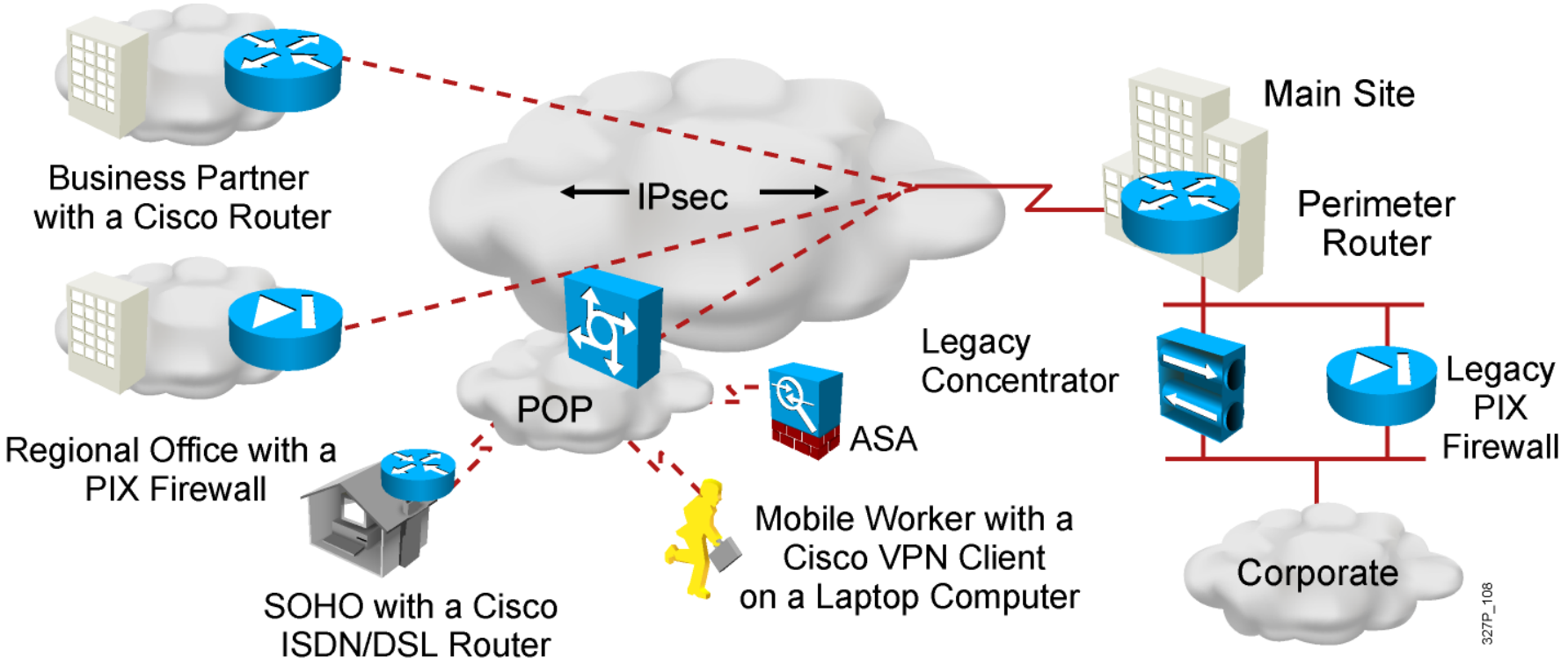
Introducing VPN Solutions

What Is a VPN?



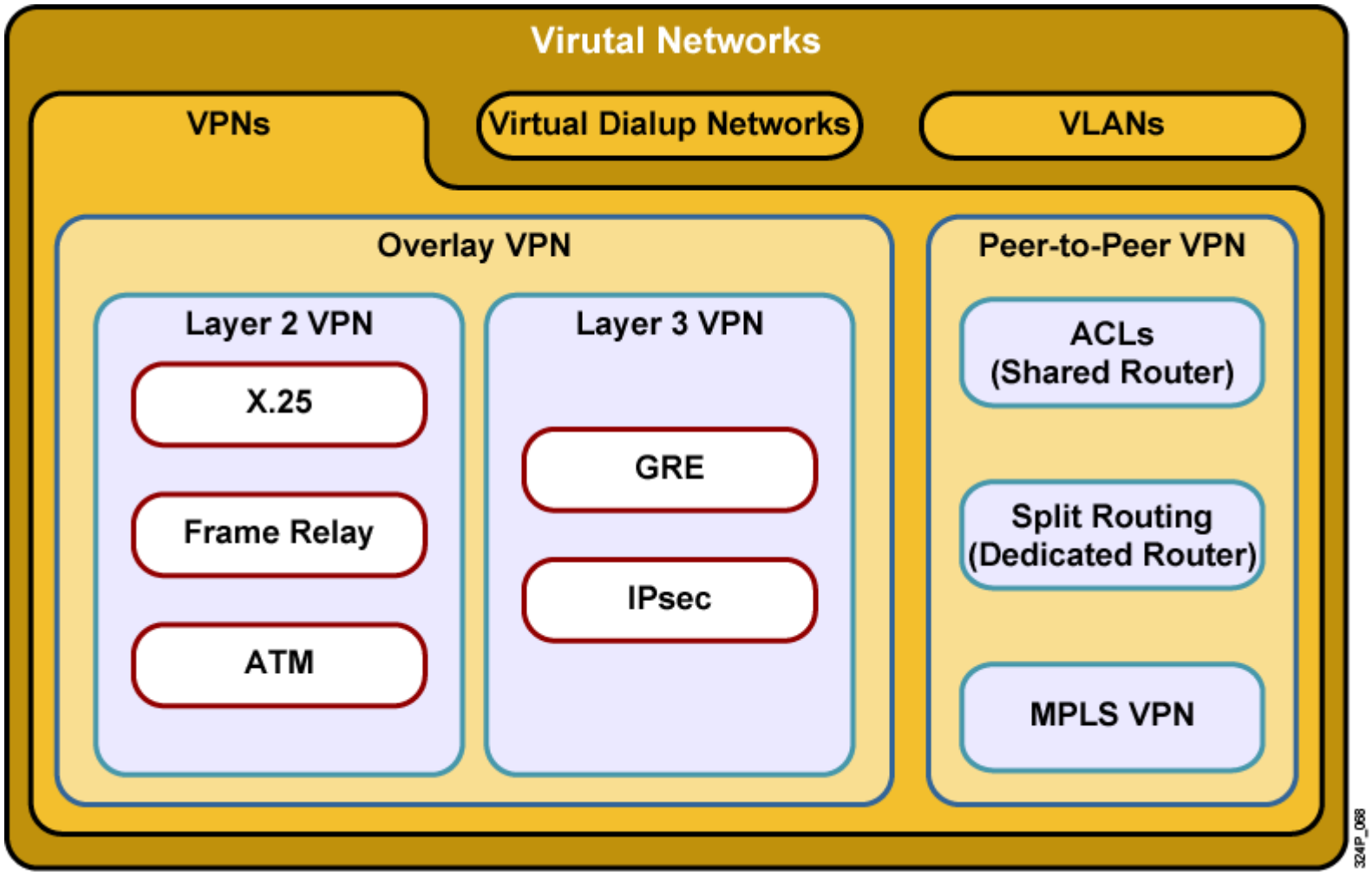
- Virtual private networks (**VPNs**) to create end-to-end private network connections.
- **Virtual:** in that it carries information within a private network, but that information is actually transported over a public network.
- **Private:** the traffic is encrypted to keep the data confidential while it is transported across the public network.

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.

VPN Taxonomy

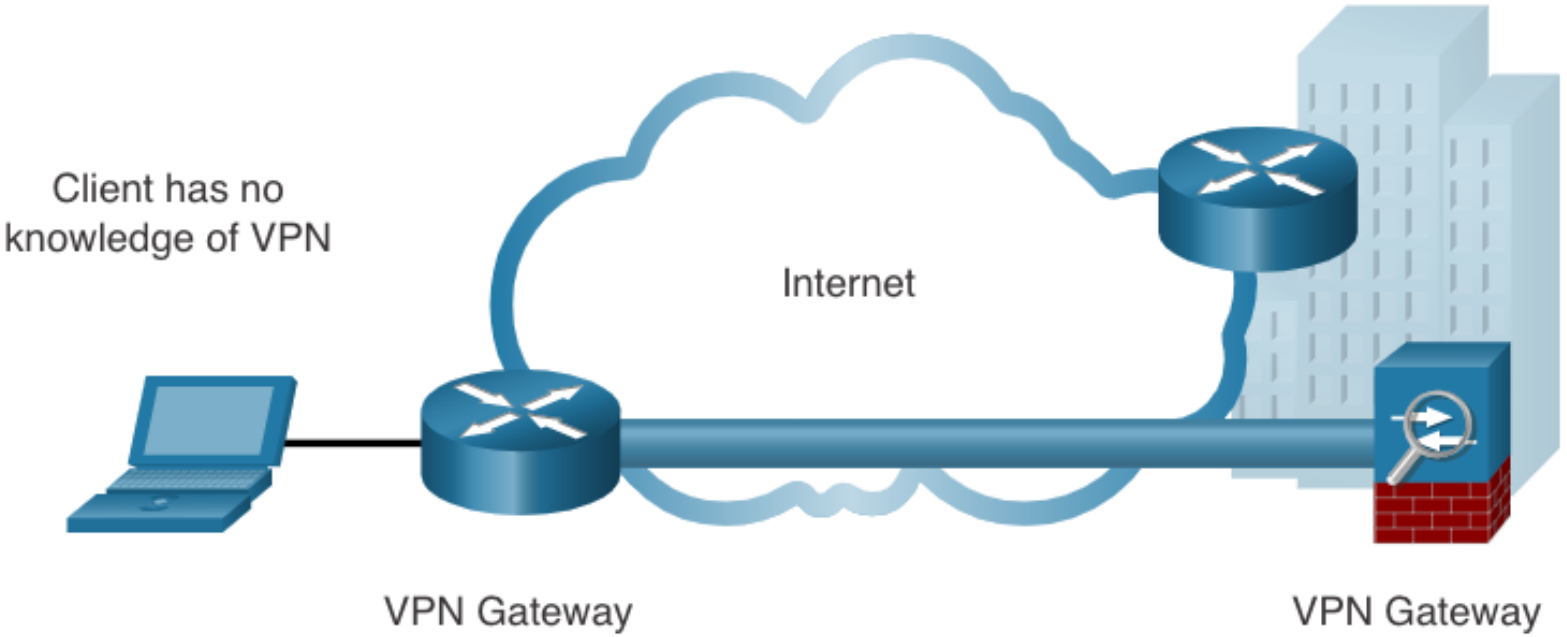


VPN Models

VPN services can be offered based on two major models:

- **Overlay VPNs, in which the service provider provides virtual point-to-point links between customer sites**
- **Peer-to-peer VPNs, in which the service provider participates in the customer routing**

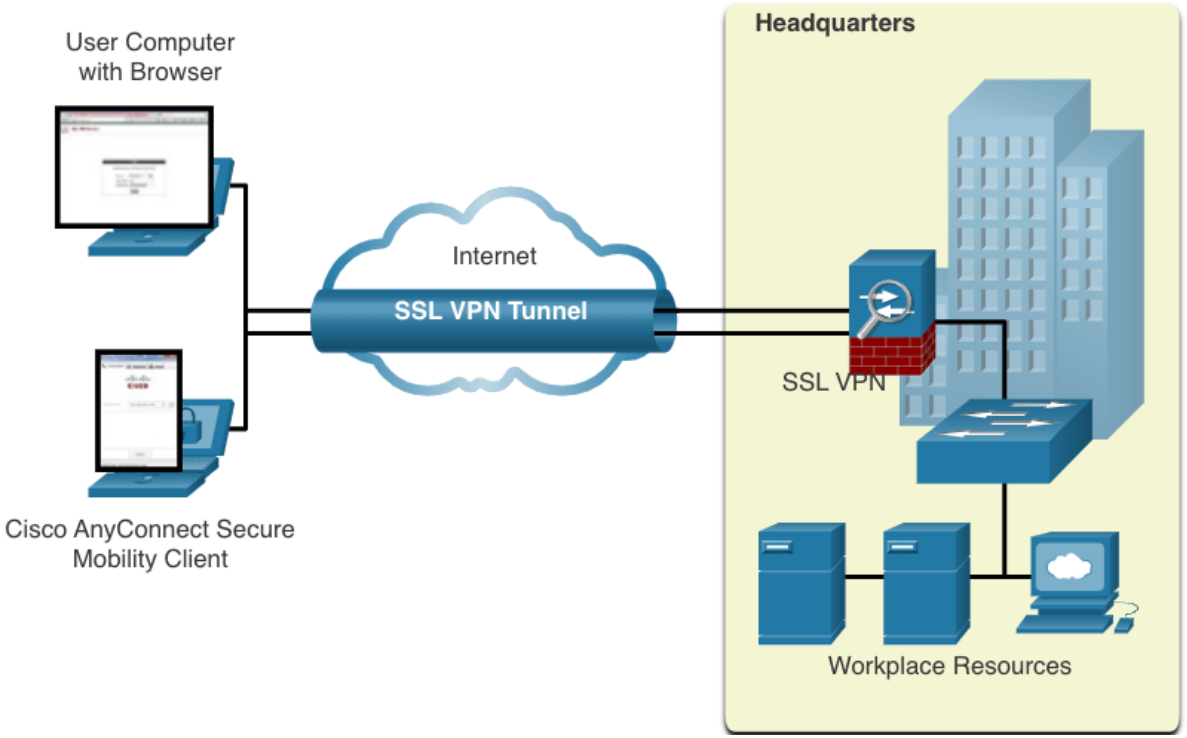
Site-to-Site VPNs



- 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.

Site-to-site VPN: extension of classic WAN

Remote-Access VPNs



- 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 VPN

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

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.
- 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).

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.

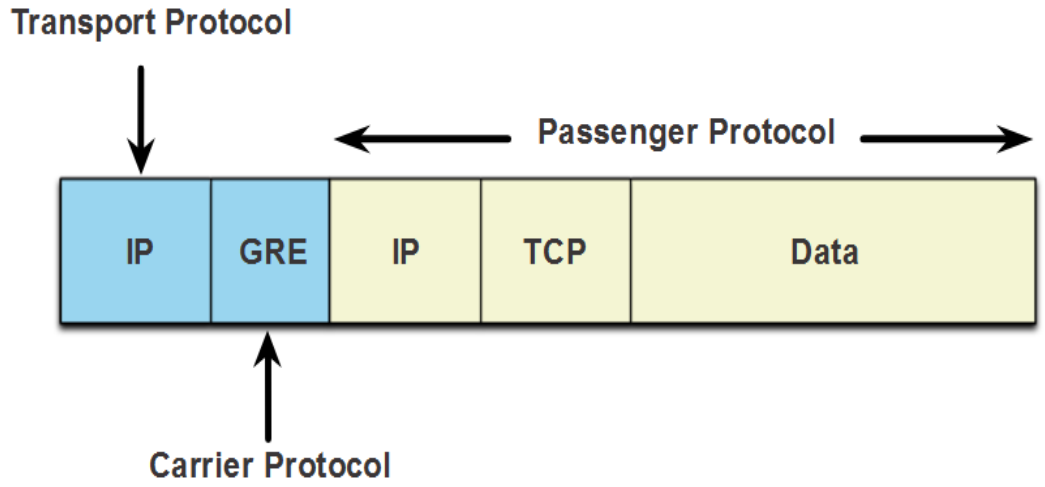
GRE over IPsec

- 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.

GRE over IPsec (Cont.)

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

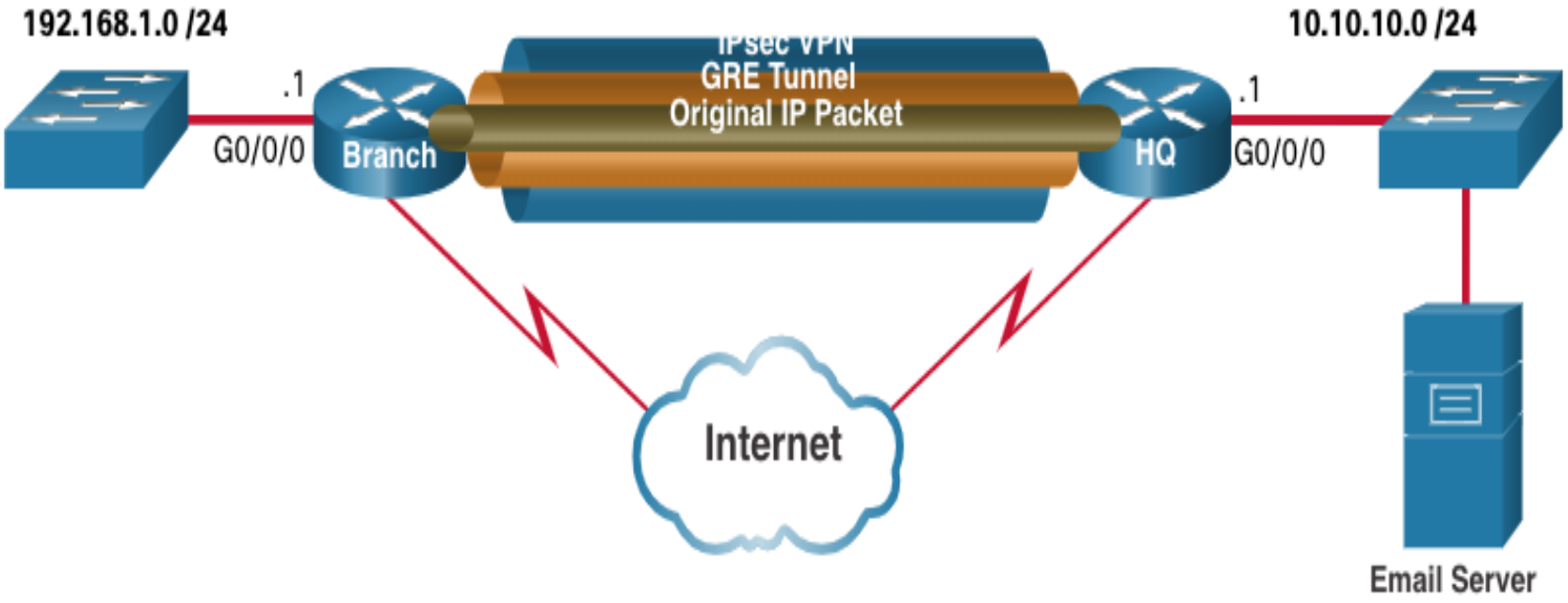
- **Passenger protocol** – This is the original packet that is to be encapsulated by GRE. It could be an IPv4 or IPv6 packet, a routing update, and more.
- **Carrier protocol** – GRE is the carrier protocol that encapsulates the original passenger packet.
- **Transport protocol** – This is the protocol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



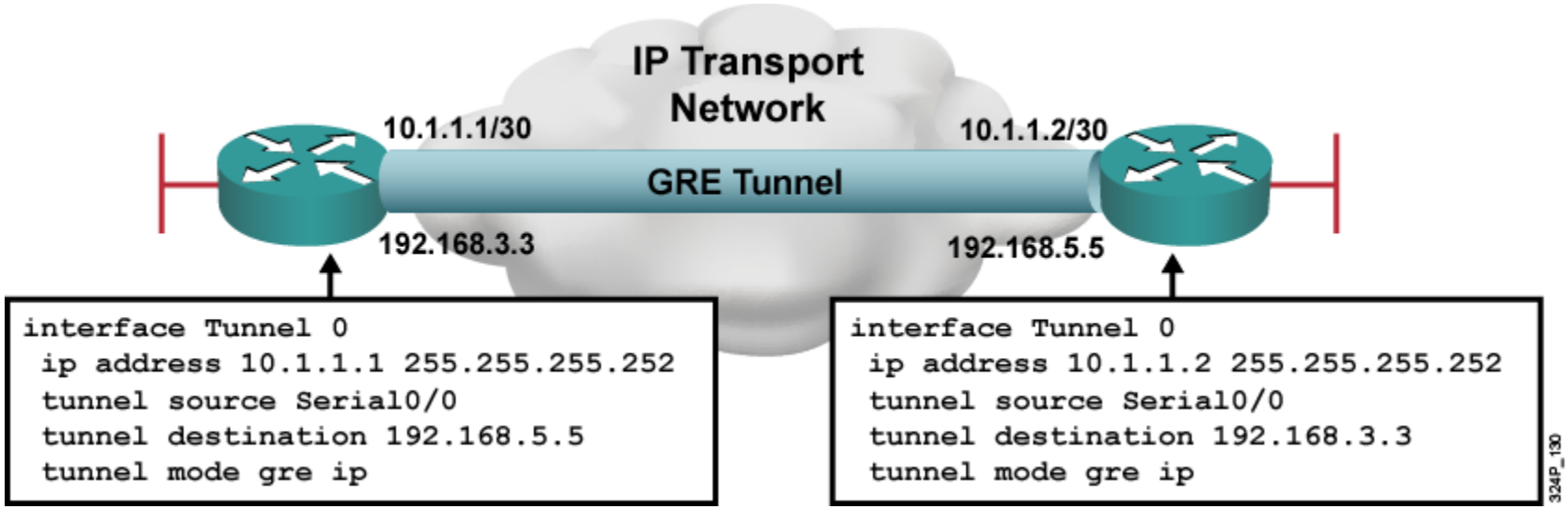
GRE over IPsec (Cont.)

For example, Branch and HQ need to exchange OSPF routing information over an IPsec VPN.

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.



GRE Configuration Example



- **GRE tunnel is up and protocol up if:**
  - Tunnel source and destination are configured
  - Tunnel destination is in routing table
  - GRE keepalives are received (if used)
- **GRE is the default tunnel mode.**

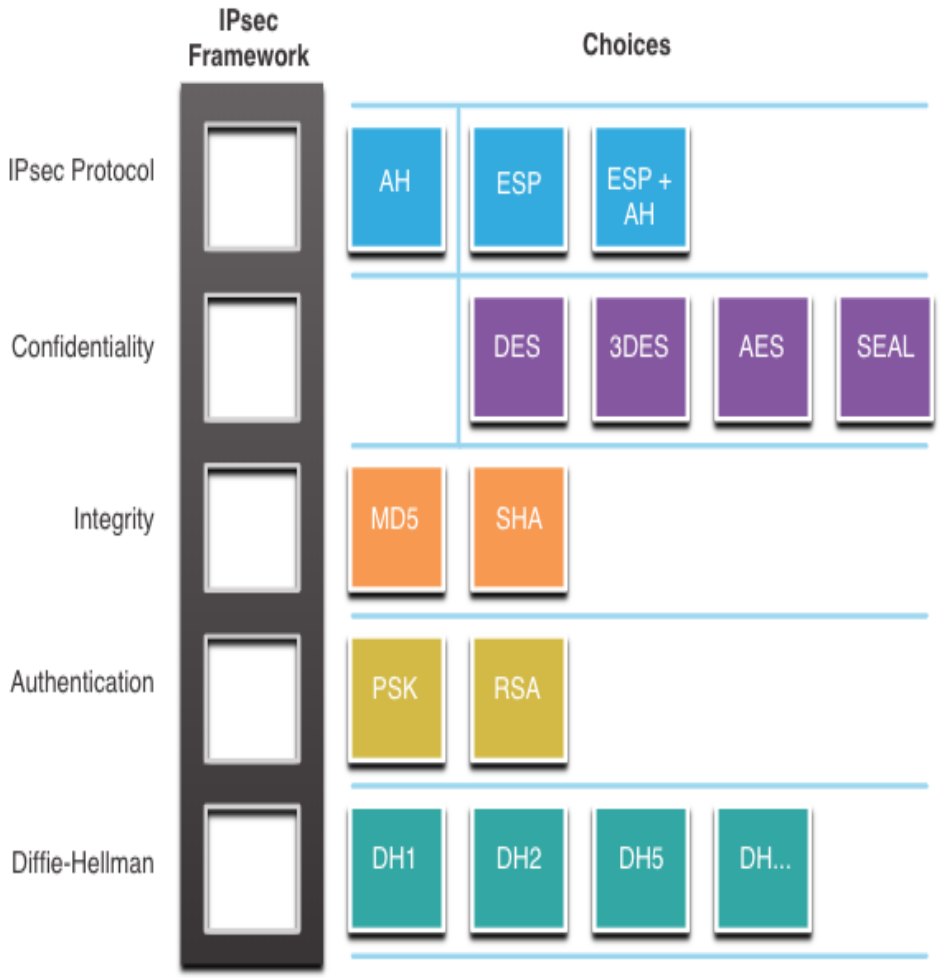
IPsec Technologies

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.)

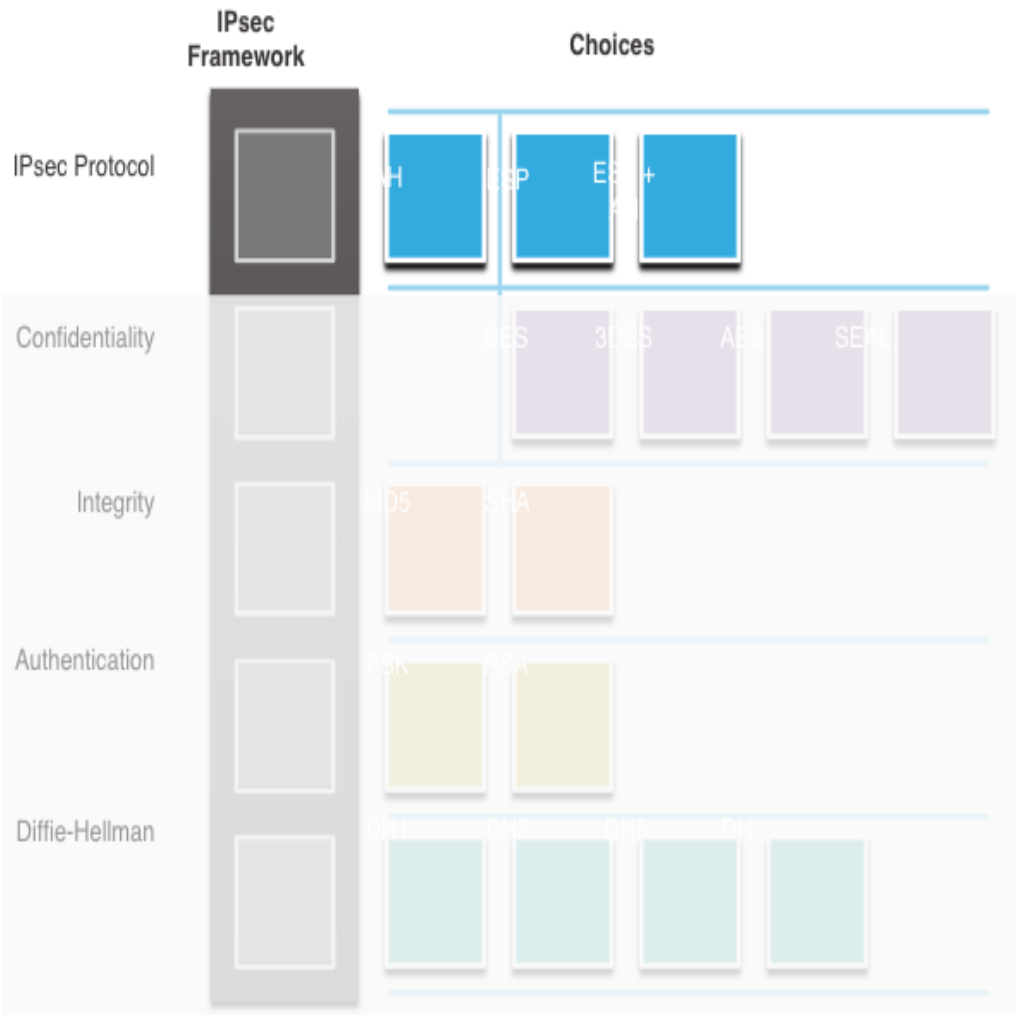
- IPsec is not bound to any specific rules for secure communications.
- IPsec can easily integrate new security technologies without updating existing IPsec standards.
- The open slots in the IPsec framework shown in the figure can be filled with any of the choices that are available for that IPsec function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



IPsec Protocol Encapsulation

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

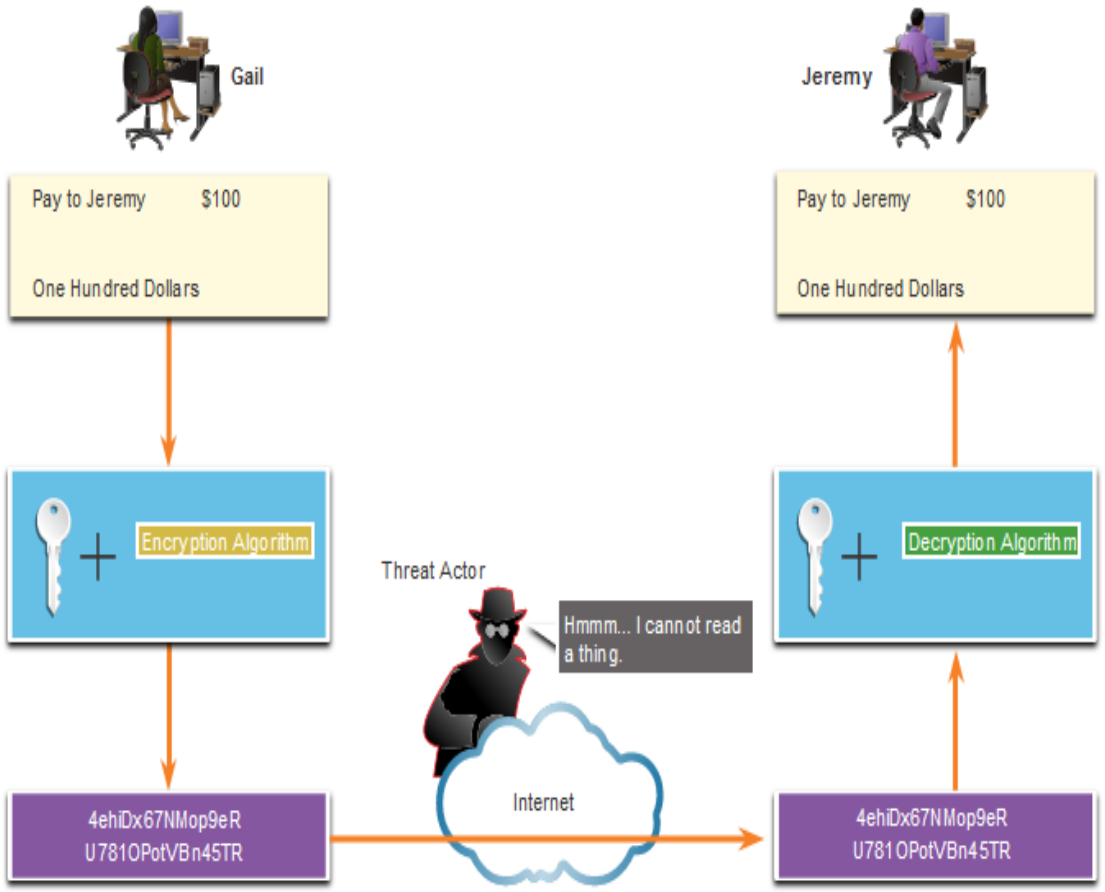
- IPsec encapsulates packets using Authentication Header (AH) or Encapsulation Security Protocol (ESP).
- The choice of AH or ESP establishes which other building blocks are available.
  - AH is appropriate only when confidentiality is not required or permitted.
  - ESP provides both confidentiality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



Confidentiality

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

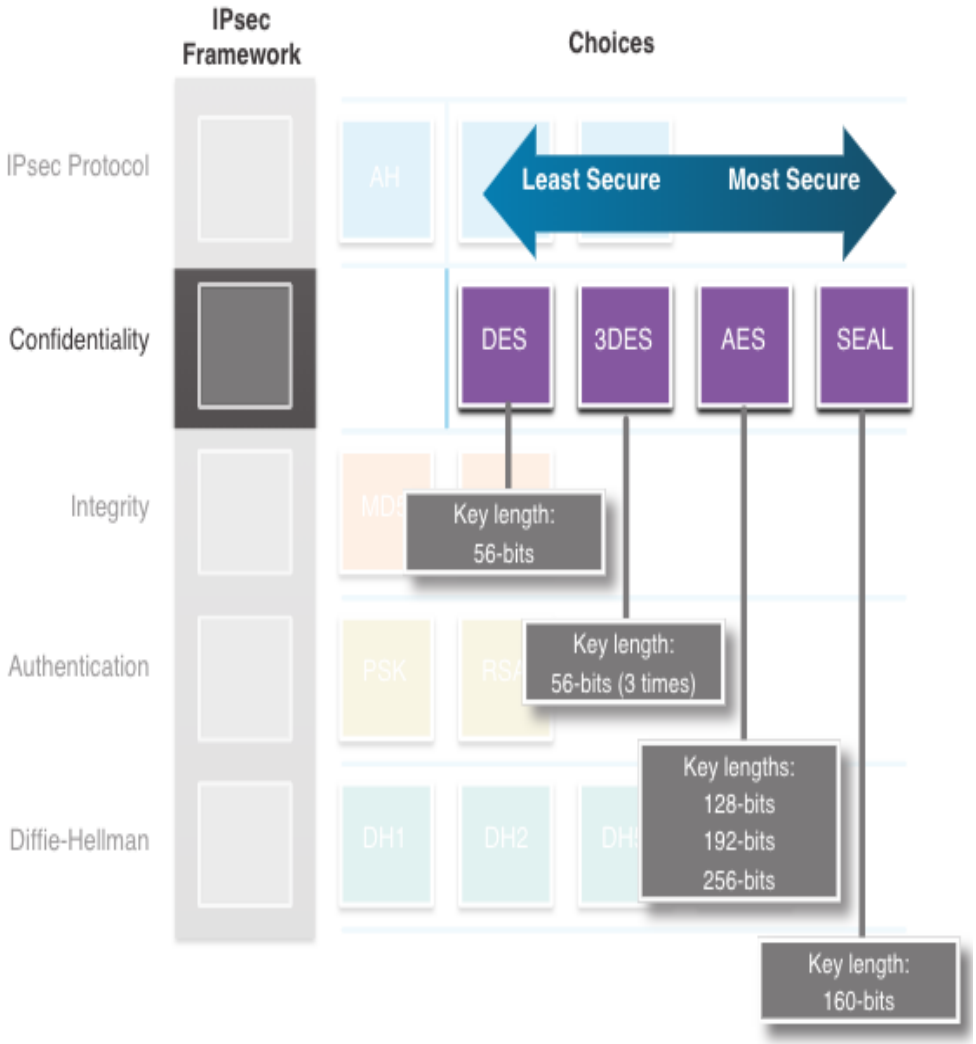
The number of possibilities to try to hack the key is a function of the length of the key - the shorter the key, the easier it is to break.



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.



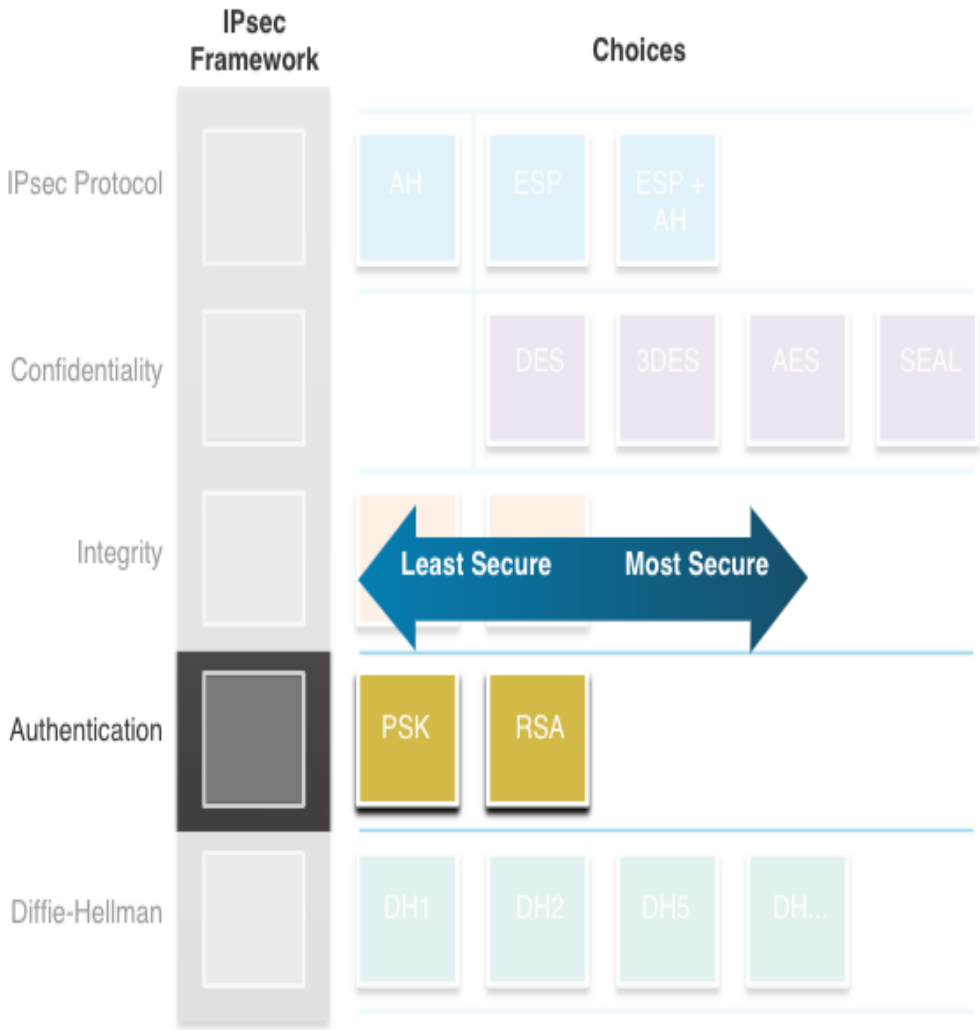
Integrity

- 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.

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.

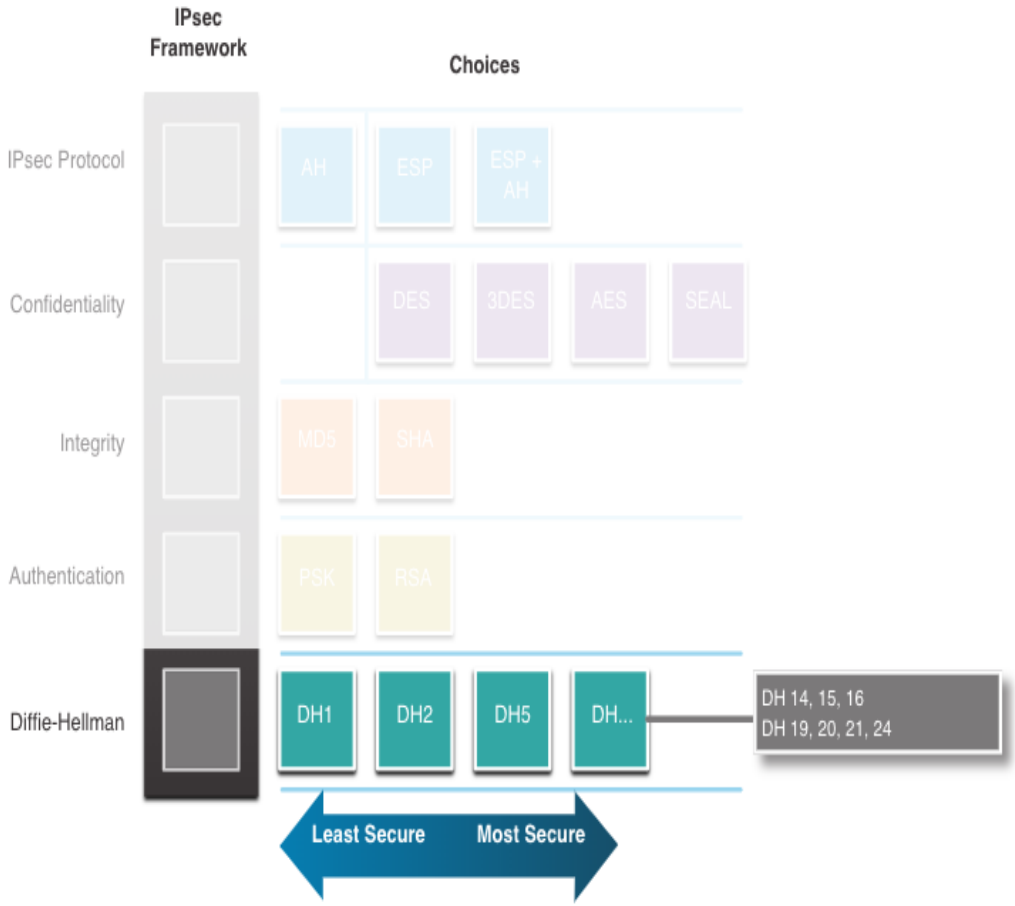


Secure Key Exchange with Diffie - Hellman

DH provides allows two peers to establish a shared secret key over an insecure channel.

Variations of the DH key exchange ar 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.




CISCO