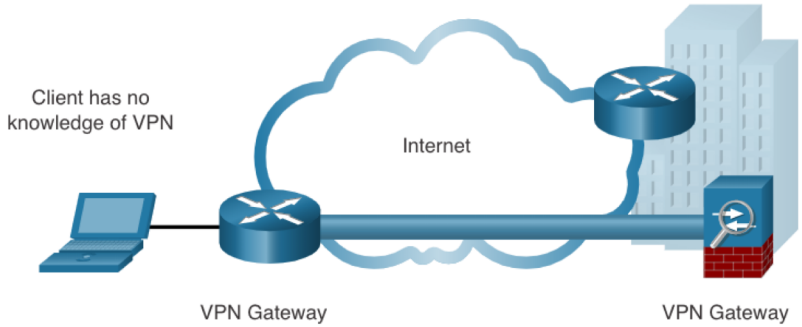
SSL VPNs

SSL uses the public key infrastructure and digital certificates to authenticate peers. 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	**Limited** – Only web-based applications and file sharing
Authentication strength	**Strong** – Two-way authentication with shared keys or digital certificates	**Moderate** – one-way or two-way authentication
Encryption strength	**Strong** – Key lengths 56 – 256 bits	**Moderate to strong** - Key lengths 40 – 256 bits
Connection complexity	**Medium** – Requires VPN client installed on a host	**Low** – Requires 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

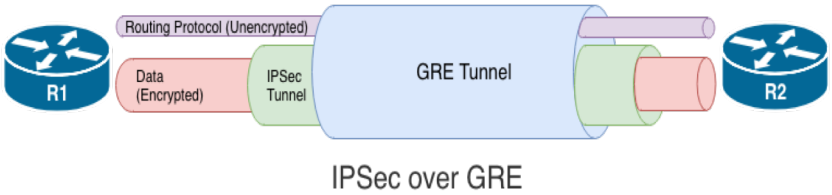
Site-to-Site IPsec VPNs

- Site-to-site VPNs connect networks across an untrusted network such as the internet.
- End hosts send and receive normal unencrypted TCP/IP traffic through a VPN gateway.
- The VPN gateway encapsulates and encrypts outbound traffic from a site and sends the traffic through the VPN tunnel to the VPN gateway at the target site. The receiving VPN gateway strips the headers, decrypts the content, and relays the packet toward the target host inside its private network.



GRE over IPsec

- Generic Routing Encapsulation (GRE) is a non-secure site-to-site VPN tunneling protocol.
- A GRE tunnel can encapsulate various network layer protocols as well as multicast and broadcast traffic.
- GRE does not by default support encryption; and therefore, it does not provide a secure VPN tunnel.
- A GRE packet can be encapsulated into an IPsec packet to forward it securely to the destination VPN gateway.
  - Standard IPsec VPNs (non-GRE) can only create secure tunnels for unicast traffic.
  - Encapsulating GRE into IPsec allows multicast routing protocol updates to be secured through a VPN. (i.e., With GRE, you can transport packets that are multicast or broadcast)



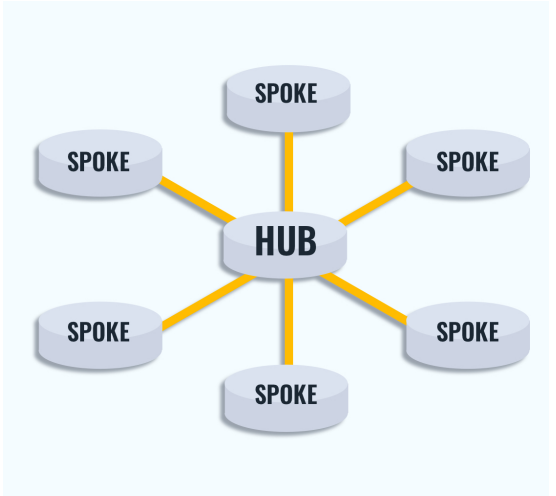
IPSec over GRE

Types of VPNs

Dynamic Multipoint VPNs

Site-to-site IPsec VPNs and GRE over IPsec are not sufficient when the enterprise adds many more sites. Dynamic Multipoint VPN (DMVPN) is a Cisco software solution for building multiple VPNs in an easy, dynamic, and scalable manner.

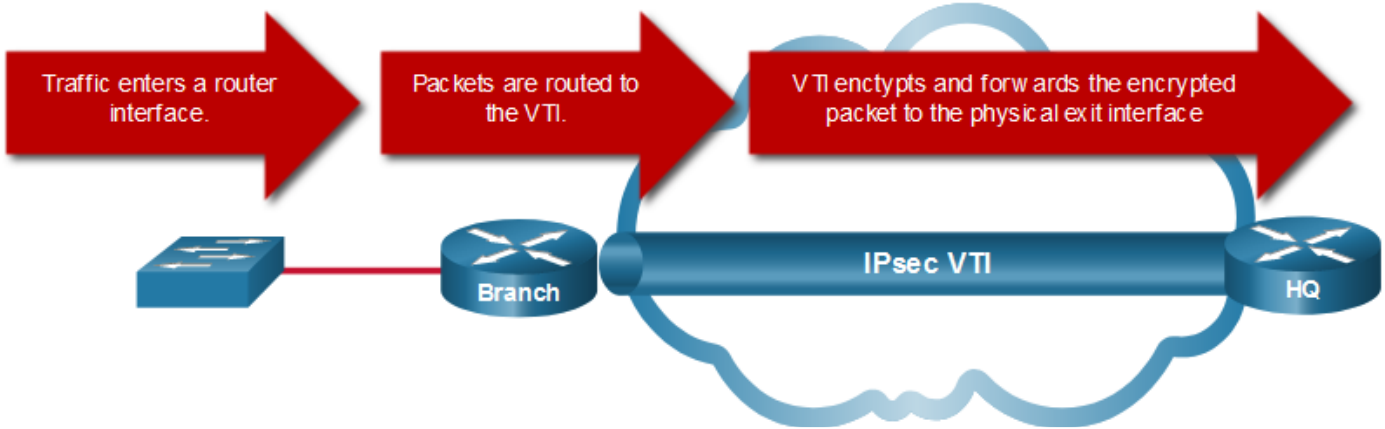
- DMVPN simplifies the VPN tunnel configuration and provides a flexible option to connect a central site with branch sites.
- It uses a hub-and-spoke configuration to establish a full mesh topology. (The hub and spoke topology is a network design where we have a central device (the hub) that is connected to multiple other devices (the spokes))
- Spoke sites establish secure VPN tunnels with the hub site.
- Each site is configure using Multipoint Generic Routing Encapsulation (mGRE). The mGRE tunnel interface allows a single GRE interface to dynamically support multiple IPsec tunnels.
- Spoke sites can also obtain information about each other, and alternatively build direct tunnels between themselves (spoke-to-spoke tunnels).



IPsec Virtual Tunnel Interface

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.



Service Provider MPLS VPNs

Today, service providers use MPLS in their core network. Traffic is forwarded through the MPLS backbone using labels. 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.
  - **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.

VPNs comparison

VPN Type	Description & Key Features	Primary Use Cases	Advantages	Limitations / Considerations
Remote-Access VPNs	Allows individual users to securely connect to a corporate or private network over the Internet. Often leverages protocols such as IPSec or SSL/TLS.	Telecommuting, mobile workers, remote system administration	Easy access for remote users; flexible authentication options	Requires client software; may have performance issues with high user counts; endpoint security is critical
Site-to-Site IPsec VPNs	Establishes secure encrypted tunnels between fixed sites or networks using IPSec. Traffic is securely transmitted between pre-defined endpoints.	Connecting branch offices or data centers	High security with IPSec; stable, always-on connections	Configuration can be complex; static endpoints require pre-planning and may not handle dynamic networks easily
GRE over IPsec	Combines Generic Routing Encapsulation (GRE) with IPSec encryption. GRE provides tunneling for various protocols (including multicast), while IPSec secures the data within the tunnel.	Routing between networks that need to handle multicast or non-IP traffic	Supports non-IP protocols and complex routing; flexibility by separating tunnel and encryption layers	Adds overhead due to double encapsulation; increased configuration complexity when compared to native IPsec tunnels
Dynamic Multipoint VPN (DMVPN)	A scalable VPN architecture that uses multipoint GRE (mGRE) for dynamic tunnel establishment, combined with IPSec for encryption. Employs Next Hop Resolution Protocol (NHRP) to enable on-demand connectivity.	Flexible connectivity for distributed networks; frequent branch-to-branch communication	Scalability; dynamic, on-demand tunnel creation; reduced static configuration	Initial set-up and NHRP configuration can be complex; troubleshooting dynamic tunnels may require additional expertise
IPsec Virtual Tunnel Interface (VTI)	Implements IPsec encryption over virtual interfaces, creating tunnel interfaces that allow IPsec to be managed like a typical routed interface. This supports dynamic routing protocols efficiently.	Integration with dynamic routing protocols for site-to-site connectivity or datacenter interconnects	Simplifies integration with routing protocols; more flexible tunnel management	May require additional configuration steps compared to classic policy-based IPsec; performance impact if not properly tuned
Service Provider MPLS VPNs	A carrier-based solution using Multiprotocol Label Switching (MPLS) to segregate customer traffic within a service provider's network. Customers receive a virtual private network without needing to manage end-to-end tunnels.	Enterprise-level inter-site connectivity via service providers; WAN services with QoS guarantees	High scalability; reliable service with managed performance and QoS guarantees; minimal on-premises configuration	Less control over underlying infrastructure; potential vendor lock-in and higher ongoing service costs compared to self-managed VPNs

IPsec

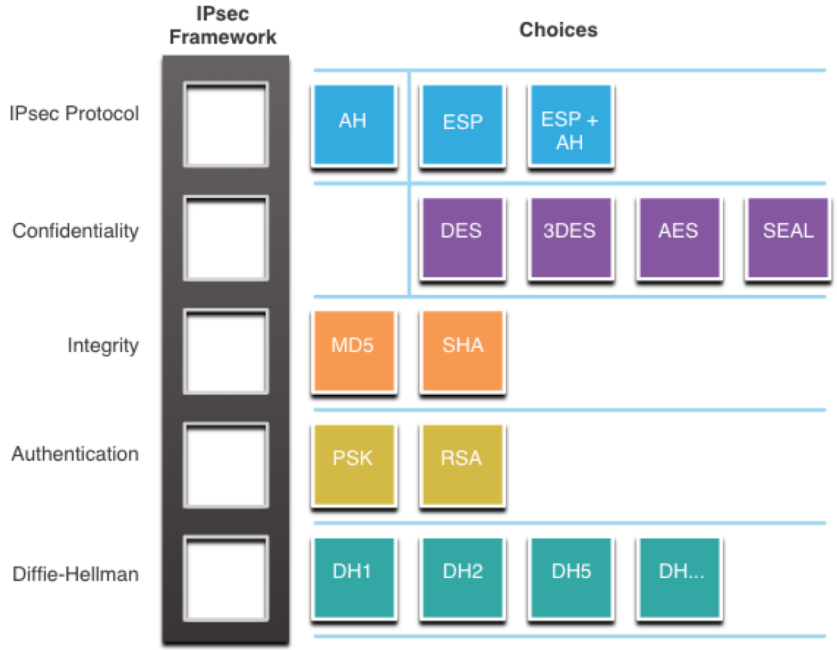
IPsec Technologies

IPsec is an IETF standard that defines how a VPN can be secured across IP networks. IPsec protects and authenticates IP packets between source and destination and provides these essential security functions:

- **Confidentiality** - Uses encryption algorithms to prevent cybercriminals from reading the packet contents.
- **Integrity** - Uses hashing algorithms to ensure that packets have not been altered between source and destination.
- **Origin authentication** - Uses the Internet Key Exchange (IKE) protocol to authenticate source and destination.
- **Diffie-Hellman** – Used to secure key exchange.

IPsec Technologies (Cont.)

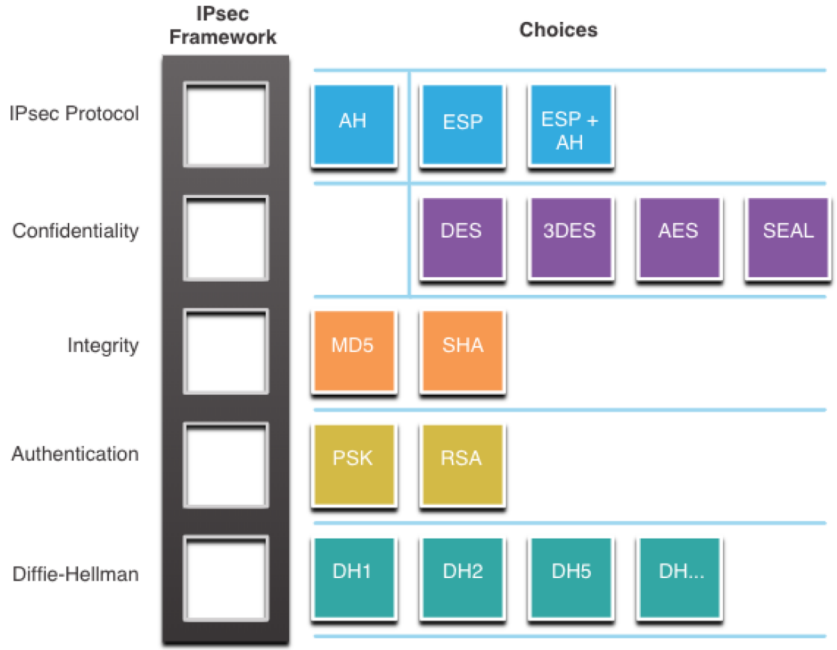
- IPsec is not bound to any specific rules for secure communications.
- IPsec can easily integrate new security technologies without updating existing IPsec standards.
- The open slots in the IPsec framework shown in the figure can be filled with any of the choices that are available for that IPsec function to create a unique security association (SA).
- SA is a contract that outlines the cryptographic parameters and methods to be used, ensuring confidentiality, integrity, and authenticity of the data.



IPsec Protocol Encapsulation

Choosing the IPsec protocol encapsulation is the first building block of the framework.

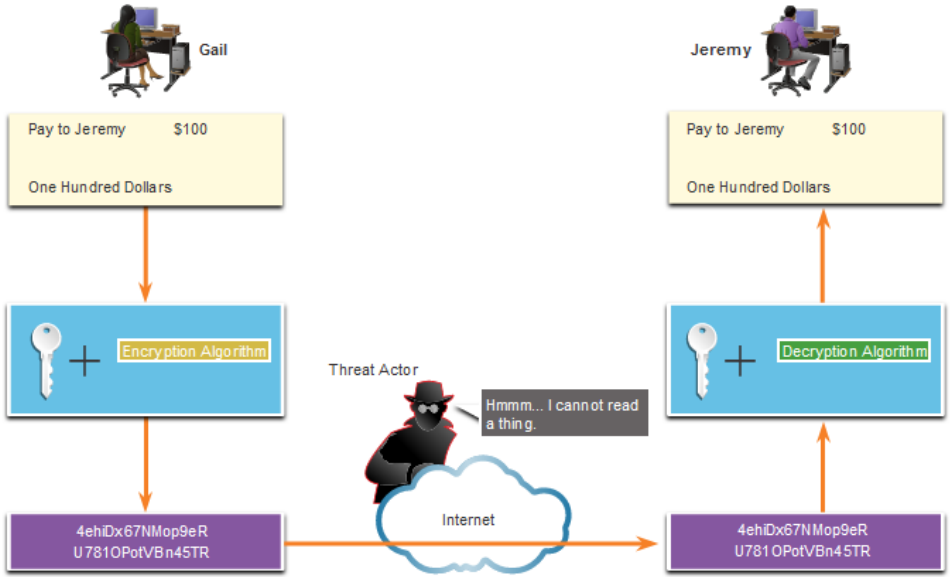
- IPsec encapsulates packets using Authentication Header (AH) or Encapsulation Security Protocol (ESP).
- The choice of AH or ESP establishes which other building blocks are available.
  - AH is appropriate only when confidentiality is not required or permitted.
  - ESP provides both confidentiality and authentication.



IPSec
Confidentiality

The degree of confidentiality depends on the encryption algorithm and the length of the key used in the encryption algorithm.

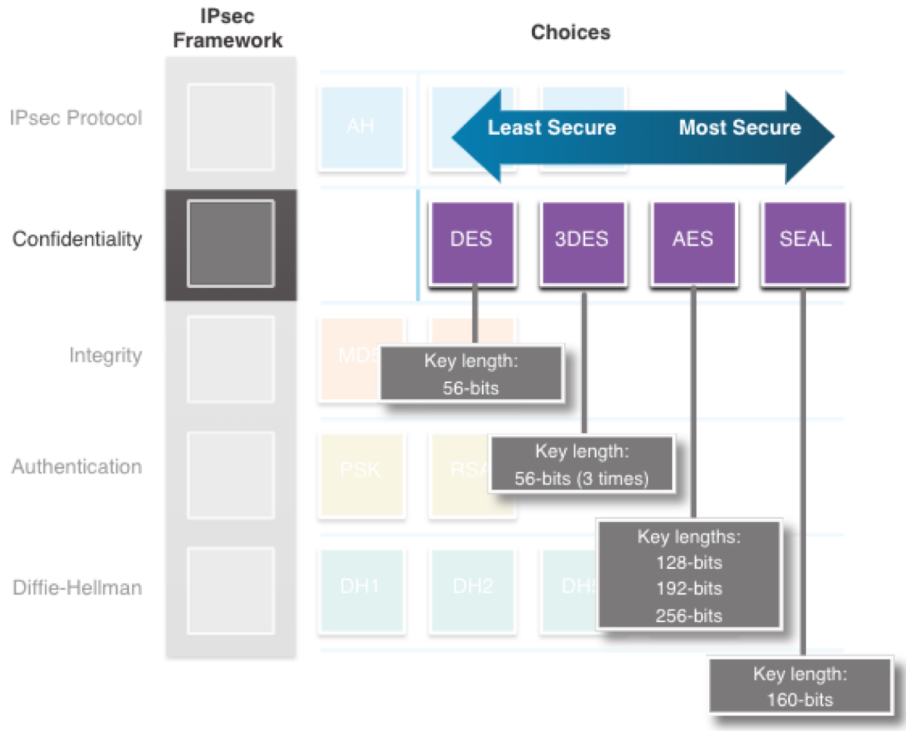
The number of possibilities to try to hack the key is a function of the length of the key - the shorter the key, the easier it is to break.



Confidentiality (Cont.)

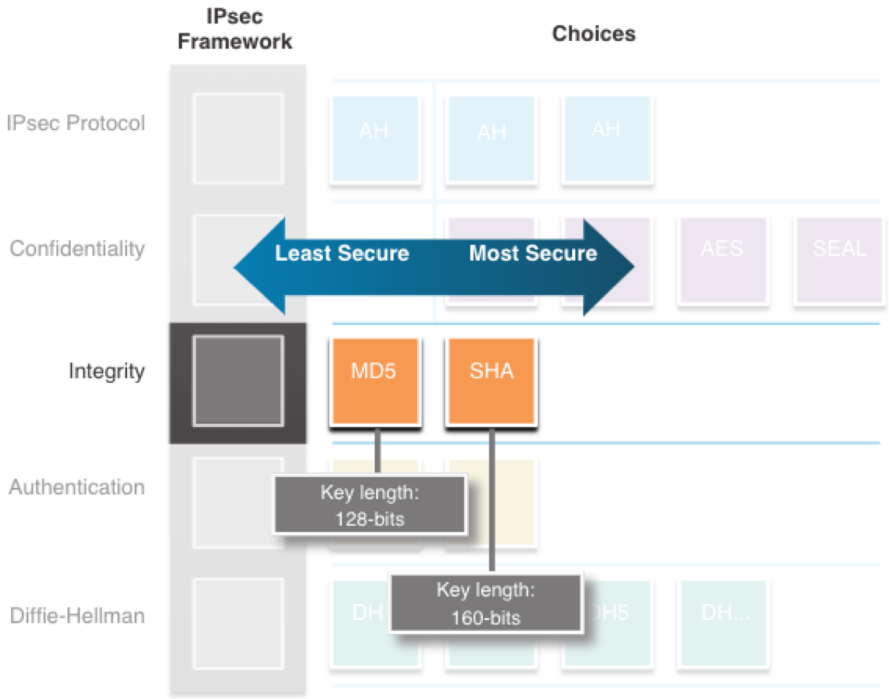
The encryption algorithms highlighted in the figure are all symmetric key cryptosystems:

- DES uses a 56-bit key.
- 3DES uses three independent 56-bit encryption keys per 64-bit block.
- 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.



IPSec
Integrity

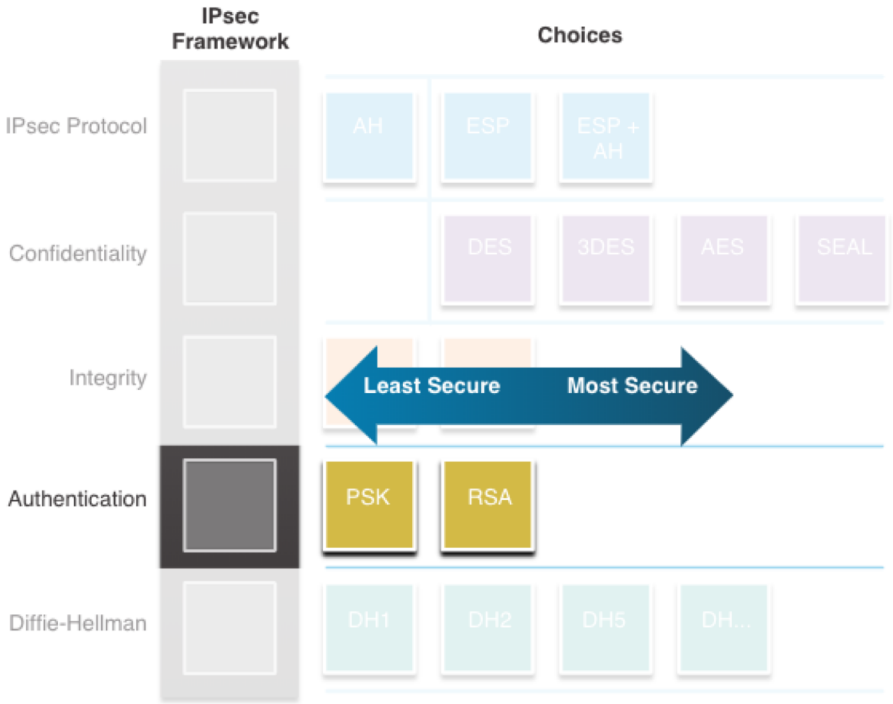
- Data integrity means that the data has not changed in transit.
- A method of proving data integrity is required.
- The Hashed Message Authentication Code (HMAC) is a data integrity algorithm that guarantees the integrity of the message using a hash value.
  - Message-Digest 5 (MD5) uses a 128-bit shared-secret key.
  - The Secure Hash Algorithm (SHA) uses a 160-bit secret key.



IPSec
Authentication

There are two IPsec peer authentication methods:

1. **Pre-shared key (PSK)** - (PSK) value is entered into each peer manually.
   - Easy to configure manually
   - Does not scale well
   - Must be configured on every peer
2. **Rivest, Shamir, and Adleman (RSA)** - authentication uses digital certificates to authenticate the peers.
   - Each peer must authenticate its opposite peer before the tunnel is considered secure.



Secure Key Exchange with Diffie - Hellman

DH provides allows two peers to establish a shared secret key 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.
- DH groups 14, 15, and 16 use larger key sizes with 2048 bits, 3072 bits, and 4096 bits, respectively
- 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.

What did I learn in this module?

- 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.
- 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.
- 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.
- 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.

What did I learn in this module? (Cont.)

- 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.
- 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.
- 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.

New Terms and Commands

- Cisco Adaptive Security Appliance (ASA) firewall
- SOHO
- Cisco AnyConnect
- Generic Routing Encapsulation (GRE)
- Site-to-Site VPN
- Remote access VPN
- Multiprotocol Label Switching (MPLS)
- SSL VPN
- IPsec
- Dynamic Multipoint VPN (DMVPN)
- Multipoint Generic Routing Encapsulation (mGRE)
- Virtual Tunnel Interface (VTI)
- Diffie-Hellman
- Security Association (SA)
- Authentication Header (AH)
- Encapsulation Security Protocol (ESP)

- DES
- 3DES
- AES
- SEAL
- Secure Hash Algorithm (SHA)
- Message-Digest 5 (MD5)
- Rivest, Shamir, and Adleman (RSA)
- pre-shared secret key (PSK)