VPNs: Virtual Private Networks

Module 18

VPN Terminology

- Tunnel: established VPN
- Payload: data sent over the VPN
- Label: tag applied to VPN packets for faster routing
- Leased-line: private connection only used for one company's traffic; leased by an ISP
- SSL (Secure Socket Layer): security technology for establishing an encrypted link between a server and client
- Hash: unique fixed-length string generated by an algorithm

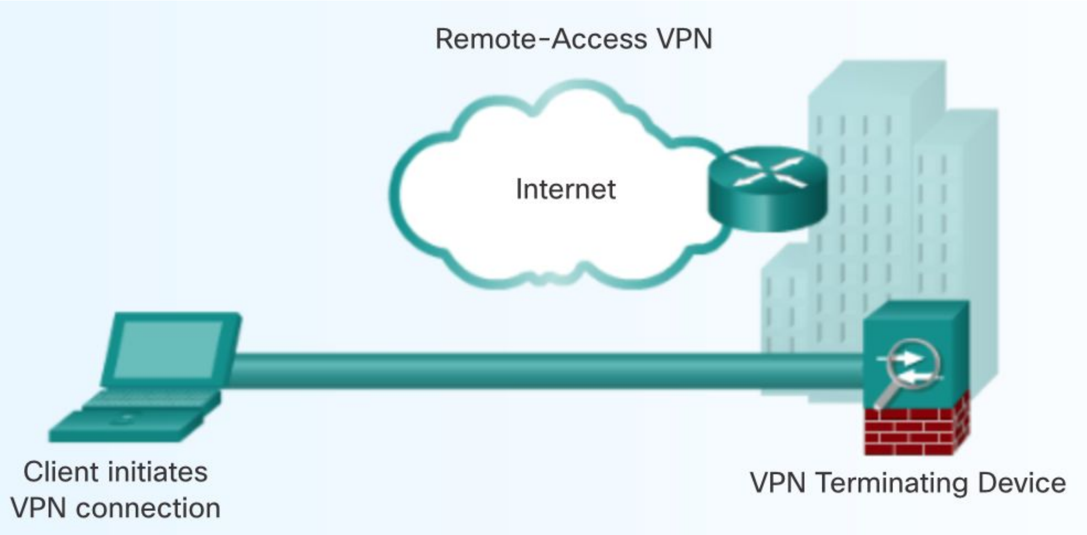
What is a VPN?

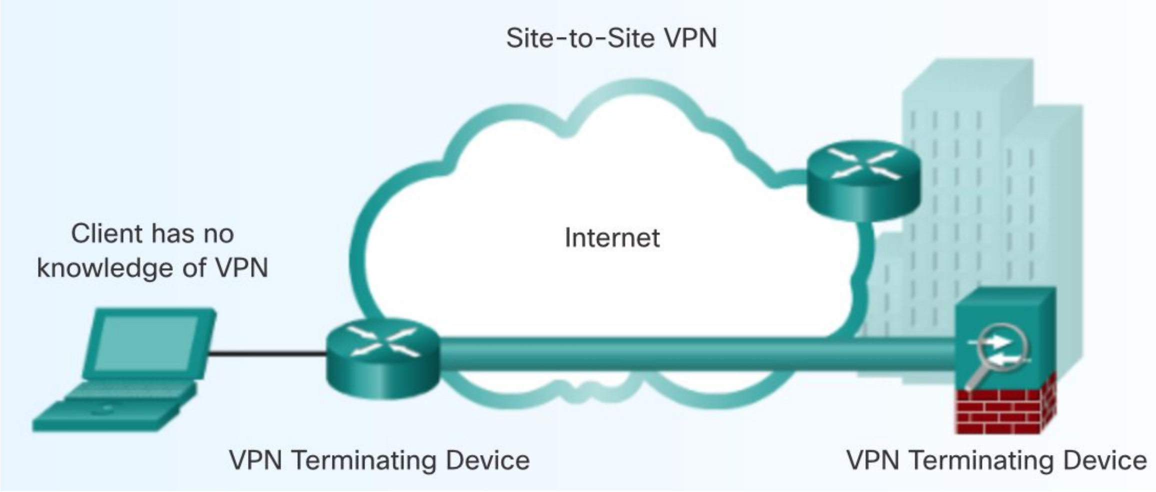
- Creates an end-to-end private network connection (tunnel) over third-party networks, such as the Internet
- Uses encryption for confidentiality
- Benefits include cost savings, security, scalability, and compatibility with broadband networks

Types of VPNs

- Layer 2 or layer 3: the VPN takes place at different layers but is essentially the same
- GRE (Generic Routing Encapsulation): provides an unencrypted tunnel
- Point-to-point VPNs using GRE or IPsec
- Any-to-any connections using MPLS (Multiprotocol Label Switching)
- Site-to-site VPNs exist statically and may be implemented without user knowledge
- Remote access VPNs can be easily disabled and enabled

Types of VPNs





Client Software

- Cisco VPN Client: legacy software
- Cisco AnyConnect Secure Mobility Client
  - Clientless: HTTP(S) content only
  - Thin client: any TCP-based protocol
  - Full client: virtually anything
- Cisco Remote Router VPN Client: uses the router as a client

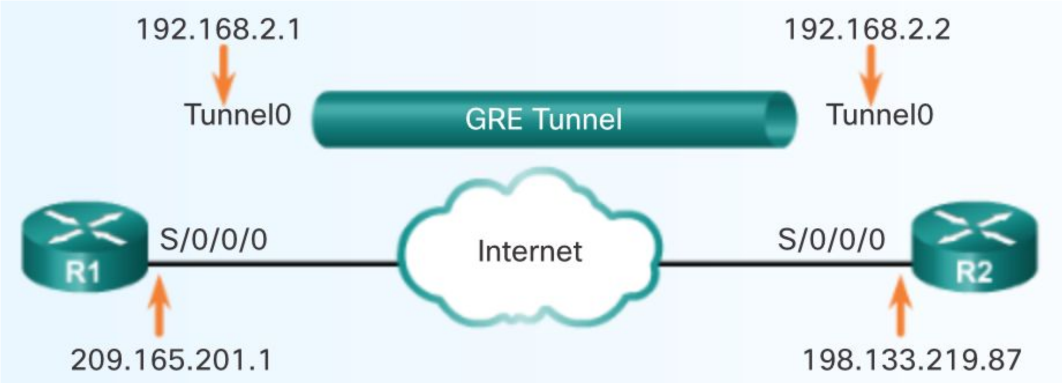
GRE

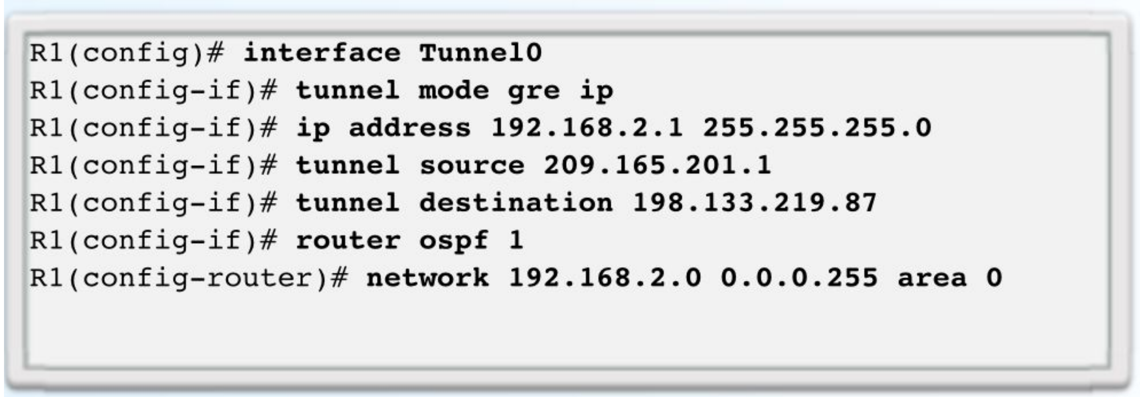
- Supports multiprotocol tunneling
- Does not have security features
- Encapsulates packets with a header containing a GRE flag and protocol type
- Can tunnel non-IP traffic over an IP network

GRE Config

Step Description	Placement	Command	Category
create/access a tunnel interface	anywhere on a router	int tunnel 0	requirement
assign the tunnel an IP address	tunnel config	ip address [ip]	requirement
identify the tunnel's source interface	tunnel config	tunnel source [interface ip]	requirement
identify the tunnel's destination interface	tunnel config	tunnel destination [interface ip]	requirement
specify a protocol to encapsulate	tunnel config	tunnel mode gre [protocol]	requirement
verify the connection	anywhere on a router	do show int tunnel	optional

GRE Config Example



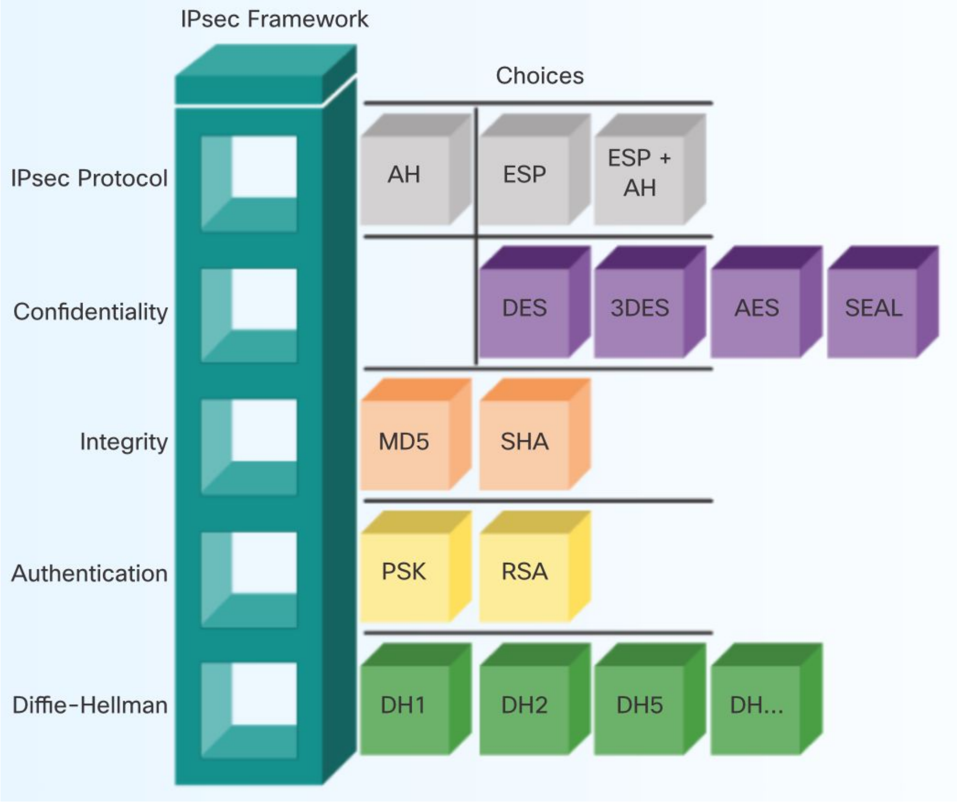


```
R1(config)# interface Tunnel0
R1(config-if)# tunnel mode gre ip
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# tunnel source 209.165.201.1
R1(config-if)# tunnel destination 198.133.219.87
R1(config-if)# router ospf 1
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

Note: Example config is for R1; R2 config not shown

IPsec

- Framework of standards for secure communication
- Works at the networking layer
- Consists of 5 parts: protocol, encryption, data integrity, key signature, Diffie-Hellman key exchange algorithm
- Provides confidentiality, integrity, authentication, and secure key exchange

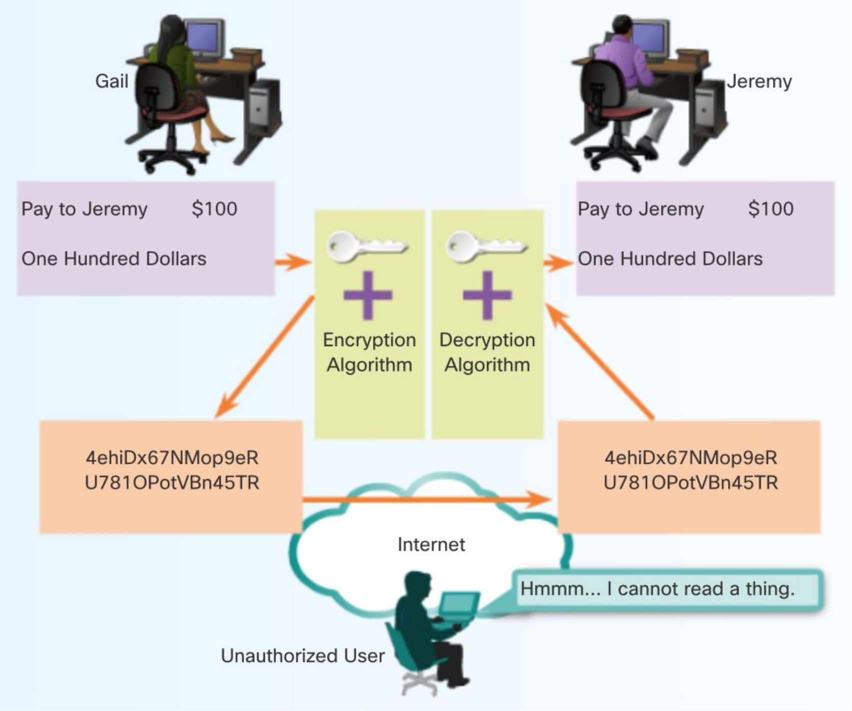


Protocols

- Choice of protocol determines which other IPsec algorithms are available
- AH (Authentication Header): provides data authentication and integrity, but not confidentiality
- ESP (Encapsulating Security Payload): can provide confidentiality and authentication
  - includes anti-replay protection
  - encryption is performed before authentication

Confidentiality Algorithms

- DES (56-bit): least secure
- 3DES (56-bit): uses 3 keys per 64-bit block of data
- AES (128, 192, or 256 bits): stronger security than DES and more efficient than 3DES
- SEAL: Software-Optimized Encryption Algorithm (160-bit)



Integrity Algorithms

- Combine a shared key and variable-length message, which is run through the algorithm to form a hash with a set length
- Ensure that the data has not been altered during transmission
- HMAC-Message Digest 5 (HMAC-MD5) uses a 128-bit key; the output is a 128-bit hash
- HMAC-Secure Hash Algorithm 1 (HMAC-SHA-1) uses a 160-bit key; the output is a 160-bit hash
- MD5 < SHA-1 < SHA-256

Authentication

- Ensures the receiving device is authentic
- PSKs (Pre-Shared Keys)
  - entered into each peer manually
  - do not scale well
- RSA signatures
  - use digital certificates to automatically authenticate devices
  - local device derives a hash and encrypts it with its private key
  - at the remote end, the encrypted hash is decrypted using the public key of the local end

Secure Key Exchange

- Encryption algorithms require a shared secret key
- Diffie-Hellman (DH) key agreement: public key exchange method that provides a way for two peers to establish a shared secret key only they know
  - DH groups 1, 2, and 5 have key sizes of 768, 1024, and 1536 bits; not recommended for use after 2012
  - DH groups 14, 15, and 16 have key sizes with 2048, 3072, and 4096 bits; recommended for use until 2030
  - DH groups 19, 20, and 24 support Elliptical Curve Cryptography (ECC) for more efficient key generation; key sizes are 256, 384, and 2048 bits; group 24 preferred for longevity

IPsec VPN Config

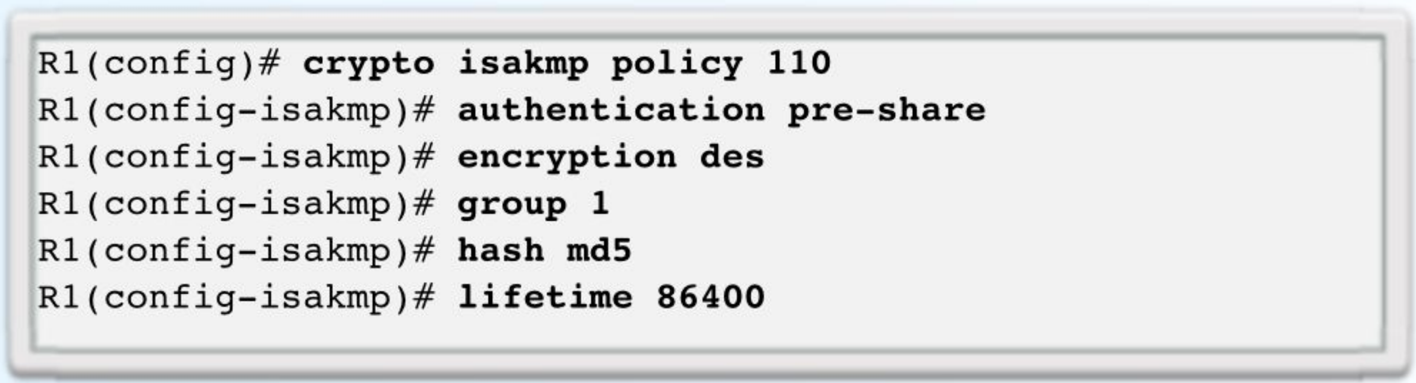
1. Ensure preexisting ACLs are compatible with the IPsec configuration (for example, block all traffic that is not IPsec or IKE)
2. Create an ISAKMP policy to determine the parameters used to establish the tunnel
3. Use a transform set to define the parameters the tunnel uses, such as encryption and integrity algorithms
4. Create an ACL to determine which traffic is sent through the tunnel

IPsec VPN Config (cont.)

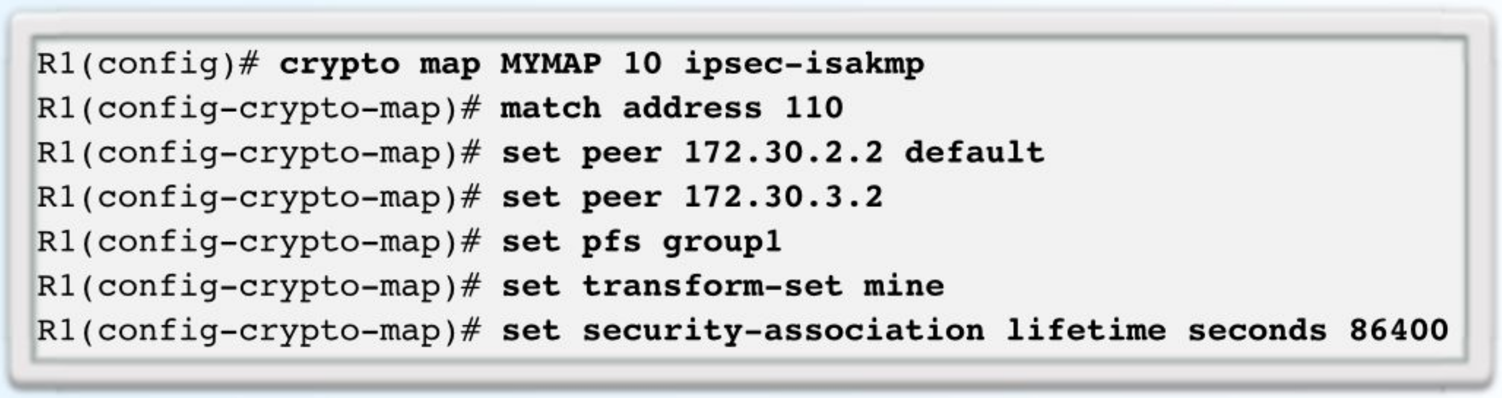
5. Create and apply a crypto map to group the previously configured parameters together and define peer devices
6. Apply the crypto map to the outgoing interface of the VPN device

*See packet tracer checklist for associated commands

IPsec VPN Example Commands



```
R1(config)# crypto isakmp policy 110
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption des
R1(config-isakmp)# group 1
R1(config-isakmp)# hash md5
R1(config-isakmp)# lifetime 86400
```



```
R1(config)# crypto map MYMAP 10 ipsec-isakmp
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# set peer 172.30.2.2 default
R1(config-crypto-map)# set peer 172.30.3.2
R1(config-crypto-map)# set pfs group1
R1(config-crypto-map)# set transform-set mine
R1(config-crypto-map)# set security-association lifetime seconds 86400
```

Packet Tracer Lab

CCNA 8.7.1.4

Credits

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Photographs by Unsplash