CCNA Security 2.0 Study Material – Chapter 8: Implementing Virtual Private Networks

itexamanswers.net/ccna-security-2-0-study-material-chapter-8-implementing-virtual-private-networks.html

October 9, 2017

Chapter Outline:

Section 8.1: VPNs

Upon completion of this section, you should be able to:

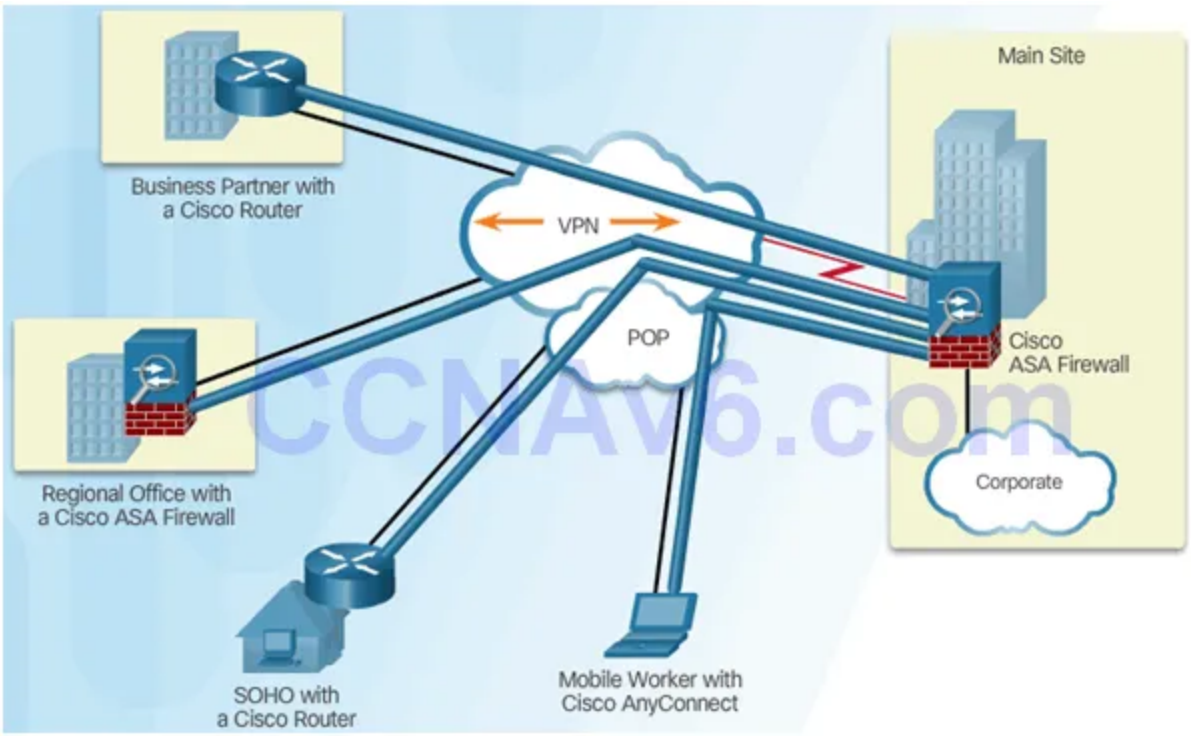
- Describe VPNs and their benefits.
- Compare site-to-site and remote-access VPNs.

Topic 8.1.1: VPN Overview

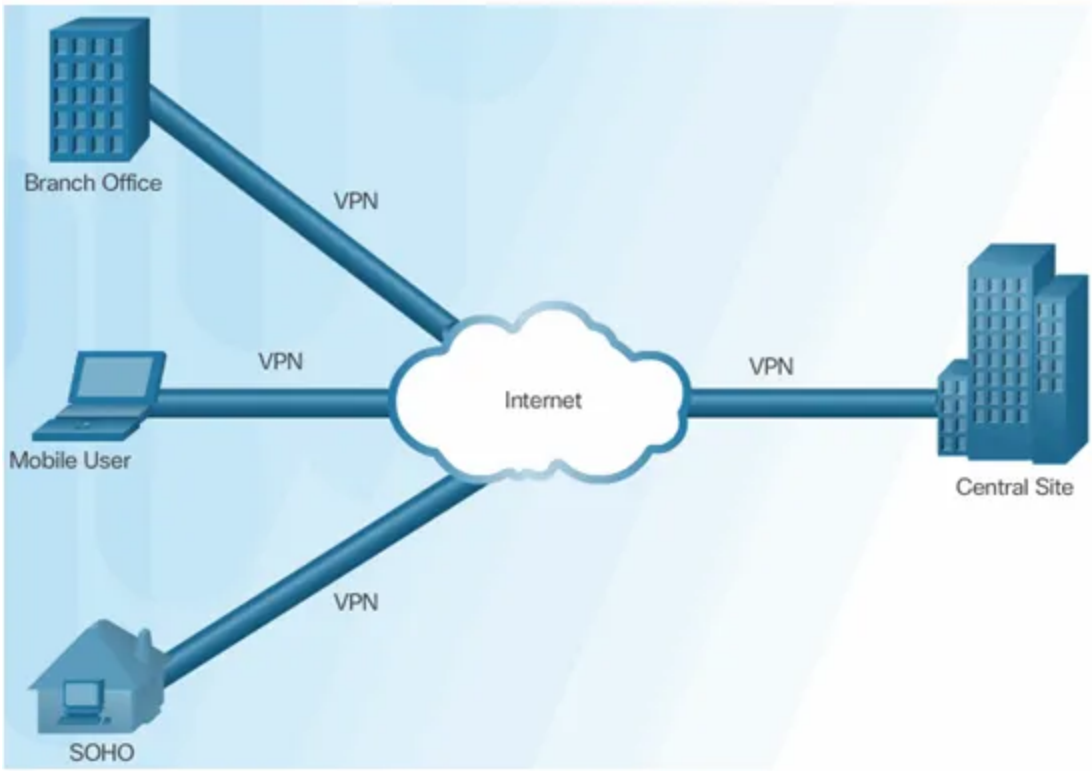
Introducing VPNs

VPN Benefits:

- Cost Savings
- Security
- Scalability
- Compatibility



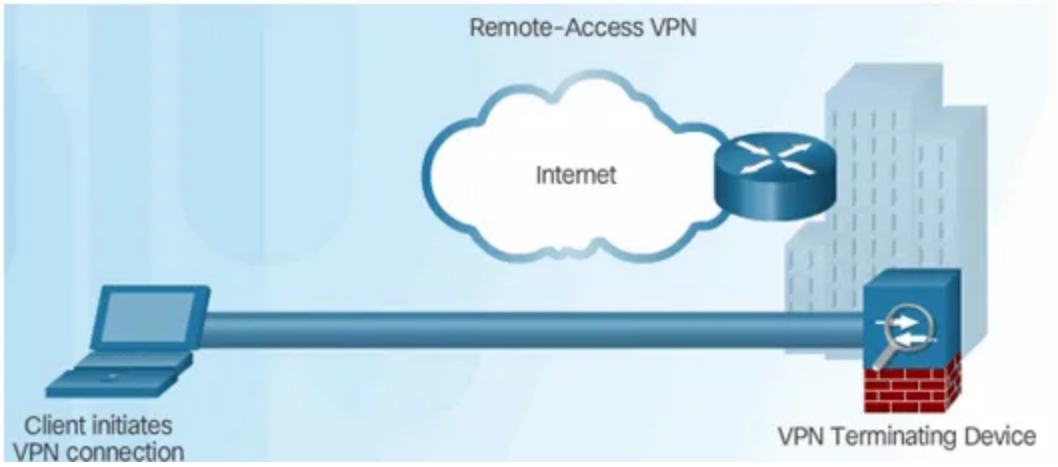
Layer 3 IPsec VPNs



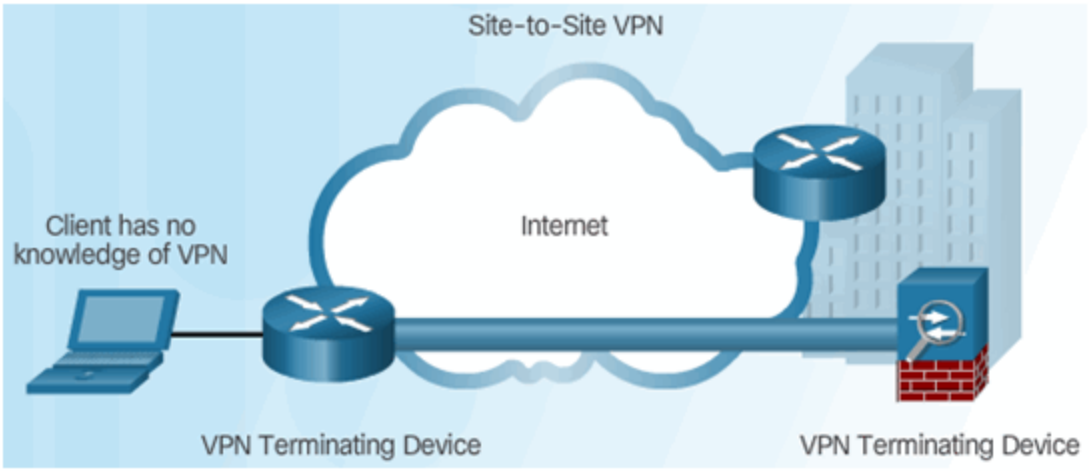
Topic 8.1.2: VPN Technologies

Two Types of VPNs

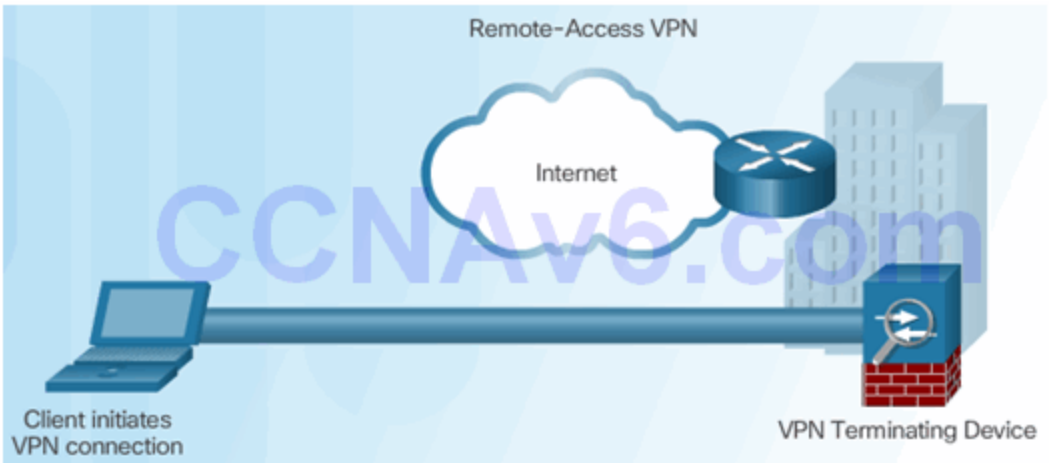
Remote-Access VPN



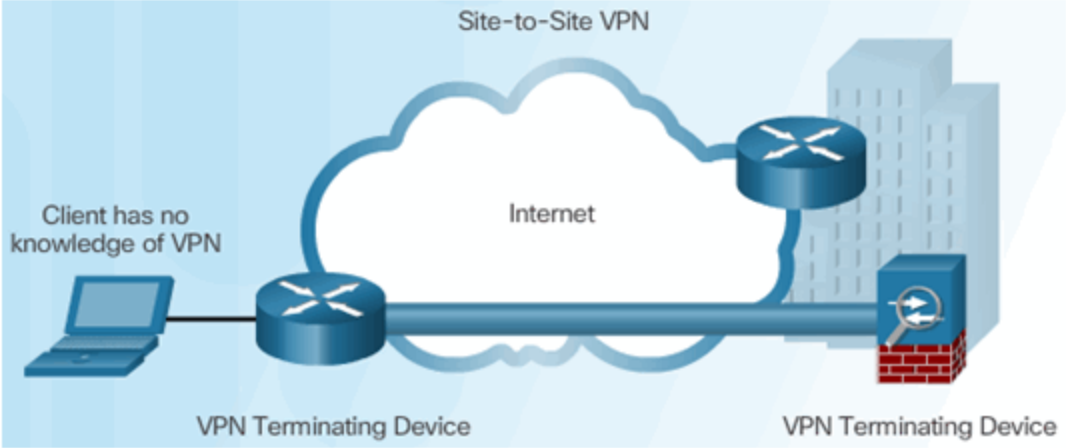
Site-to-Site VPN Access



Components of Remote-Access VPNs



Components of Site-to-Site VPNs



Section 8.2: IPsec VPN Components and Operation

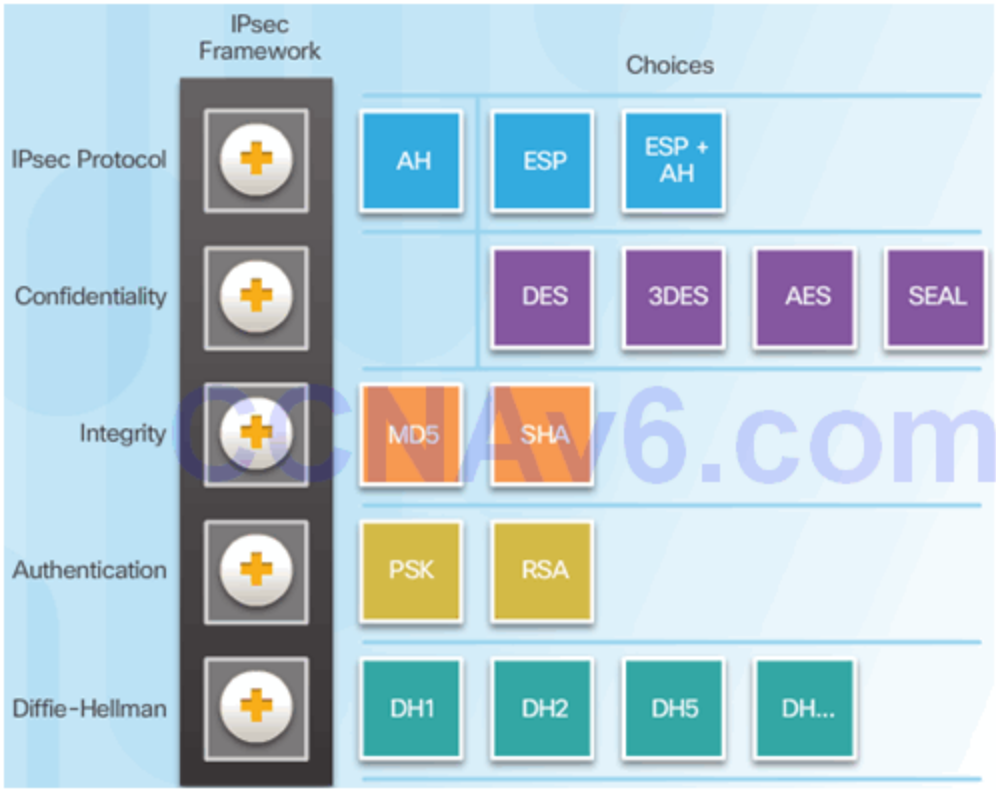
Upon completion of this section, you should be able to:

- Describe the IPsec protocol and its basic functions.
- Compare AH and ESP protocols.
- Describe the IKE protocol.

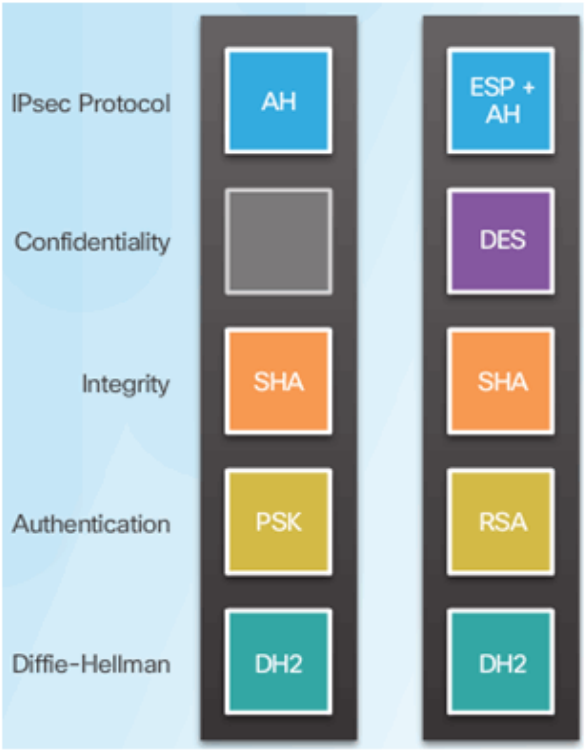
Topic 8.2.1: Introducing IPsec

IPsec Technologies

IPsec Framework

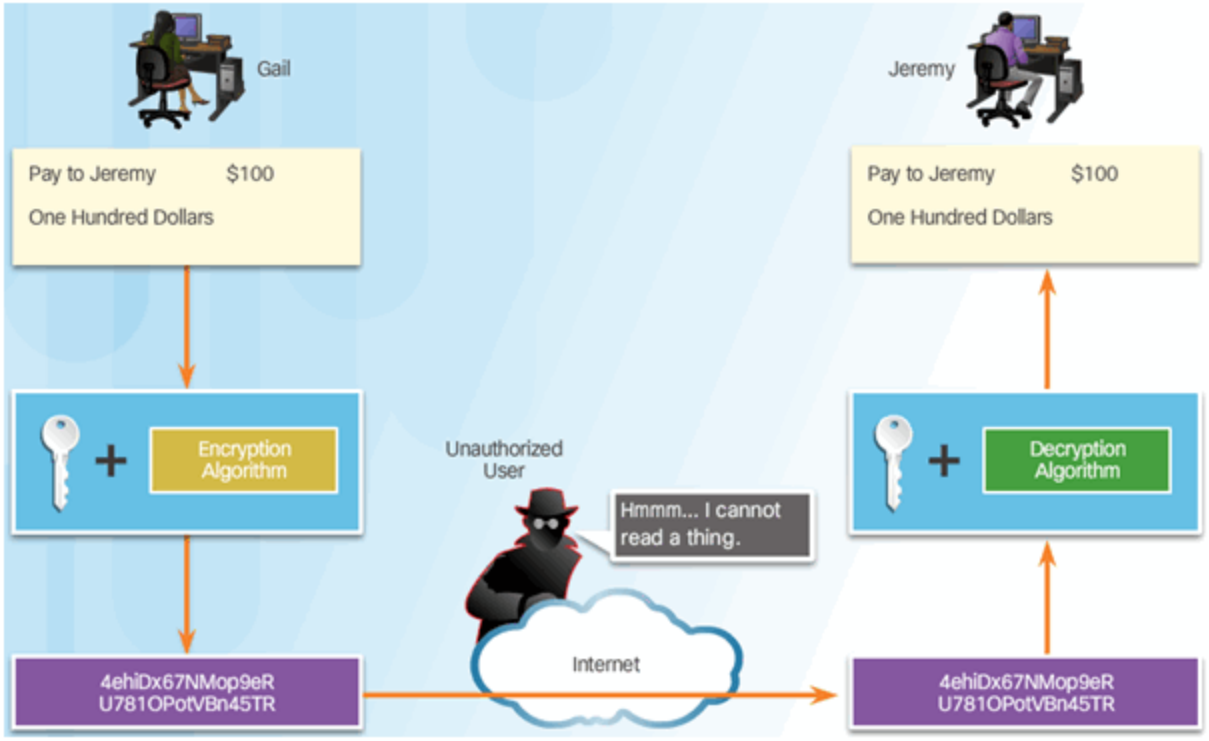


IPsec Implementation Examples

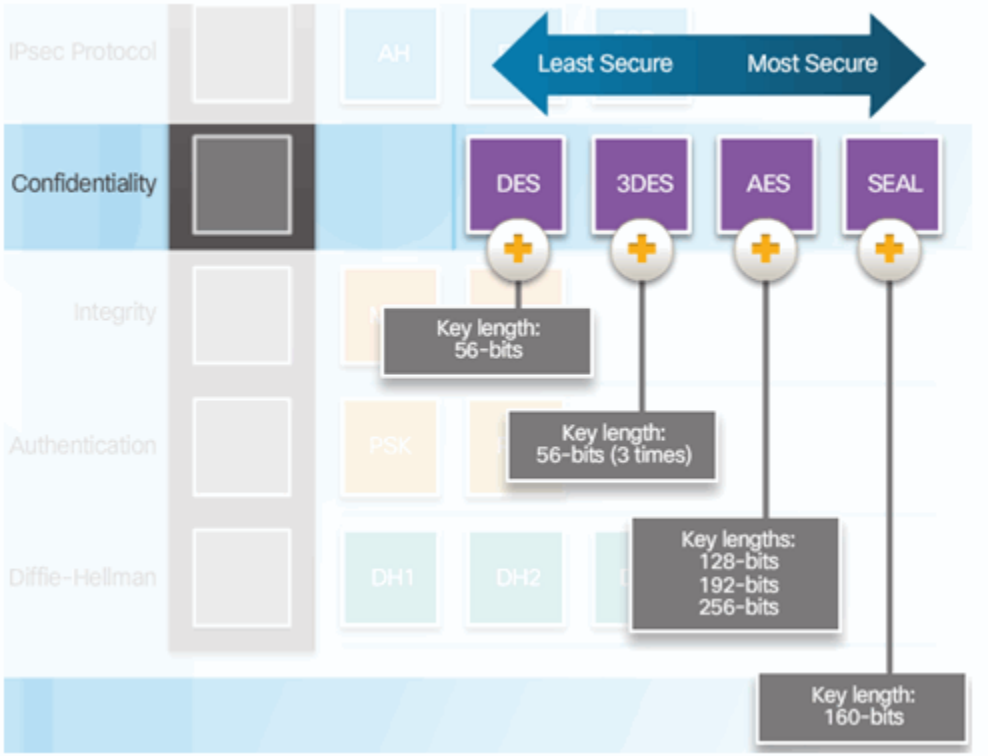


Confidentiality

Confidentiality with Encryption:

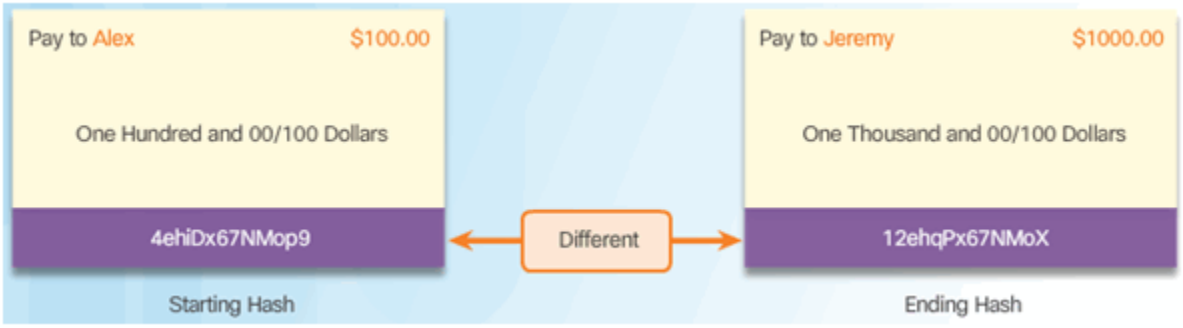


Encryption Algorithms:

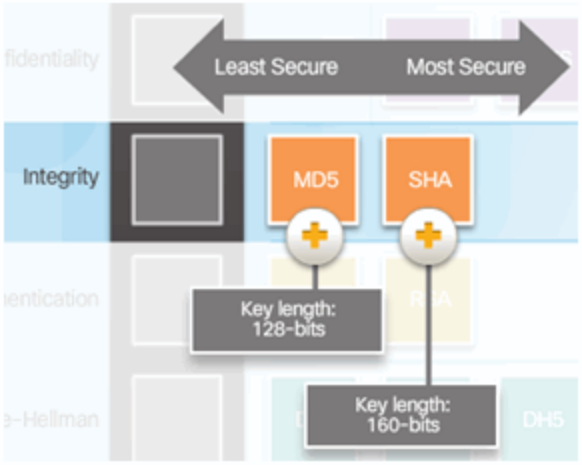


Integrity

Hash Algorithms

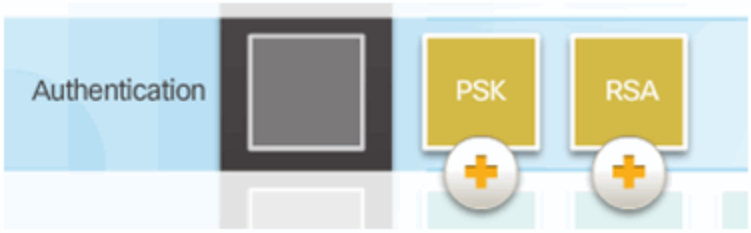


Security of Hash Algorithms

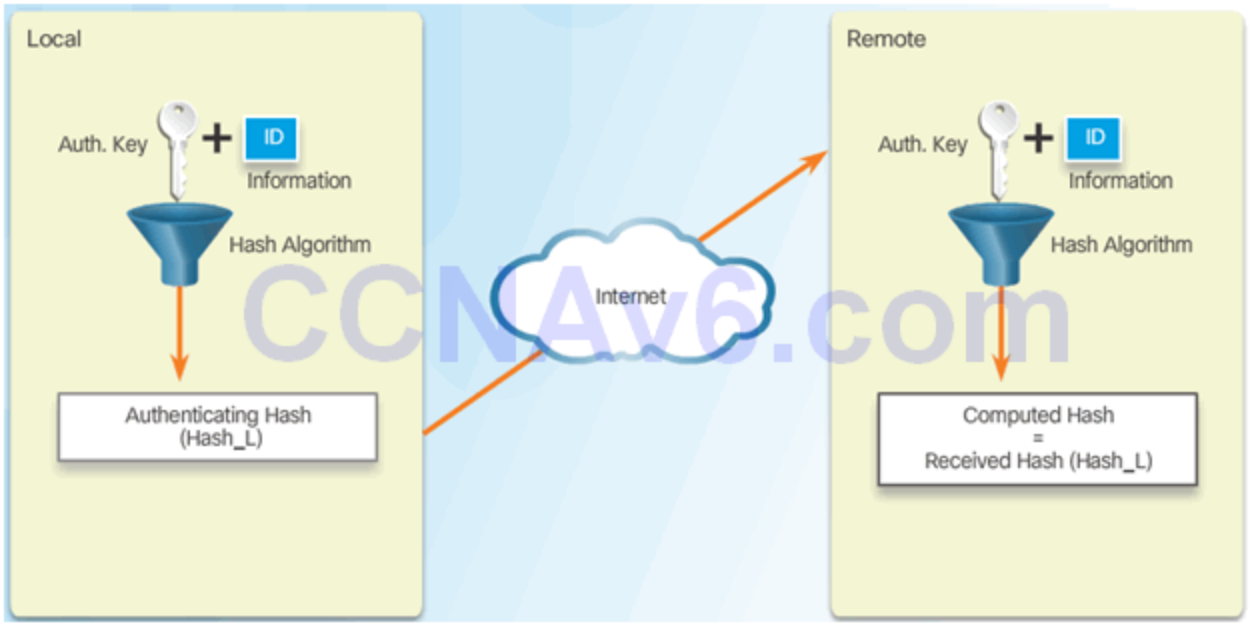


Authentication

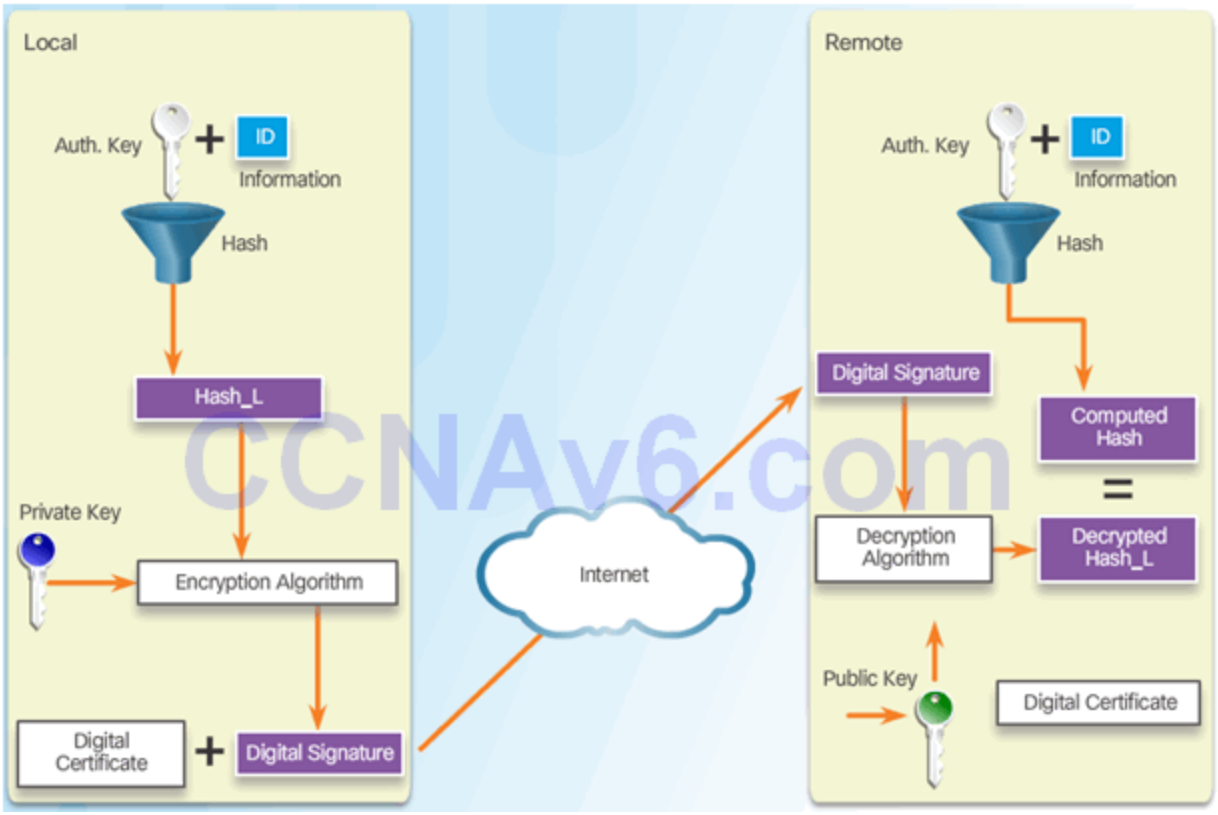
Peer Authentication Methods



PSK

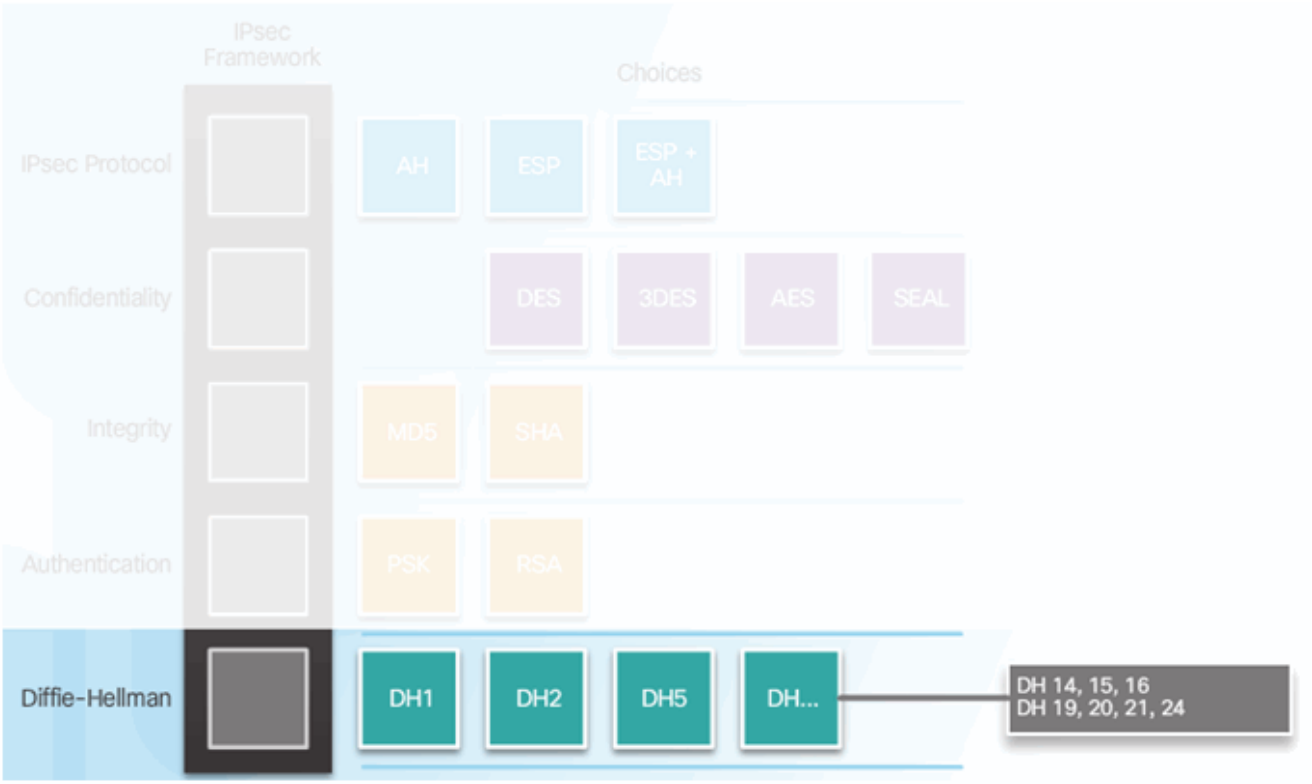


RSA



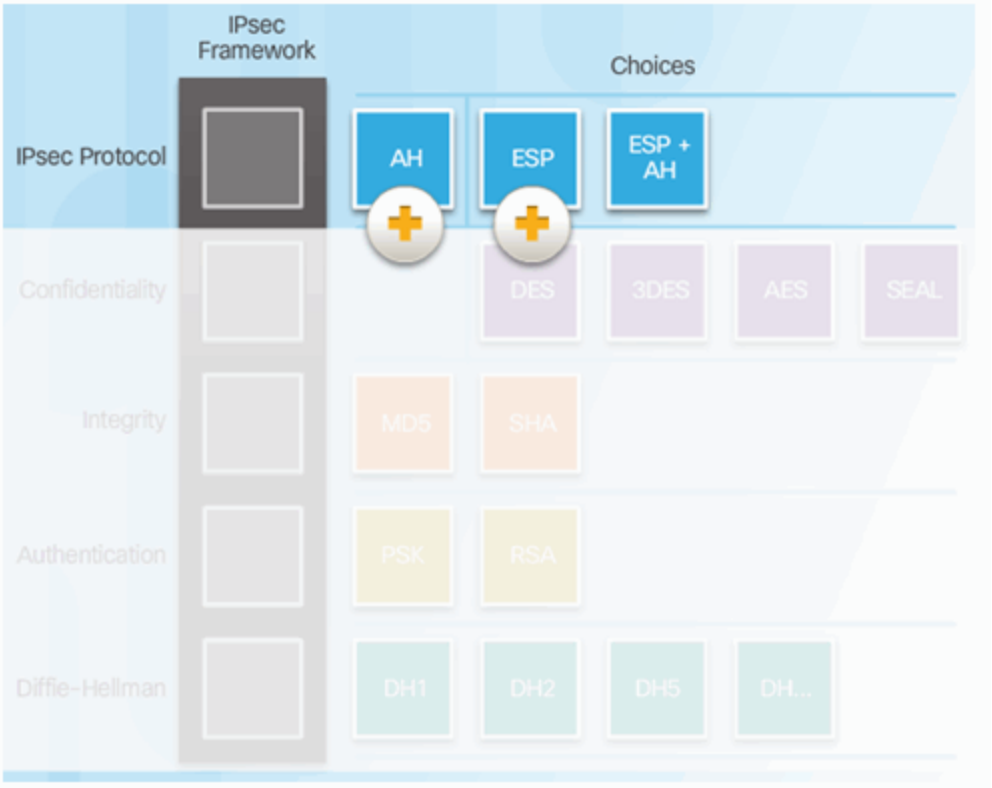
Secure Key Exchange

Diffie-Hellman Key Exchange



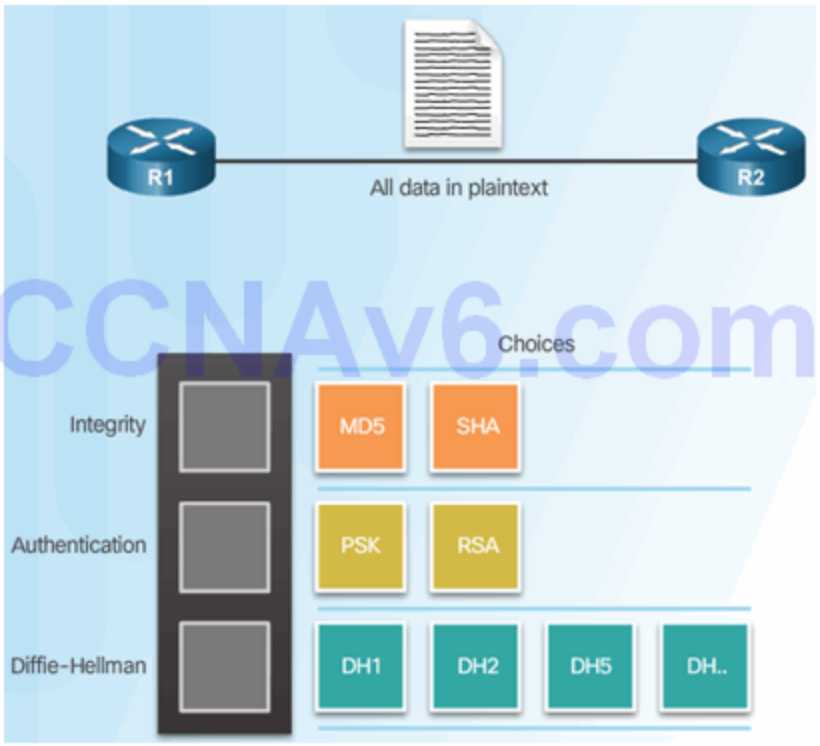
Topic 8.2.2: IPsec Protocols

IPsec Protocol Overview



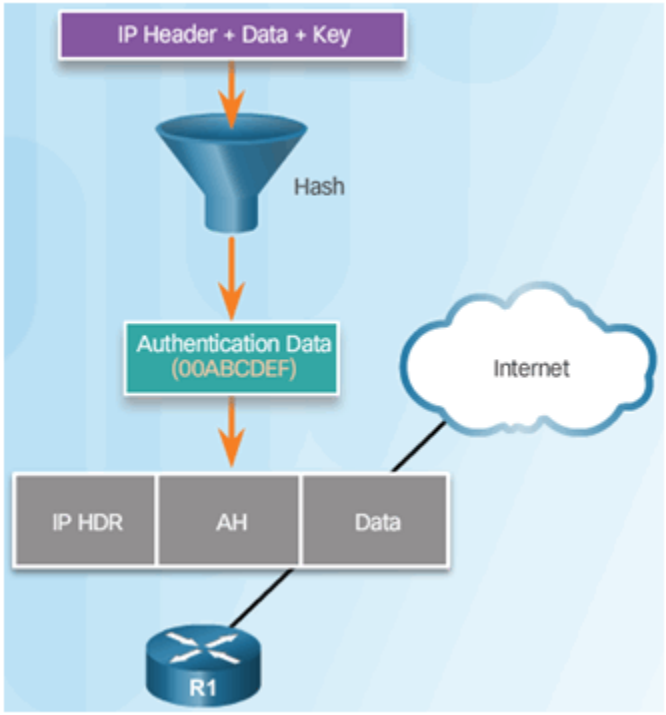
Authentication Header

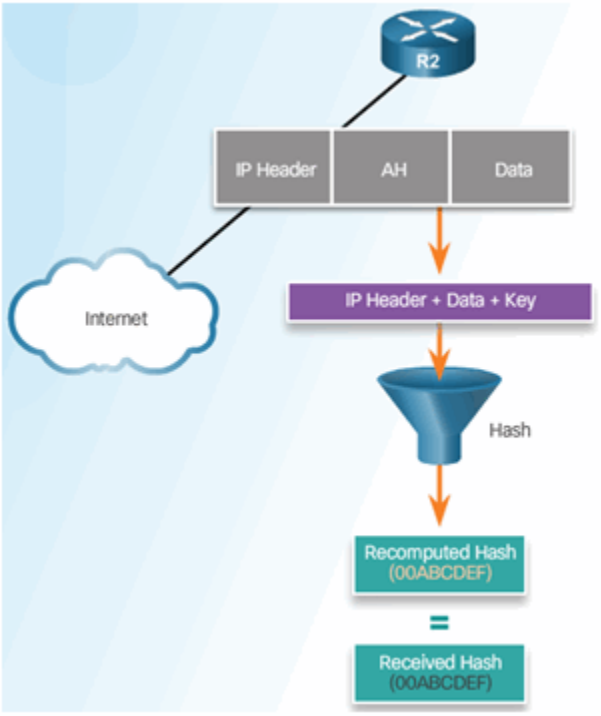
AH Protocols



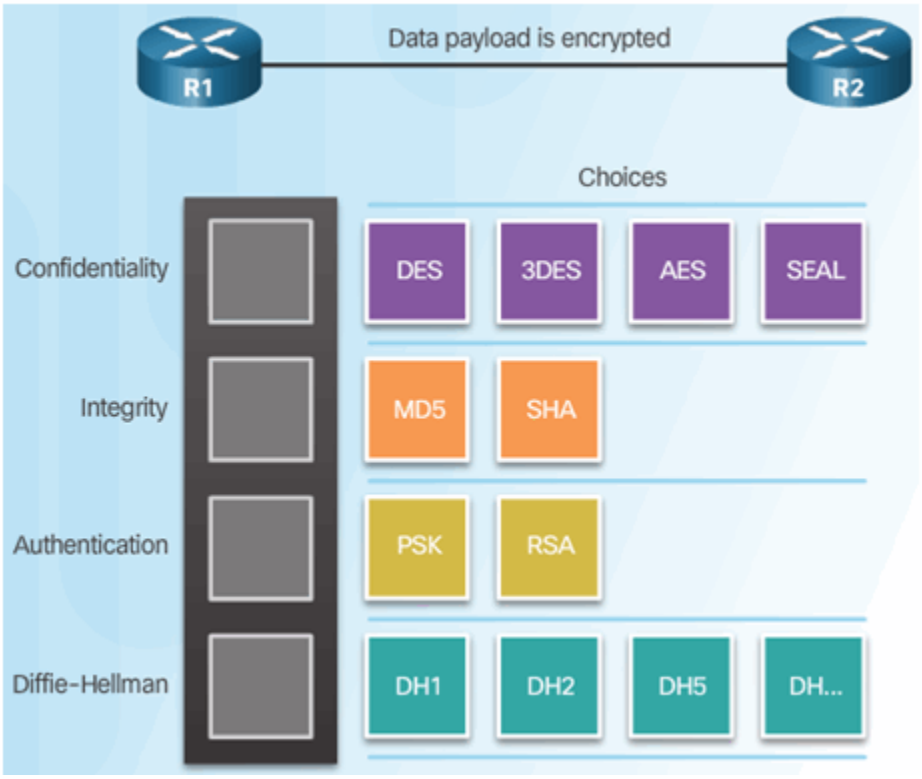
Router Creates Hash and Transmits to Peer

Peer Router Compares Recomputed Hash to Received Hash

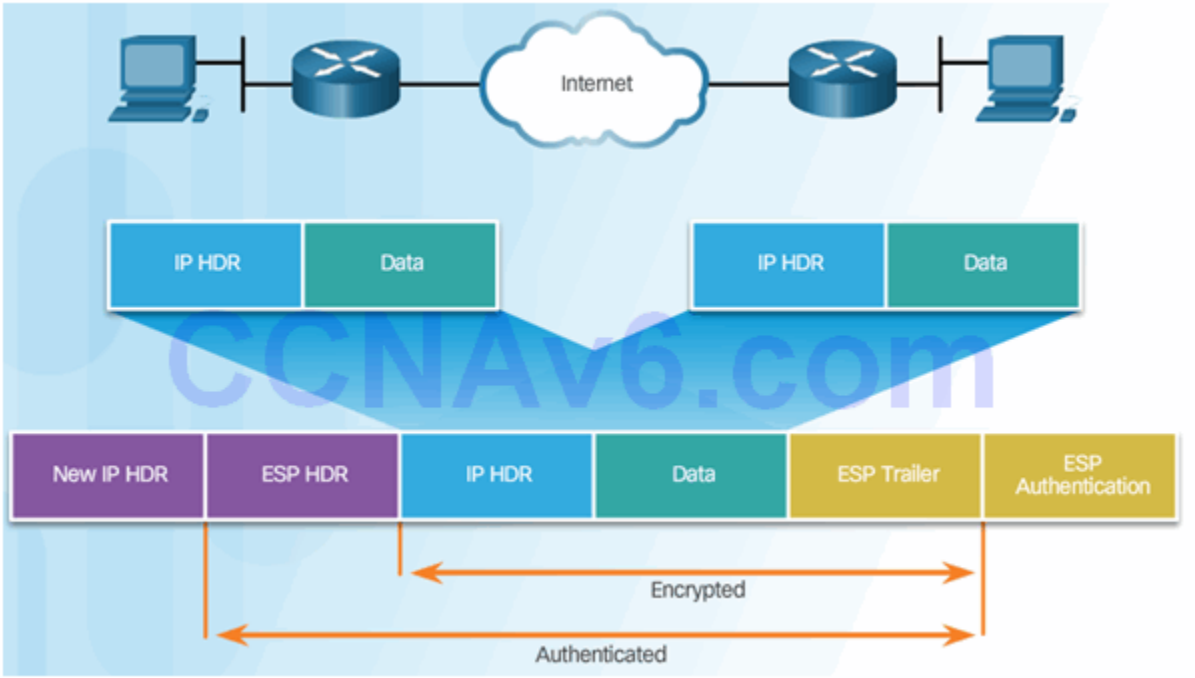




ESP

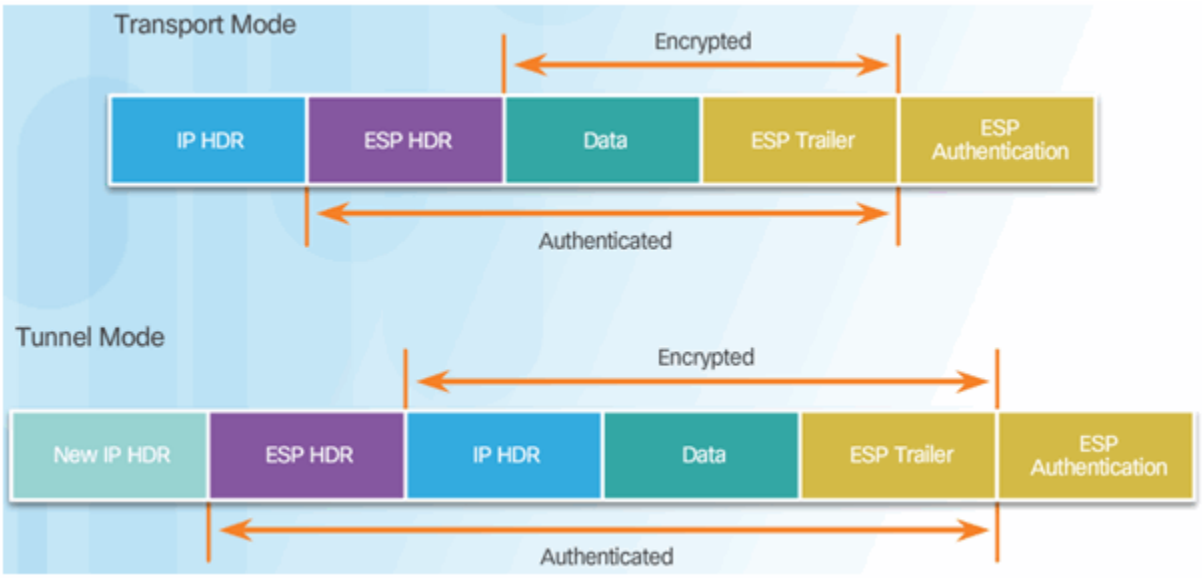


ESP Encrypts and Authenticates

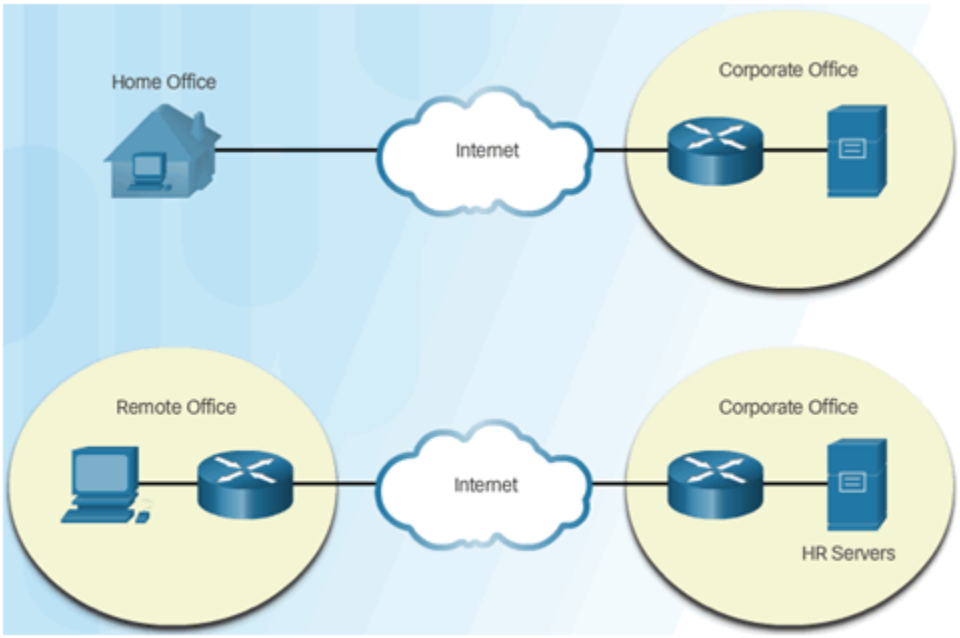


Transport and Tunnel Modes

Apply ESP and AH in Two Modes

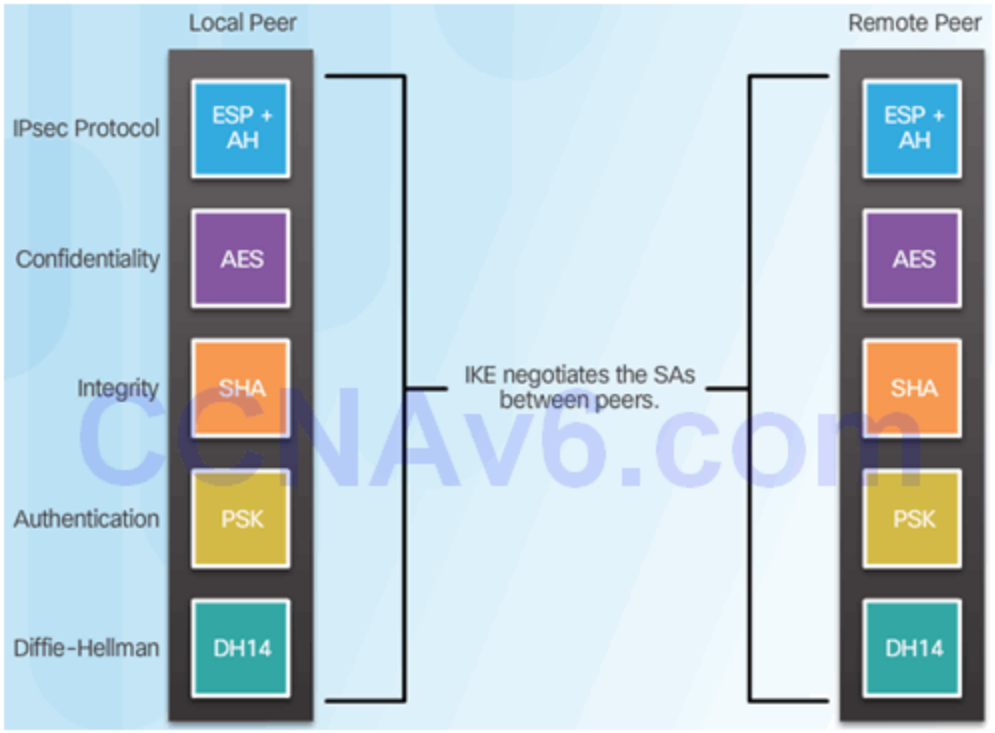


ESP Tunnel Mode

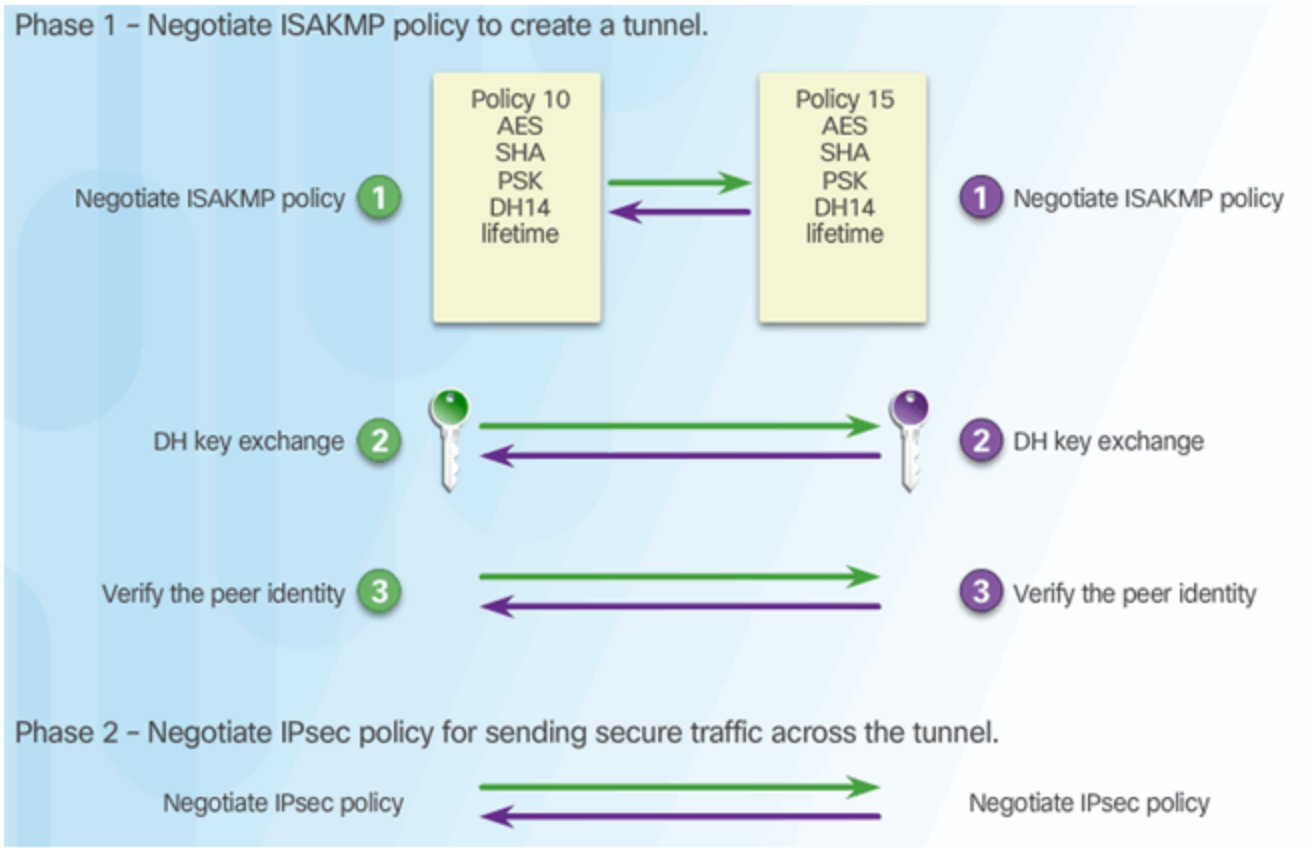


Topic 8.2.3: Internet Key Exchange

The IKE Protocol



Phase 1 and 2 Key Negotiation



Phase 2: Negotiating SAs

Section 8.3: Implementing Site-to-Site IPsec VPNs with CLI

Upon completion of this section, you should be able to:

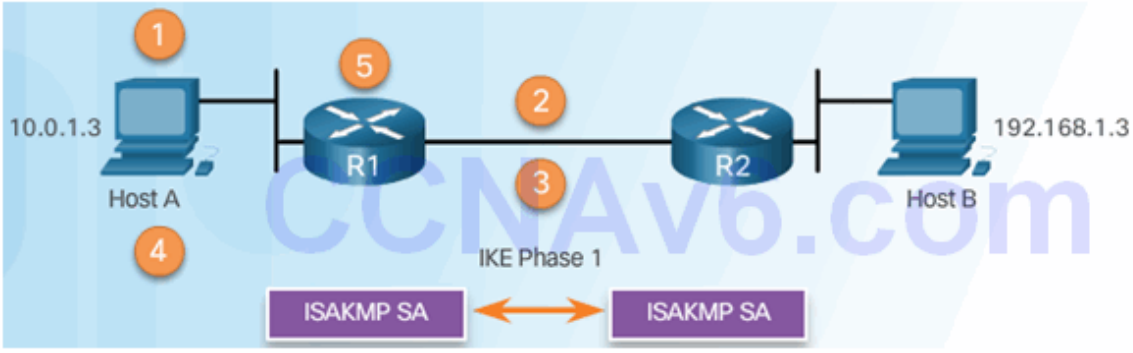
- Describe IPsec negotiation and the five steps of IPsec configuration.
- Configure the ISAKMP policy.
- Configure the IPsec policy.
- Configure and apply a crypto map.
- Verify the IPsec VPN.

Topic 8.3.1: Configuring a Site-to-Site IPsec VPN

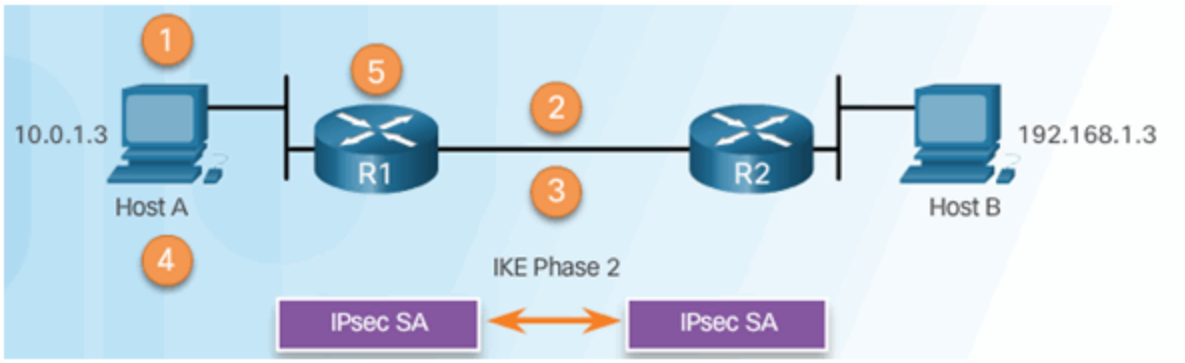
IPsec Negotiation

IPsec VPN Negotiation: Step 1 – Host A sends interesting traffic to Host B.

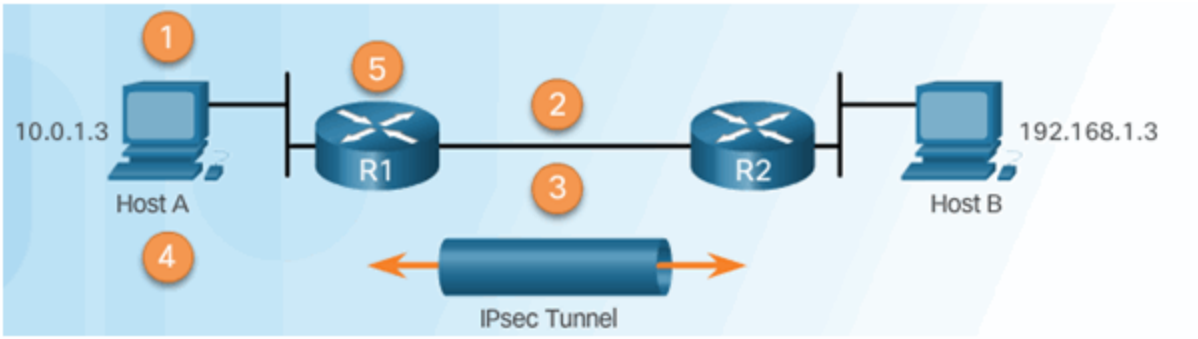
IPsec VPN Negotiation: Step 2 – R1 and R2 negotiate an IKE Phase 1 session.



IPsec VPN Negotiation: Step 3 – R1 and R2 negotiate an IKE Phase 2 session.



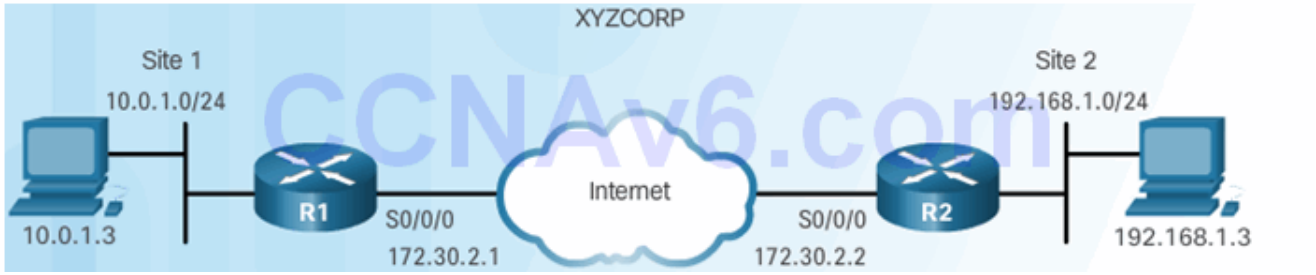
IPsec VPN Negotiation: Step 4 – Information is exchanged via IPsec tunnel.



IPsec VPN Negotiation: Step 5 – The IPsec tunnel is terminated.

Site-to-Site IPsec VPN Topology

IPsec VPN Configuration Tasks



XYZCORP Security Policy	Configuration Tasks
Encrypt traffic with AES 256 and SHA	1. Configure the ISAKMP policy for IKE Phase 1
Authentication with PSK	2. Configure the IPsec policy for IKE Phase 2
Exchange keys with group 24	3. Configure the crypto map for IPsec policy
ISAKMP tunnel lifetime is 1 hour	4. Apply the IPsec policy
IPsec tunnel uses ESP with a 15-min. lifetime	5. Verify the IPsec tunnel is operational

Existing ACL Configurations

ACL Syntax for IPsec Traffic

Permit ISAKMP Traffic

```
Router(config)#
access-list acl permit udp source wildcard destination wildcard eq isakmp
```

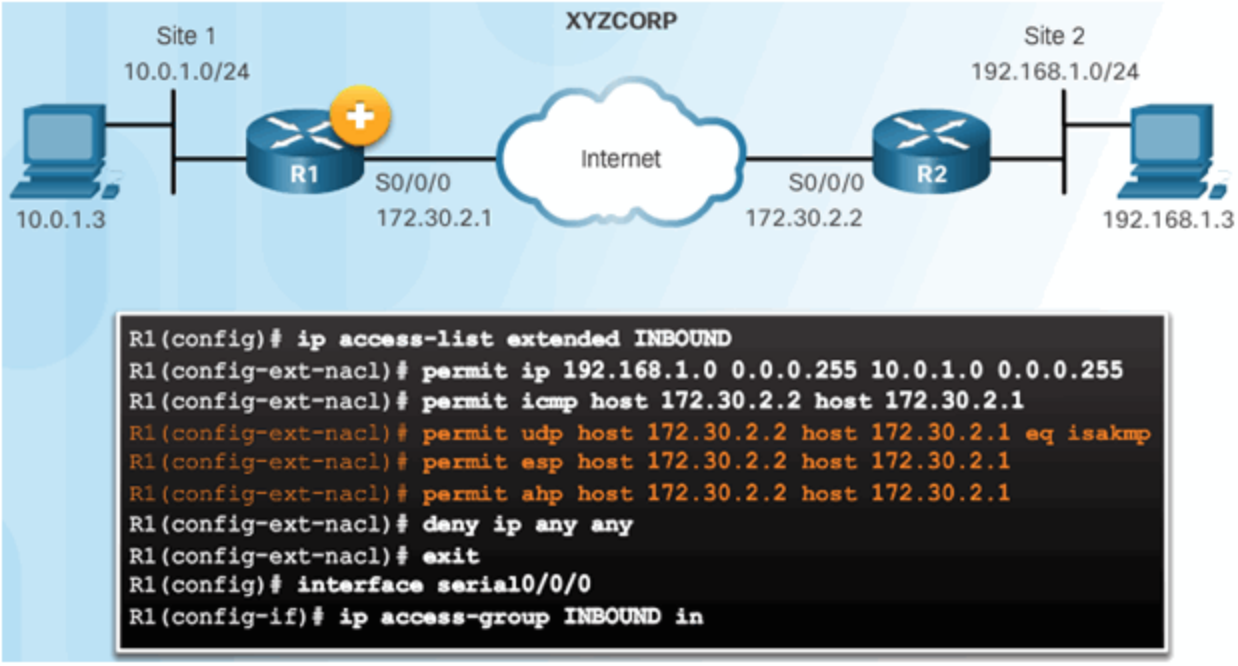
Permit ESP Traffic

```
Router(config)#
access-list acl permit esp source wildcard destination wildcard
```

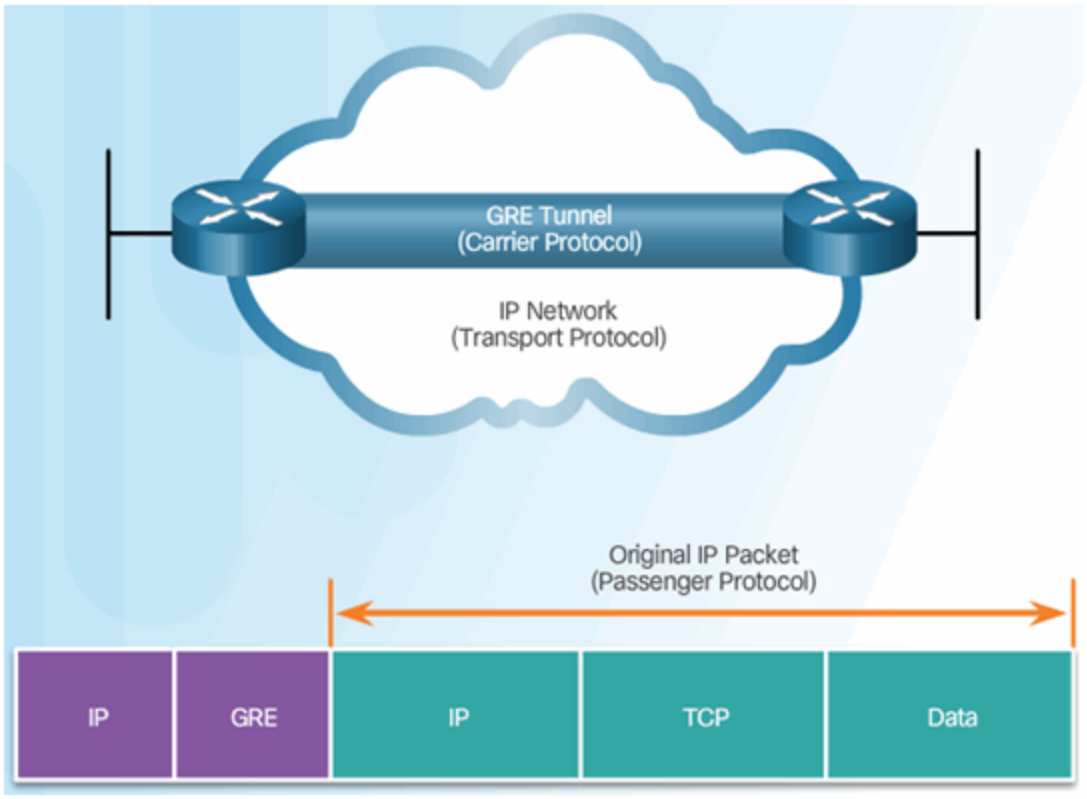
Permit AH Traffic

```
Router(config)#
access-list acl permit ahp source wildcard destination wildcard
```

Permitting Traffic for IPsec Negotiations

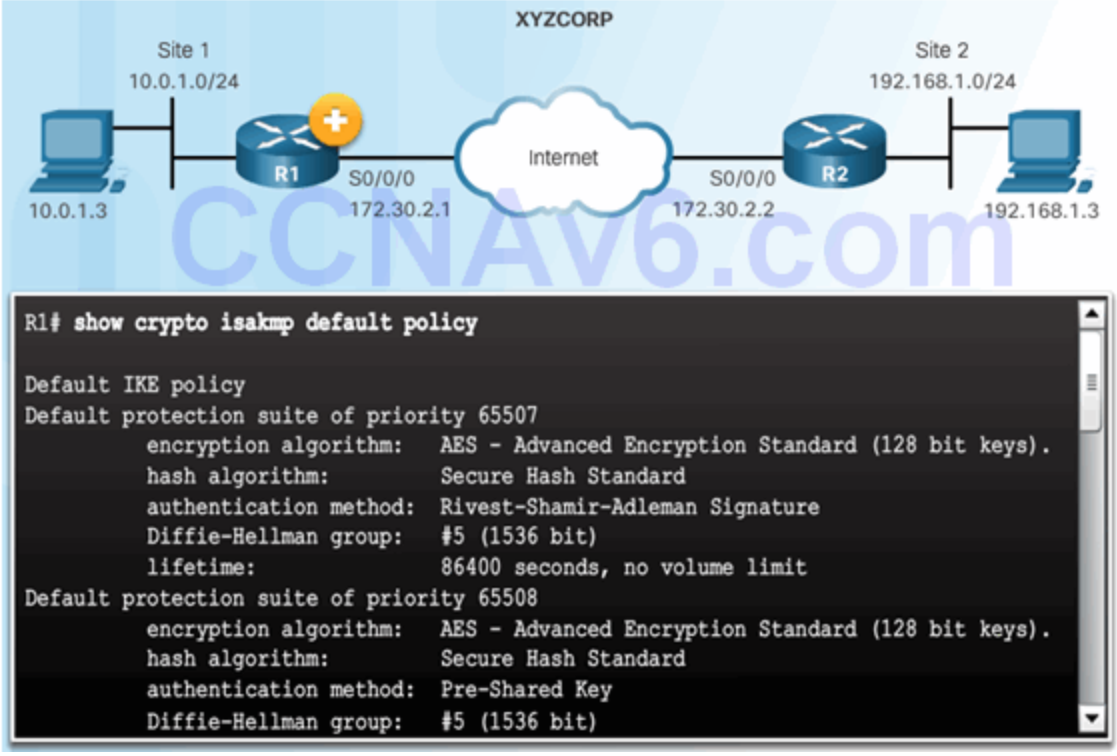


Introduction to GRE Tunnels

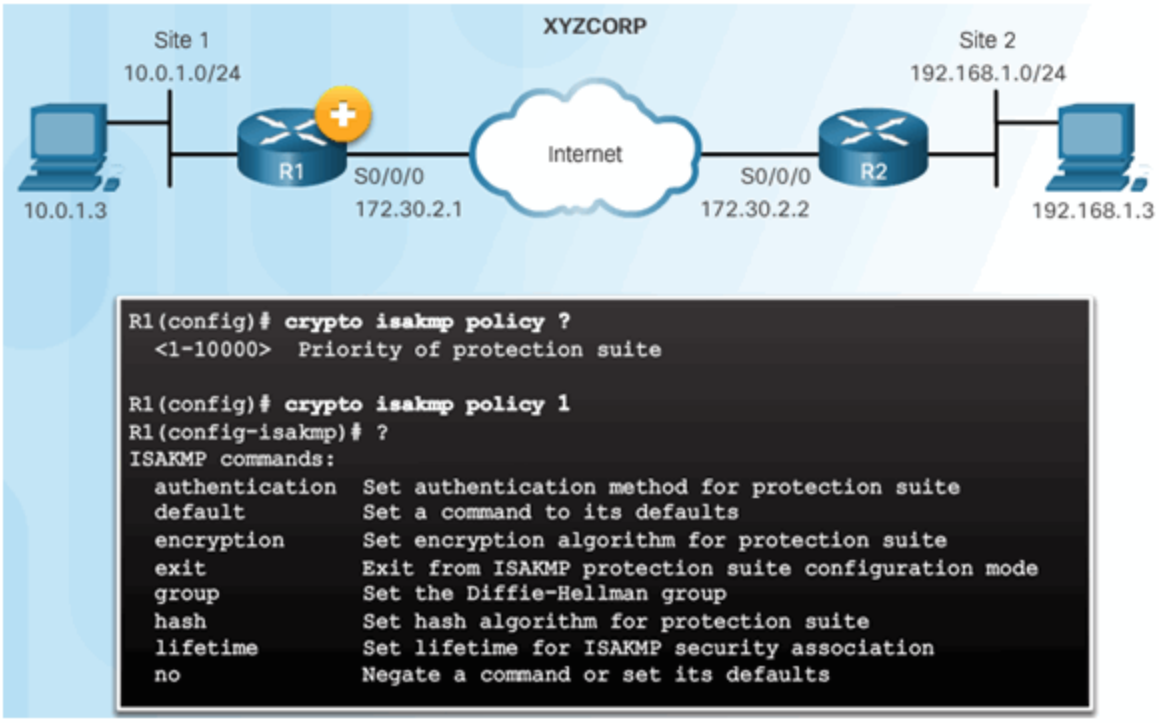


Topic 8.3.2: ISAKMP Policy

The Default ISAKMP Policies



Syntax to Configure a New ISAKMP Policy



XYZCORP ISAKMP Policy Configuration


```
R1(config)# crypto isakmp policy 1
R1(config-isakmp)# hash sha
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 24
R1(config-isakmp)# lifetime 3600
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# end
R1# show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:    AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:          Secure Hash Standard
        authentication method:   Pre-Shared Key
        Diffie-Hellman group:    #24 (2048 bit, 256 bit subgroup)
        lifetime:                3600 seconds, no volume limit
R1#
```

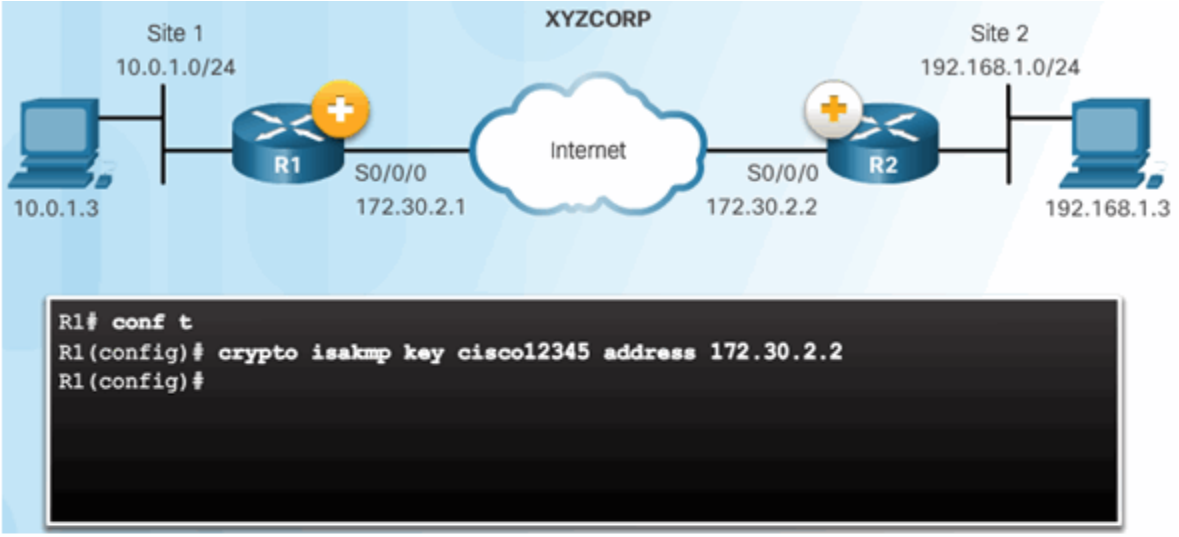
Configuring a Pre-Shared Key

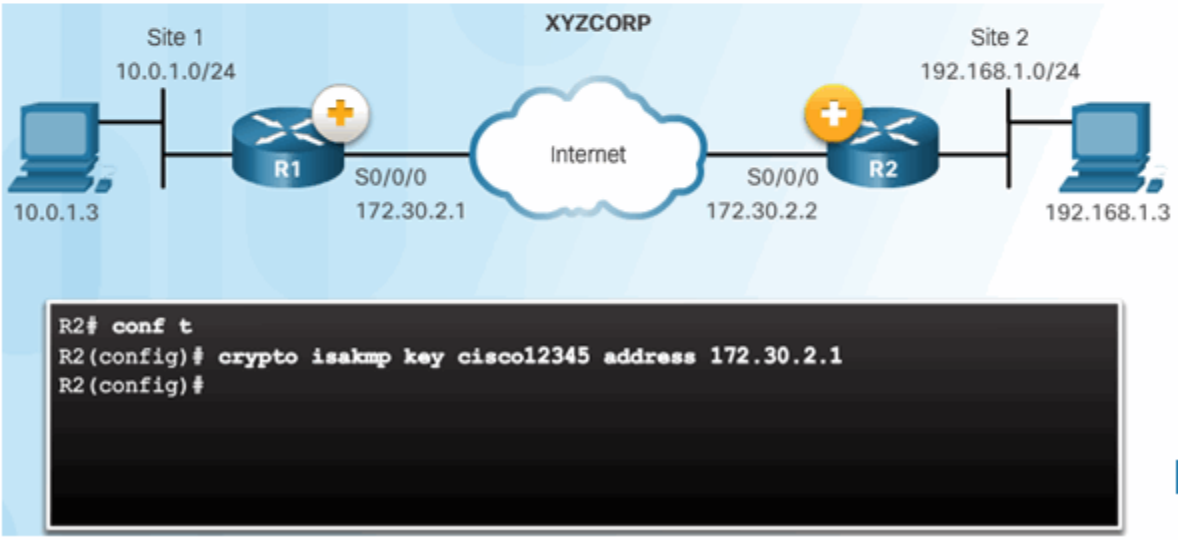
The crypto isakmp key Command

```
Router(config)#
crypto isakmp key keystring address peer-address

Router(config)#
crypto isakmp key keystring hostname peer-hostname
```


Pre-Shared Key Configuration

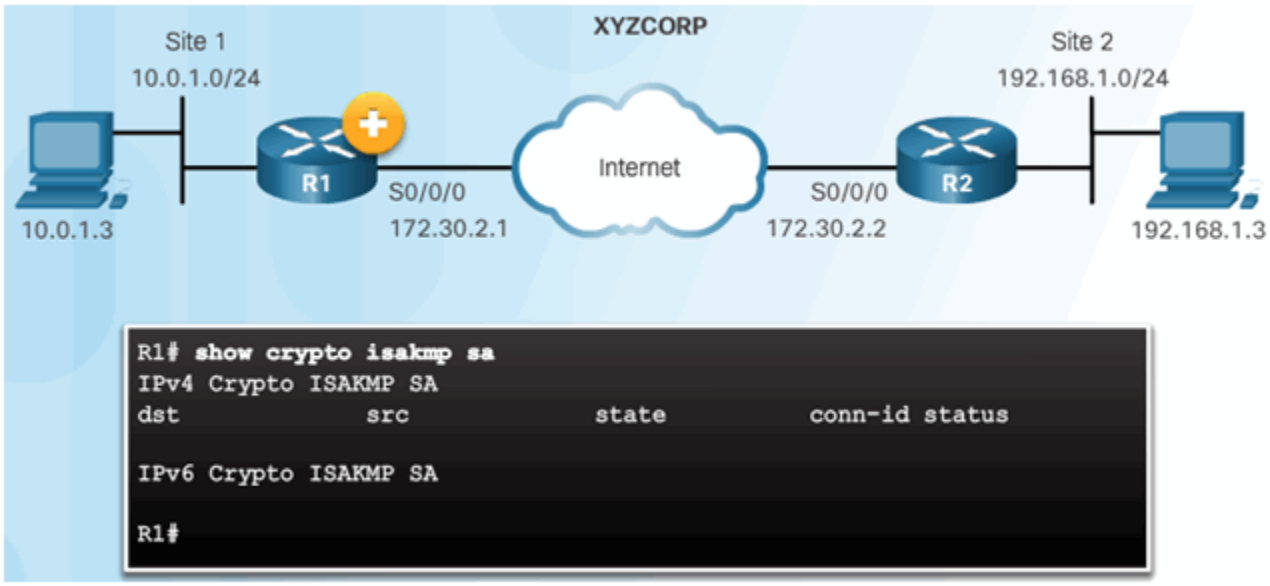




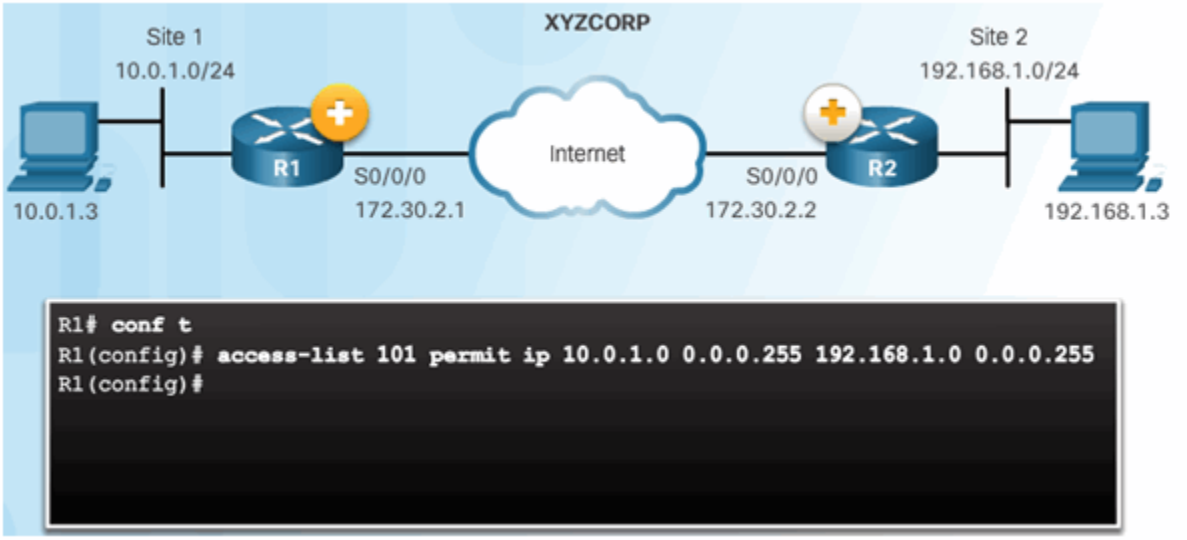
Topic 8.3.3: IPsec Policy

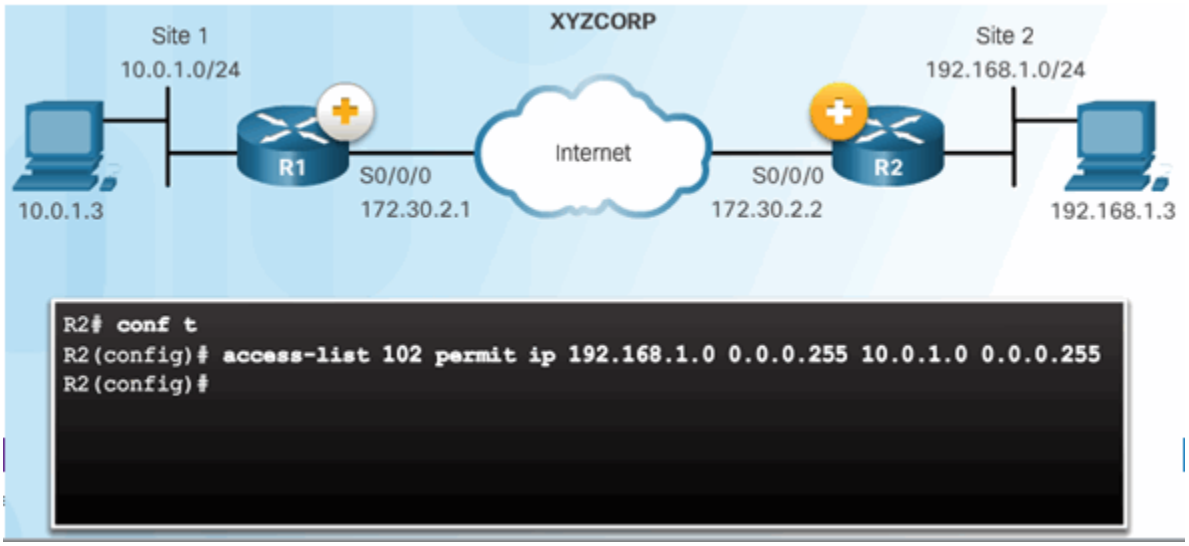
Define Interesting Traffic

The IKE Phase 1 Tunnel Does Not Exist Yet



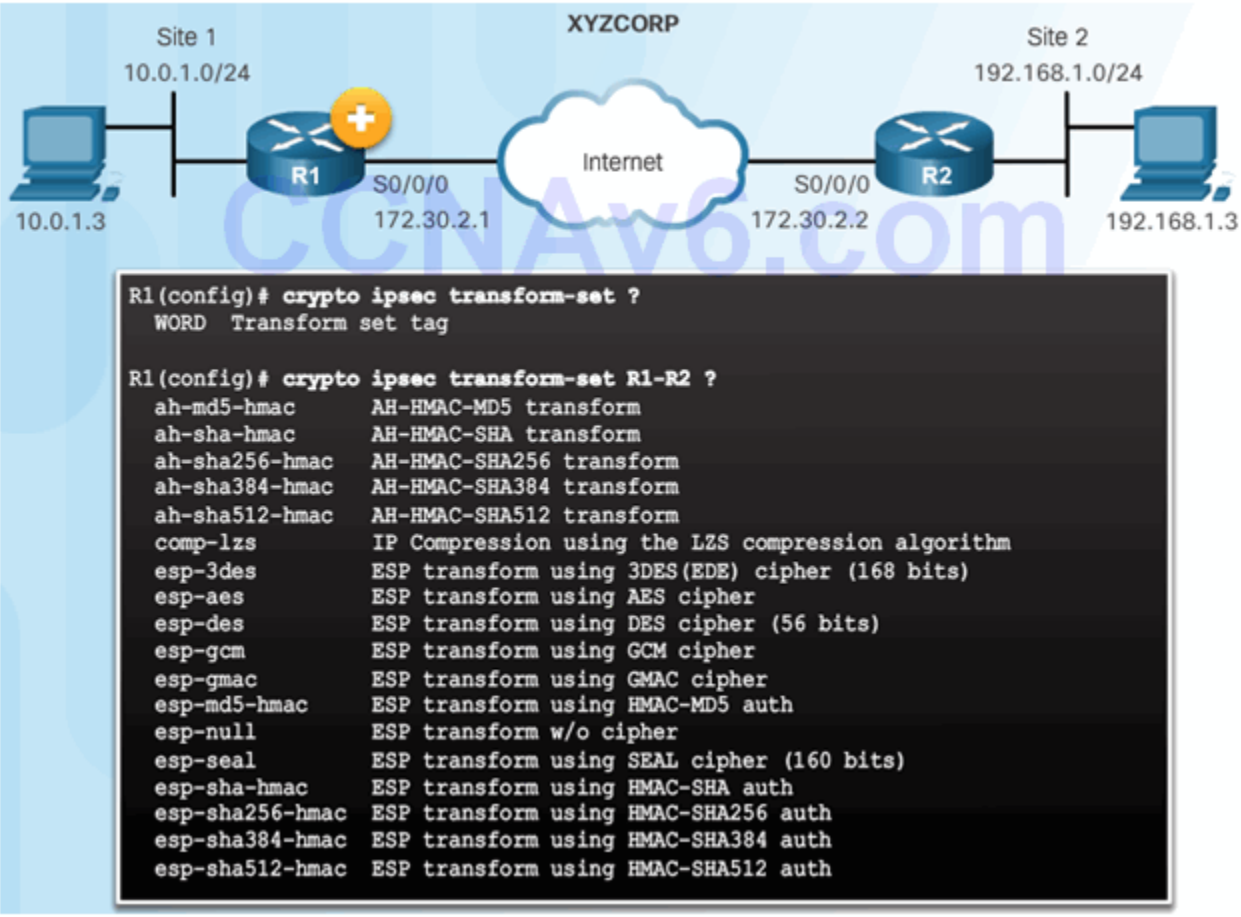
Configure an ACL to Define Interesting Traffic



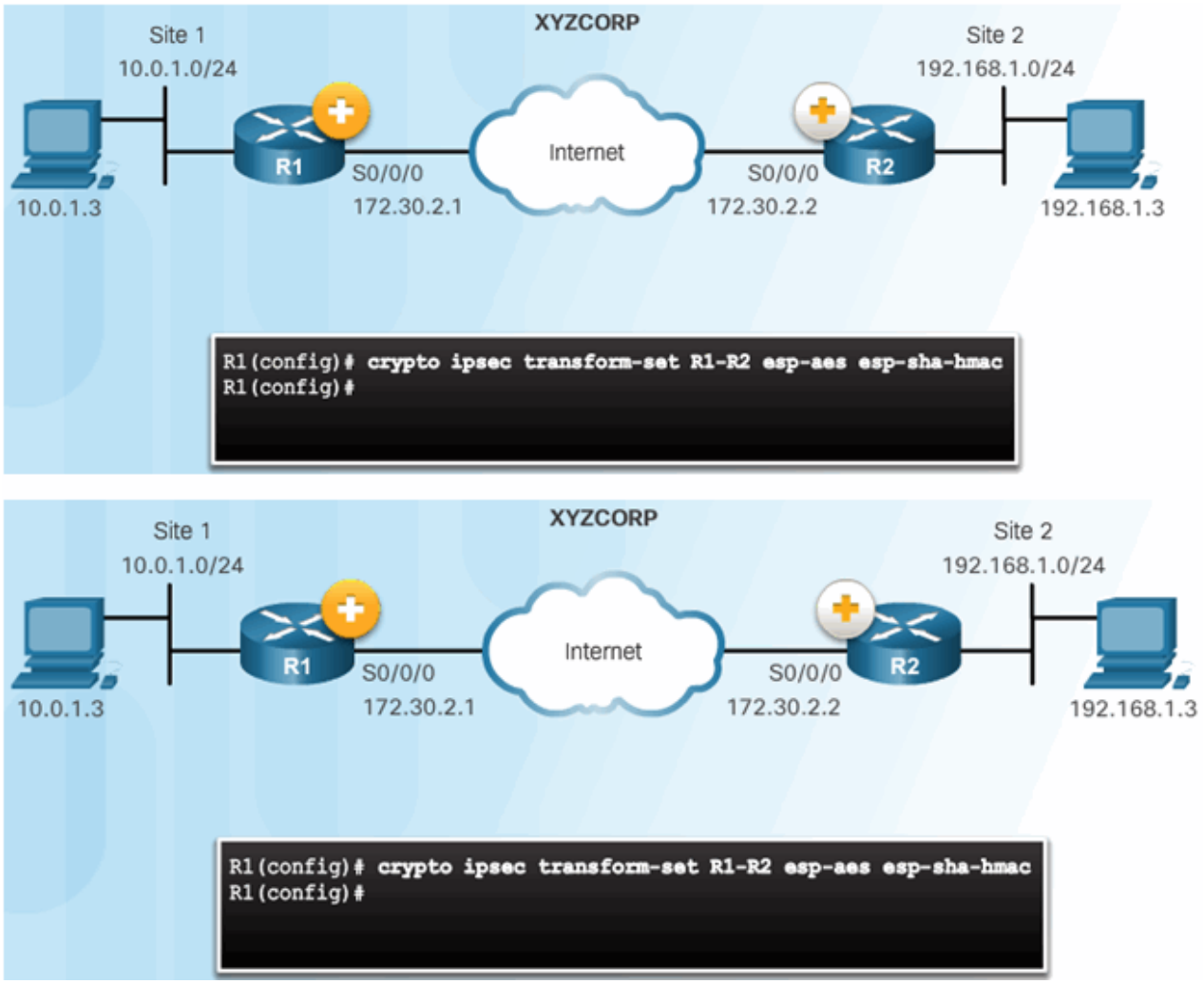


Configure IPsec Transform Set

The crypto ipsec transform-set Command



The crypto ipsec transform-set Command



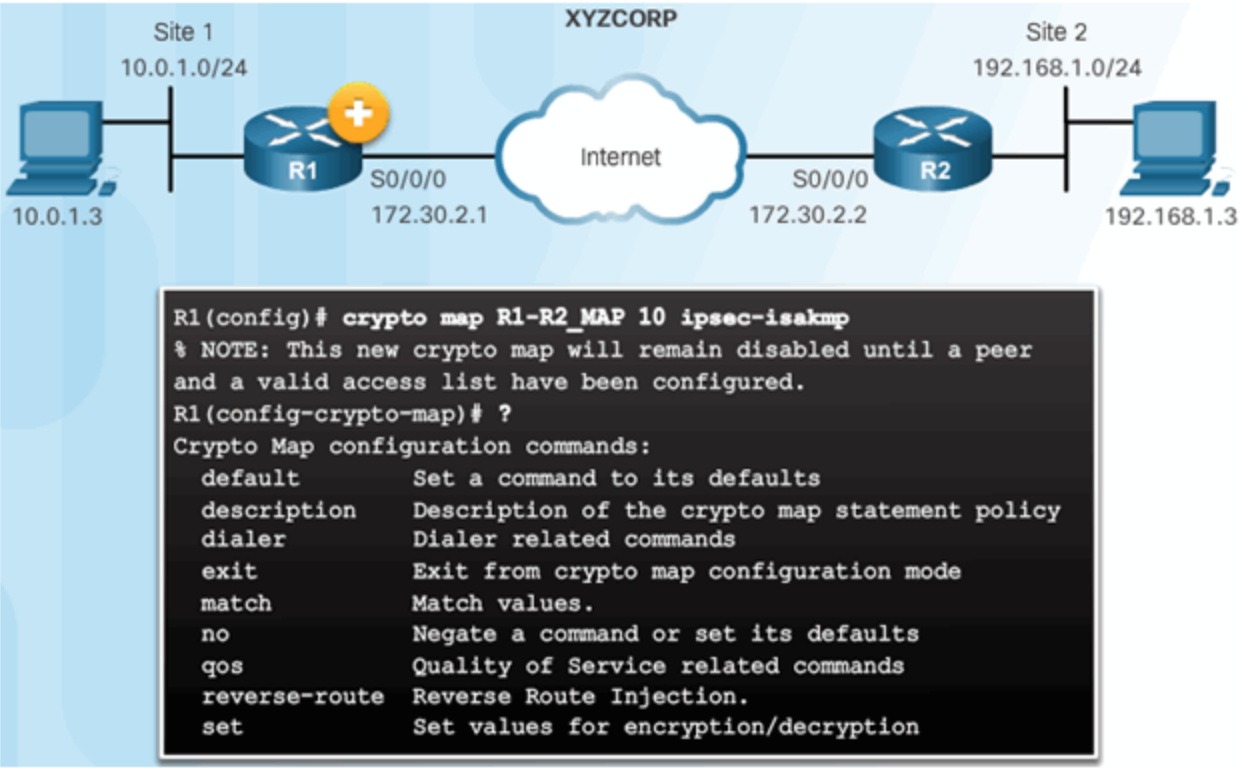
Topic 8.3.4: Crypto Map

Syntax to Configure a Crypto Map

```
Router(config)#
crypto map map-name seq-num [ipsec-isakmp | ipsec-manual]
```

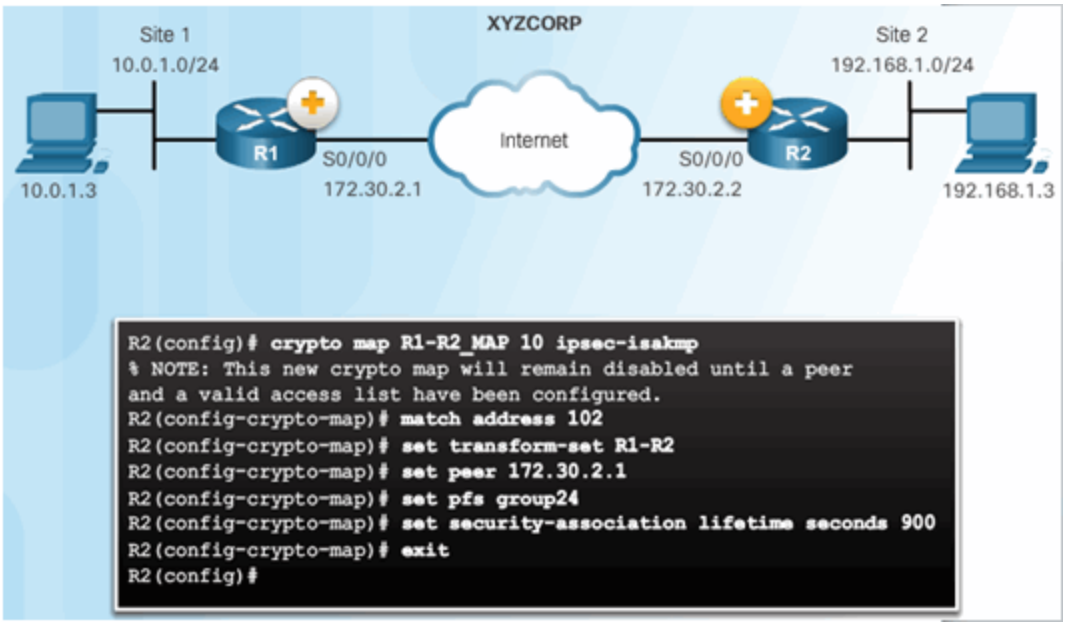
Parameter	Description
map-name	Identifies the crypto map set.
seq-num	Sequence number you assign to the crypto map entry. Use the crypto map map-name seq-num command without any keyword to modify the existing crypto map entry or profile
ipsec-isakmp	Indicates that IKE will be used to establish the IPsec for protecting the traffic specified by this crypto map entry.
ipsec-manual	Indicates that IKE will not be used to establish the IPsec SAs for protecting the traffic specified by this crypto map entry

Crypto Map Configuration Commands

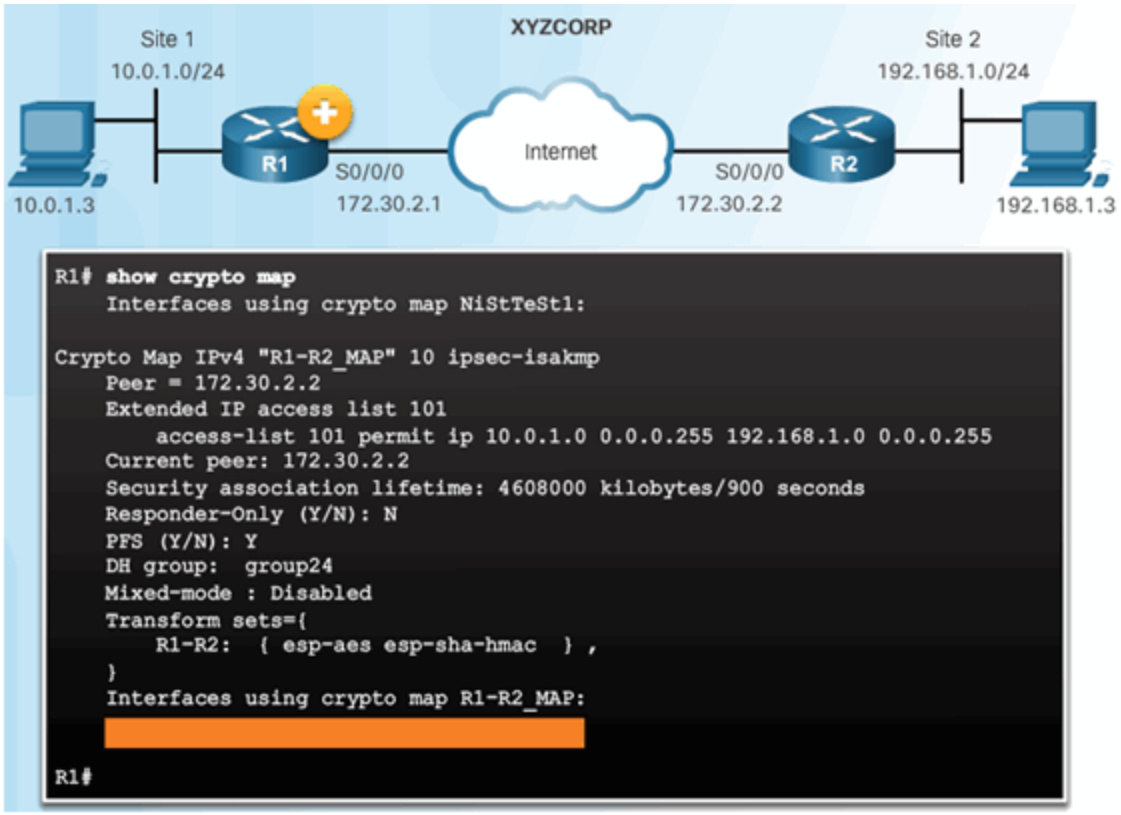


XYZCORP Crypto Map Configuration

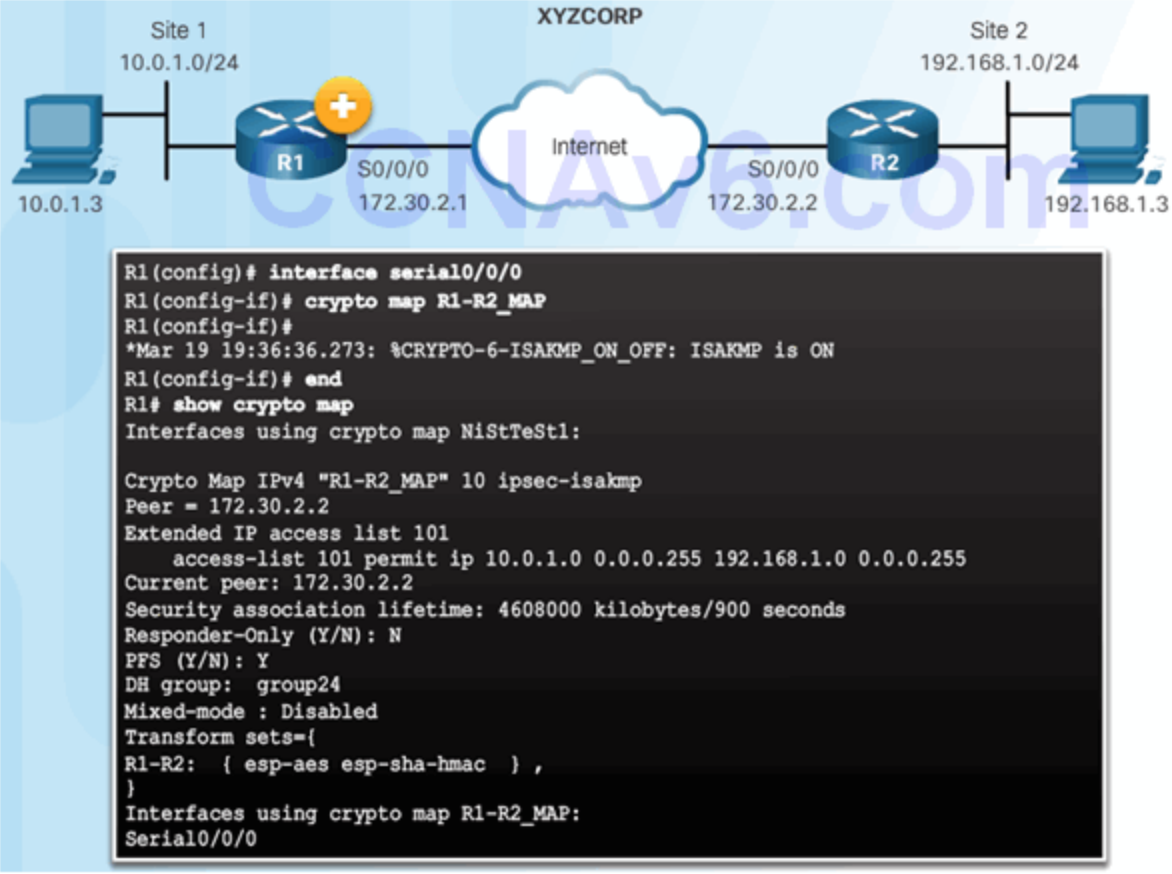
Crypto Map Configuration:



Crypto Map Configuration:



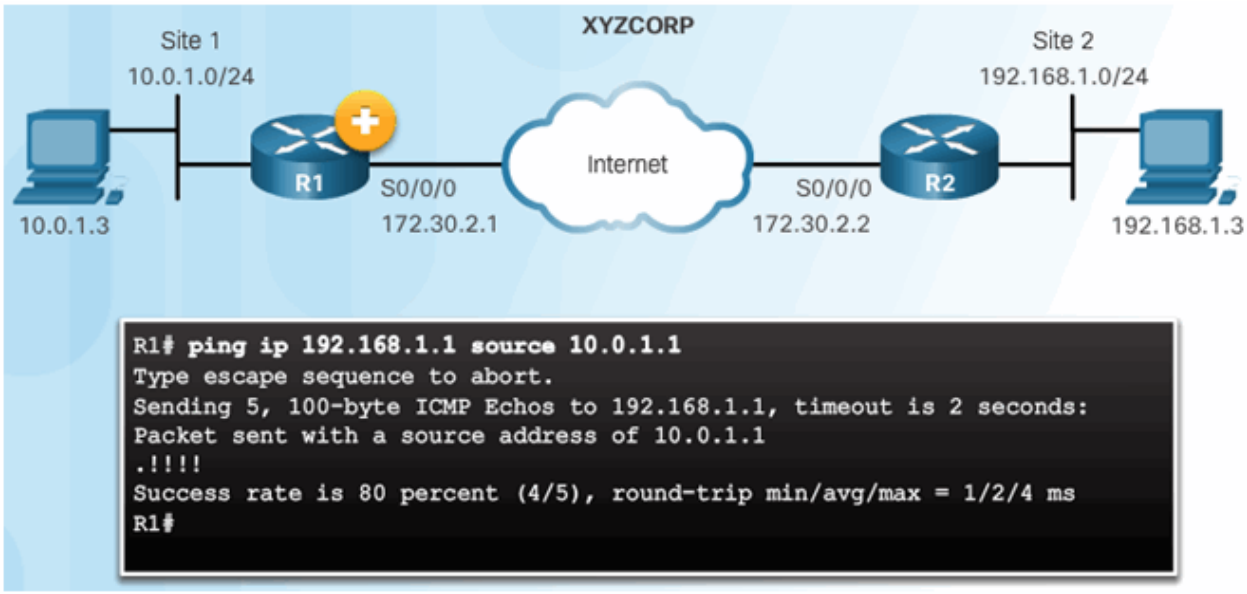
Apply the Crypto Map



Topic 8.3.5: IPsec VPN

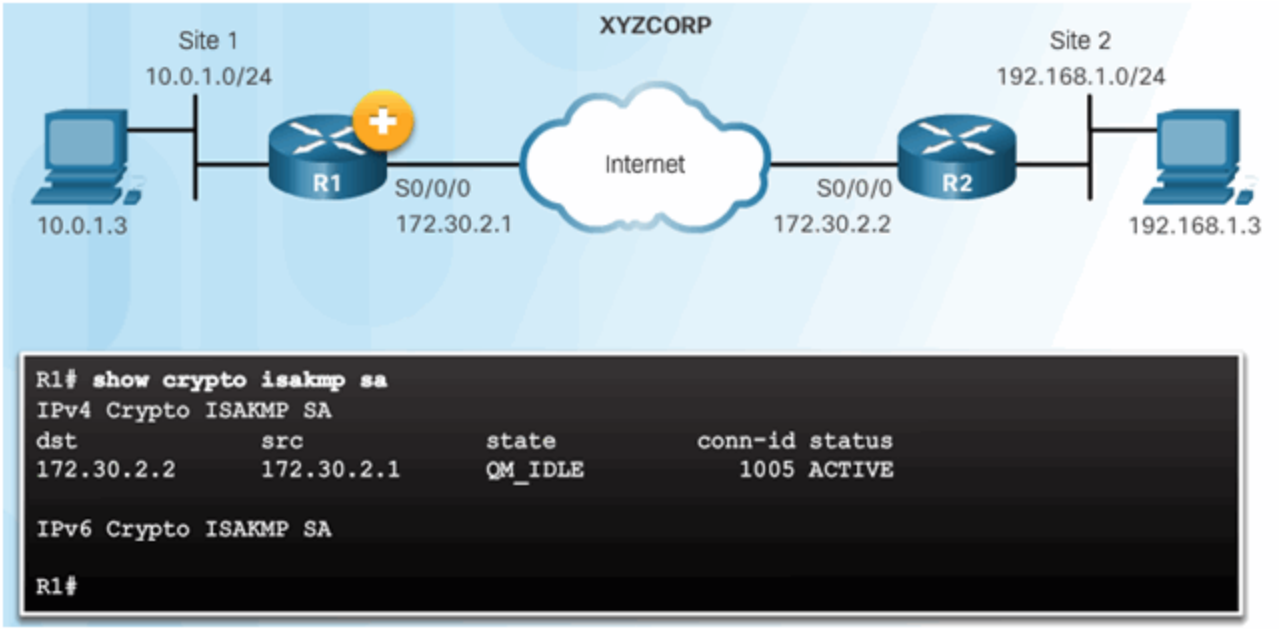
Send Interesting Traffic

Use Extended Ping to Send Interesting Traffic

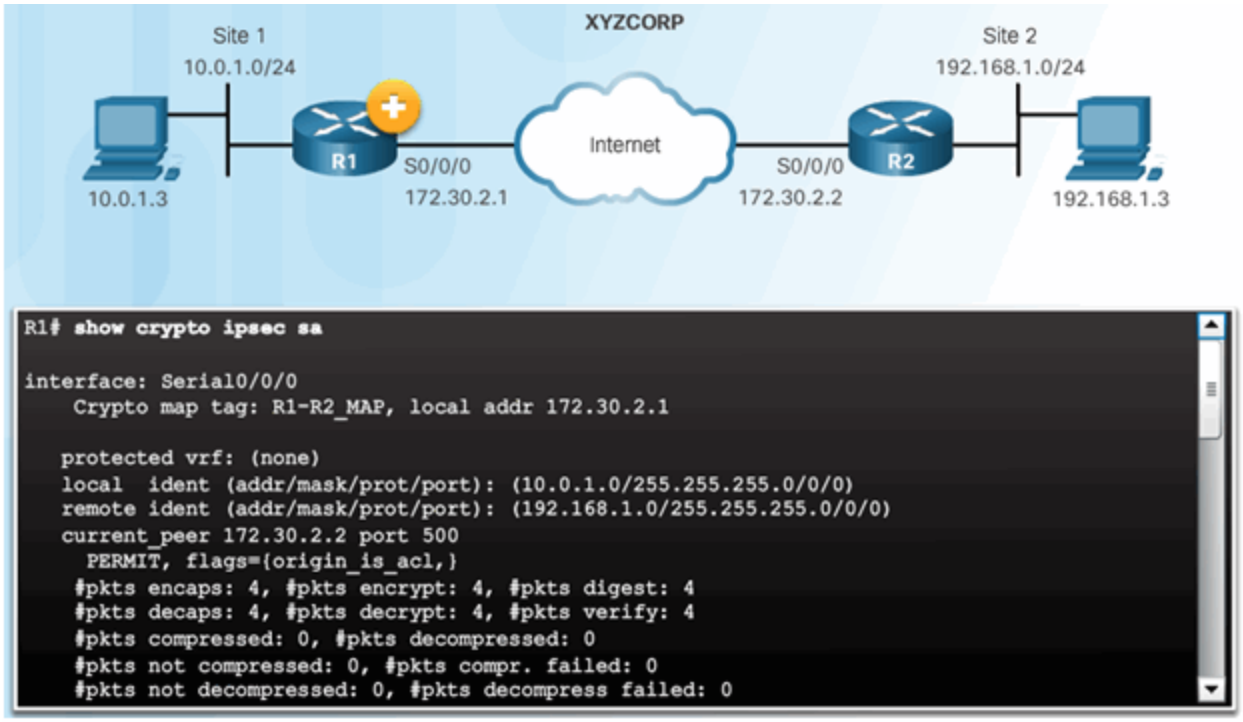


Verify ISAKMP and IPsec Tunnels

Verify the ISAKMP Tunnel is Established



Verify the IPsec Tunnel is Established



Section 8.4: Summary

Chapter Objectives:

- Explain the purpose of VPNs.
- Explain how IPsec VPNs operate.
- Configure a site-to-site IPsec VPN, with pre-shared key authentication, using the CLI.

Download Slide PowerPoint (pptx):

[sociallocker id=”54558″]

CCNASv2_InstructorPPT_CH8.pptx **4.03 MB** **2015 downloads**

...

Download

[/sociallocker]