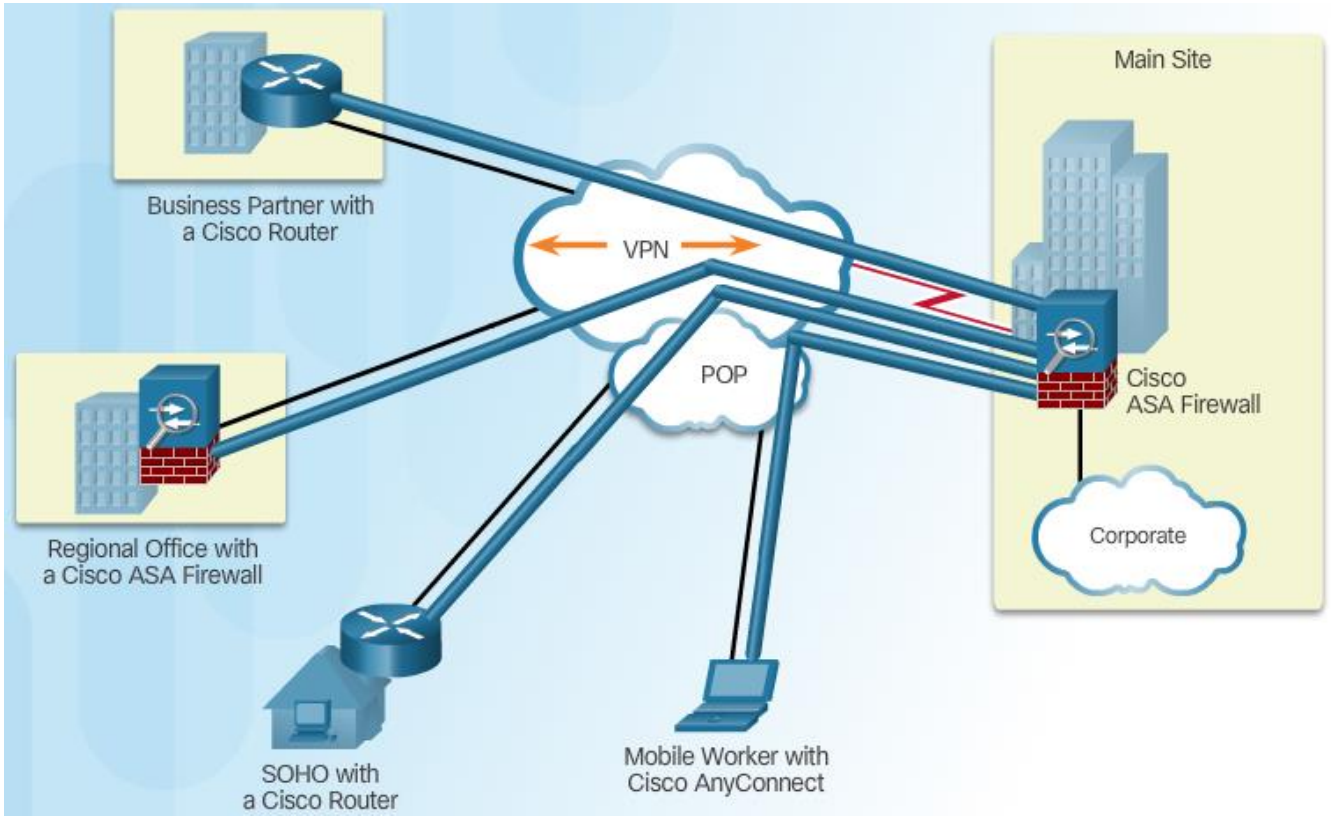
VPN Technologies

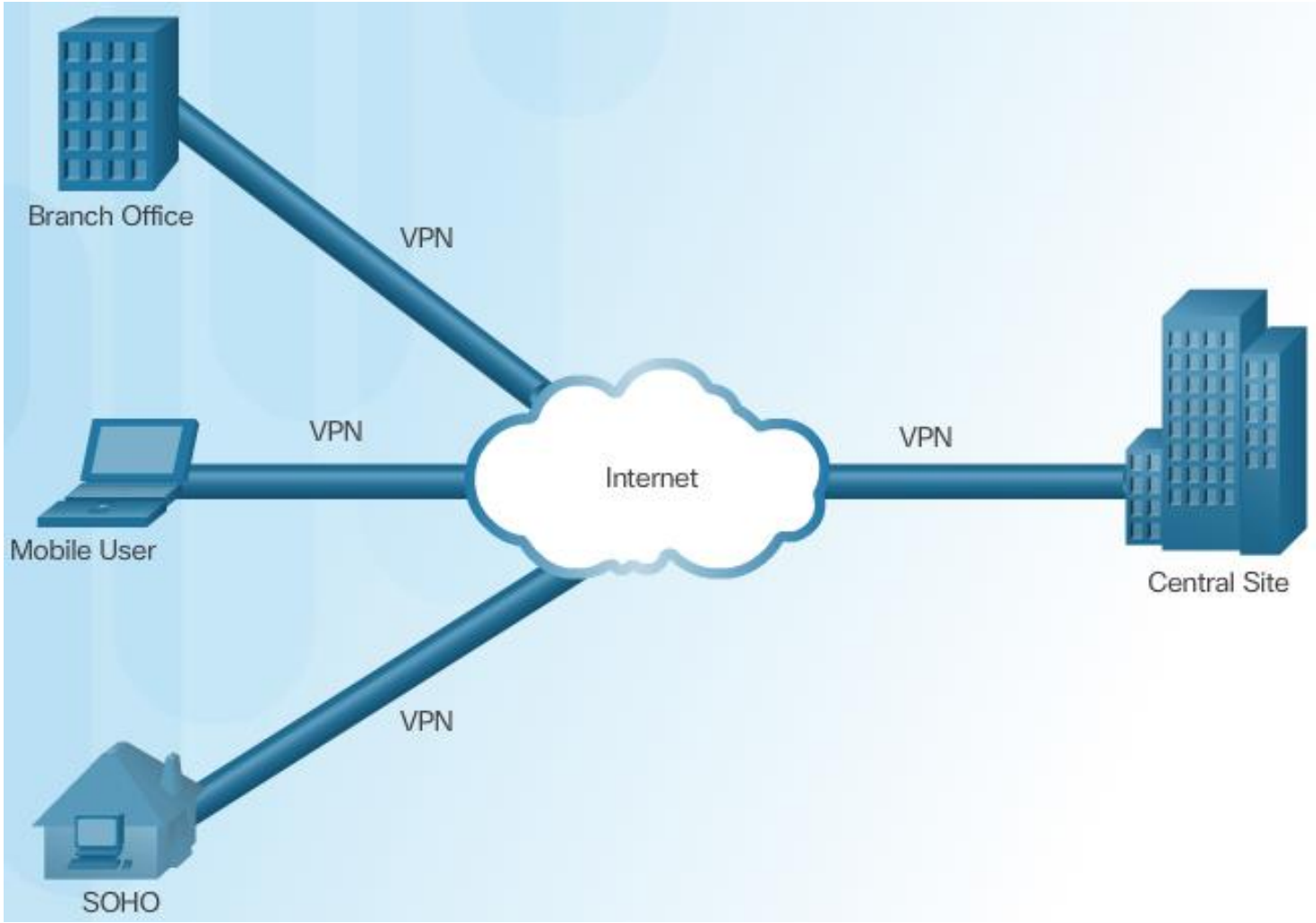
Introducing VPNs

VPN Benefits:

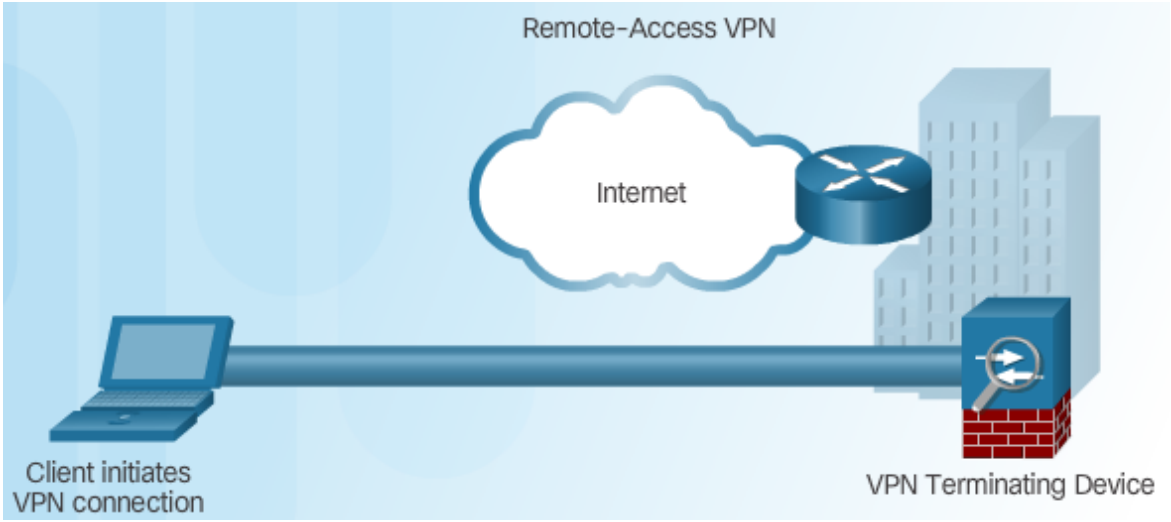
- Cost Savings
- Security
- Scalability
- Compatibility



Layer 3 IPsec VPNs

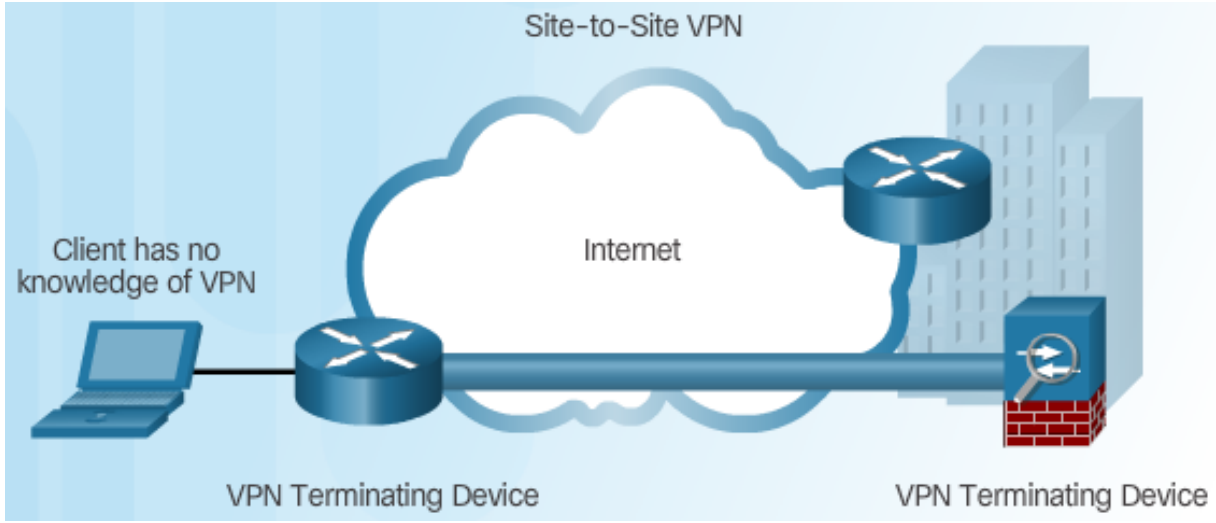


Two Types of VPNs

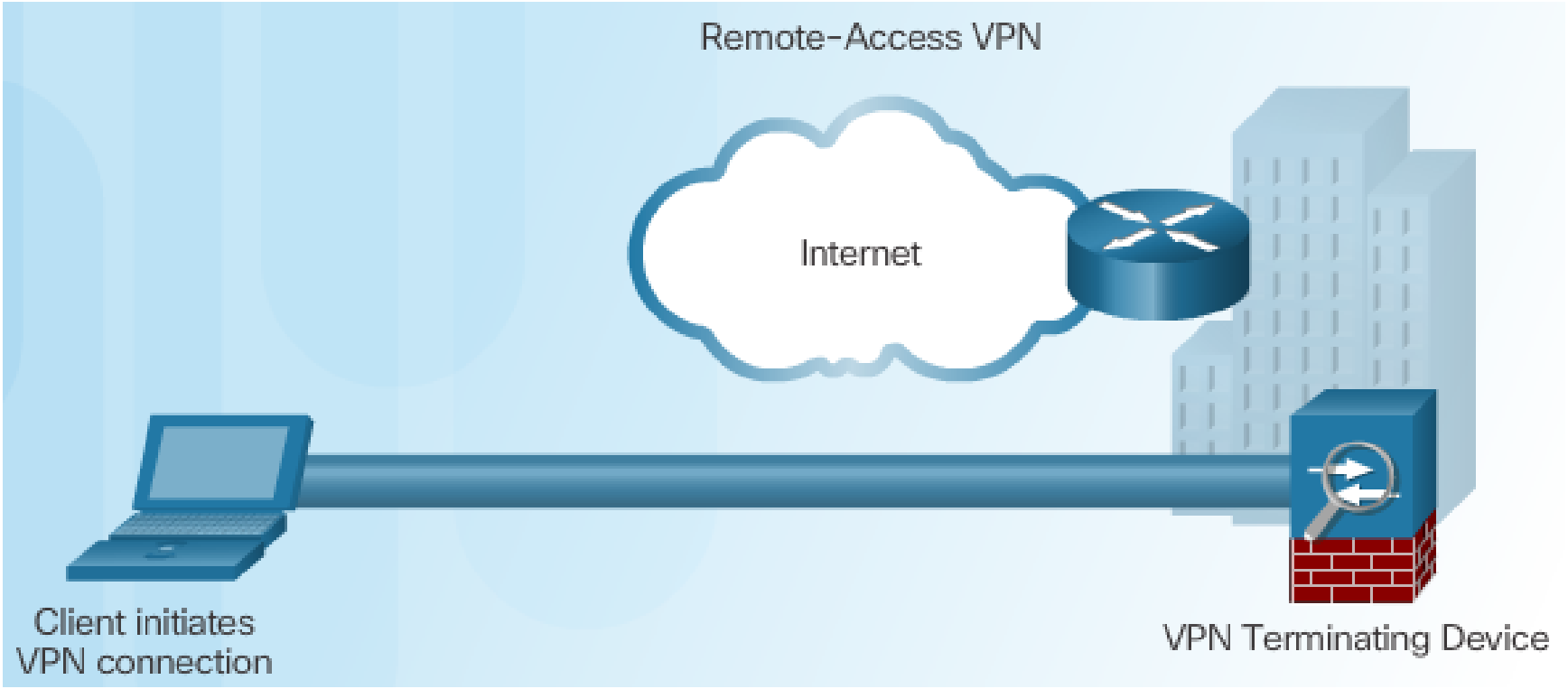


Remote-Access VPN

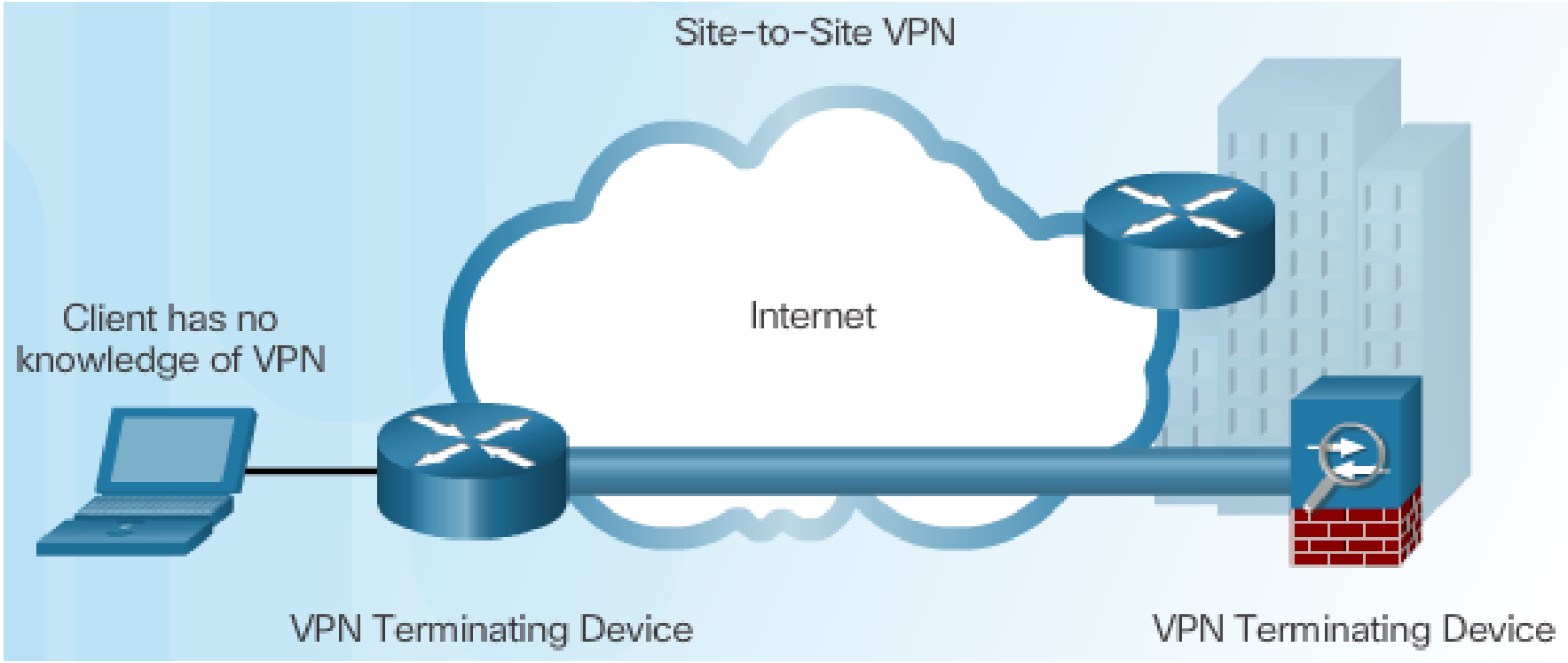
Site-to-Site VPN Access



Components of Remote-Access VPNs



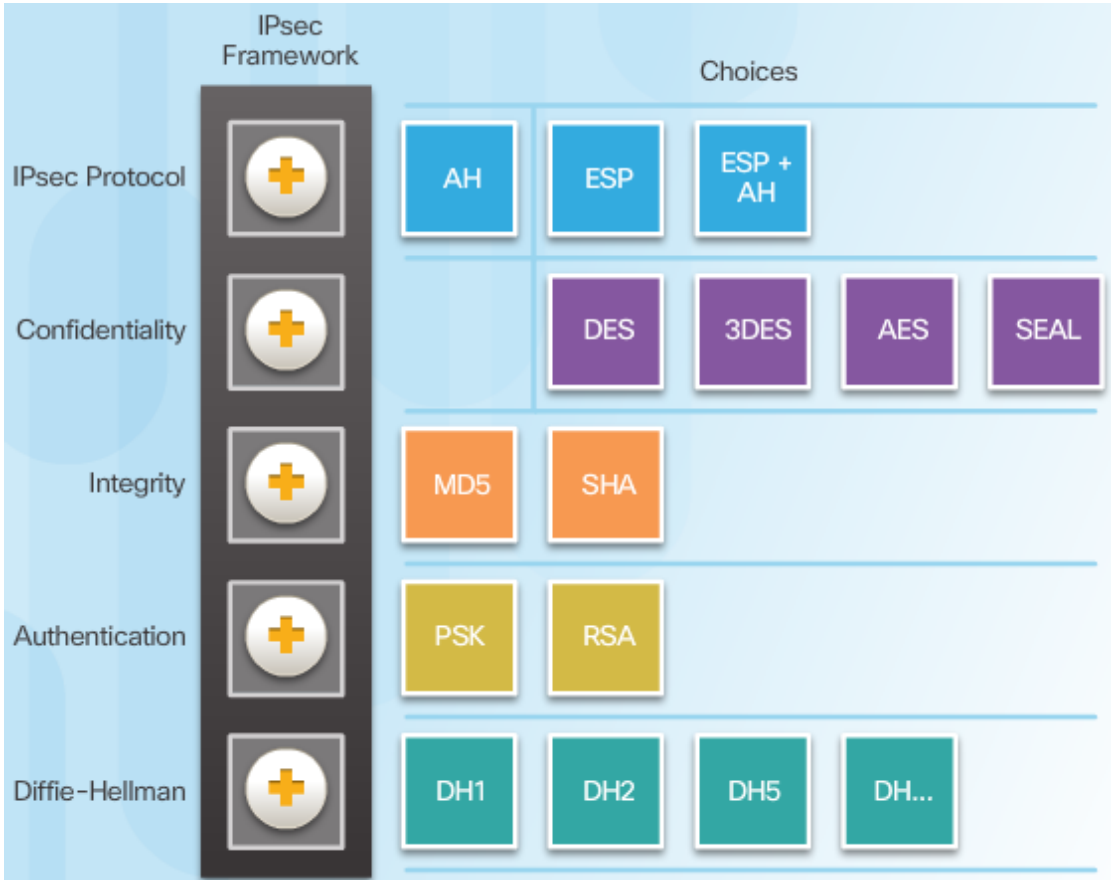
Components of Site-to-Site VPNs



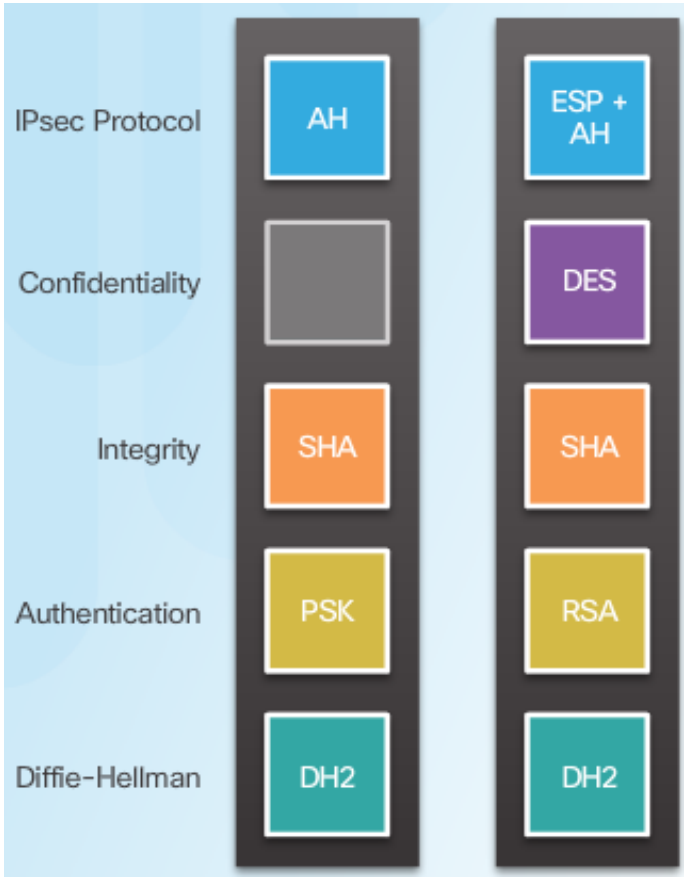
Topic 8.2.1:
Introducing IPsec

IPsec Technologies

IPsec Framework

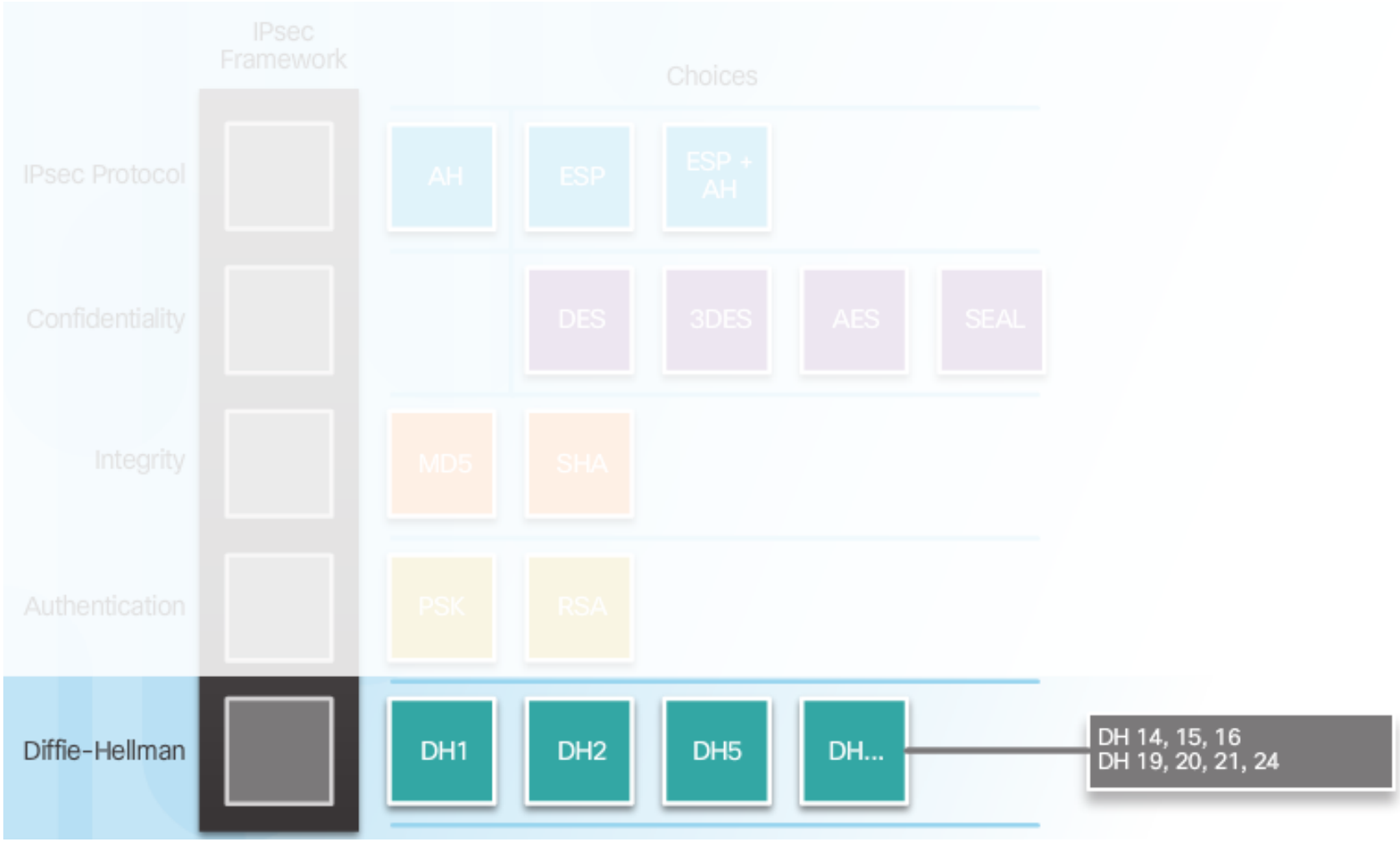


IPsec Implementation Examples



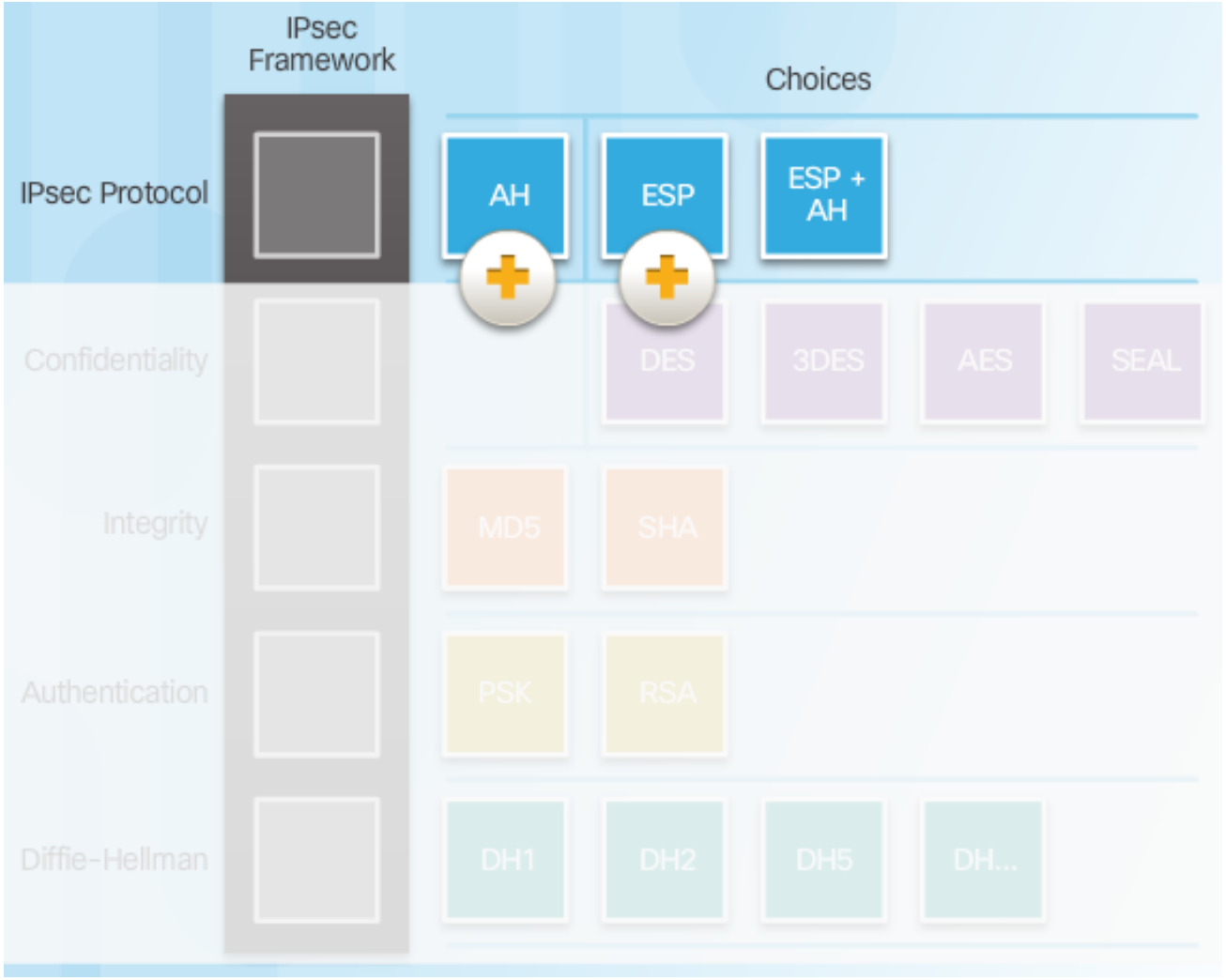
Secure Key Exchange

Diffie-Hellman Key Exchange



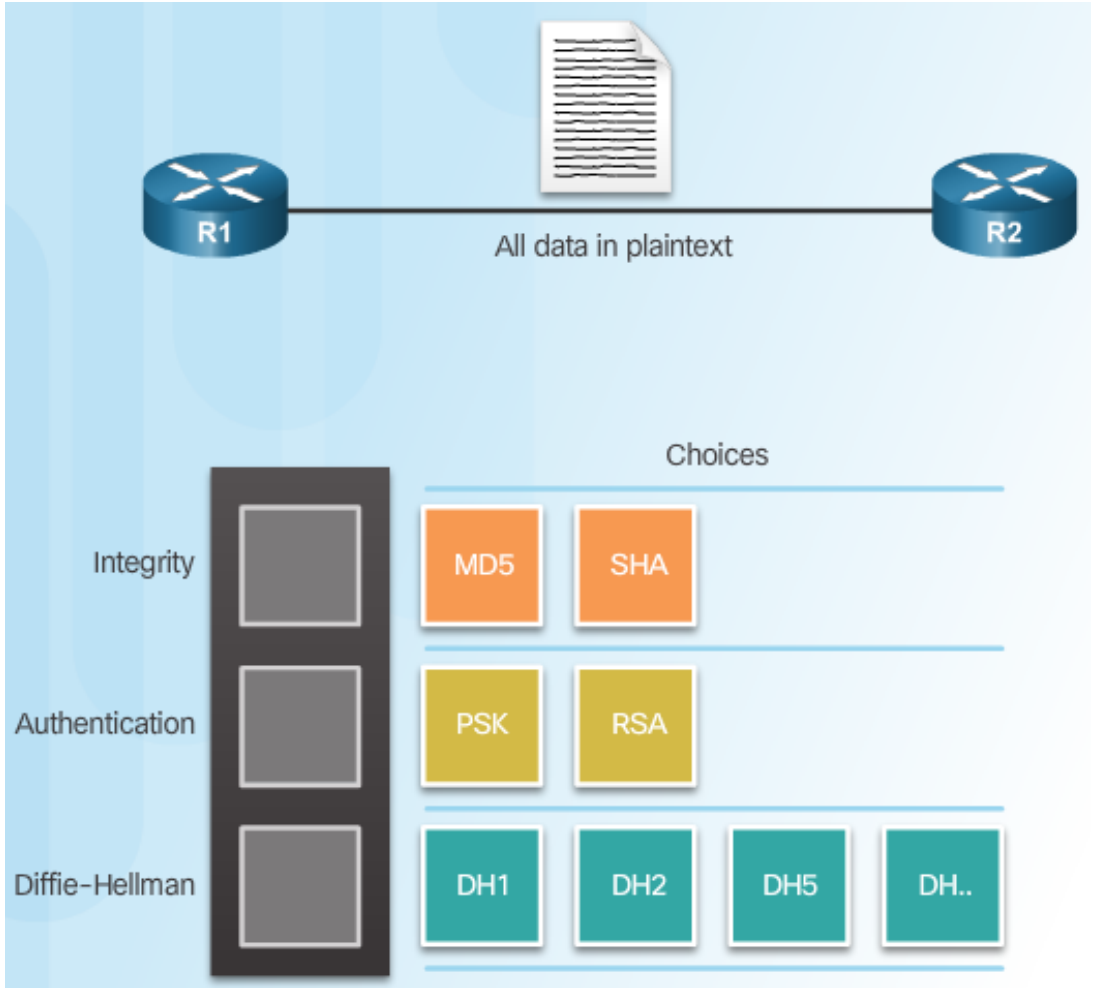
Topic 8.2.2:
IPsec Protocols

IPsec Protocol Overview

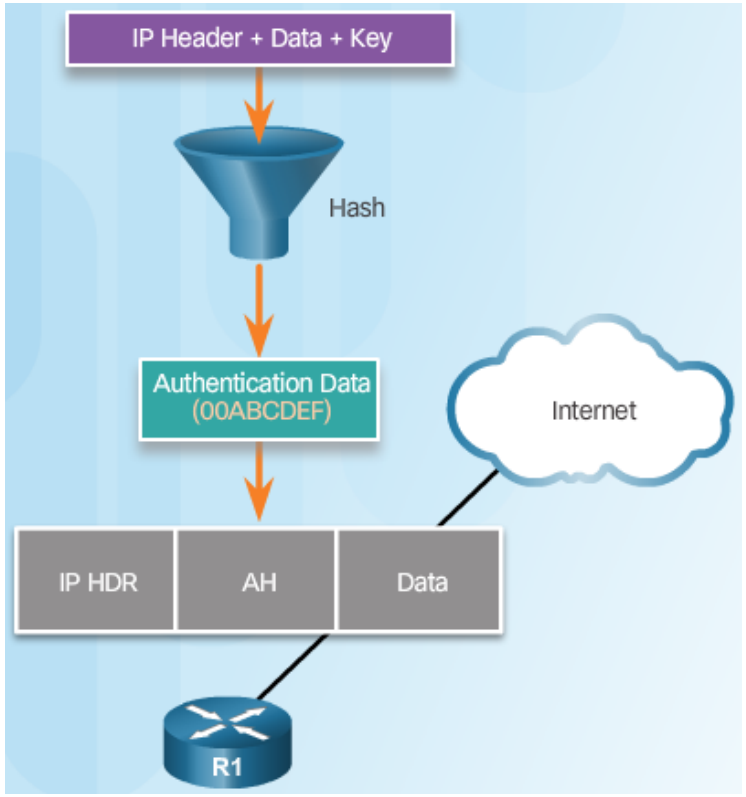


Authentication Header

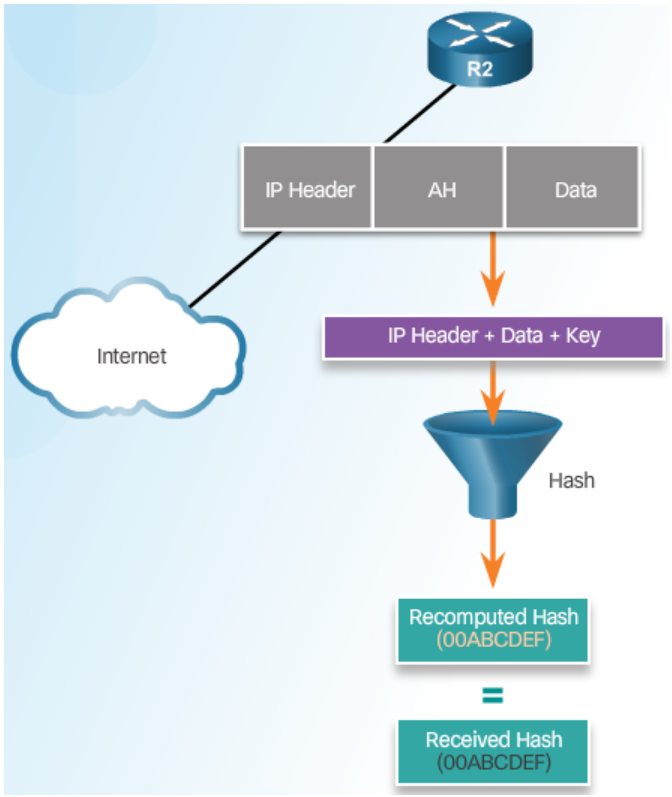
AH Protocols



Authentication Header (Cont.)

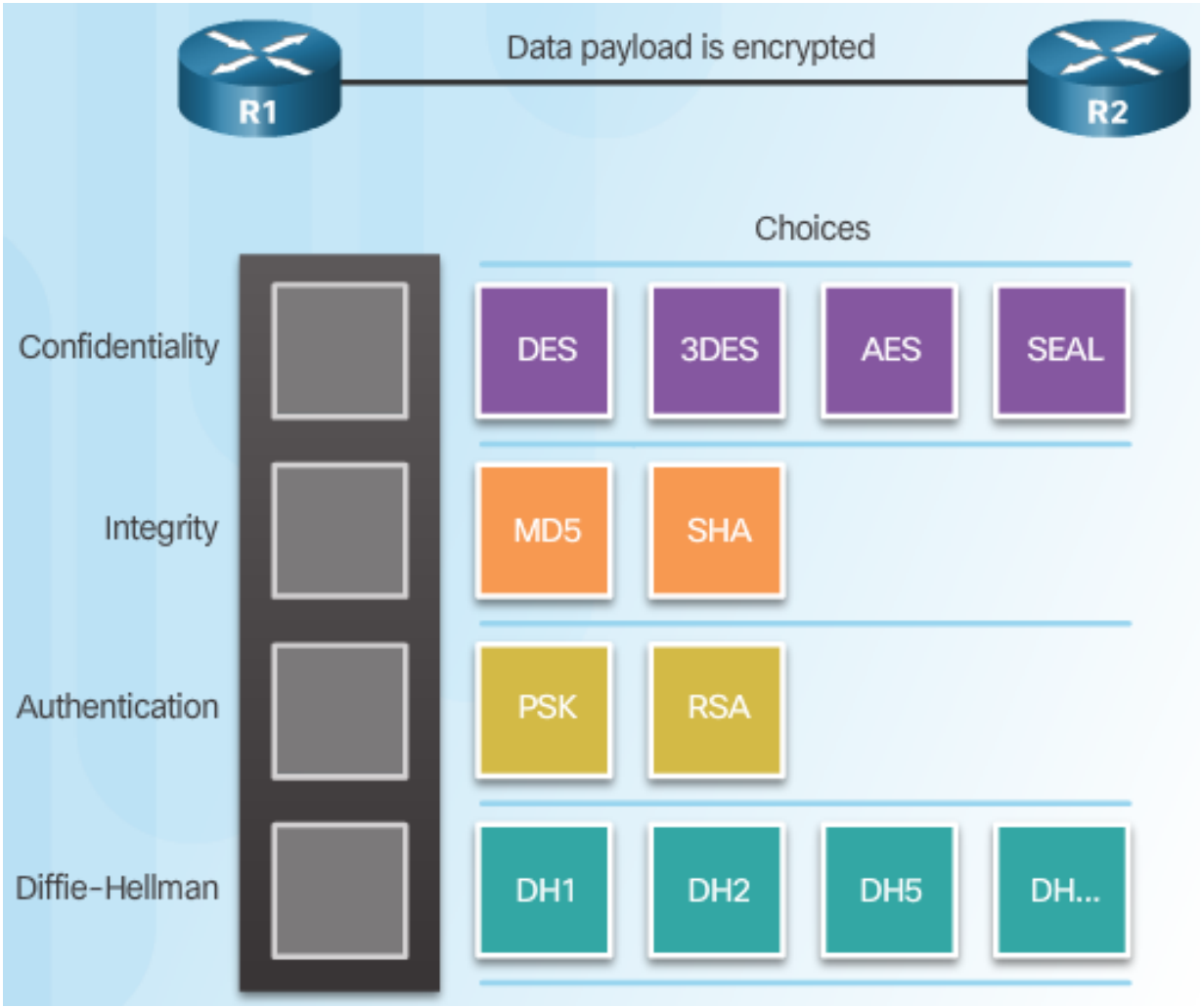


Router Creates Hash and Transmits to Peer



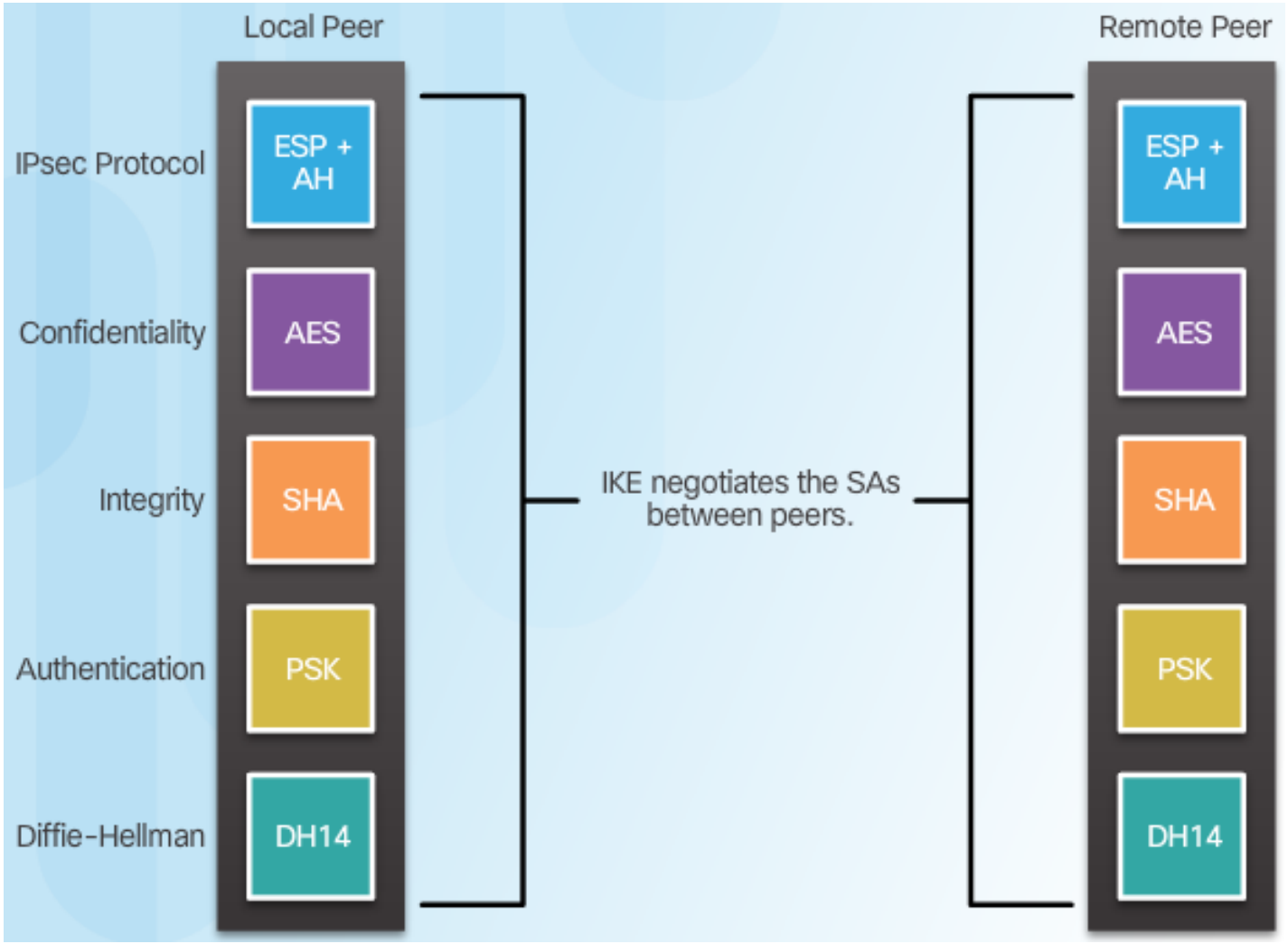
Peer Router Compares Recomputed Hash to Received Hash

ESP

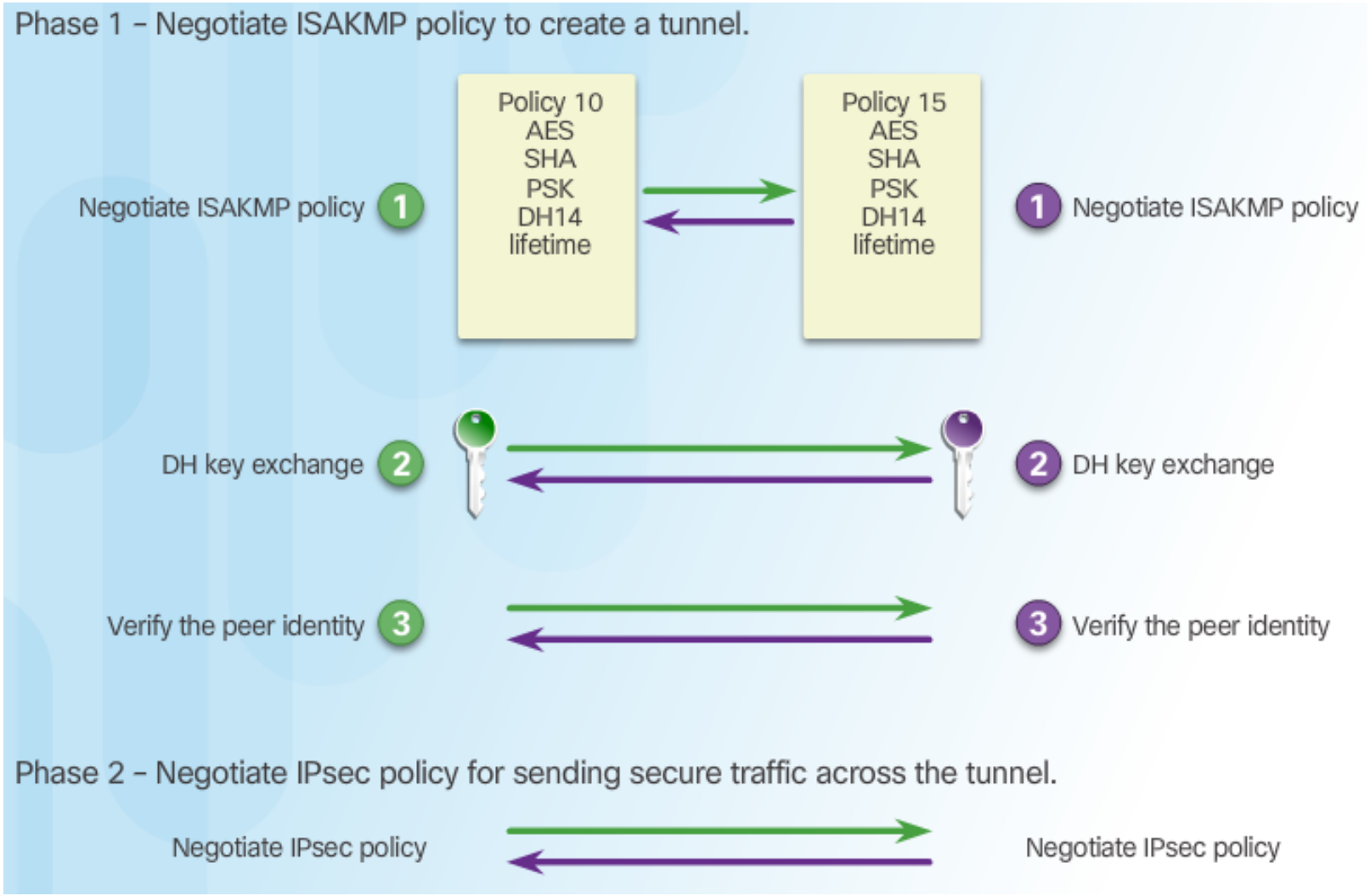

Data payload is encrypted
R1
R2
Choices
Confidentiality
DES
3DES
AES
SEAL
Integrity
MD5
SHA
Authentication
PSK
RSA
Diffie-Hellman
DH1
DH2
DH5
DH...

Topic 8.2.3:
Internet Key Exchange

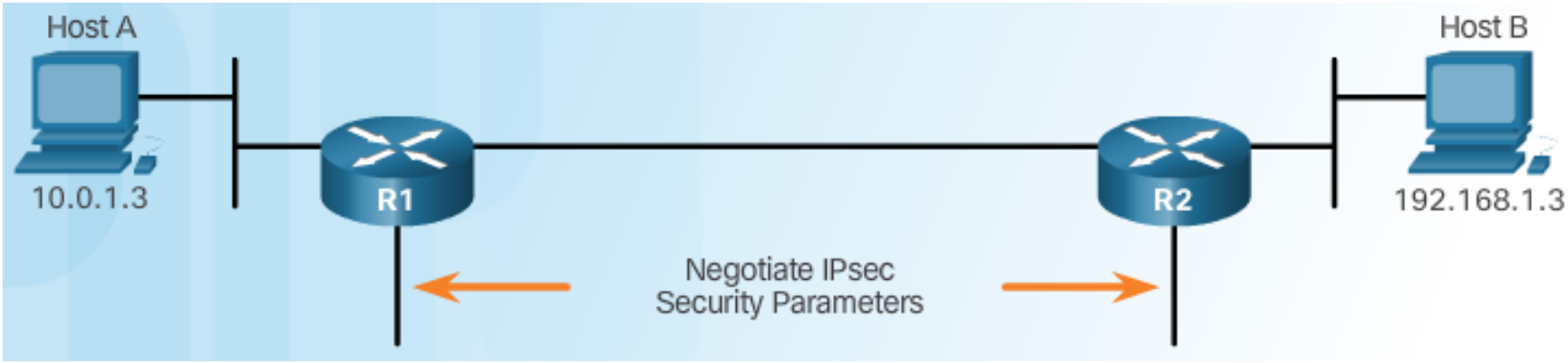
The IKE Protocol



Phase 1 and 2 Key Negotiation



Phase 2: Negotiating SAs

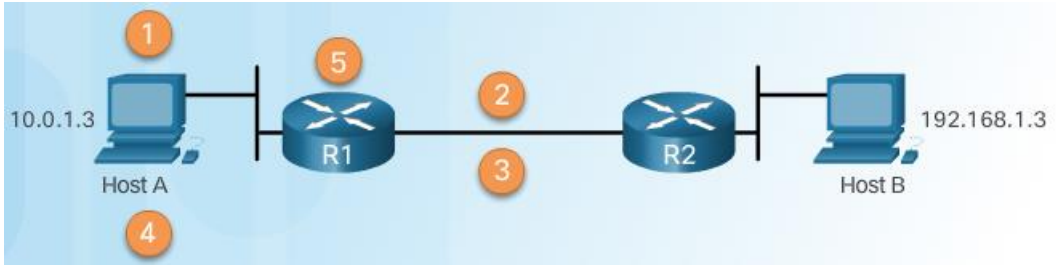


Section 8.3: Implementing Site-to-Site IPsec VPNs with CLI

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

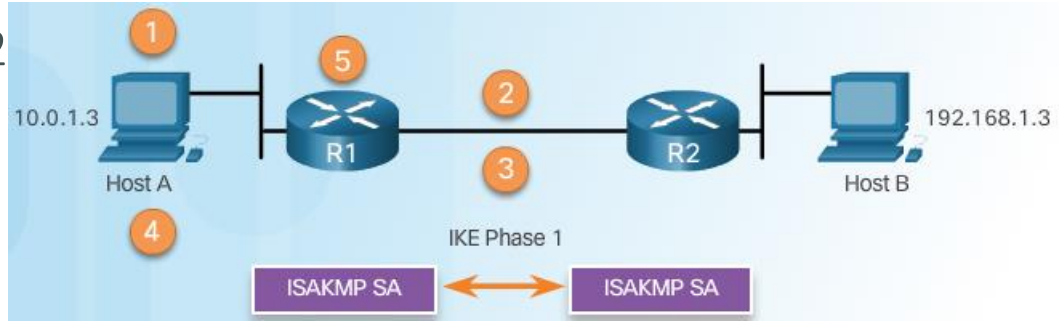
- Describe IPsec negotiation and the five steps of IPsec configuration.
- Configure the ISAKMP policy.
- Configure the IPsec policy.
- Configure and apply a crypto map.
- Verify the IPsec VPN.

IPsec Negotiation

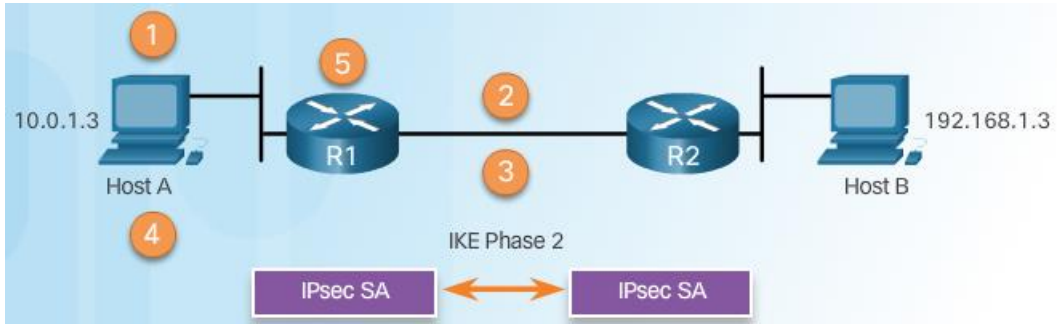


IPsec VPN Negotiation: Step 1 - Host A sends interesting traffic to Host B.

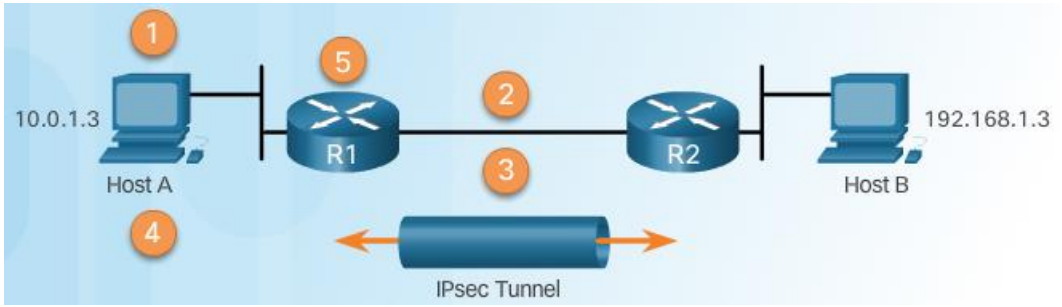
IPsec VPN Negotiation: Step 2 - R1 and R2 negotiate an IKE Phase 1 session.



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

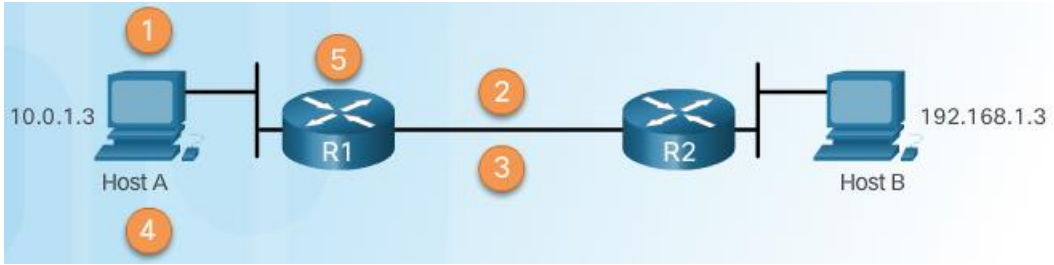


IPsec Negotiation (Cont.)



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

Existing ACL Configurations

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
```

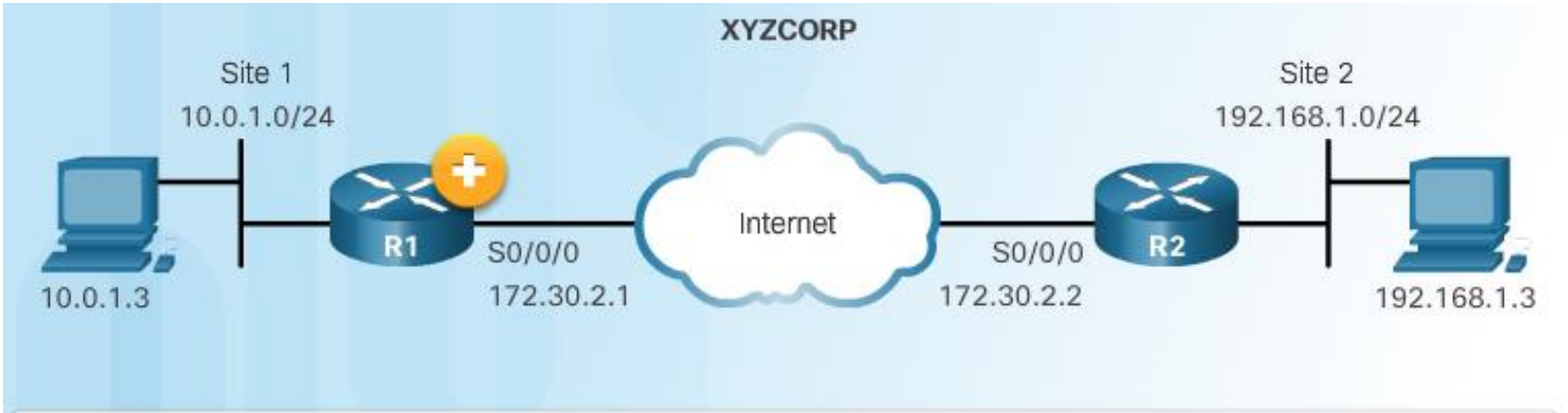
ACL Syntax for IPsec Traffic

Existing ACL Configurations (Cont.)

Permitting Traffic for IPsec Negotiations


```
R1(config)# ip access-list extended INBOUND
R1(config-ext-nacl)# permit ip 192.168.1.0 0.0.0.255 10.0.1.0 0.0.0.255
R1(config-ext-nacl)# permit icmp host 172.30.2.2 host 172.30.2.1
R1(config-ext-nacl)# permit udp host 172.30.2.2 host 172.30.2.1 eq isakmp
R1(config-ext-nacl)# permit esp host 172.30.2.2 host 172.30.2.1
R1(config-ext-nacl)# permit ahp host 172.30.2.2 host 172.30.2.1
R1(config-ext-nacl)# deny ip any any
R1(config-ext-nacl)# exit
R1(config)# interface serial0/0/0
R1(config-if)# ip access-group INBOUND in
```

The Default ISAKMP Policies




```
R1# show crypto isakmp default policy

Default IKE policy
Default protection suite of priority 65507
          encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
          hash algorithm:         Secure Hash Standard
          authentication method:  Rivest-Shamir-Adleman Signature
          Diffie-Hellman group:   #5 (1536 bit)
          lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65508
          encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
          hash algorithm:         Secure Hash Standard
          authentication method:  Pre-Shared Key
          Diffie-Hellman group:   #5 (1536 bit)
```

Syntax to Configure a New ISAKMP Policy


```
R1(config)# crypto isakmp policy ?
  <1-10000>  Priority of protection suite

R1(config)# crypto isakmp policy 1
R1(config-isakmp)# ?
ISAKMP commands:
  authentication  Set authentication method for protection suite
  default         Set a command to its defaults
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
```

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#
```

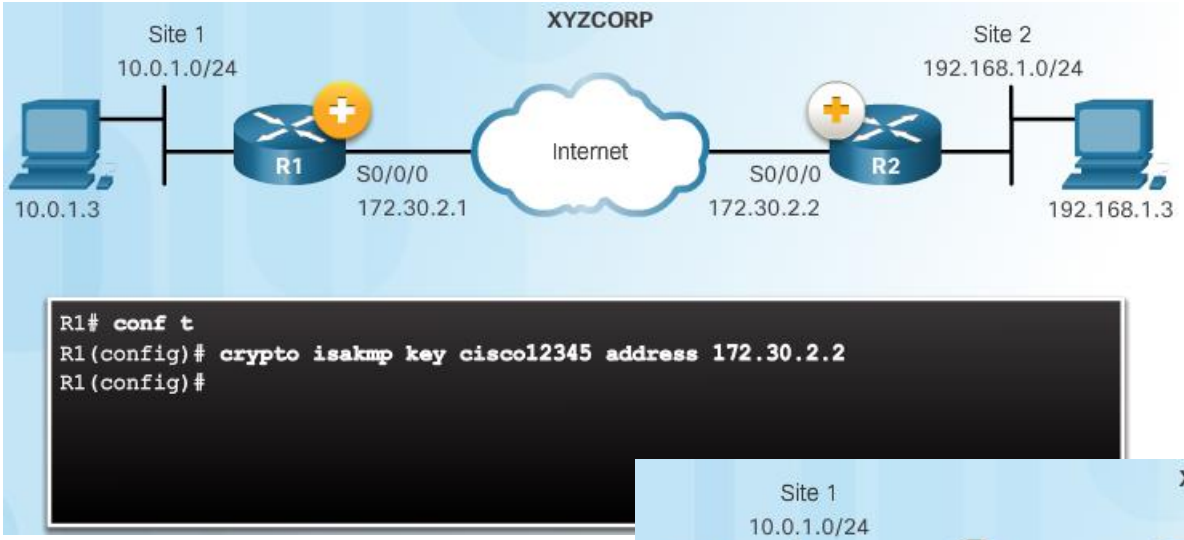
Configuring a Pre-Shared Key

The `crypto isakmp key` Command

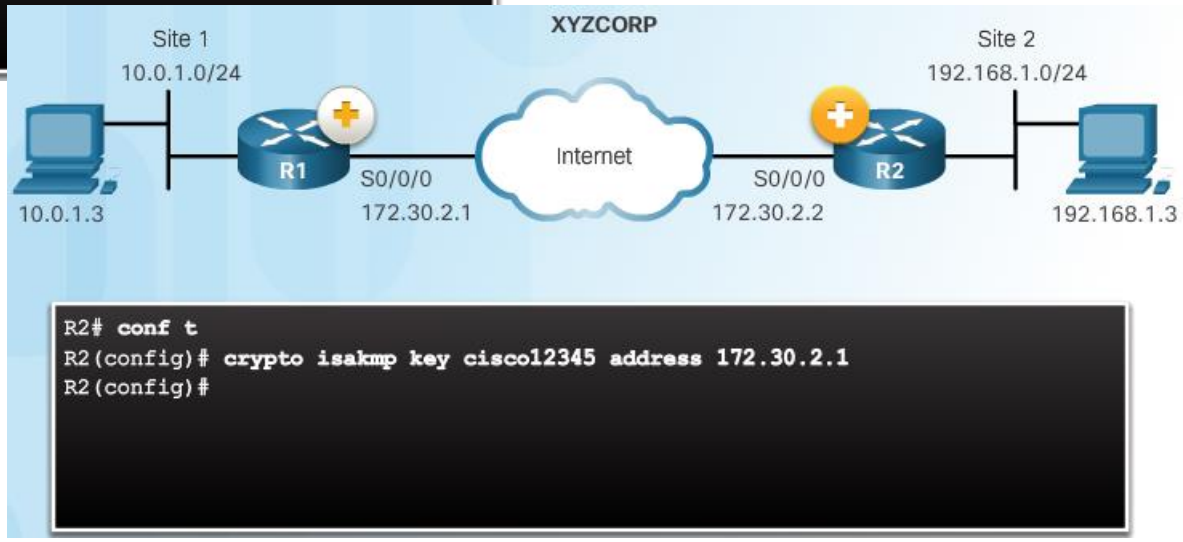
```
Router(config)#
crypto isakmp key keystring address peer-address

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

Configuring a Pre-Shared Key (Cont.)

Pre-Shared Key Configuration




```
R1# conf t
R1(config)# crypto isakmp key cisco12345 address 172.30.2.2
R1(config)#
```

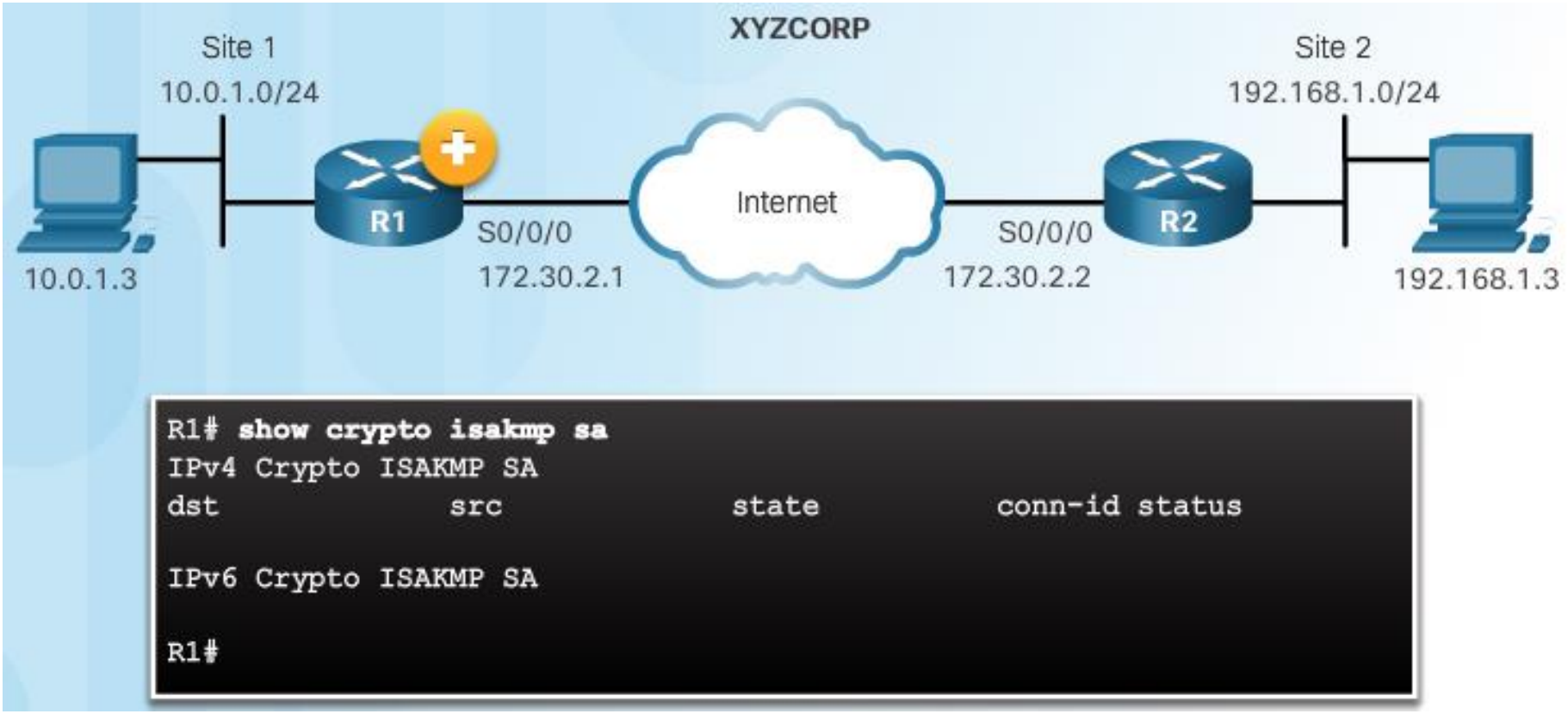



```
R2# conf t
R2(config)# crypto isakmp key cisco12345 address 172.30.2.1
R2(config)#
```

Topic 8.3.3:
IPsec Policy

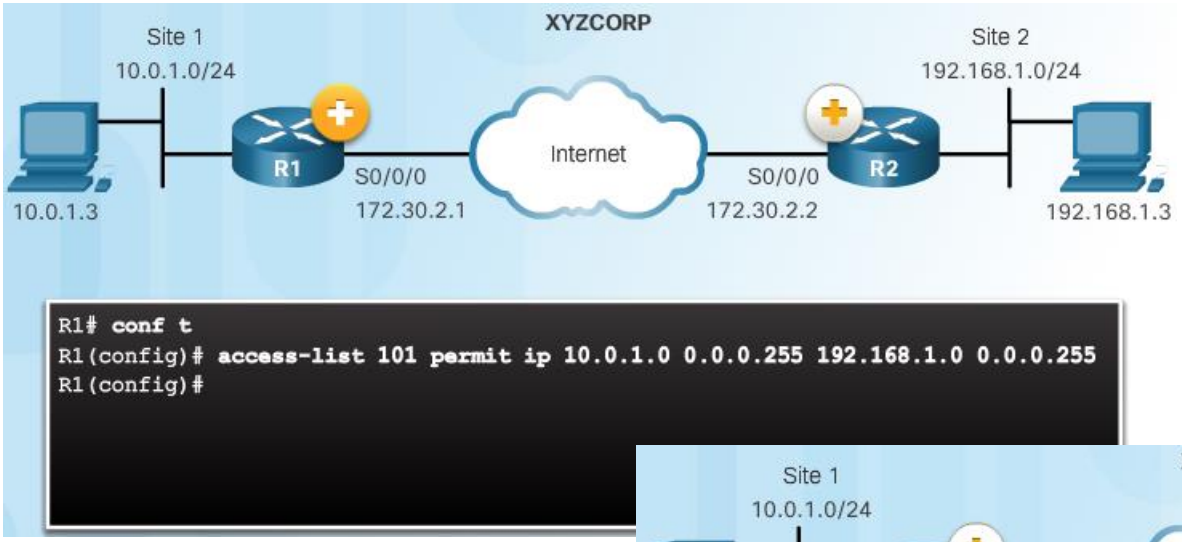
Define Interesting Traffic

The IKE Phase 1 Tunnel Does Not Exist Yet

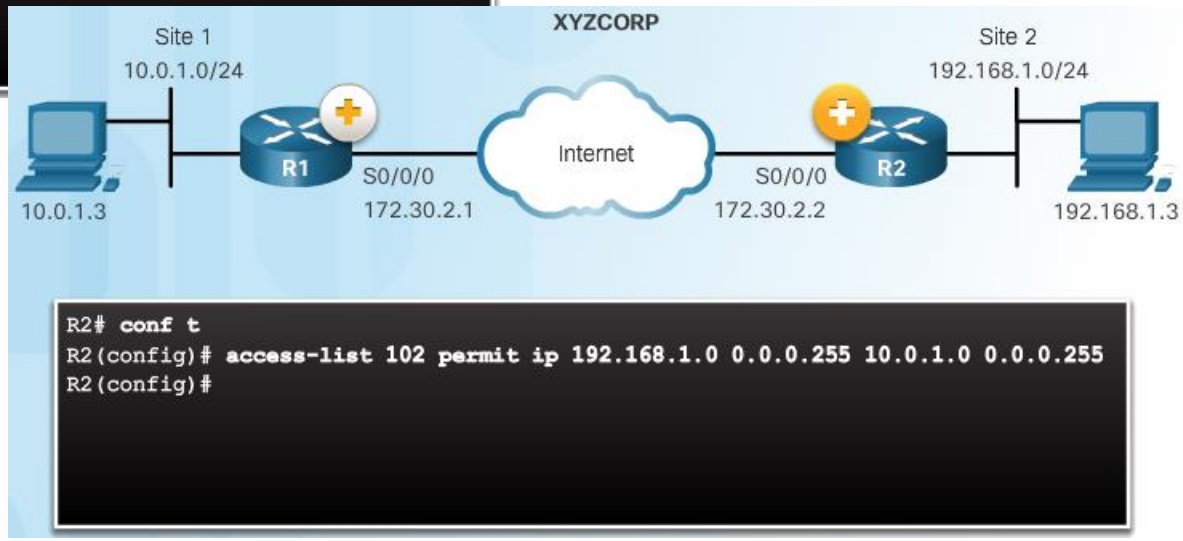


Define Interesting Traffic (Cont.)

Configure an ACL to Define Interesting Traffic



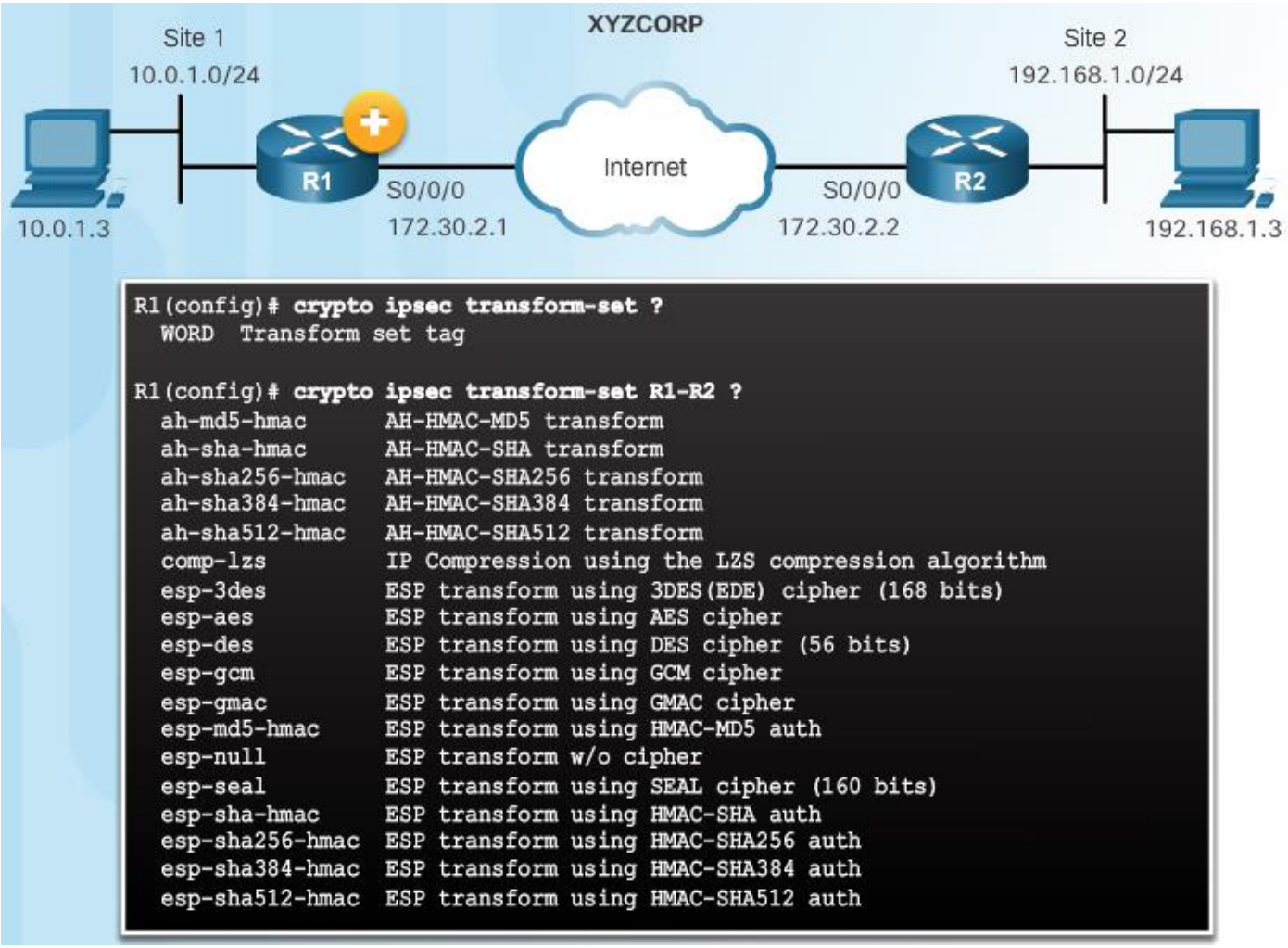

```
R1# conf t
R1(config)# access-list 101 permit ip 10.0.1.0 0.0.0.255 192.168.1.0 0.0.0.255
R1(config)#
```




```
R2# conf t
R2(config)# access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.1.0 0.0.0.255
R2(config)#
```

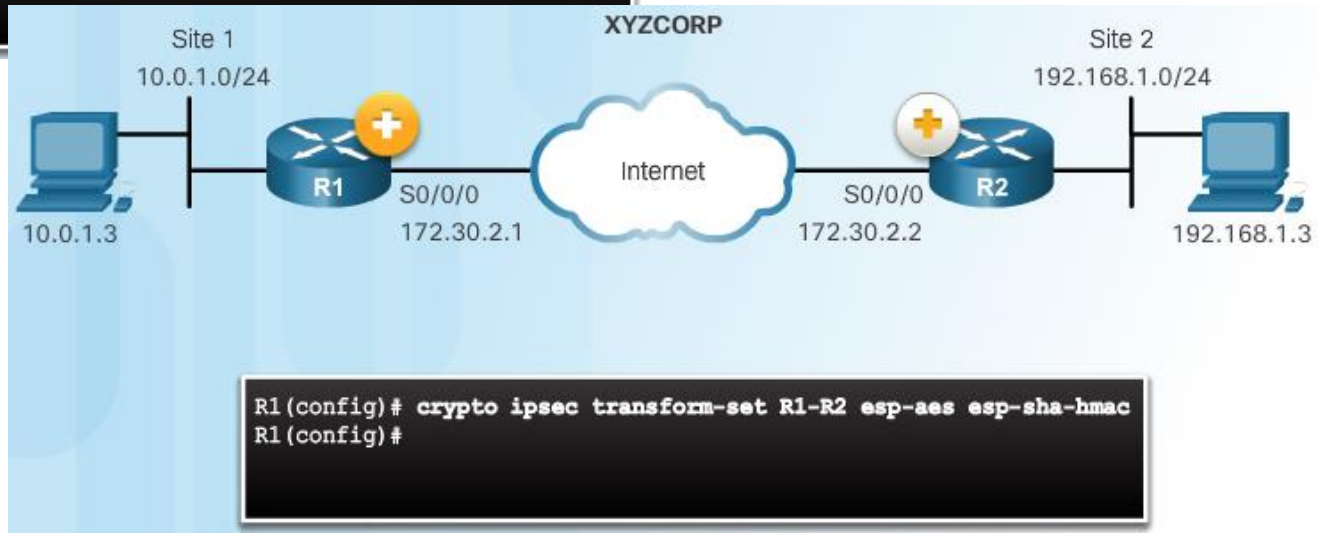
Configure IPsec Transform Set

The `crypto ipsec transform-set` Command



Configure IPsec Transform Set (Cont.)

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

Syntax to Configure a Crypto Map (Cont.)

Crypto Map Configuration Commands


```
R1(config)# crypto map R1-R2_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R1(config-crypto-map)# ?
Crypto Map configuration commands:
  default         Set a command to its defaults
  description     Description of the crypto map statement policy
  dialer          Dialer related commands
  exit            Exit from crypto map configuration mode
  match           Match values.
  no              Negate a command or set its defaults
  qos             Quality of Service related commands
  reverse-route   Reverse Route Injection.
  set             Set values for encryption/decryption
```

XYZCORP Crypto Map Configuration

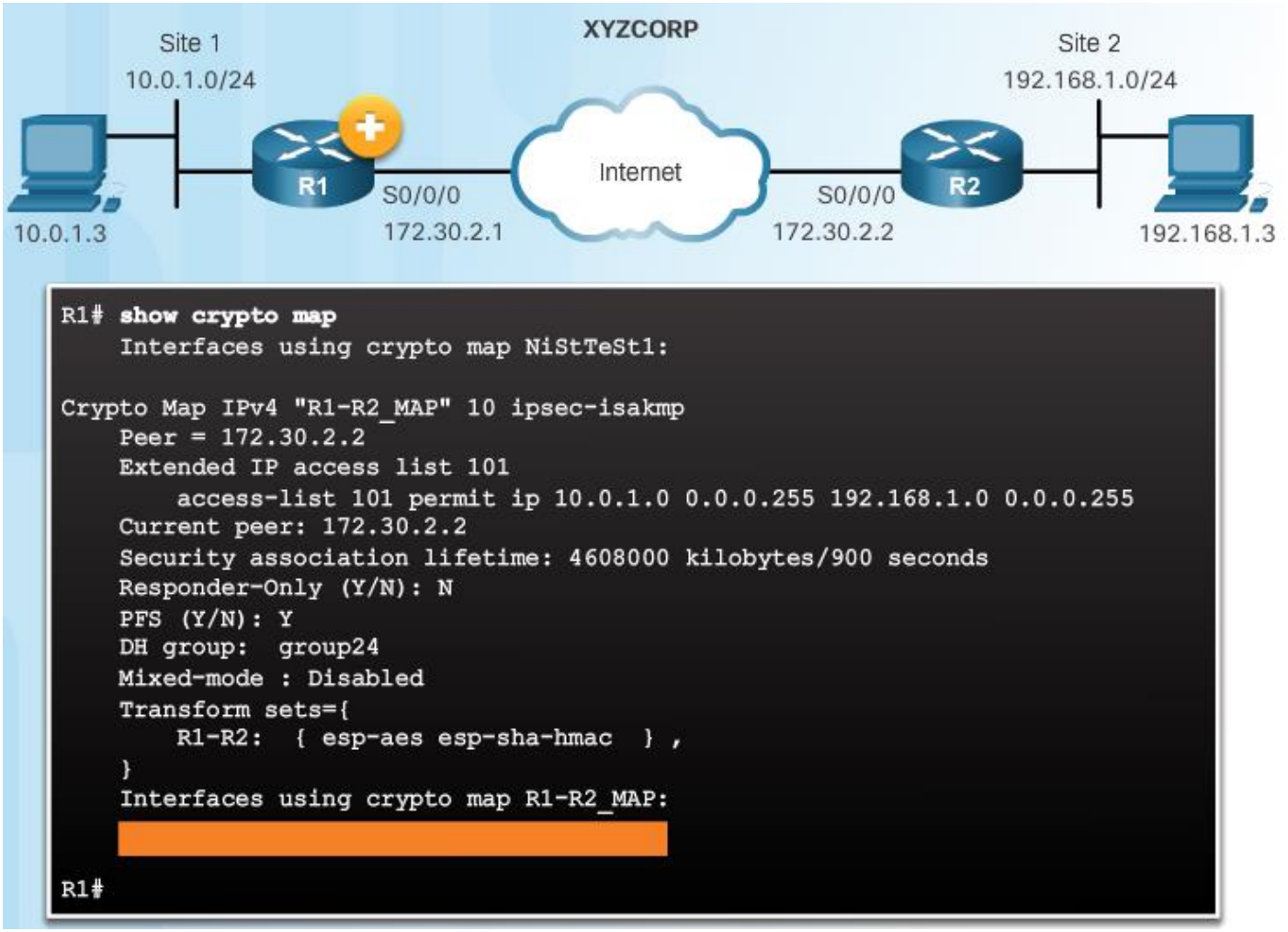
Crypto Map Configuration:


```
R1(config)# crypto map R1-R2_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R1(config-crypto-map)# match address 101
R1(config-crypto-map)# set transform-set R1-R2
R1(config-crypto-map)# set peer 172.30.2.2
R1(config-crypto-map)# set pfs group24
R1(config-crypto-map)# set security-association lifetime seconds 900
R1(config-crypto-map)# exit
R1(config)#
```


```
R2(config)# crypto map R1-R2_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R2(config-crypto-map)# match address 102
R2(config-crypto-map)# set transform-set R1-R2
R2(config-crypto-map)# set peer 172.30.2.1
R2(config-crypto-map)# set pfs group24
R2(config-crypto-map)# set security-association lifetime seconds 900
R2(config-crypto-map)# exit
R2(config)#
```

XYZCORP Crypto Map Configuration (Cont.)

Crypto Map Configuration:



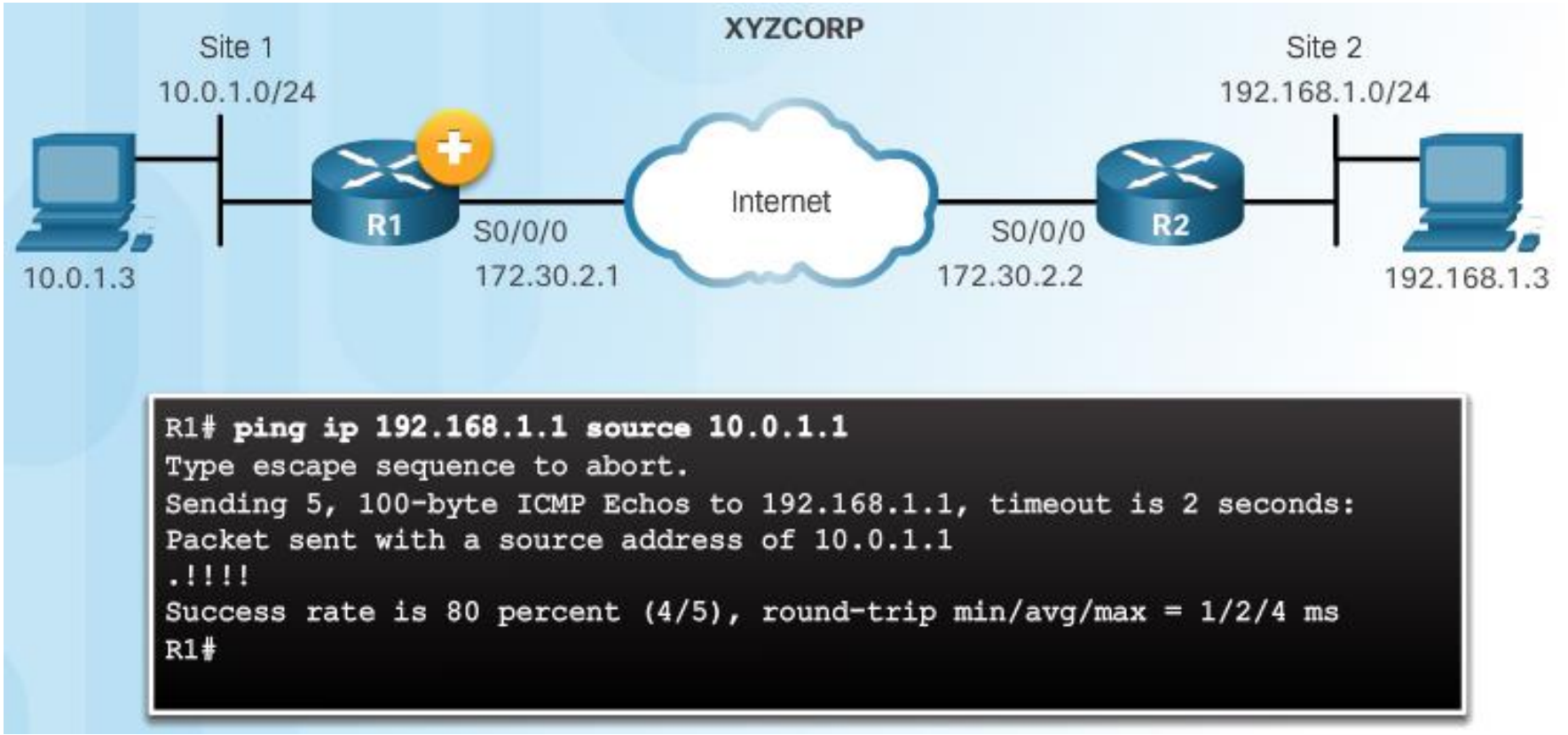
Apply the Crypto Map


```
R1(config)# interface serial0/0/0
R1(config-if)# crypto map R1-R2_MAP
R1(config-if)#
*Mar 19 19:36:36.273: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)# end
R1# show crypto map
Interfaces using crypto map NiStTeSt1:

Crypto Map IPv4 "R1-R2_MAP" 10 ipsec-isakmp
Peer = 172.30.2.2
Extended IP access list 101
    access-list 101 permit ip 10.0.1.0 0.0.0.255 192.168.1.0 0.0.0.255
Current peer: 172.30.2.2
Security association lifetime: 4608000 kilobytes/900 seconds
Responder-Only (Y/N): N
PFS (Y/N): Y
DH group:  group24
Mixed-mode : Disabled
Transform sets={
R1-R2:  { esp-aes esp-sha-hmac  } ,
}
Interfaces using crypto map R1-R2_MAP:
Serial0/0/0
```

Topic 8.3.5:
IPsec VPN

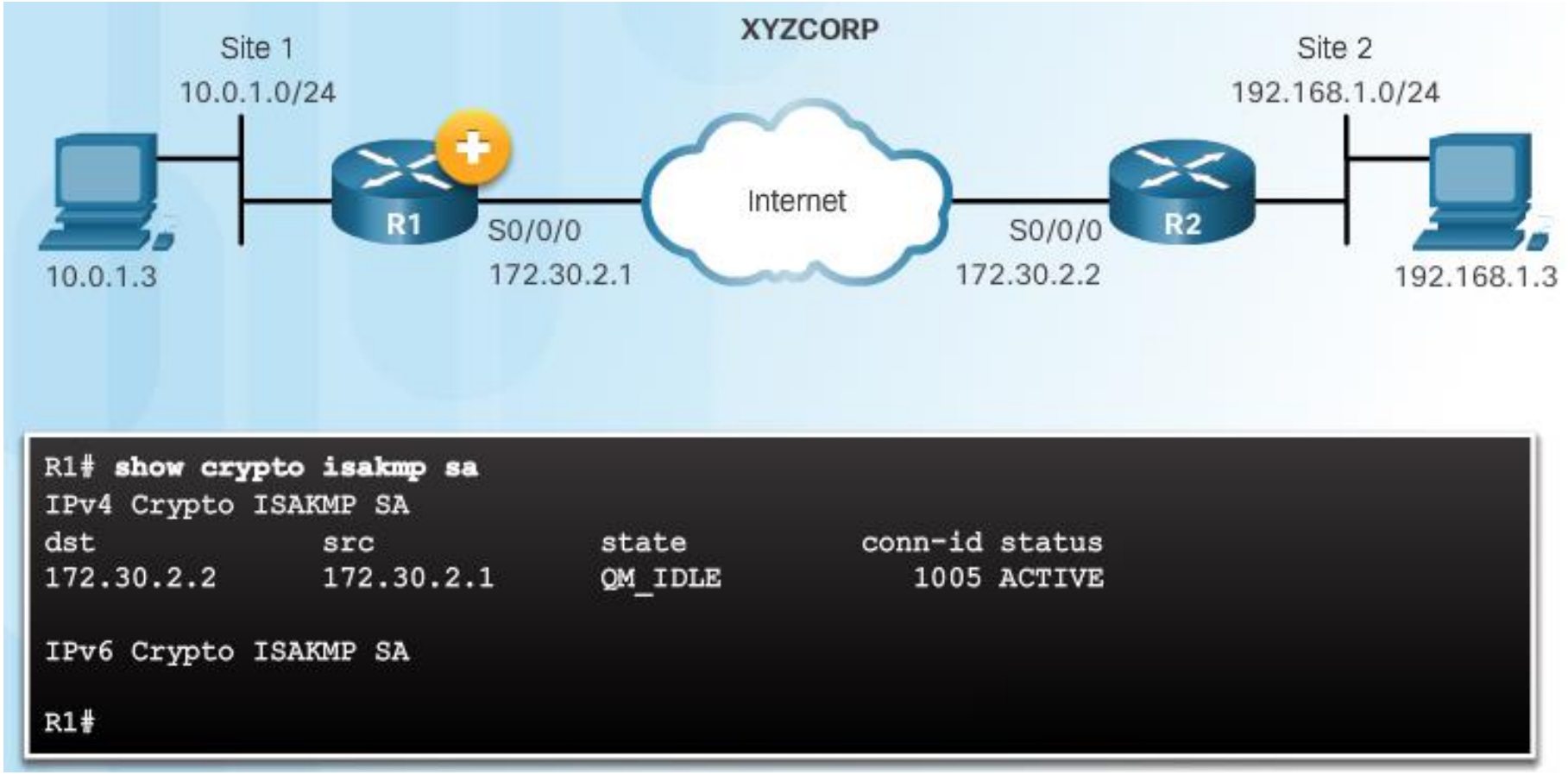
Send Interesting Traffic

Use Extended Ping to Send Interesting Traffic



Verify ISAKMP and IPsec Tunnels

Verify the ISAKMP Tunnel is Established




```
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.30.2.2      172.30.2.1      QM_IDLE           1005 ACTIVE

IPv6 Crypto ISAKMP SA

R1#
```

Verify ISAKMP and IPsec Tunnels (Cont.)

Verify the IPsec Tunnel is Established


```
R1# show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: R1-R2_MAP, local addr 172.30.2.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.0.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 172.30.2.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
```