Chapter 7: Securing Site-to-Site Connectivity

Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™

Chapter 7: Securing Site-to-Site Connectivity

7.1 VPNs

7.2 Site-to-Site GRE Tunnels

7.3 Introducing IPsec

7.4 Remote Access

7.5 Summary

Chapter 7: Objectives

After completing this chapter, students will be able to:

- Describe benefits of VPN technology.
- Describe site-to-site and remote access VPNs.
- Describe the purpose and benefits of GRE tunnels.
- Configure a site-to-site GRE tunnel.
- Describe the characteristics of IPsec.
- Explain how IPsec is implemented using the IPsec protocol framework.
- Explain how the Anyconnect client and clientless SSL remote access VPN implementations support business requirements.
- Compare IPsec and SSL remote access VPNs.

Chapter 7: Introduction

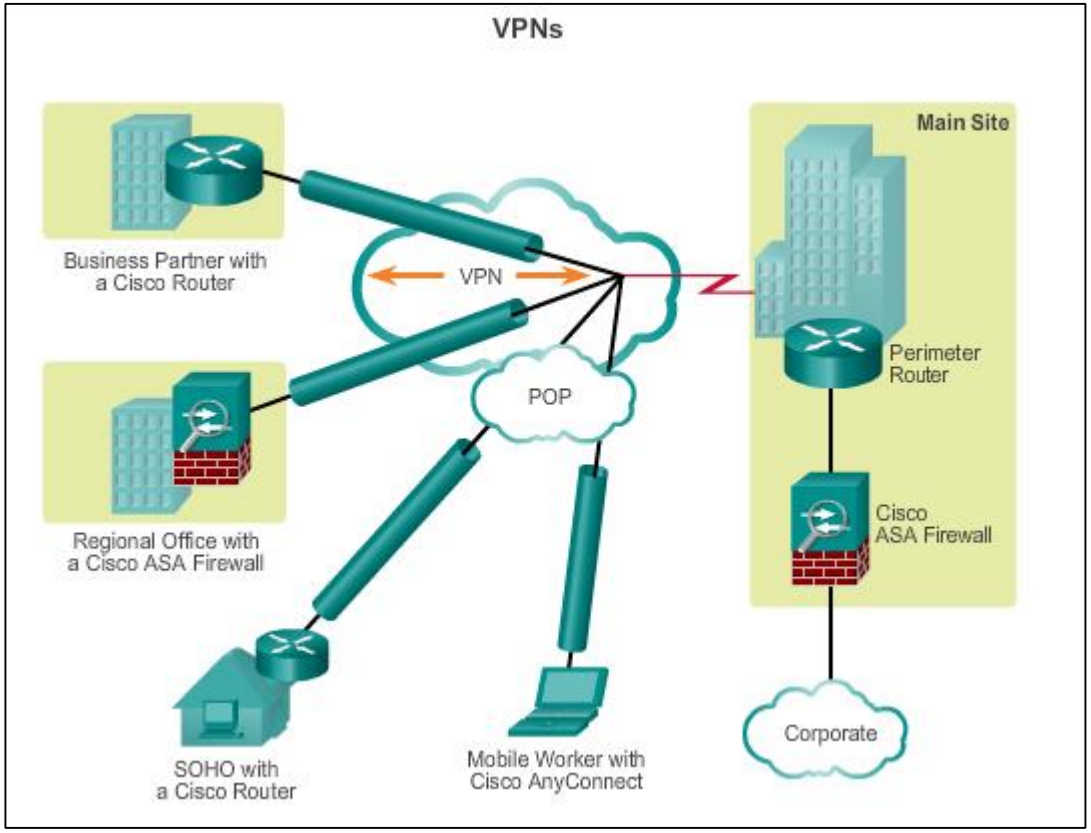
- Security is a concern when using the public Internet to conduct business.
- Virtual Private Networks (VPNs) are used to ensure the security of data across the Internet.
- A VPN is used to create a private tunnel over a public network.
- Data can be secured by using encryption in this tunnel through the Internet and by using authentication to protect data from unauthorized access.
- This chapter explains the concepts and processes related to VPNs, as well as the benefits of VPN implementations, and the underlying protocols required to configure VPNs.

7.1 VPNs

Cisco | Networking Academy®
Mind Wide Open™

Introducing VPNs

- VPNs are used to create an end-to-end private network connection over third-party networks, such as the Internet or extranets.
- To implement VPNs, a VPN gateway is necessary: Could be a router, a firewall, or a Cisco Adaptive Security Appliance (ASA).



Benefits of VPNs

- **Cost savings**
  - Enable organizations to use cost-effective, third-party Internet transport to connect remote offices and remote users to the main site.
- **Scalability**
  - Enable organizations to use the Internet infrastructure within ISPs and devices, which makes it easy to add new users.

Benefits of VPNs (cont.)

- **Compatibility with broadband technology**
  - Allow mobile workers and telecommuters to take advantage of high-speed, broadband connectivity, such as DSL and cable, to gain access to the networks of their organization, providing workers flexibility and efficiency.
  - Provide a cost-effective solution for connecting remote offices.
- **Security**
  - Can include security mechanisms that provide the highest level of security by using advanced encryption and authentication protocols that protect data from unauthorized access.

Types of VPNs

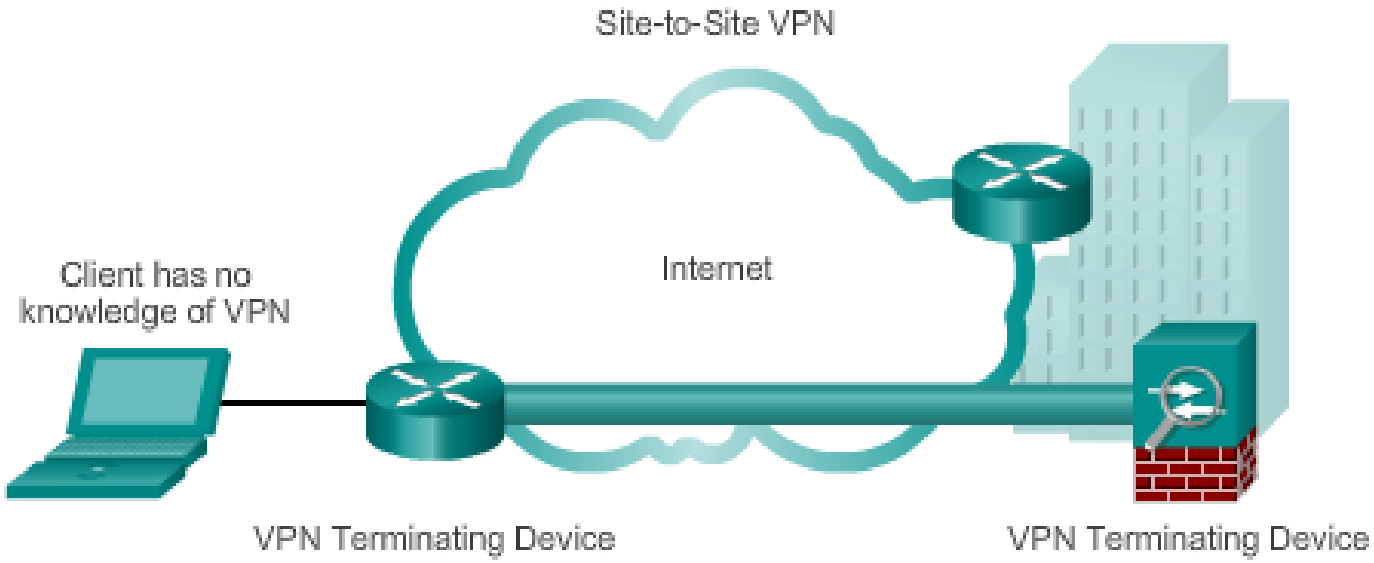
Site-to-Site VPNs

- Connect entire networks to each other, in the past, a leased line or Frame Relay connection was required to connect sites, but because most corporations now have Internet access, these connections can be replaced with site-to-site VPNs.
- Internal hosts have no knowledge that a VPN exists.
- Created when devices on both sides of the VPN connection are aware of the VPN configuration in advance.

Site-to-Site VPNs (cont.)

- End hosts send and receive normal TCP/IP traffic through a VPN gateway.
- The VPN gateway is responsible for encapsulating and encrypting outbound traffic for all traffic from a particular site
- The VPN gateway then sends it through a VPN tunnel over the Internet to a peer VPN gateway at the target site.
- Upon receipt, the peer VPN gateway strips the headers, decrypts the content, and relays the packet toward the target host inside its private network.

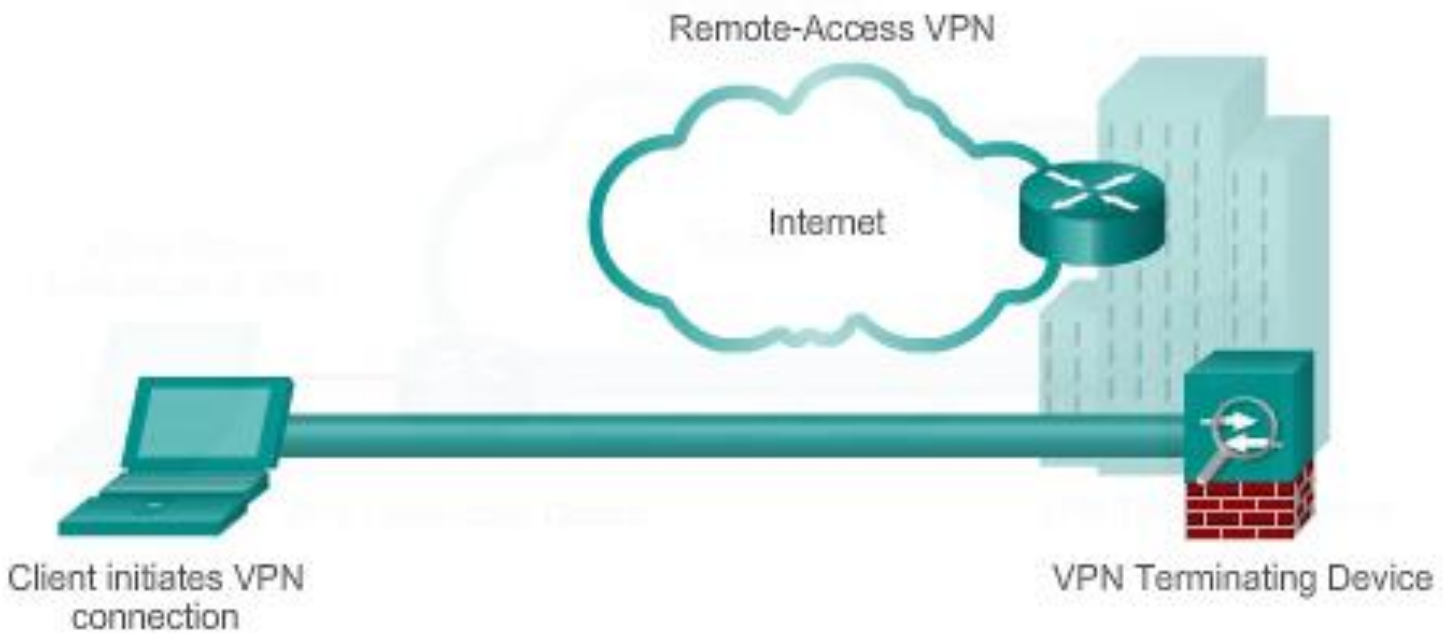
Site-to-Site VPNs (cont.)



Remote Access VPNs

- Support the needs of telecommuters, mobile users, and extranet, consumer-to-business traffic.
- Support a client/server architecture, where the VPN client (remote host) gains secure access to the enterprise network via a VPN server device at the network edge.
- Used to connect individual hosts that must access their company network securely over the Internet.
- VPN client software may need to be installed on the mobile user's end device (Cisco AnyConnect Secure Mobility Client).
- When the host tries to send any traffic, the VPN Client software encapsulates and encrypts this traffic and sends over the Internet to the VPN gateway at the edge of the target network.

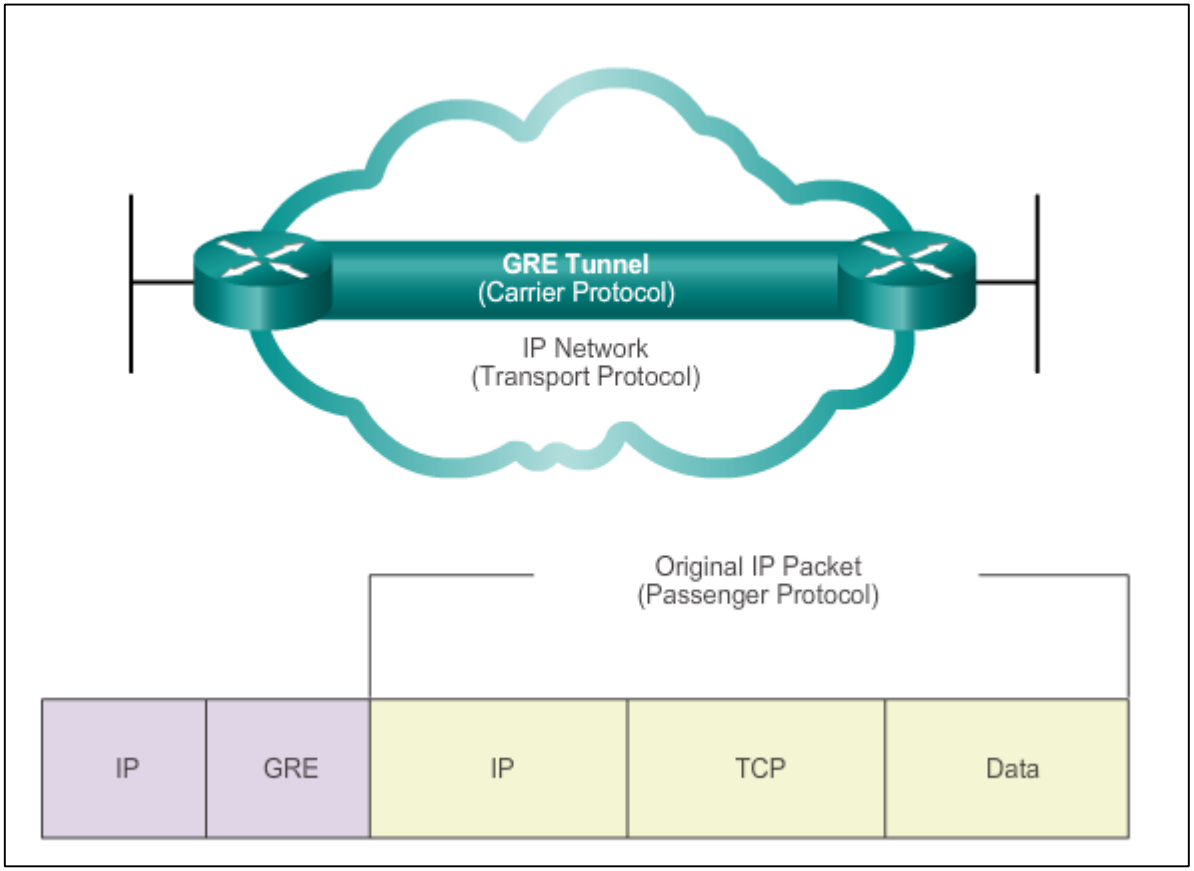
Remote Access VPNs (cont.)



7.2 Site-to-Site GRE Tunnels

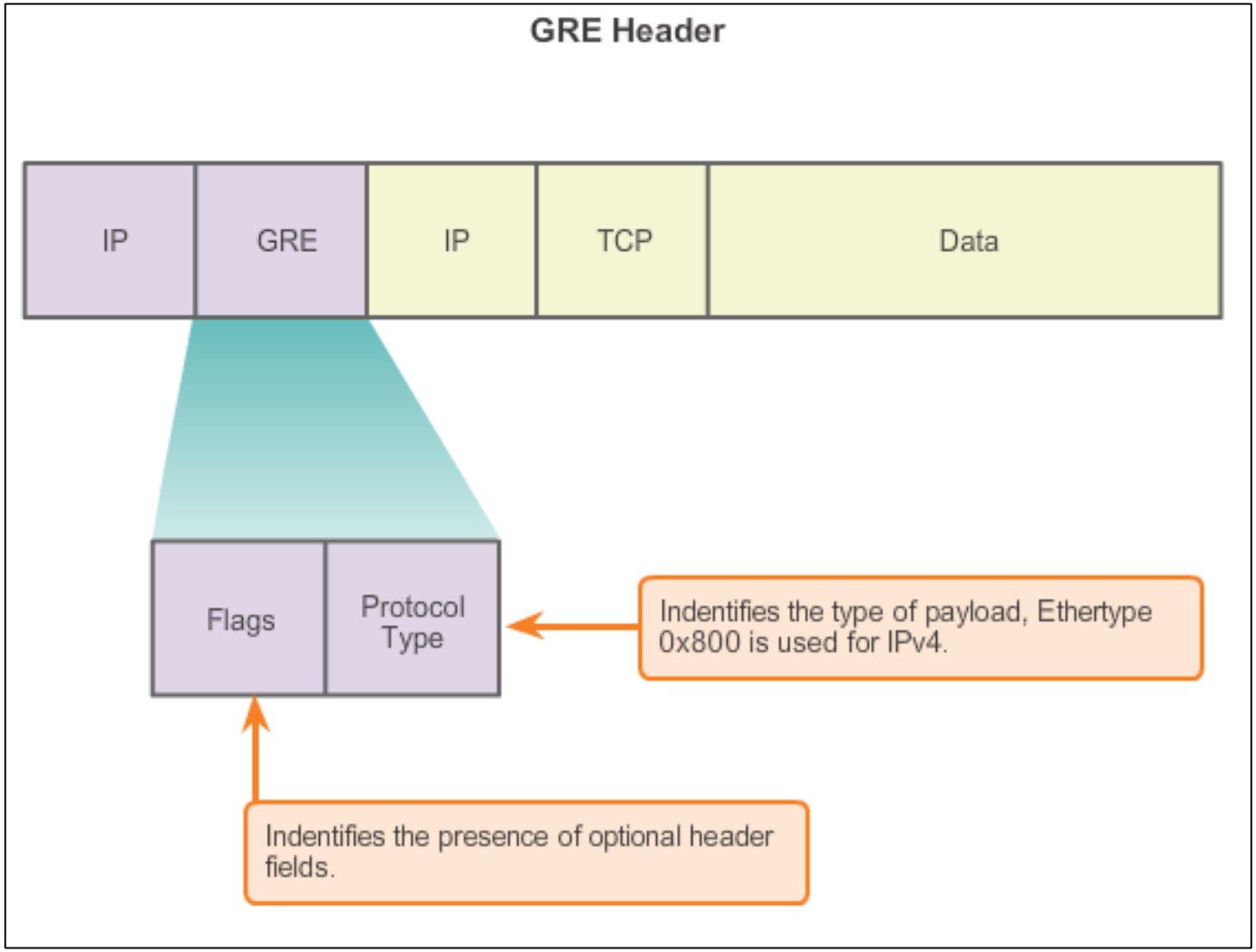
Cisco | Networking Academy®
Mind Wide Open™

Introduction to GRE



- Basic, non-secure, site-to-site VPN tunneling protocol developed by Cisco
- Encapsulates a wide variety of protocol packet types inside IP tunnels
- Creates a virtual point-to-point link to routers at remote points, over an IP internetwork

Characteristics of GRE



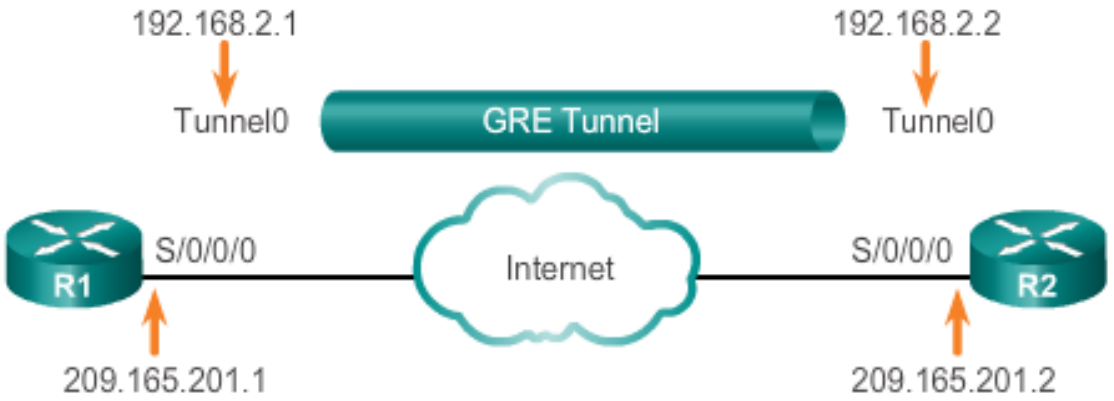
Characteristics of GRE

GRE has these characteristics:

- GRE is defined as an IETF standard.
- IP protocol 47 is used to identify GRE packets.
- GRE encapsulation uses a protocol type field in the GRE header to support the encapsulation of any OSI Layer 3 protocol.
- GRE itself is stateless; it does not include any flow-control mechanisms, by default.
- GRE does not include any strong security mechanisms to protect its payload.
- The GRE header, together with the tunneling IP header, creates at least 24 bytes of additional overhead for tunneled packets.

GRE Tunnel Configuration

GRE Tunnel Configuration



R1 configuration:

```
R1(config)# interface Tunnel0
R1(config-if)# tunnel mode gre ip
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# tunnel source 209.165.201.1
R1(config-if)# tunnel destination 209.165.201.2
R1(config-if)# router ospf 1
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

Configuring GRE Tunnels

GRE Tunnel Configuration

GRE Tunnel Commands

Command	Description
tunnel mode gre ip	Specifies GRE tunnel mode as the tunnel interface mode, in interface tunnel configuration mode.
tunnel source *ip_address*	Specifies the tunnel source IP address, in interface tunnel configuration mode.
tunnel destination *ip_address*	Specifies the tunnel destination IP address, in interface tunnel configuration mode.
ip address *ip_address mask*	Specifies the IP address of the tunnel interface.

R2 configuration:

```
R2(config)# interface Tunnel0
R2(config-if)# tunnel mode gre ip
R2(config-if)# ip address 192.168.2.2 255.255.255.0
R2(config-if)# tunnel source 209.165.201.2
R2(config-if)# tunnel destination 209.165.201.1
R2(config-if)# router ospf 1
R2(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

Stav rozhraní Tunnel

- Rozhrania Tunnel pri GRE budú „up, protocol up“, ak sú splnené súčasne všetky nasledujúce podmienky
  - Rozhranie má definovaný zdroj a cieľ príkazmi **tunnel source**, **tunnel destination**
    - Tunel má definovanú platnú zdrojovú a cieľovú IP
  - Skutočné rozhranie, z ktorého si požičiavame zdrojovú IP v príkaze **tunnel source**, je v stave „up, protocol up“
    - Zdrojová IP adresa musí byť živá
  - V smerovacej tabuľke vieme vyhľadať cestu k náprotivnému koncu tunela definovanému príkazom **tunnel destination**
    - Cieľová IP adresa musí byť podľa našej RT dosiahnuteľná
  - Ak je zapnuté použitie GRE Keepalive, druhá strana odpovedá na naše Keepalive pakety
    - Vnútro transportnej siete musí byť schopné doručovať pakety medzi koncami tunela

Stav rozhraní Tunnel

- Rozhrania Tunnel pri GRE budú „up, protocol up“, ak sú splnené súčasne všetky nasledujúce podmienky
  - Rozhranie má definovaný zdroj a cieľ príkazmi **tunnel source**, **tunnel destination**
    - Tunel má definovanú platnú zdrojovú a cieľovú IP
  - Skutočné rozhranie, z ktorého si požičiavame zdrojovú IP v príkaze **tunnel source**, je v stave „up, protocol up“
    - Zdrojová IP adresa musí byť živá
  - V smerovacej tabuľke vieme vyhľadať cestu k náprotivnému koncu tunela definovanému príkazom **tunnel destination**
    - Cieľová IP adresa musí byť podľa našej RT dosiahnuteľná
  - Ak je zapnuté použitie GRE Keepalive, druhá strana odpovedá na naše Keepalive pakety
    - Vnútro transportnej siete musí byť schopné doručovať pakety medzi koncami tunela

GRE Tunnel Verification

Verify Tunnel Interface is Up

```
R1# show ip interface brief | include Tunnel
Tunnel0                192.168.2.1     YES manual up        up
```

```
R1# show interface Tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.2.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 209.165.201.1, destination 209.165.201.2
  Tunnel protocol/transport GRE/IP
<output omitted>
```

Verify OSPF Adjacency

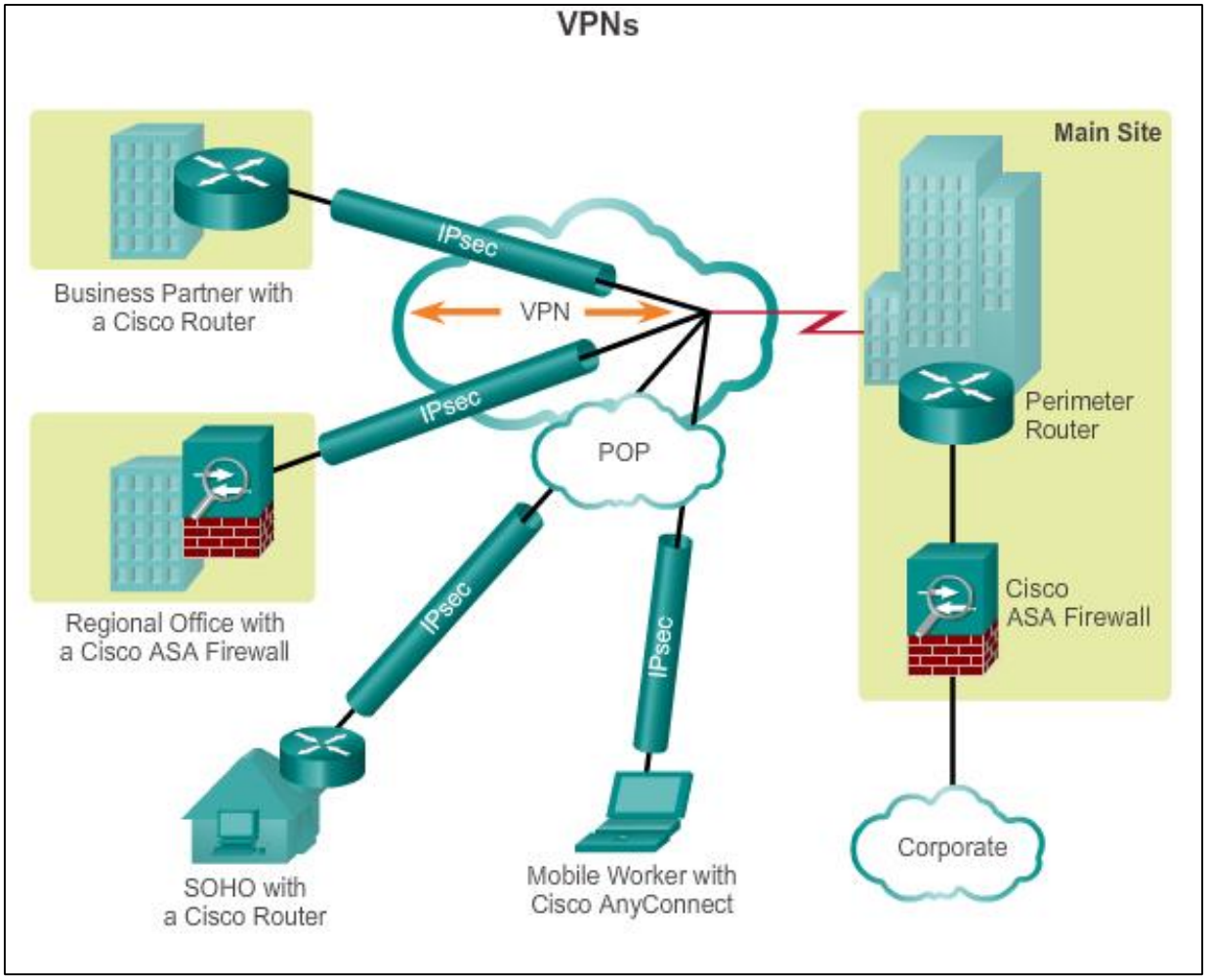
```
R1# show ip ospf neighbor

Neighbor ID     Pri State           Dead Time   Address      Interface
209.165.201.2   0   FULL/  -        00:00:37    192.168.2.2    Tunnel0
```

7.3 Introducing IPsec

Cisco | Networking Academy®
Mind Wide Open™

IPsec VPNs



- Information from a private network is securely transported over a public network.
- Forms a virtual network instead of using a dedicated Layer 2 connection.
- To remain private, the traffic is encrypted to keep the data confidential.

IPsec Functions

- Defines how a VPN can be configured in a secure manner using IP.
- Framework of open standards that spells out the rules for secure communications.
- Not bound to any specific encryption, authentication, security algorithms, or keying technology.
- Relies on existing algorithms to implement secure communications.
- Works at the network layer, protecting and authenticating IP packets between participating IPsec devices.
- Secures a path between a pair of gateways, a pair of hosts, or a gateway and host.
- All implementations of IPsec have a plaintext Layer 3 header, so there are no issues with routing.
- Functions over all Layer 2 protocols, such as Ethernet, ATM, or Frame Relay.

IPsec Characteristics

IPsec characteristics can be summarized as follows:

- IPsec is a framework of open standards that is algorithm-independent.
- IPsec provides data confidentiality, data integrity, and origin authentication.
- IPsec acts at the network layer, protecting and authenticating IP packets.

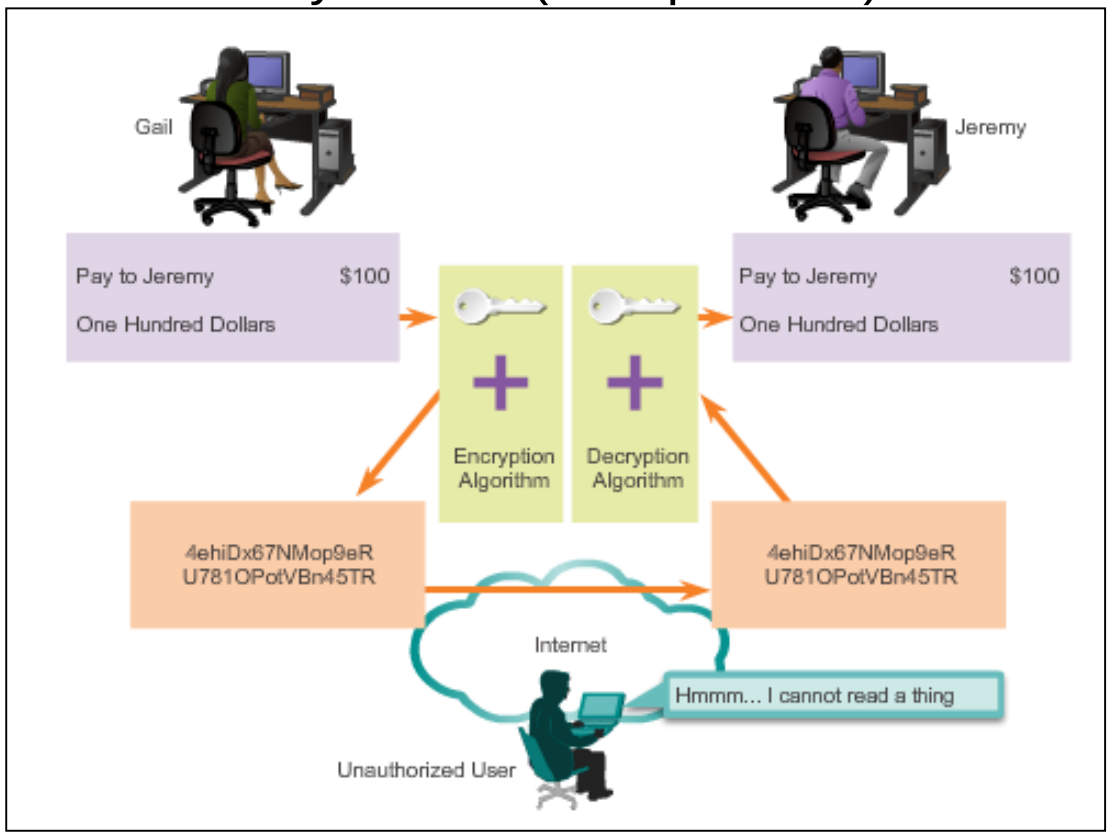
IPsec Security Services

- **Confidentiality (encryption)** – encrypt the data before transmitting across the network
- **Data integrity** – verify that data has not been changed while in transit, if tampering is detected, the packet is dropped
- **Authentication** – verify the identity of the source of the data that is sent, ensures that the connection is made with the desired communication partner, IPsec uses Internet Key Exchange (IKE) to authenticate users and devices that can carry out communication independently.
- **Anti-Replay Protection** – detect and reject replayed packets and helps prevent spoofing

CIA: confidentiality, integrity, and authentication

Confidentiality with Encryption

- For encryption to work, both the sender and the receiver must know the rules used to transform the original message into its coded form.
- Rules are based on algorithms and associated keys.
- Decryption is extremely difficult (or impossible) without the correct key.

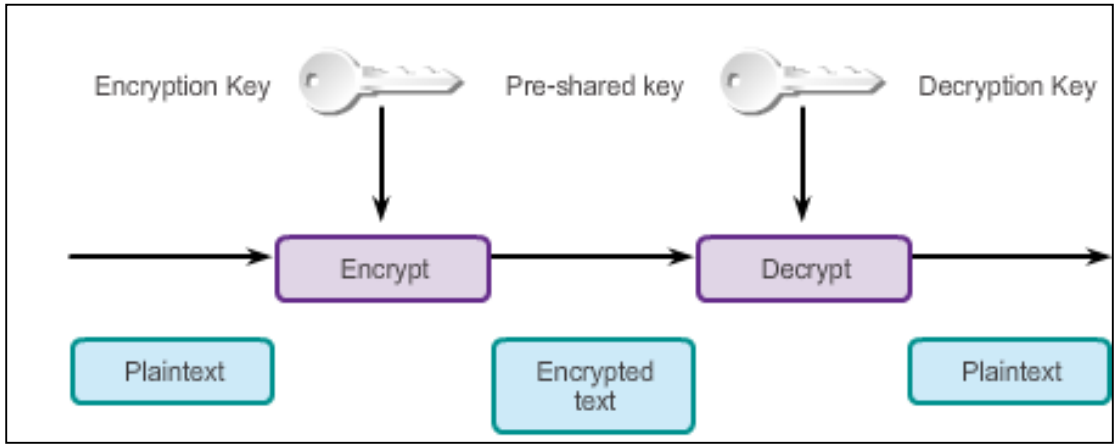


Encryption Algorithms

- As key length increases, it becomes more difficult to break the encryption. However, a longer key requires more processor resources when encrypting and decrypting data.
- Two main types of encryption are:
  - Symmetric Encryption
  - Asymmetric Encryption

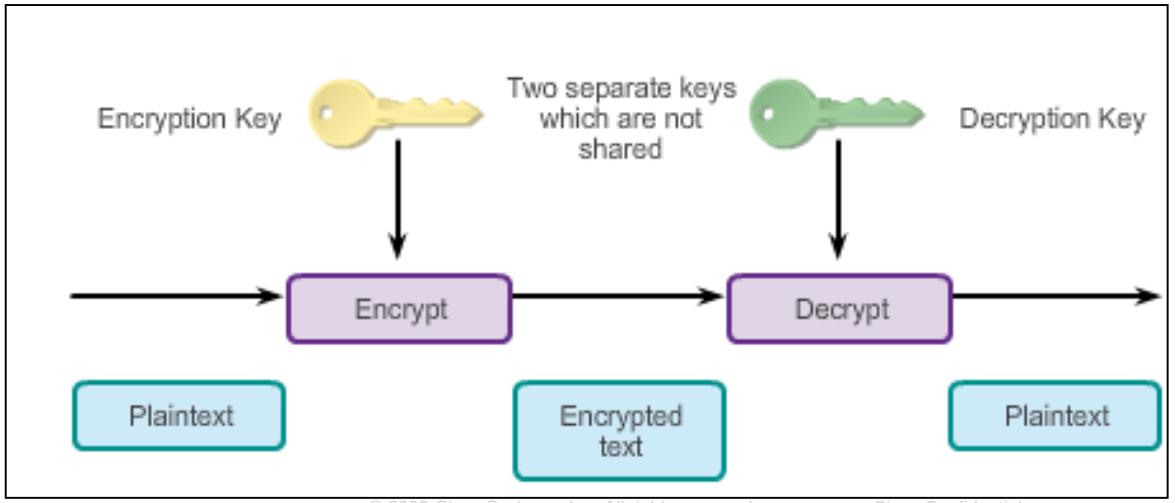
Symmetric Encryption

- Encryption and decryption use the same key.
- Each of the two networking devices must know the key to decode the information.
- Each device encrypts the information before sending it over the network to the other device.
- Typically used to encrypt the content of the message.
- Examples: DES and 3DES (no longer considered secure) and AES (256-bit recommended for IPsec encryption).



Asymmetric Encryption

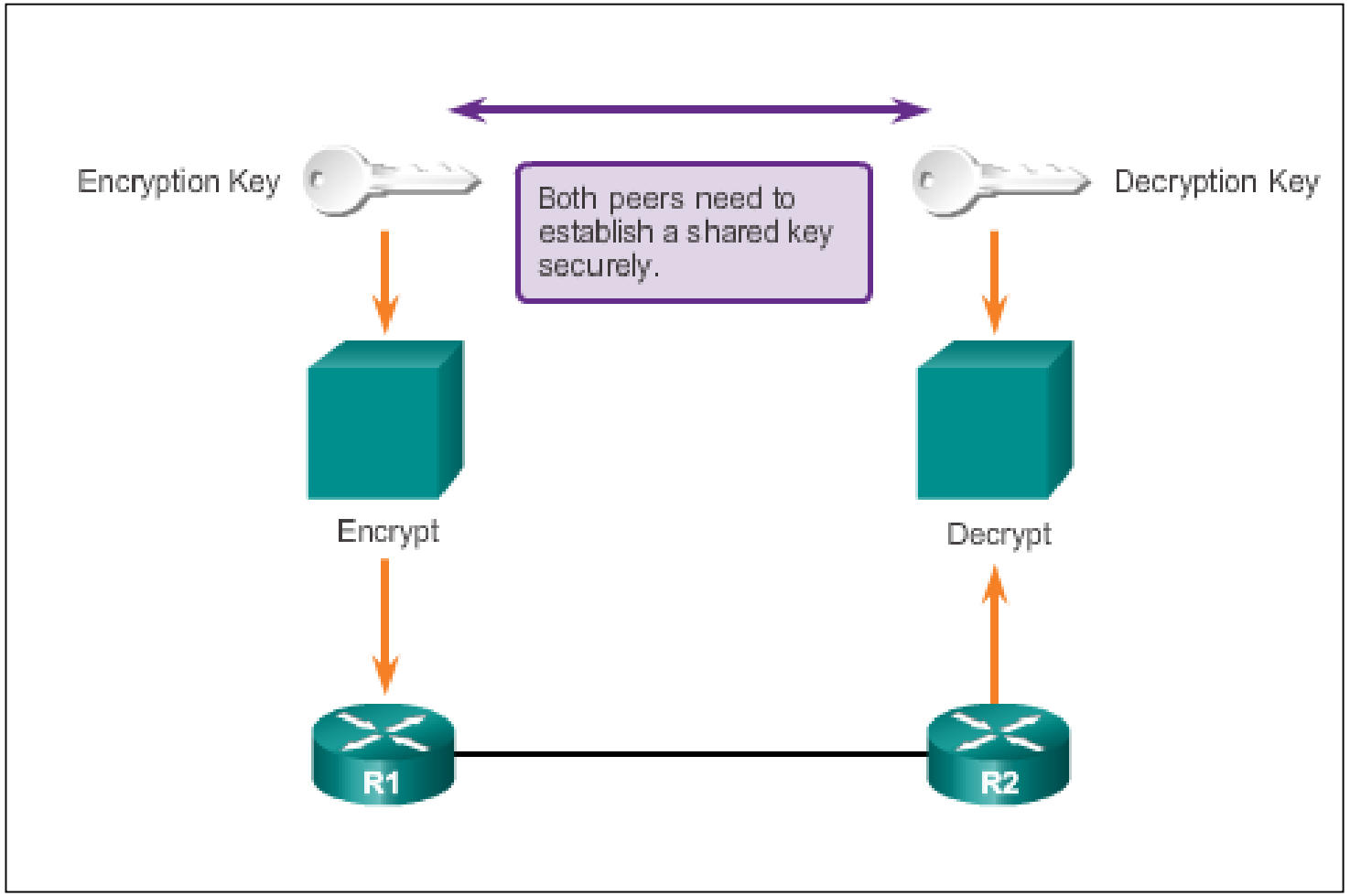
- Uses different keys for encryption and decryption.
- Knowing one of the keys does not allow a hacker to deduce the second key and decode the information.
- One key encrypts the message, while a second key decrypts the message.
- Public key encryption is a variant of asymmetric encryption that uses a combination of a private key and a public key.
- Typically used in digital certification and key management
- Example: RSA



Diffie-Hellman Key Exchange

- Diffie-Hellman (DH) is not an encryption mechanism and is not typically used to encrypt data.
- DH is a method to securely exchange the keys that encrypt data.
- DH algorithms allow two parties to establish a shared secret key used by encryption and hash algorithms.
- DH is part of the IPsec standard.
- Encryption algorithms, such as DES, 3DES, and AES, as well as the MD5 and SHA-1 hashing algorithms, require a symmetric, shared secret key to perform encryption and decryption.
- DH algorithm specifies a public key exchange method that provides a way for two peers to establish a shared secret key that only they know, although they are communicating over an insecure channel.

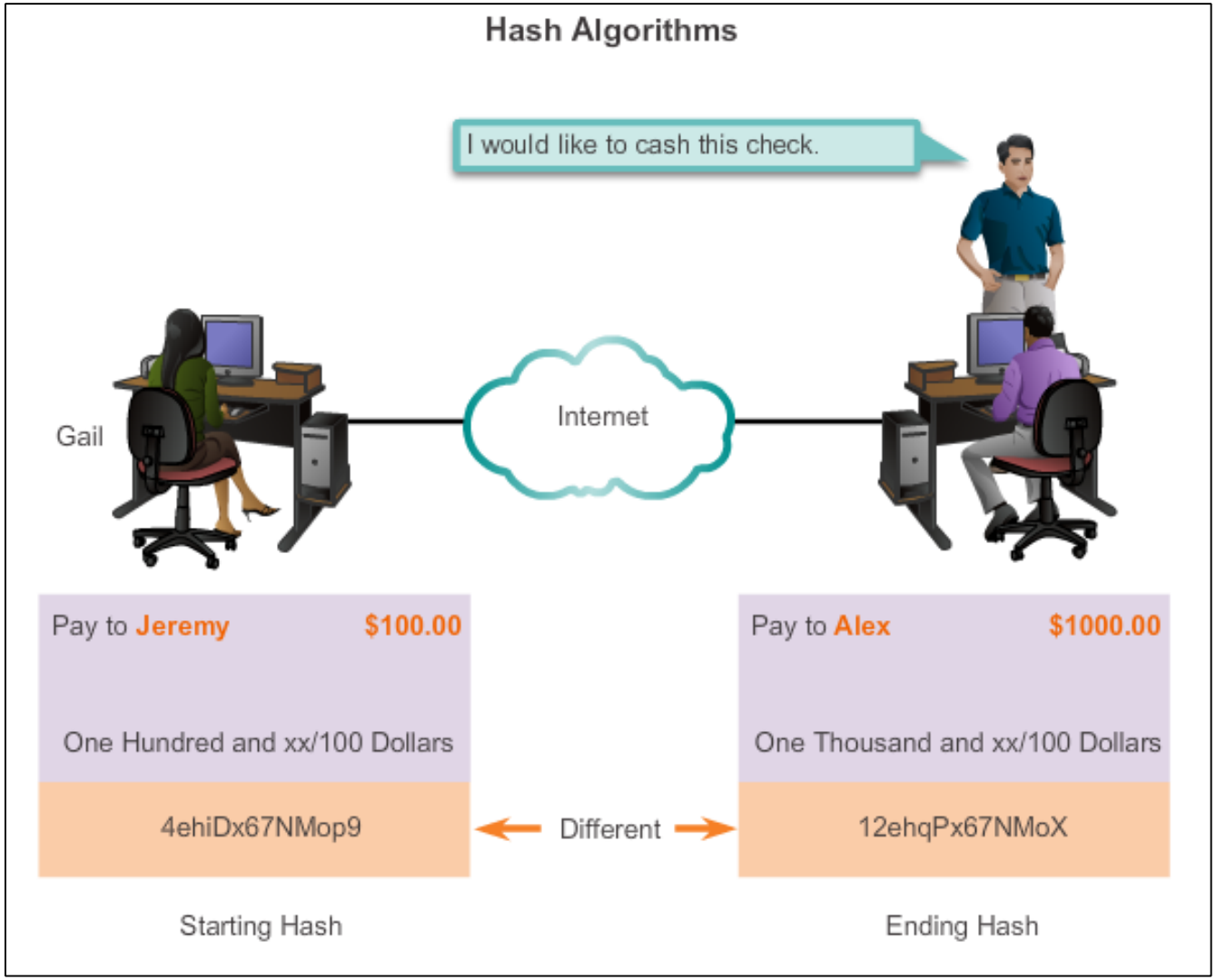
Diffie-Hellman Key Exchange



Integrity with Hash Algorithms

- The original sender generates a hash of the message and sends it with the message itself.
- The recipient parses the message and the hash, produces another hash from the received message, and compares the two hashes.
- If they are the same, the recipient can be reasonably sure of the integrity of the original message.

Integrity with Hash Algorithms (cont.)



Integrity with Hash Algorithms (cont.)

Hash-based Message Authentication Code (HMAC) is a mechanism for message authentication using hash functions.

- HMAC has two parameters: A message input and a secret key known only to the message originator and intended receivers.
- Message sender uses an HMAC function to produce a value (the message authentication code) formed by condensing the secret key and the message input.
- Message authentication code is sent along with the message.
- Receiver computes the message authentication code on the received message using the same key and HMAC function as the sender used.
- Receiver compares the result that is computed with the received message authentication code.
- If the two values match, the message has been correctly received and the receiver is assured that the sender is a user community member who share the key.

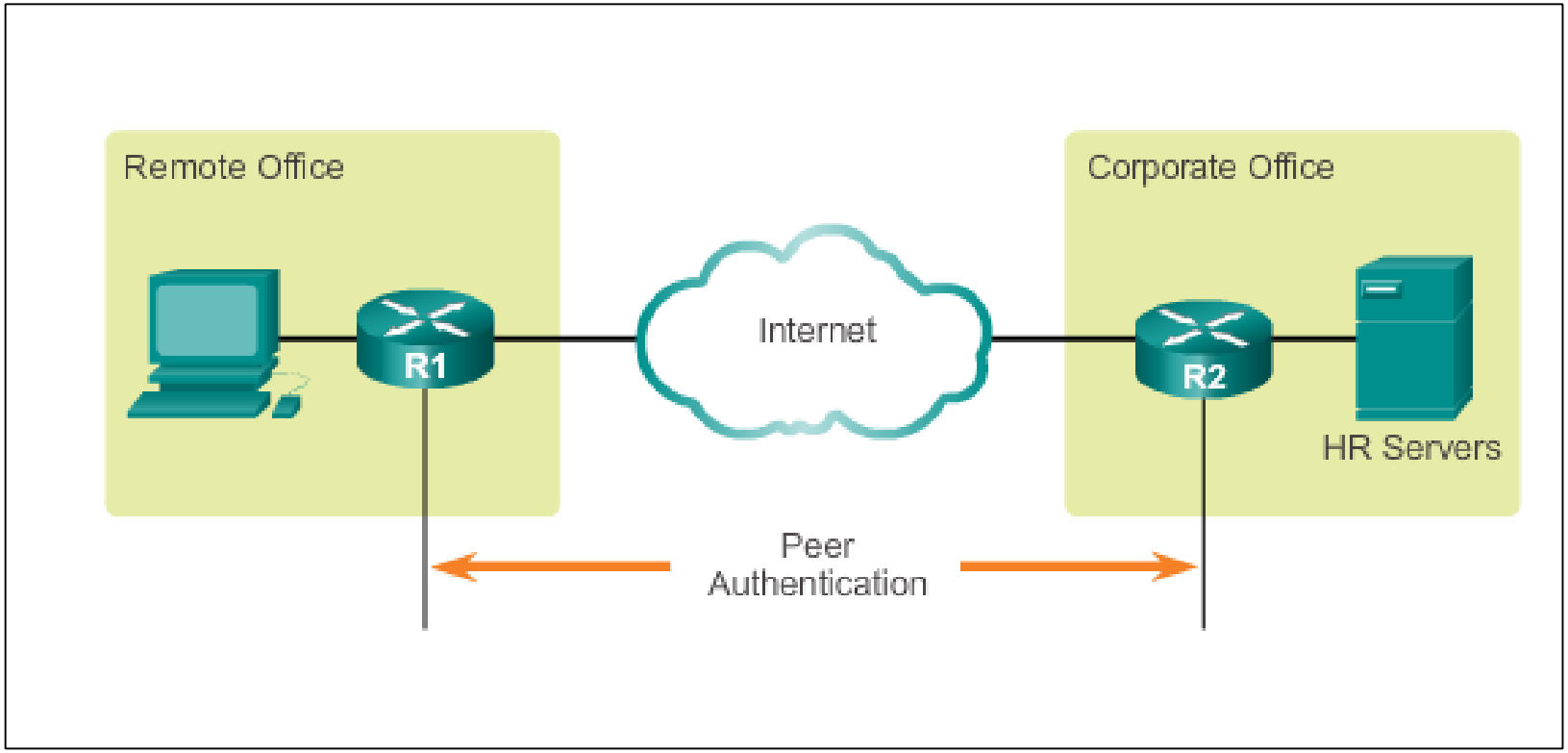
Integrity with Hash Algorithms (cont.)

There are two common HMAC algorithms:

- **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 hash is appended to the original message and forwarded to the remote end.
- **SHA** – SHA-1 uses a 160-bit secret key. The variable-length message and the 160-bit shared secret key are combined and run through the HMAC-SHA1 hash algorithm. The output is a 160-bit hash. The hash is appended to the original message and forwarded to the remote end.

IPsec Authentication

- IPsec VPNs support authentication.
- Device on the other end of the VPN tunnel must be authenticated before the communication path is considered secure.



IPsec Authentication (cont.)

There are two peer authentication methods, PSK and RSA signatures:

- **PSK**
  - A secret key shared between the two parties using a secure channel before it needs to be used.
  - Use symmetric key cryptographic algorithms.
  - A PSK is entered into each peer manually and is used to authenticate the peer.

IPsec Authentication (cont.)

- **RSA signatures**
  - Digital certificates are exchanged to authenticate peers.
  - Local device derives a hash and encrypts it with its private key.
  - Encrypted hash, or digital signature, is attached to the message and forwarded to the remote end.
  - 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.

IPsec Protocol Framework

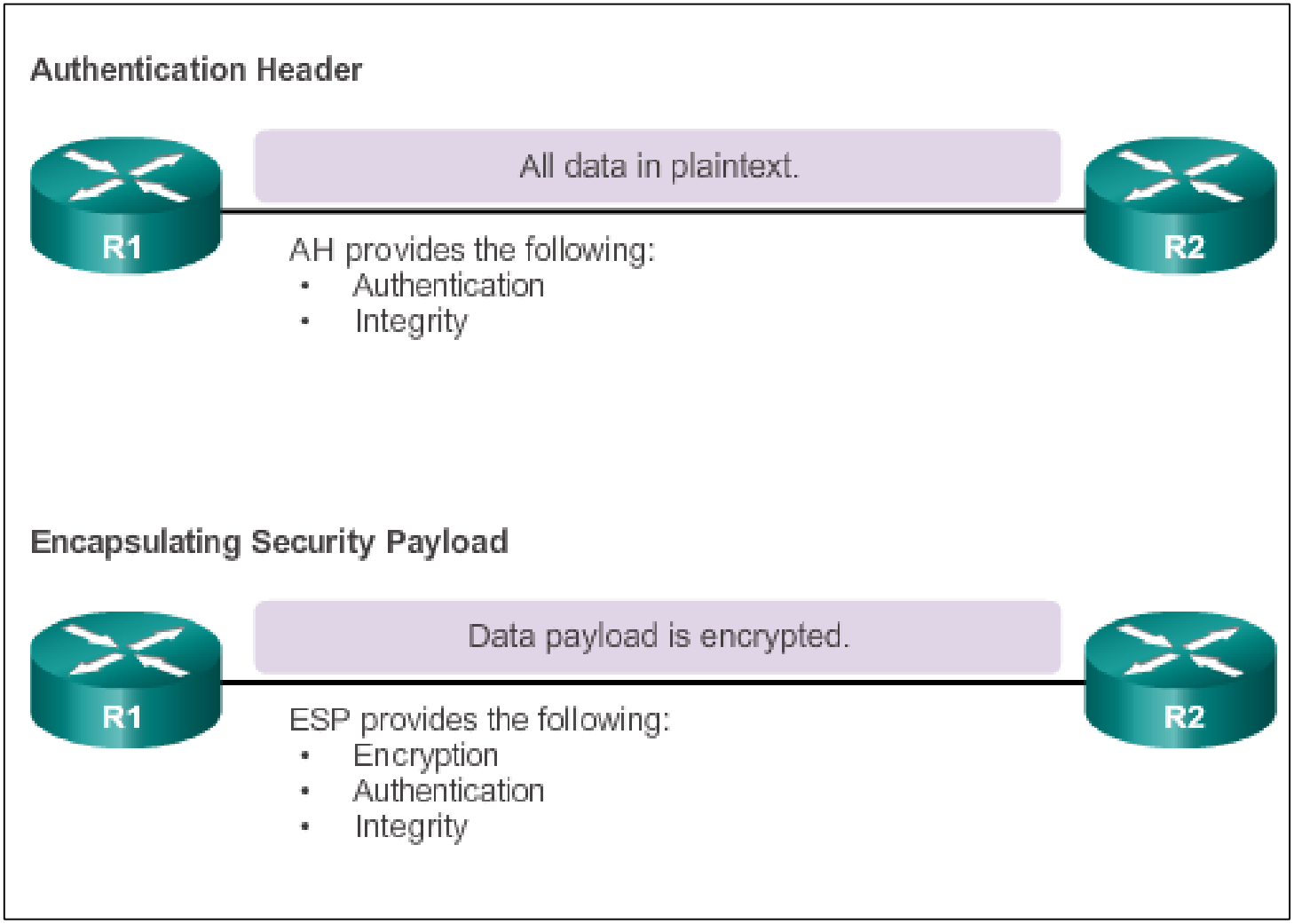
Authentication Header (AH)

- Appropriate protocol to use when confidentiality is not required or permitted.
- Provides data authentication and integrity for IP packets that are passed between two systems.
- Does not provide data confidentiality (encryption) of packets.

Encapsulating Security Payload (ESP)

- A security protocol that provides confidentiality and authentication by encrypting the IP packet.
- Authenticates the inner IP packet and ESP header.
- Both encryption and authentication are optional in ESP, at a minimum, one of them must be selected.

IPsec Protocol Framework (cont.)

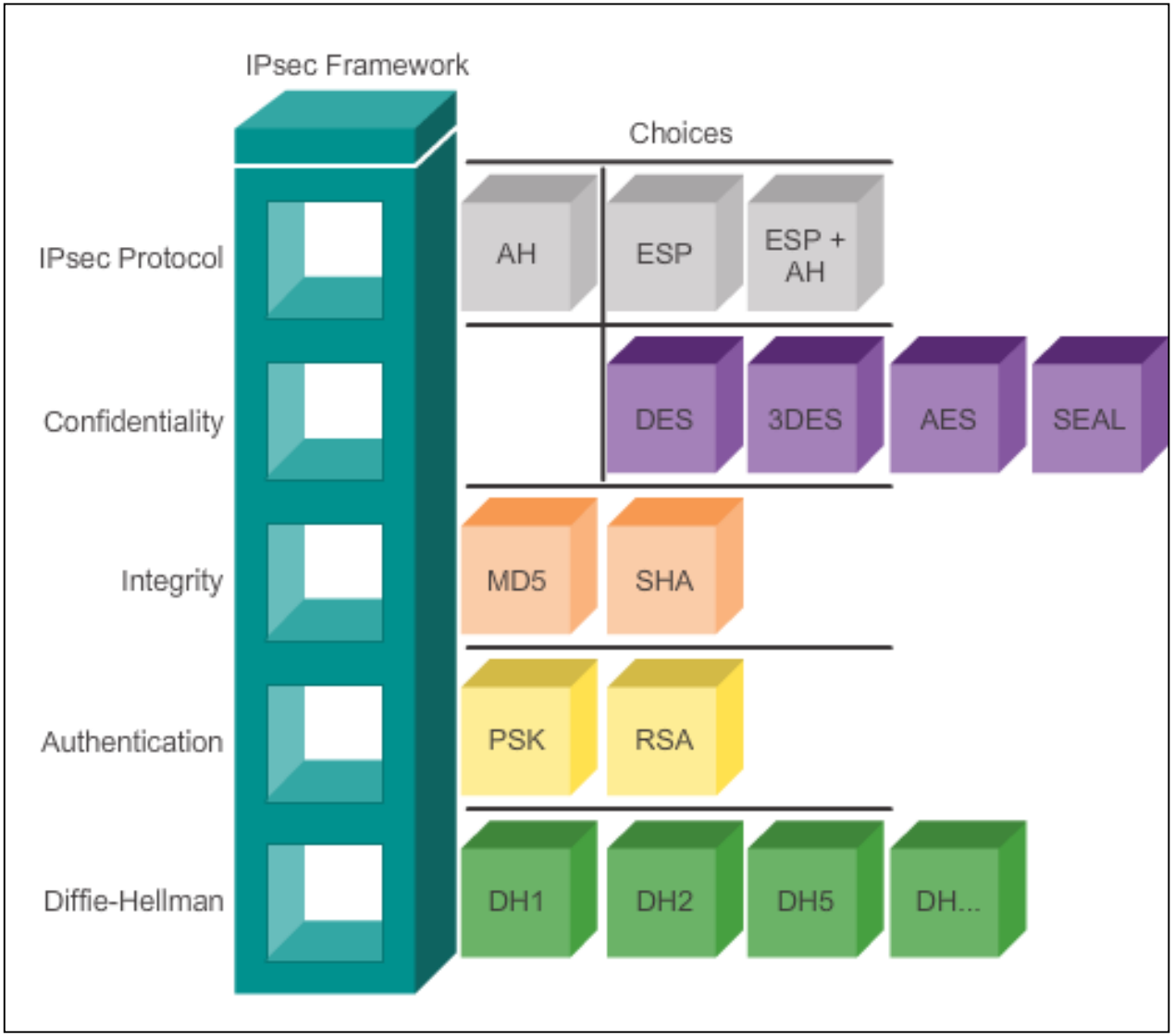


IPsec Protocol Framework (cont.)

Four basic building block of the IPsec framework that must be selected:

- **IPsec framework protocol** – A combination of ESP and AH, ESP or ESP+AH options are almost always selected because AH itself does not provide encryption.
- **Confidentiality** (if IPsec is implemented with ESP) – DES, 3DES, or AES, AES is strongly recommended since provides the greatest security.
- **Integrity** – Guarantees that the content has not been altered in transit using hash algorithms (MD5 or SHA).
- **Authentication** – Represents how devices on either end of the VPN tunnel are authenticated (PSK or RSA).
- **DH algorithm group** – Represents how a shared secret key is established between peers, DH24 provides the greatest security.

IPsec Protocol Framework (cont.)



1. Host A sends interesting traffic to Host B.

2. Routers A and B negotiate an IKE Phase 1 session.

3. Routers A and B negotiate an IKE Phase 2 session.

4. Information is exchanged via the IPsec tunnel.

5. The IPsec tunnel is terminated.

Vytvorenie spojenia: IKE fáza 1

- IKE fáza 1 má tri kroky:
  - Dohodnutie ISAKMP politík
  - Výmenu kľúčov pomocou Diffie-Hellmanovho algoritmu
  - Overenie **totožnosti susedov**
- Dohodnutie ISAKMP politík
  - Aký šifrovací algoritmus? (confident.)
  - Aký hashovací algoritmus? (integr.)
  - Aká Diffie-Hellmanova grupa?
  - Aký spôsob overenia totožnosti? (auth.)
- Overenie totožnosti
  - Podľa spôsobu dohodnutého v prvom kroku
- IKE fáza 1 si vytvára zabezpečený kanál pre overenie totožnosti IPsec susedov a prípadne používateľov
  - Nedohaduje samotné vlastnosti pre činnosť IPsec
  - Tie sa dohodnú až vo fáze 2 pomocou tohto zabezpečeného kanála

Vytvorenie spojenia: IKE fáza 2

- IKE fáza 2 zodpovedá za dojednanie spôsobu použitia IPsec medzi susedmi
  - Aký protokol – AH, ESP, AH+ESP?
  - Aký režim – tunelový alebo transportný?
  - Aký šifrovací algoritmus?
  - Aký hashovací mechanizmus?
  - Aké šifrovacie kľúče?
  - Aká životnosť dohodnutých informácií?
- Prvé štyri vlastnosti sa nazývajú aj *transformačná sada*

Kroky pri konfigurácii IPsec

- Postup pri konfigurácii IPsec

  Vytvoriť aspoň jednu ISAKMP politiku pre fázu 1

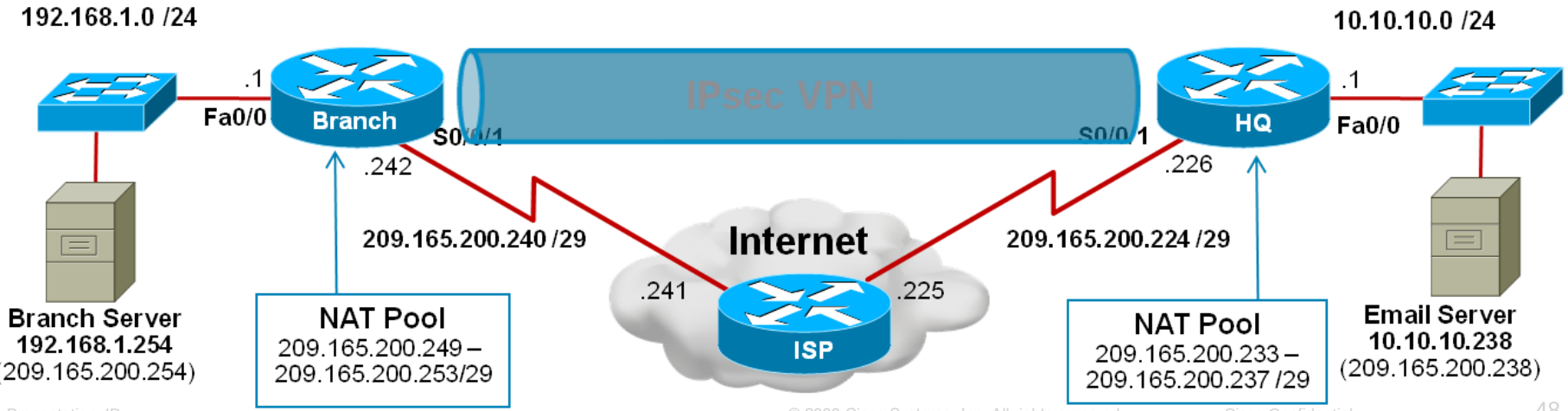
  Vytvoriť aspoň jednu transformačnú sadu pre fázu 2

  Vytvoriť kryptovaciu mapu a ACL, ktoré popisujú, čo sa má zabezpečiť pomocou IPsec a ako

  Aplikovať kryptovaciu mapu na výstupné rozhranie

- Poznámka:

  Internet je v príklade použitý len ako záložne spojenie pre private WAN



Kompletná konfigurácia Branch Router IPsec VPN

```
Branch# conf t
Branch(config)# crypto isakmp policy 1
Branch(config-isakmp)# encryption aes
Branch(config-isakmp)# authentication pre-share
Branch(config-isakmp)# group 2
Branch(config-isakmp)# exit
Branch(config)# crypto isakmp key cisco123 address 209.165.200.226
Branch(config)#
Branch(config)# crypto ipsec transform-set HQ-VPN esp-sha-hmac esp-3des
Branch(cfg-crypto-trans)# exit
Branch(config)#
Branch(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 10.10.10.0 0.0.0.255
Branch(config)#
Branch(config)#
Branch(config)# crypto map HQ-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
Branch(config-crypto-map)# set transform-set HQ-VPN
Branch(config-crypto-map)# set peer 209.165.200.226
Branch(config-crypto-map)# match address 110
Branch(config-crypto-map)# exit
Branch(config)# int s0/0/1
Branch(config-if)# crypto map HQ-MAP
Branch(config-if)# ^Z
Branch#
```

❶ **ISAKMP Policy**
Specifies the initial VPN security details

❷ **IPsec Details**
Specifies how the IPsec packet will be encapsulated

❸ **Crypto ACL**
Specifies the traffic that will trigger the VPN to activate

❹ **VPN Tunnel Information**
Creates the crypto map that combines the ISAKMP policy, IPsec transform set, VPN peer address, and crypto ACL

❺ **Apply the Crypto Map**
Identifies which interface is actively looking to create a VPN

IPsec: Záverečné poznámky

- Pre NAT-T musia byť na firewalloch otvorené porty

  UDP/500

  UDP/4500

- Vzhľadom na pomerne vysokú technickú náročnosť IPsec sa pre mobilných klientov odporúča nová technológia SSLVPN, ktorá má nižšie technické nároky

7.4 Remote Access

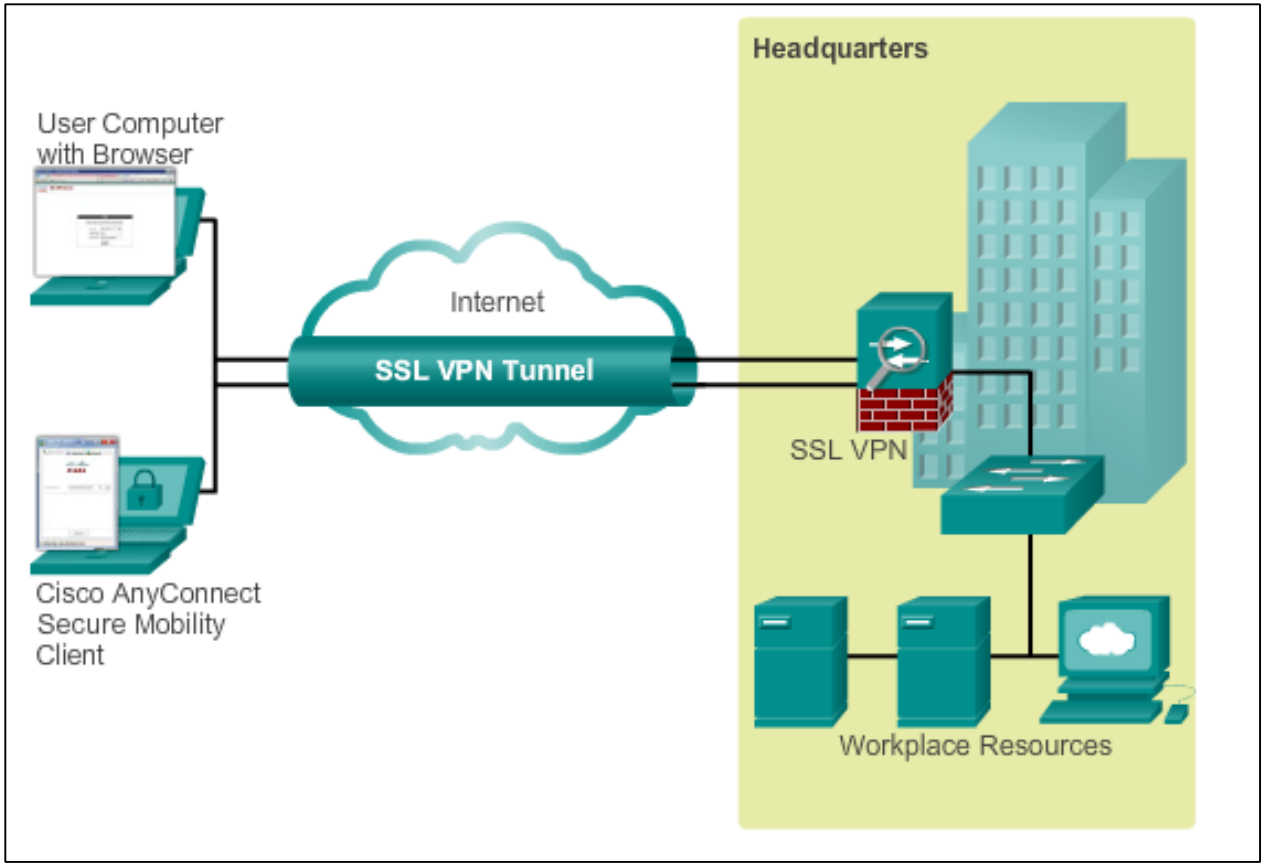
Cisco | Networking Academy®
Mind Wide Open™

Types of Remote Access VPNs

- There are two primary methods for deploying remote access VPNs:
  - Secure Sockets Layer (SSL)
  - IP Security (IPsec)
- Type of VPN method based on the access requirements of the users and the organization's IT processes.
- Both types offer access to virtually any network application or resource.

Cisco SSL VPN

- Provides remote access by using a web browser and the web browser's native SSL encryption.
- Can provide remote access using the Cisco AnyConnect Secure Mobility Client software



Cisco SSL VPN Solutions

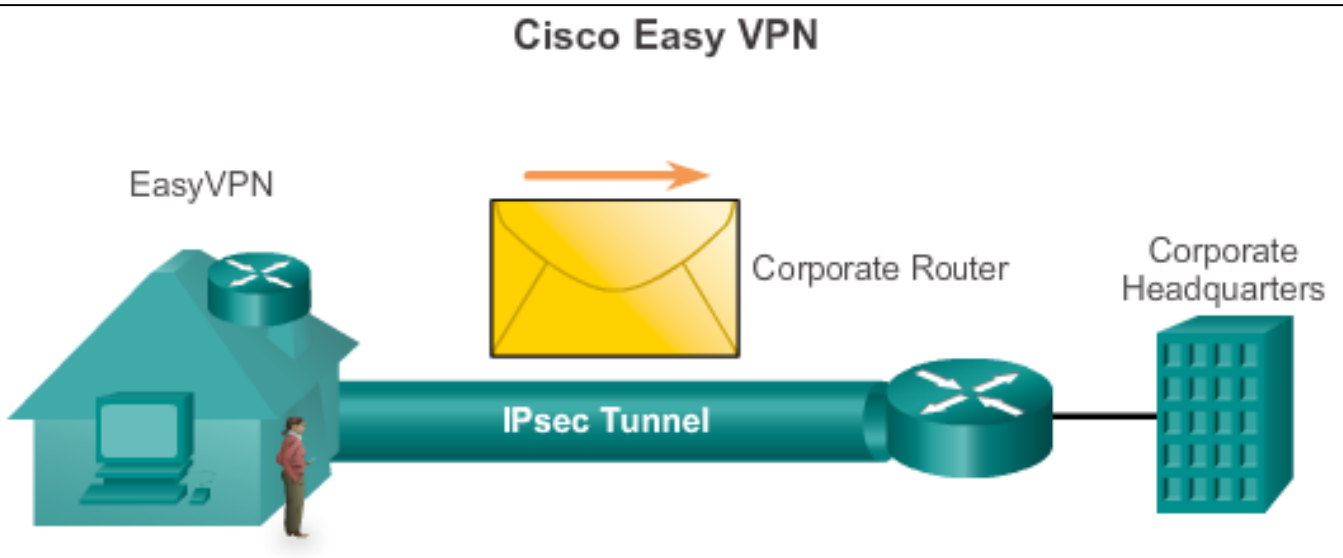
Cisco AnyConnect Secure Mobility Client with SSL

- Client-Based SSL VPNs provide authenticated users with LAN-like, full network access to corporate resources
- The remote devices require a client application, such as the Cisco VPN Client or the newer AnyConnect client to be installed on the end-user device

Cisco Secure Mobility Clientless SSL VPN

- Enables corporations to provide access to corporate resources even when the remote device is not corporately-managed
- Cisco ASA is used as a proxy device to network resources
- Provides a web portal interface for remote devices to navigate the network using port-forwarding capabilities

IPsec Remote Access



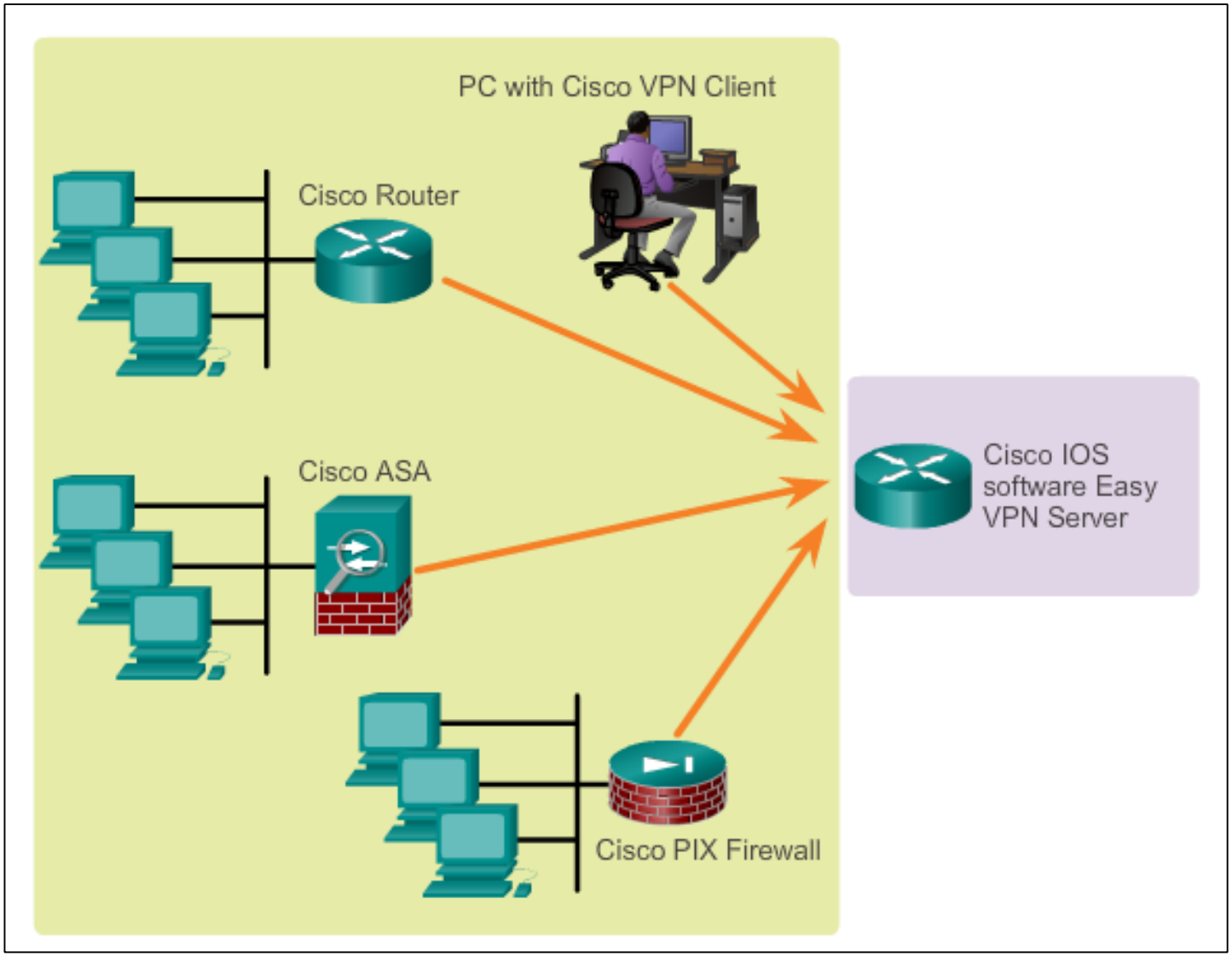
Cisco Easy VPN

- Negotiates tunnel parameters
- Establishes tunnels according to set parameters
- Authenticates users by usernames, group names, and passwords
- Manages security keys for encryption and decryption
- Authenticates, encrypts, and decrypts data through the tunnel

IPsec Remote Access (cont.)

- The Cisco Easy VPN solution consists of three components:
  - **Cisco Easy VPN Server – A Cisco IOS router or Cisco ASA** Firewall acting as the VPN head-end device in site-to-site or remote-access VPNs.
  - **Cisco Easy VPN Remote** – A Cisco IOS router or Cisco ASA Firewall acting as a remote VPN client.
  - **Cisco VPN Client** – An application supported on a PC used to access a Cisco VPN server.
- The Cisco Easy VPN solution feature offers flexibility, scalability, and ease of use for both site-to-site and remote access IPsec VPNs.

Cisco Easy VPN Server and Remote



Comparing IPsec and SSL

	SSL	IPsec
Applications	Web-enabled applications, file sharing, Email	All IP-based applications
Encryption	**Moderate to Strong** Key lengths from 40 bits to 256 bits	**Strong** Key lengths from 56 bits to 256 bits
Authentication	**Moderate** One-way or two-way authentication	**Strong** Two-way authentication using shared secrets or digital certificates
Connection Complexity	**Low** Requires only a web browser	**Medium** Can be challenging to nontechnical users
Connection Options	Any device can connect	Only specific devices with specific configurations can connect

Chapter 7: Summary

- VPNs are used to create a secure end-to-end private network connection over a third-party network, such as the Internet.
- A site-to-site VPN uses a VPN gateway device at the edge of both sites. The end hosts are unaware of the VPN and have no additional supporting software.
- A remote access VPN requires software to be installed on the individual host device that accesses the network from a remote location.
  - The two types of remote access VPNs are SSL and IPsec.
  - SSL technology can provide remote access using a client's web browser and the browser's native SSL encryption.
  - Using Cisco AnyConnect software on the client, users can have LAN-like, full network access using SSL.

Chapter 7: Summary (cont.)

- GRE is a basic, non-secure site-to-site VPN tunneling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels, thus allowing an organization to deliver other protocols through an IP-based WAN.
  - Today, it is primarily used to deliver IP multicast traffic or IPv6 traffic over an IPv4 unicast-only connection.
- IPsec, an IETF standard, is a secure tunnel operating at Layer 3 of the OSI model that can protect and authenticate IP packets between IPsec peers.
  - It can provide confidentiality by using encryption, data integrity, authentication, and anti-replay protection.
  - Data integrity is provided by using a hash algorithm, such as MD5 or SHA.
  - Authentication is provided by the PSK or RSA peer authentication method.

Chapter 7: Summary (cont.)

- The level of confidentiality provided by encryption depends on the algorithm used and the key length.
- Encryption can be symmetrical or asymmetrical.
- DH is a method used to securely exchange the keys to encrypt data.