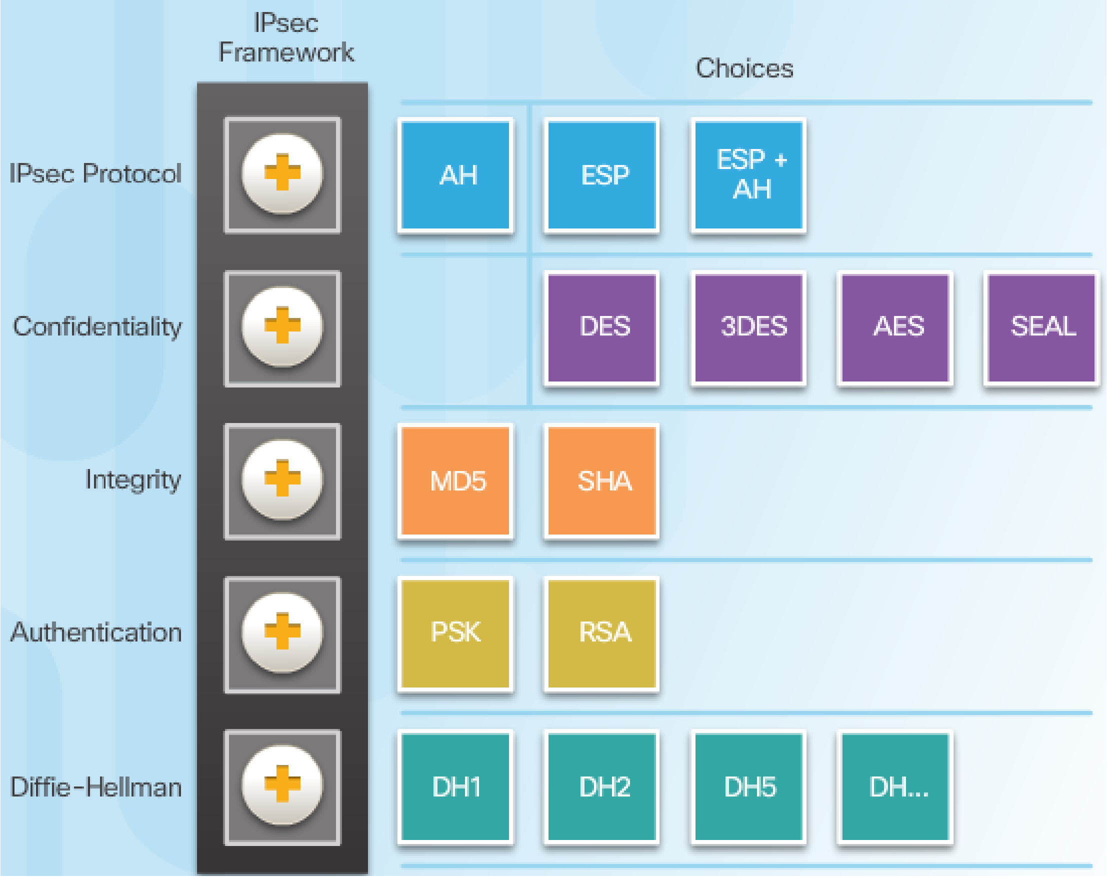
Implementing Site-to-Site IPsec VPN

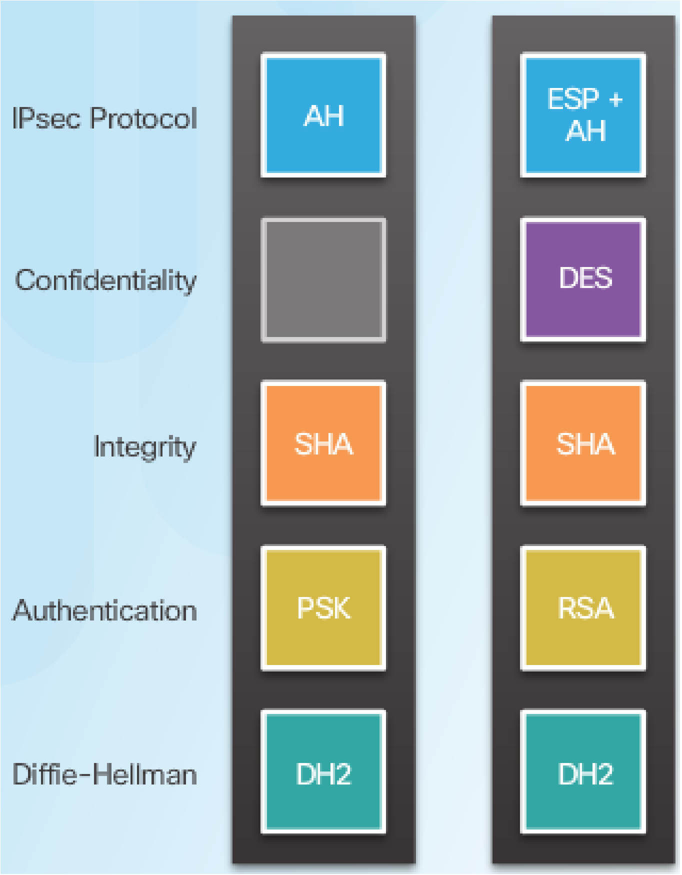
IPsec Technologies

IPsec Framework



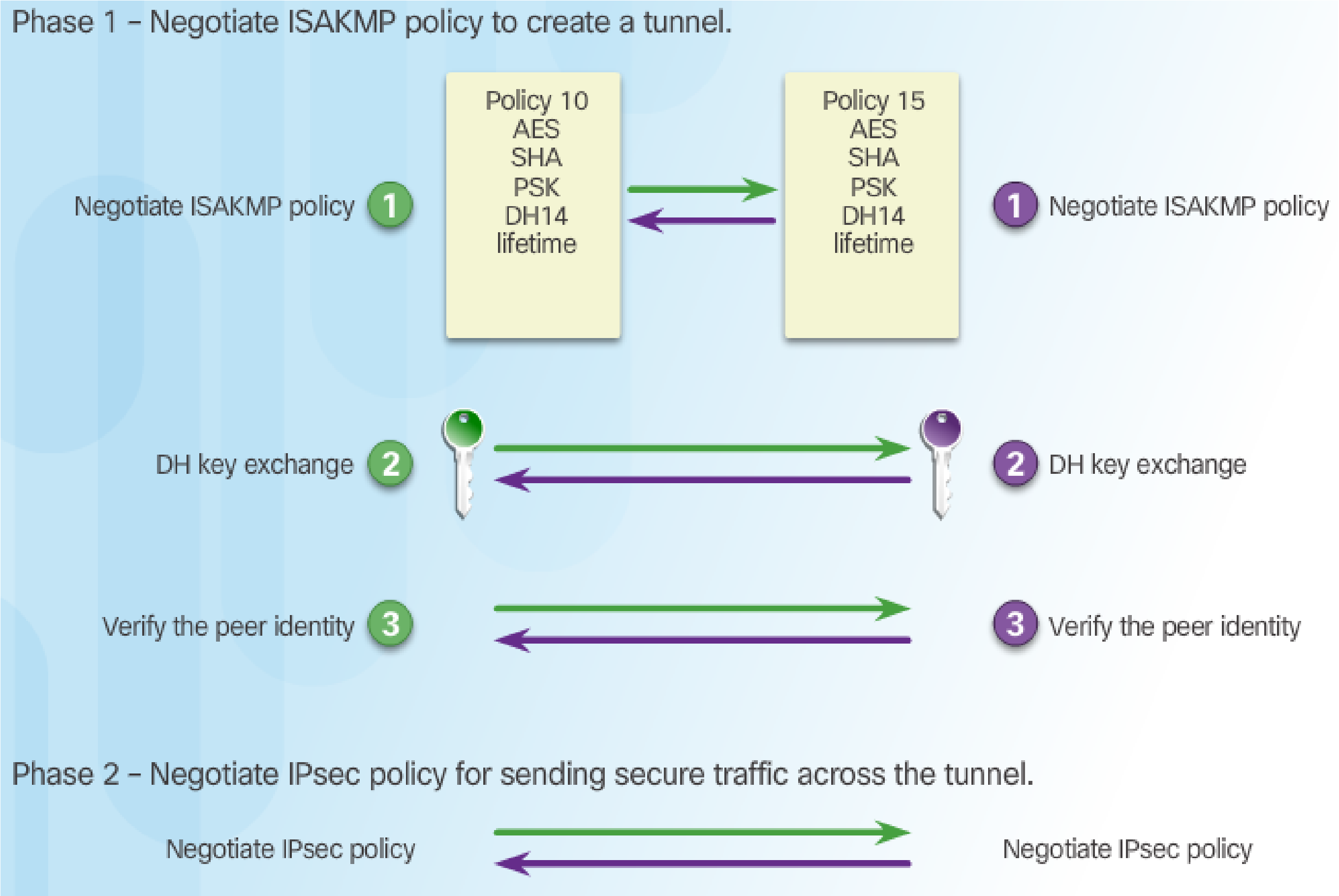
IPsec Framework	Choices				
IPsec Protocol	AH	ESP	ESP + AH		
Confidentiality		DES	3DES	AES	SEAL
Integrity	MD5	SHA			
Authentication	PSK	RSA			
Diffie-Hellman	DH1	DH2	DH5	DH...	

IPsec Implementation Examples



IPsec Protocol	AH	ESP + AH
Confidentiality		DES
Integrity	SHA	SHA
Authentication	PSK	RSA
Diffie-Hellman	DH2	DH2

Phase 1 and 2 Key Negotiation


Phase 1 – Negotiate ISAKMP policy to create a tunnel.
Policy 10
AES
SHA
PSK
DH14
lifetime
Policy 15
AES
SHA
PSK
DH14
lifetime
Negotiate ISAKMP policy 1
1 Negotiate ISAKMP policy
DH key exchange 2
2 DH key exchange
Verify the peer identity 3
3 Verify the peer identity
Phase 2 – Negotiate IPsec policy for sending secure traffic across the tunnel.
Negotiate IPsec policy
Negotiate IPsec policy

ISAKMP (Internet Security Association and Key Management Protocol)

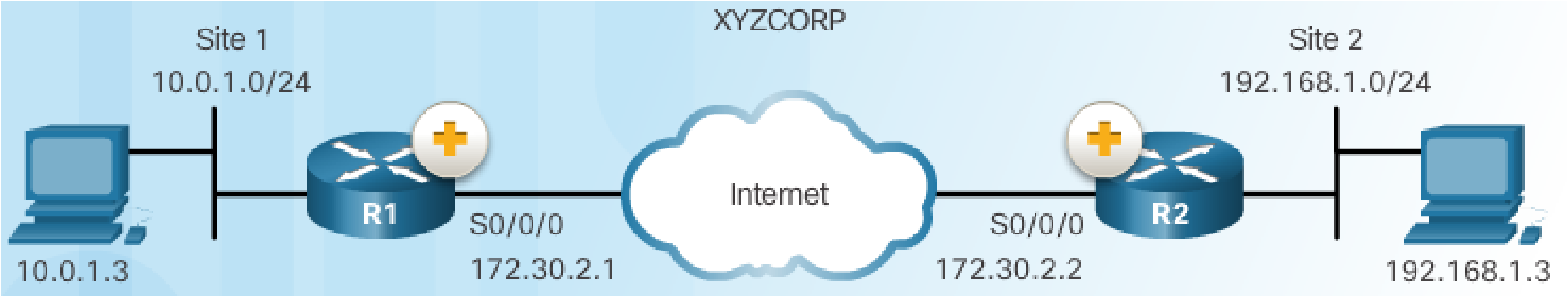
AES (Advanced Encryption Standard) Encryption Algorithm

SHA (Secure Hash Algorithm) Cryptographic hash function

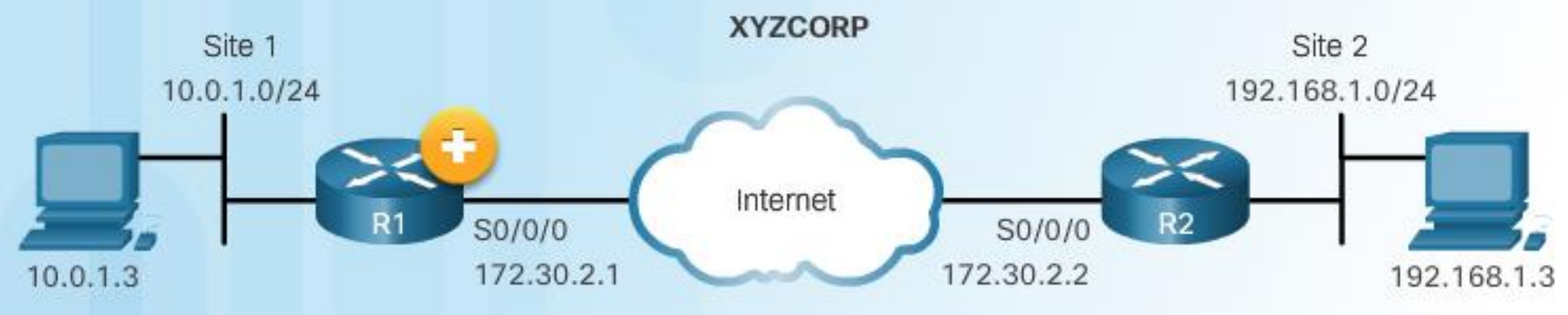
PSK (Pre-Shared Key)

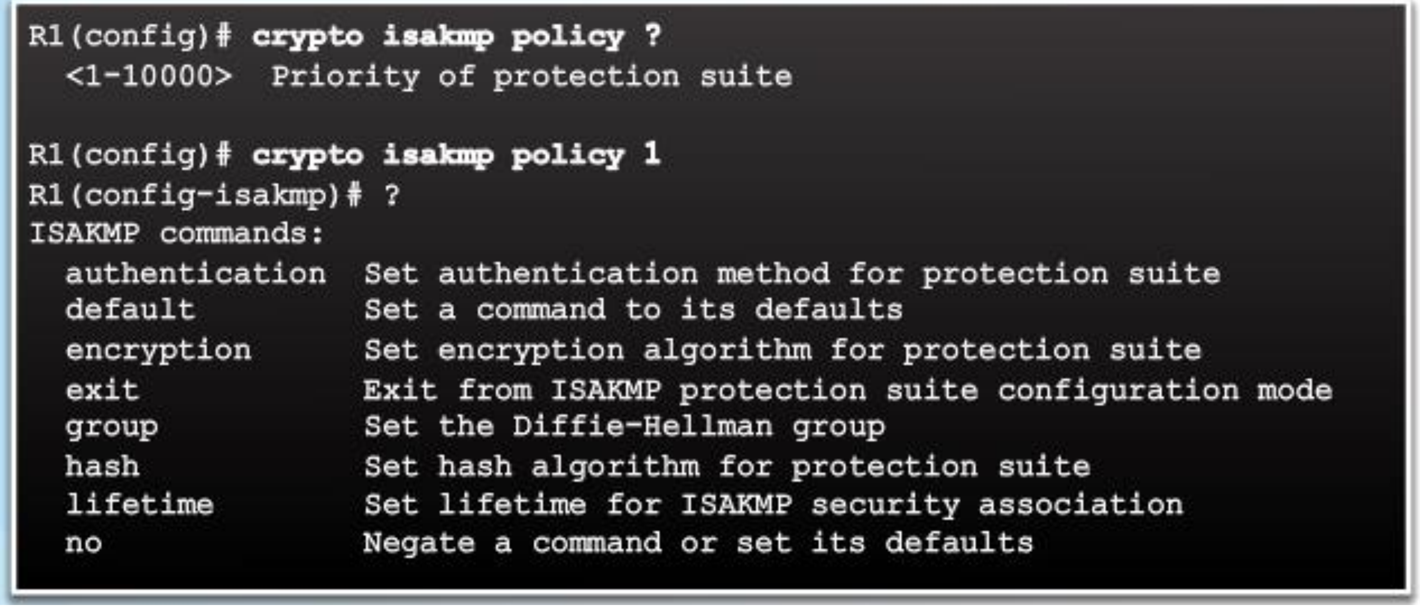
DH (Diffie-Hellman) Method of securely exchanging cryptographic keys over a public channel

Site-to-Site IPsec VPN Topology



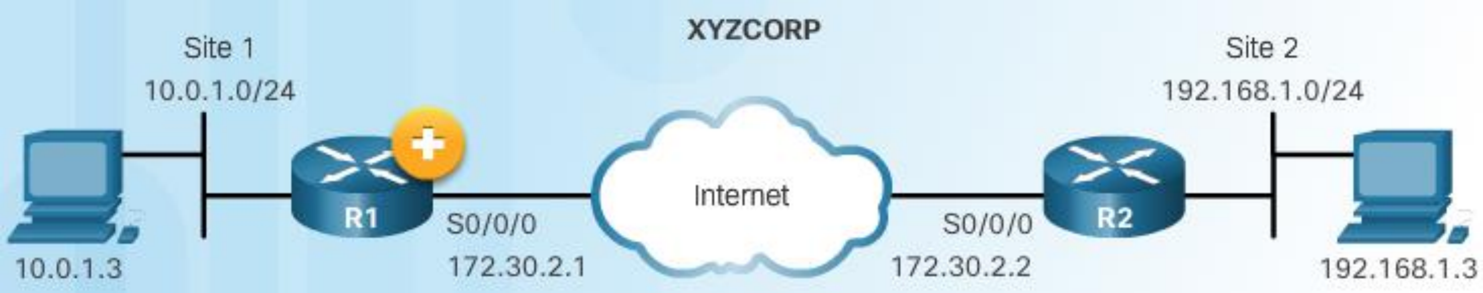
(1) Syntax to Configure a New ISAKMP Policy

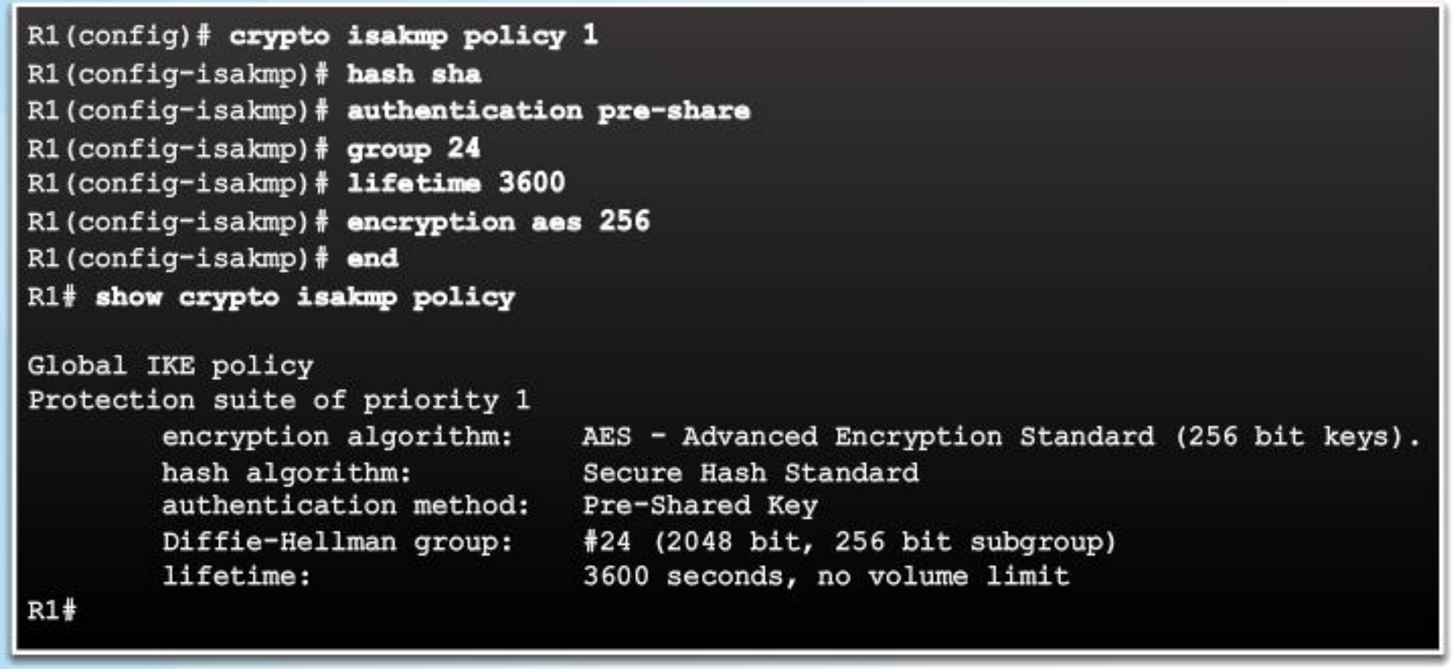




```
R1(config)# crypto isakmp policy ?
  <1-10000>  Priority of protection suite

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
```

(1) XYZCORP ISAKMP Policy Configuration

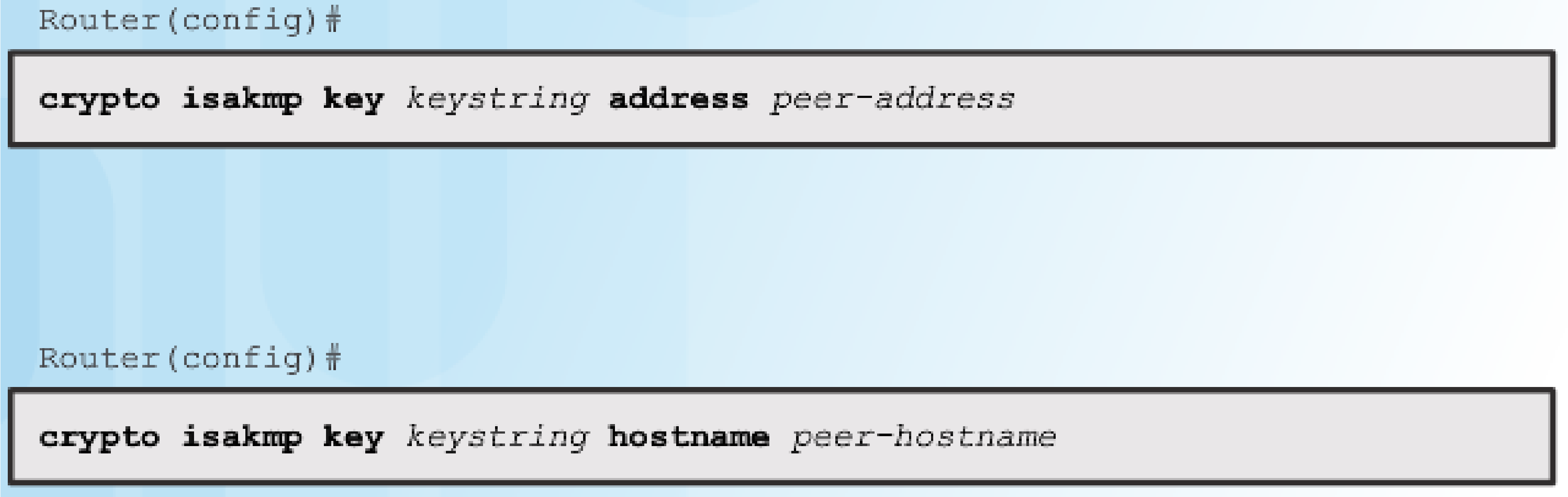




```
R1(config)# crypto isakmp policy 1
R1(config-isakmp)# hash sha
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 24
R1(config-isakmp)# lifetime 3600
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# end
R1# show crypto isakmp policy

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#
```

(2) Configuring a Pre-Shared Key

The `crypto isakmp key` Command

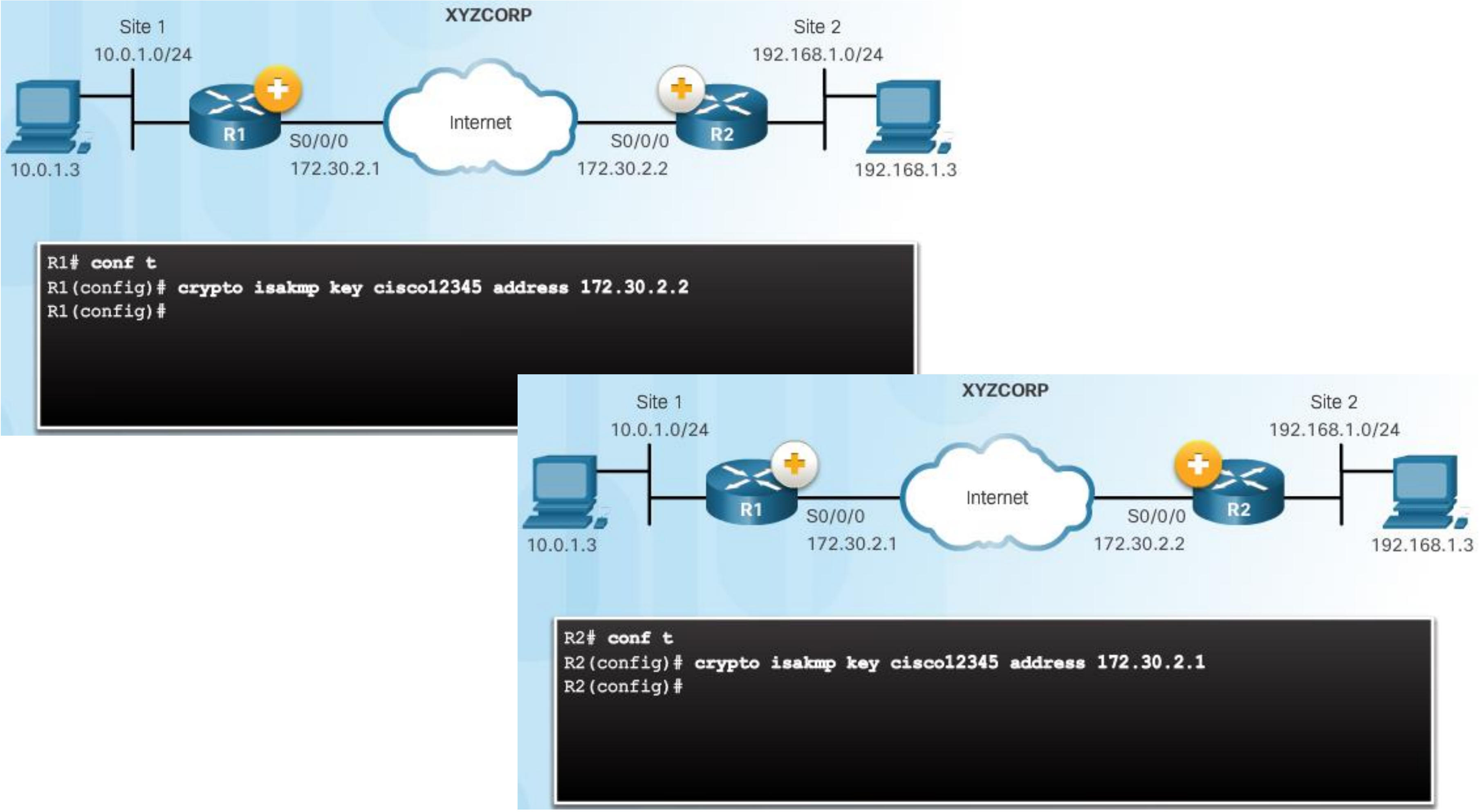


```
Router(config)#
crypto isakmp key keystring address peer-address
```

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

(2) Configuring a Pre-Shared Key (Cont.)

Pre-Shared Key Configuration

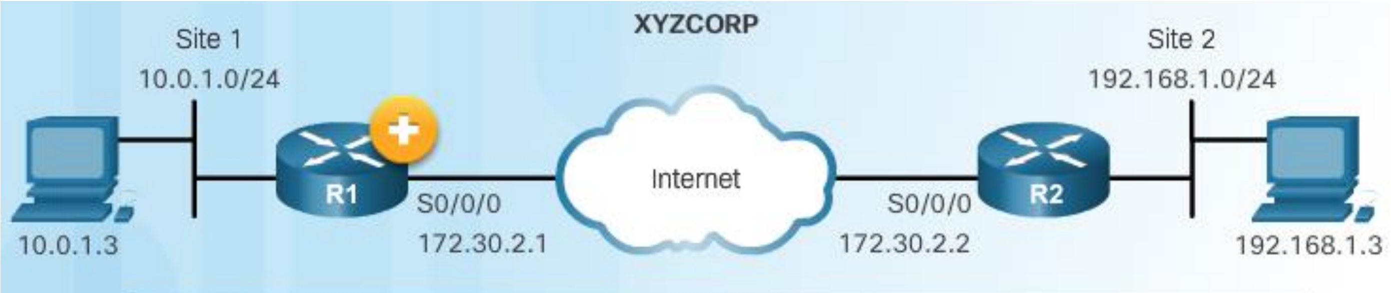


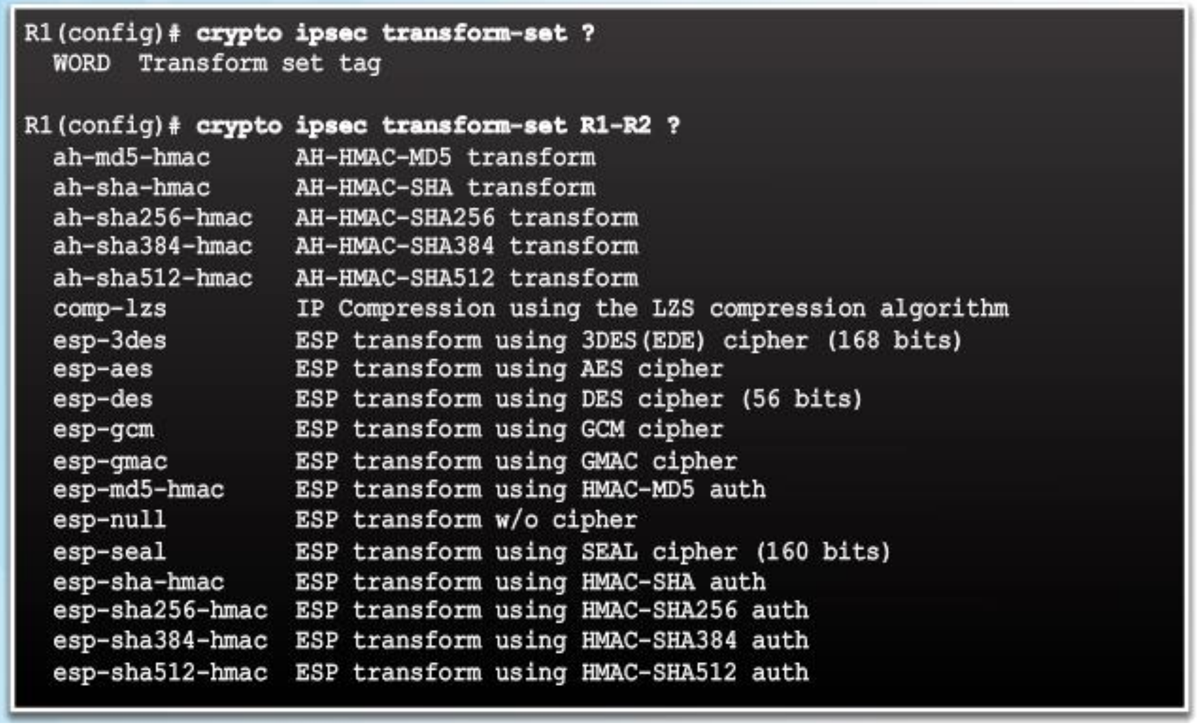
```
R1# conf t
R1(config)# crypto isakmp key cisco12345 address 172.30.2.2
R1(config)#
```

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

(3) Configure IPsec Transform Set

The `crypto ipsec transform-set` Command

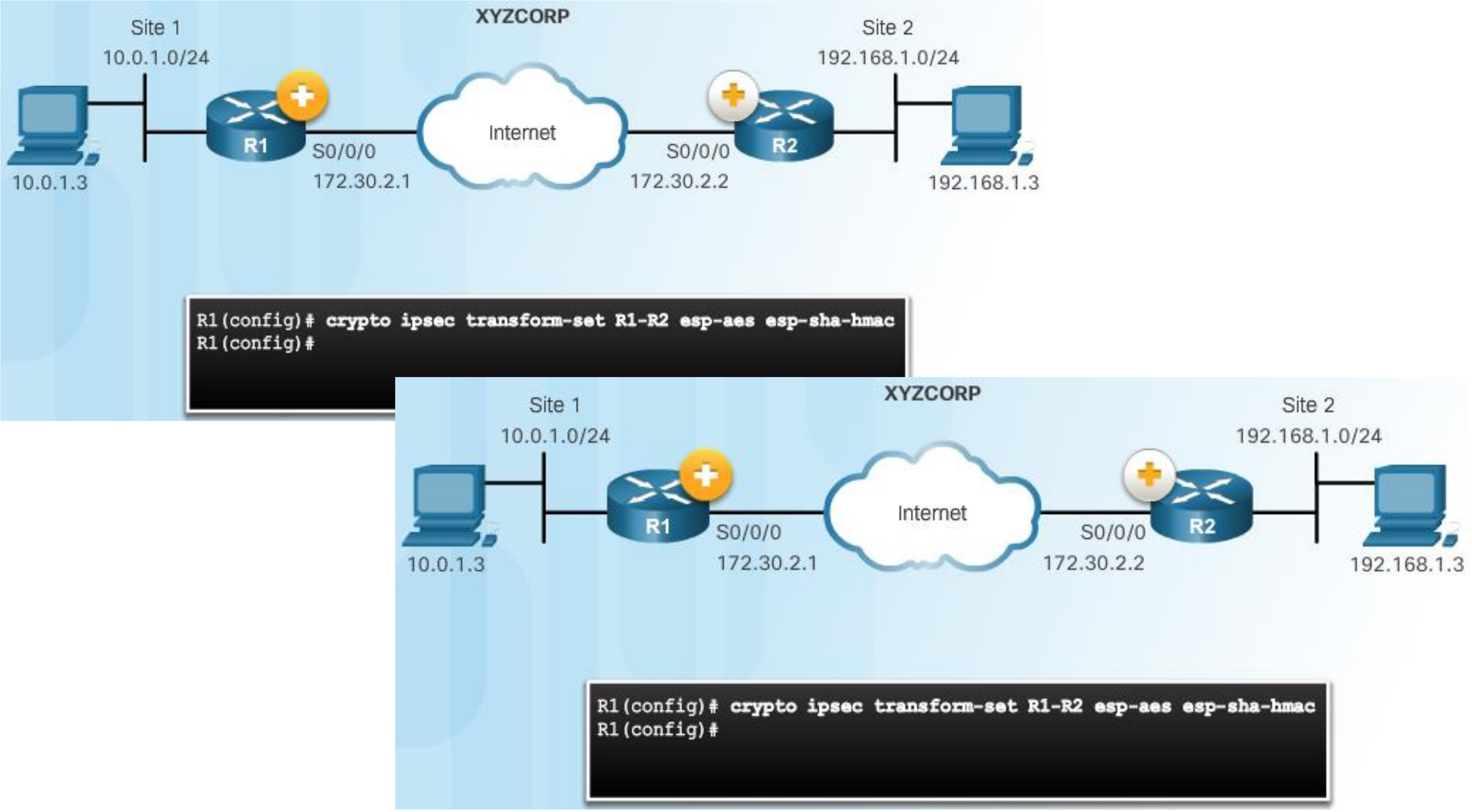




```
R1(config)# crypto ipsec transform-set ?
  WORD  Transform set tag

R1(config)# crypto ipsec transform-set R1-R2 ?
  ah-md5-hmac      AH-HMAC-MD5 transform
  ah-sha-hmac      AH-HMAC-SHA transform
  ah-sha256-hmac   AH-HMAC-SHA256 transform
  ah-sha384-hmac   AH-HMAC-SHA384 transform
  ah-sha512-hmac   AH-HMAC-SHA512 transform
  comp-lzs         IP Compression using the LZS compression algorithm
  esp-3des         ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes          ESP transform using AES cipher
  esp-des          ESP transform using DES cipher (56 bits)
  esp-gcm          ESP transform using GCM cipher
  esp-gmac         ESP transform using GMAC cipher
  esp-md5-hmac     ESP transform using HMAC-MD5 auth
  esp-null         ESP transform w/o cipher
  esp-seal         ESP transform using SEAL cipher (160 bits)
  esp-sha-hmac     ESP transform using HMAC-SHA auth
  esp-sha256-hmac  ESP transform using HMAC-SHA256 auth
  esp-sha384-hmac  ESP transform using HMAC-SHA384 auth
  esp-sha512-hmac  ESP transform using HMAC-SHA512 auth
```

(3) Configure IPsec Transform Set (Cont.)

The `crypto ipsec transform-set` Command

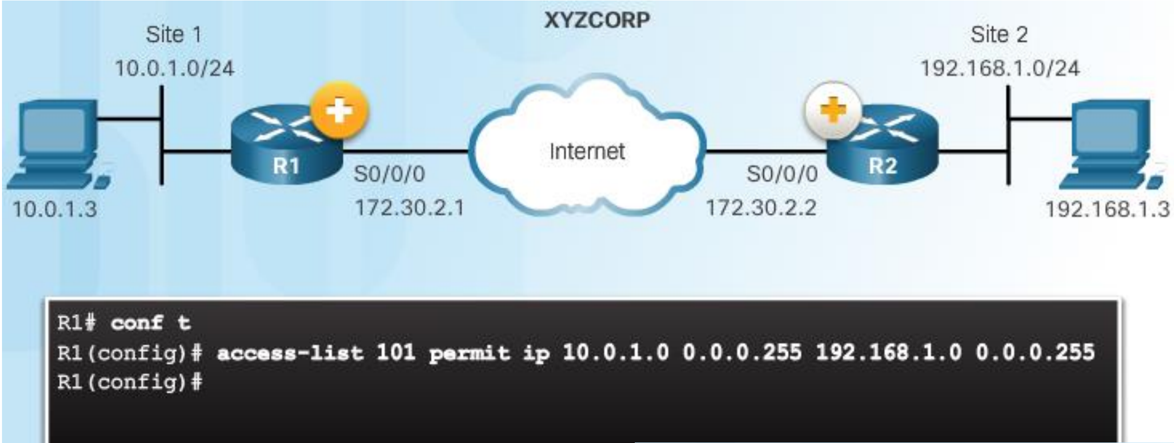


```
R1(config)# crypto ipsec transform-set R1-R2 esp-aes esp-sha-hmac
R1(config)#
```

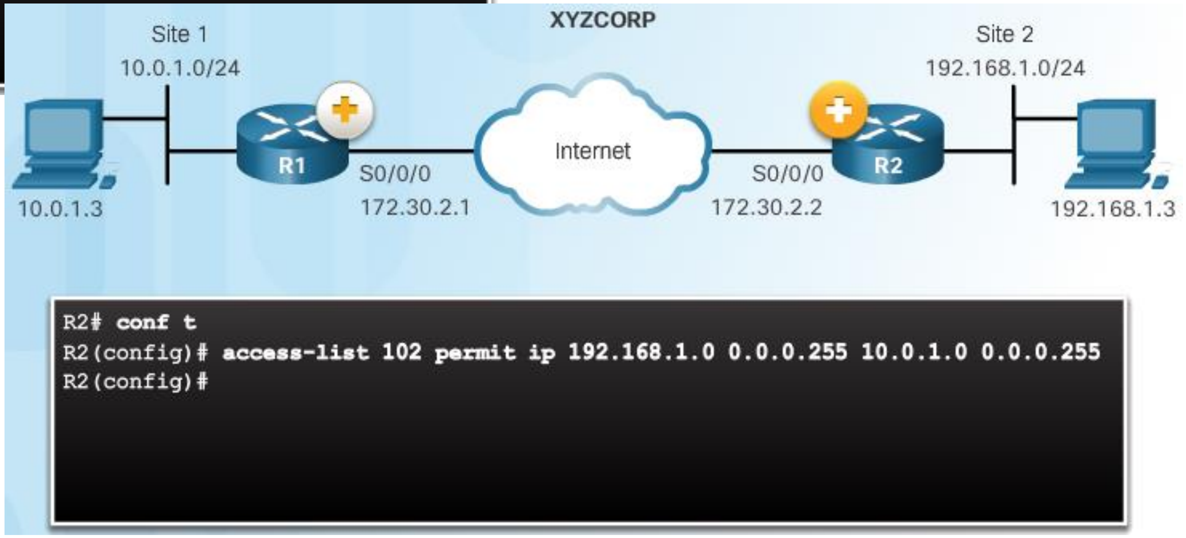
R1(config)# crypto ipsec transform-set R1-R2 esp-aes esp-sha-hmac
R1(config)#

(4) Define Interesting Traffic (Cont.)

Configure an ACL to Define Interesting Traffic



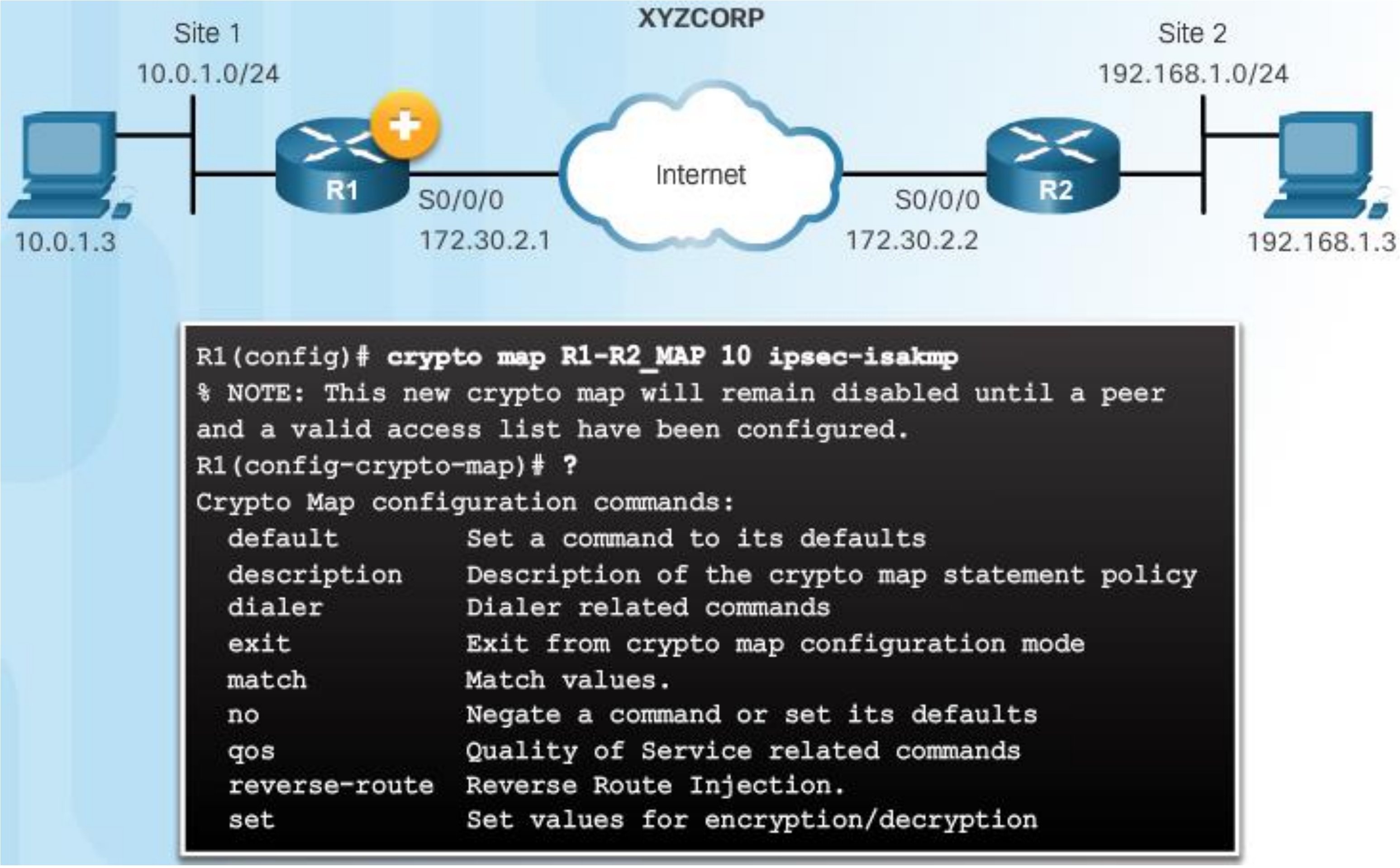
```
R1# conf t
R1(config)# access-list 101 permit ip 10.0.1.0 0.0.0.255 192.168.1.0 0.0.0.255
R1(config)#
```



```
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)#
```

(5) Syntax to Configure a Crypto Map

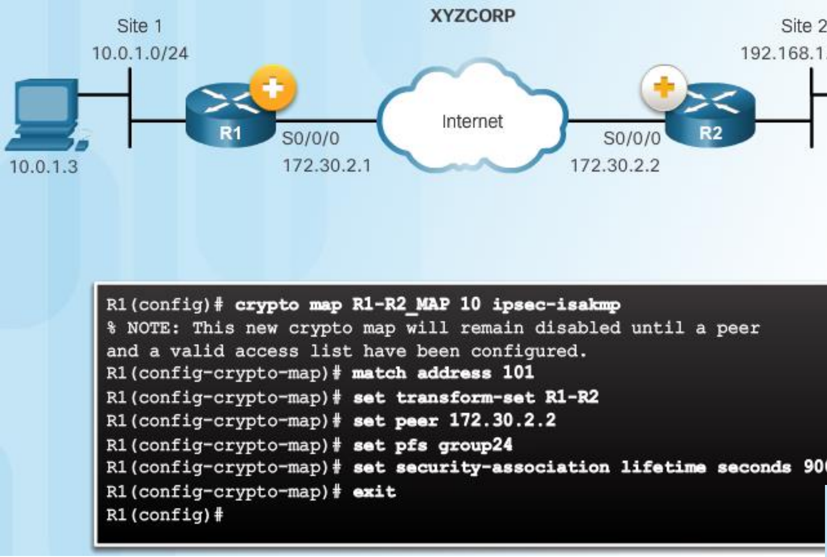
Crypto Map Configuration Commands



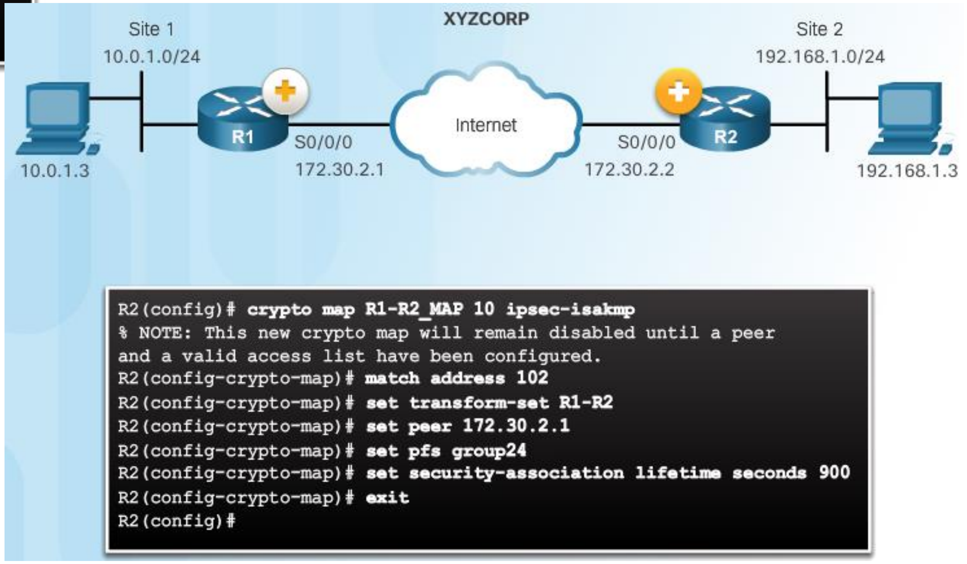
```
R1(config)# crypto map R1-R2_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R1(config-crypto-map)# ?
Crypto Map configuration commands:
  default        Set a command to its defaults
  description    Description of the 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
```

(5) XYZCORP Crypto Map Configuration

Crypto Map Configuration:

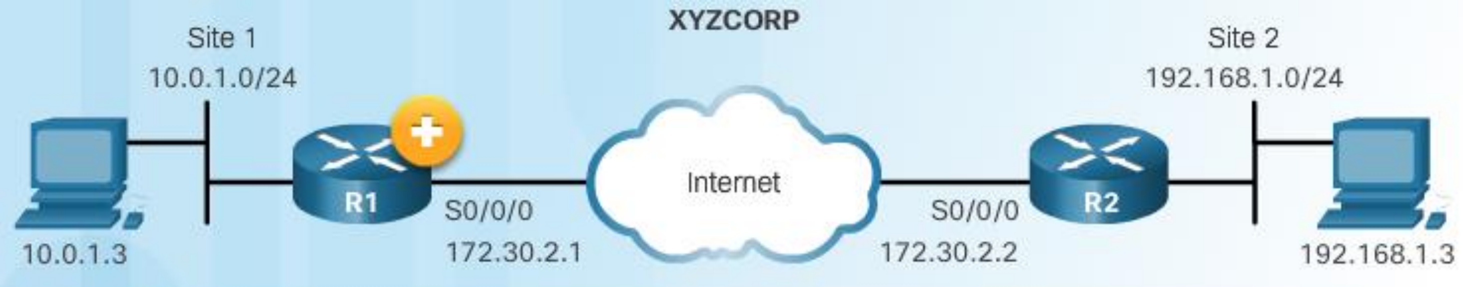


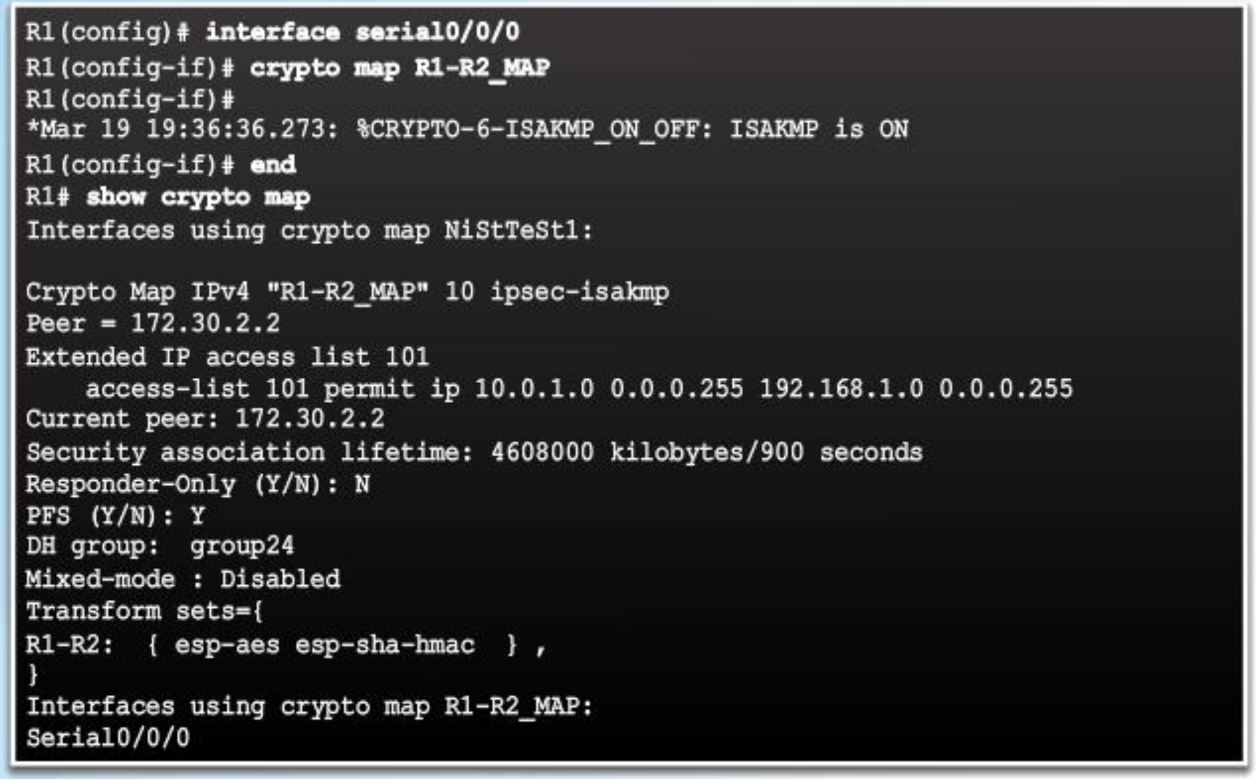
```
R1(config)# crypto map R1-R2_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R1(config-crypto-map)# match address 101
R1(config-crypto-map)# set transform-set R1-R2
R1(config-crypto-map)# set peer 172.30.2.2
R1(config-crypto-map)#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

(6) Apply the Crypto Map

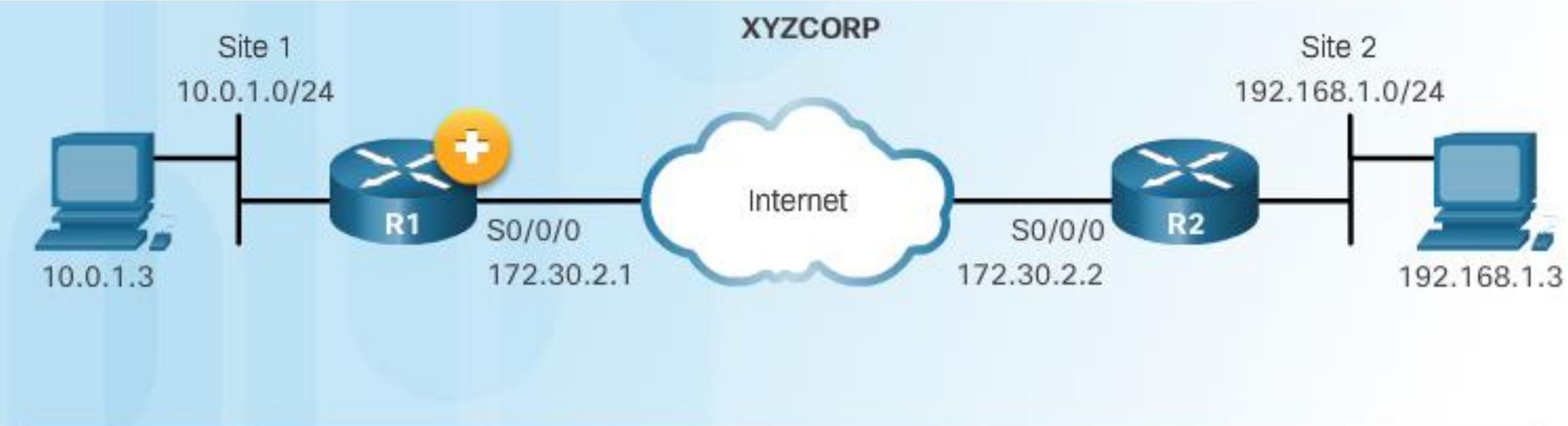


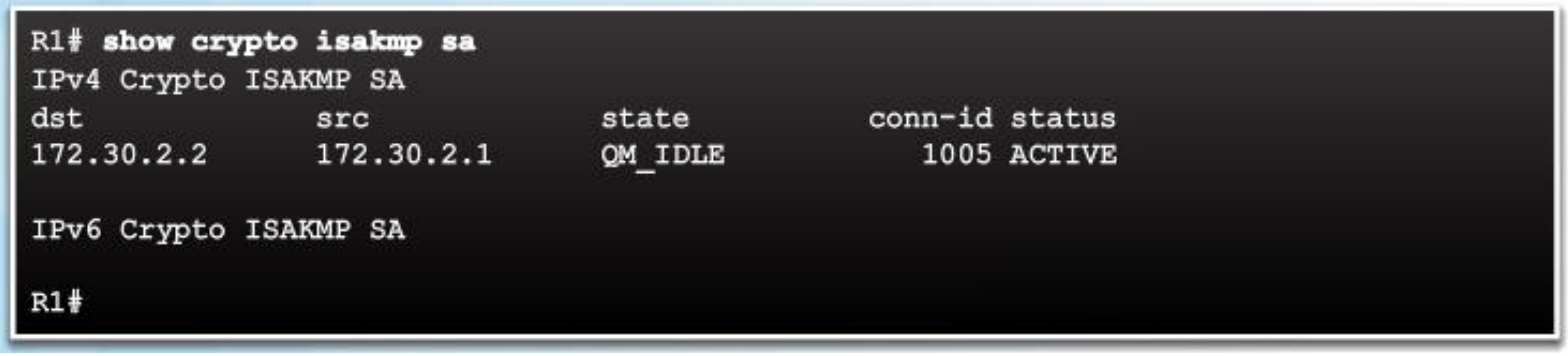


```
R1(config)# interface serial0/0/0
R1(config-if)# crypto map R1-R2_MAP
R1(config-if)#
*Mar 19 19:36:36.273: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)# end
R1# show crypto map
Interfaces using crypto map NiStTeSt1:

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
```

Verify ISAKMP and IPsec Tunnels

Verify the ISAKMP Tunnel is Established

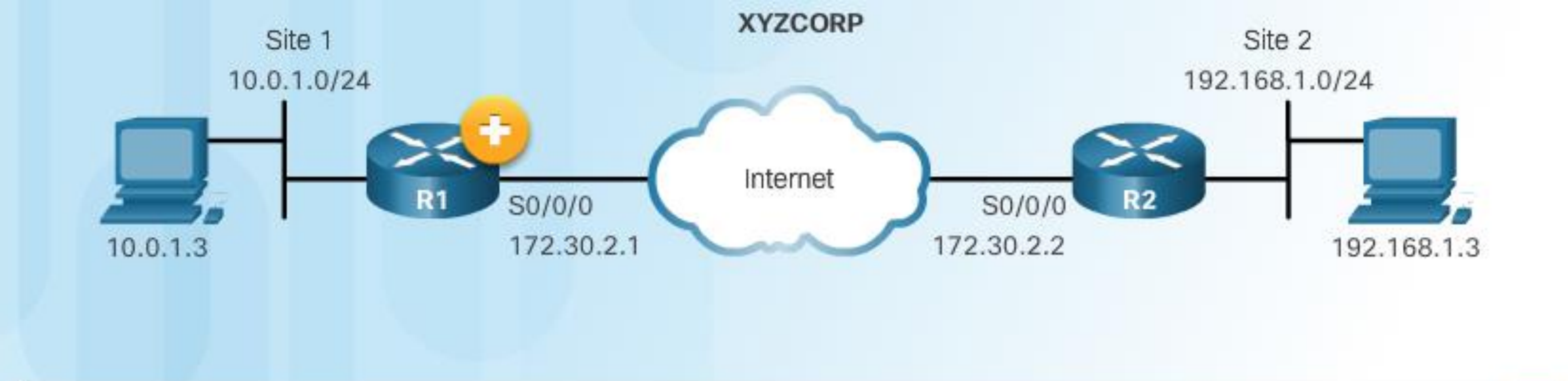


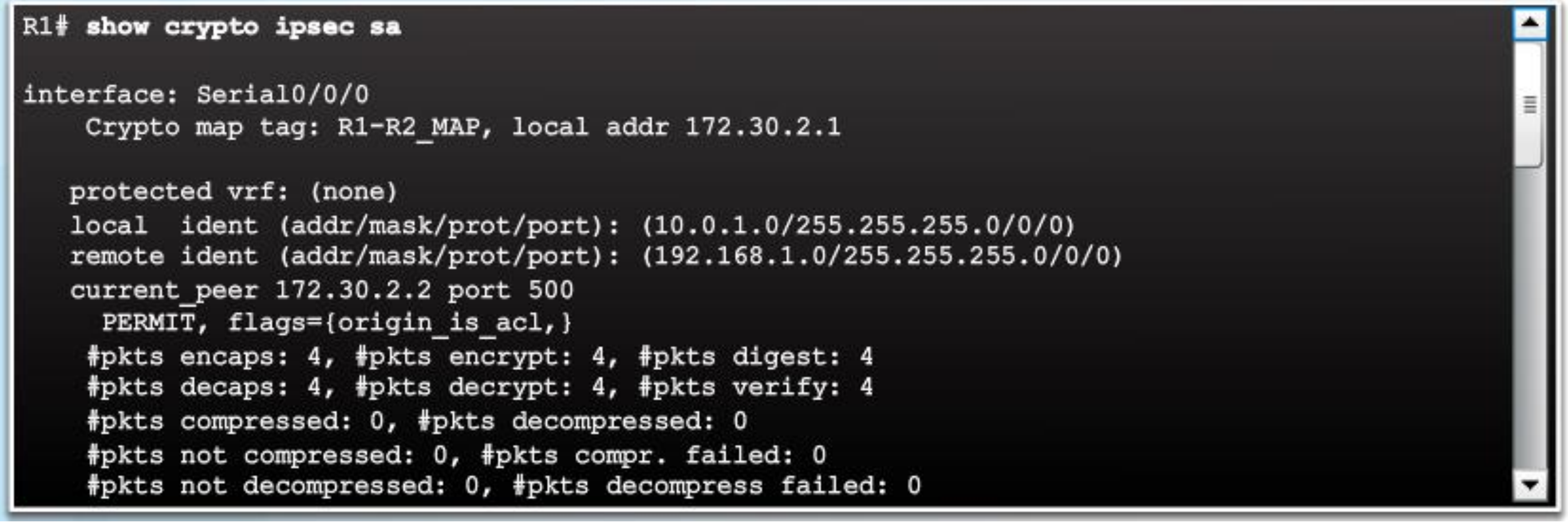


```
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.30.2.2      172.30.2.1      QM_IDLE           1005 ACTIVE

IPv6 Crypto ISAKMP SA

R1#
```

Verify ISAKMP and IPsec Tunnels (Cont.)

Verify the IPsec Tunnel is Established

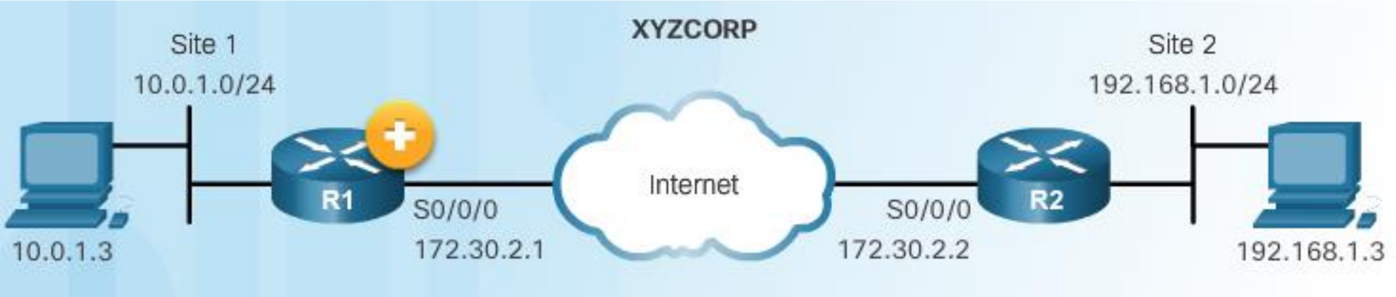


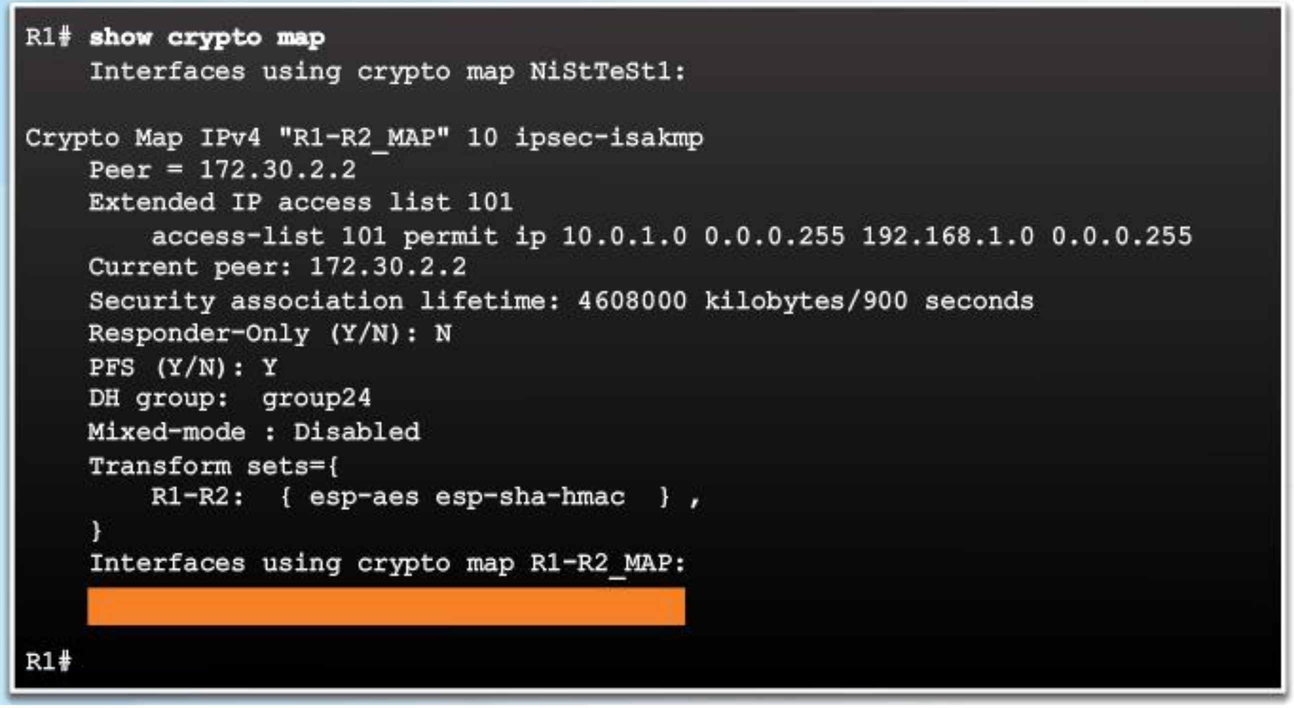


```
R1# show crypto ipsec sa

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
```

XYZCORP Crypto Map Configuration (Cont.)

Crypto Map Configuration:





```
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:
    [redacted]

R1#
```