Cisco Networking Academy
Mind Wide Open

Chapter 8:

Implémenter les réseaux privés virtuels

CCNA Security v2.0

Samir DIABI

Sommaire du chapitre

Introduction

Les VPNs

Composants et opérations des VPNs IPsec

Implémenter les VPNs Site-à-Site IPsec à l'aide de CLI

Résumé

Section 8.1: Les VPNs

À l'issue de cette section, vous devez être en mesure de :

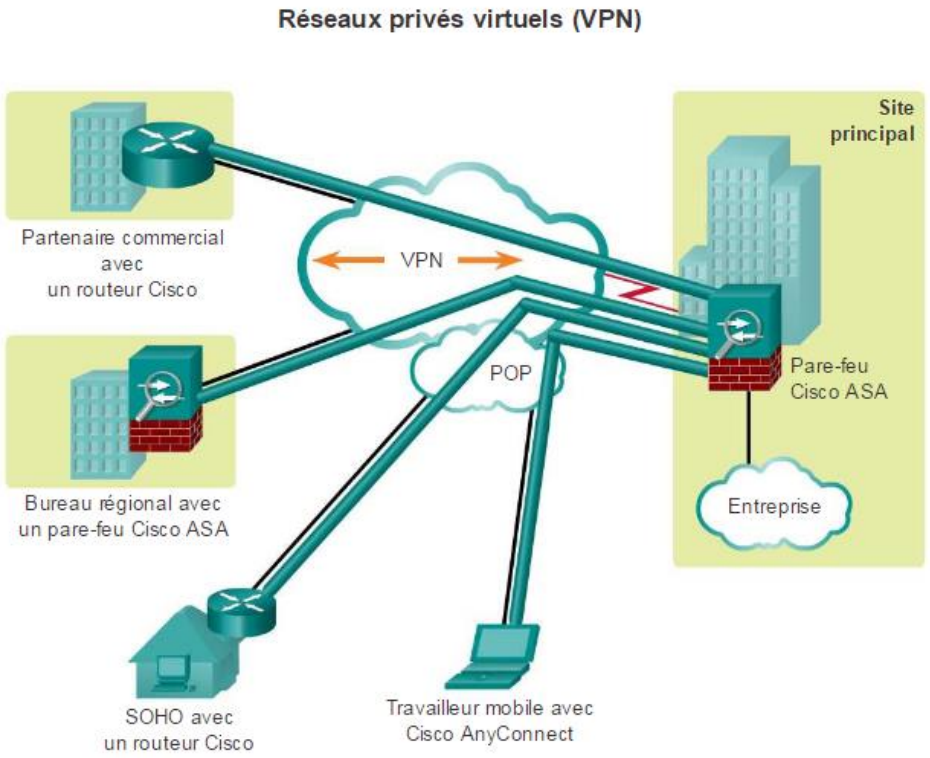
- Décrire les VPNs et leurs avantages.
- Comparer les VPNs site à site et accès distant.

Partie 8.1.1:
Présentation des VPNs

Présentation des VPN

- Les entreprises utilisent des VPN pour créer une connexion sécurisée de bout en bout par réseau privé sur des réseaux tiers, comme Internet ou des extranets.

- Une passerelle VPN est requise pour l'implémentation de VPN. La passerelle VPN peut être un routeur, un pare-feu ou un périphérique Cisco ASA (Adaptive Security Appliance).



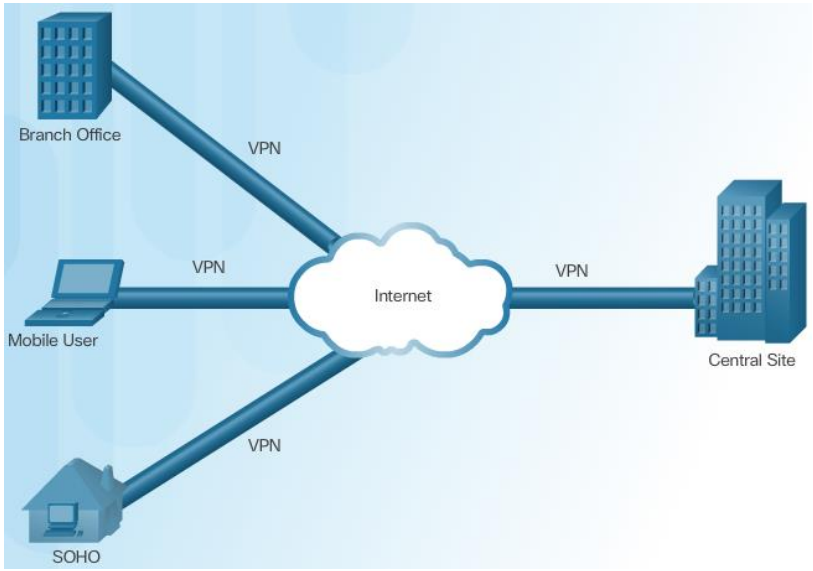
Notions de base des VPN

Avantages des réseaux privés virtuels

- **Réductions des coûts**
  - Les VPN permettent aux entreprises d'utiliser un transport Internet tiers et économique pour la connexion des bureaux et des utilisateurs distants au site principal
- **Évolutivité**
  - Les VPN permettent aux entreprises d'utiliser l'infrastructure d'Internet des FAI et des périphériques, ce qui permet d'ajouter facilement de nouveaux utilisateurs.
- **Compatibilité avec la technologie haut débit**
  - Les VPN permettent aux travailleurs mobiles et aux télétravailleurs de bénéficier d'une connectivité haut débit rapide, comme la technologie DSL et le câble, pour accéder au réseau de leur entreprise, offrant aux travailleurs mobiles flexibilité et efficacité.
  - Les VPN sont également une solution rentable pour connecter des bureaux distants.
- **Sécurité**
  - Les VPN peuvent inclure des mécanismes de sécurité offrant un niveau de sécurité très élevé grâce à l'utilisation de protocoles de chiffrement et d'authentification avancés qui protègent les données de tout accès non autorisé.

Layer 3 IPsec VPNs

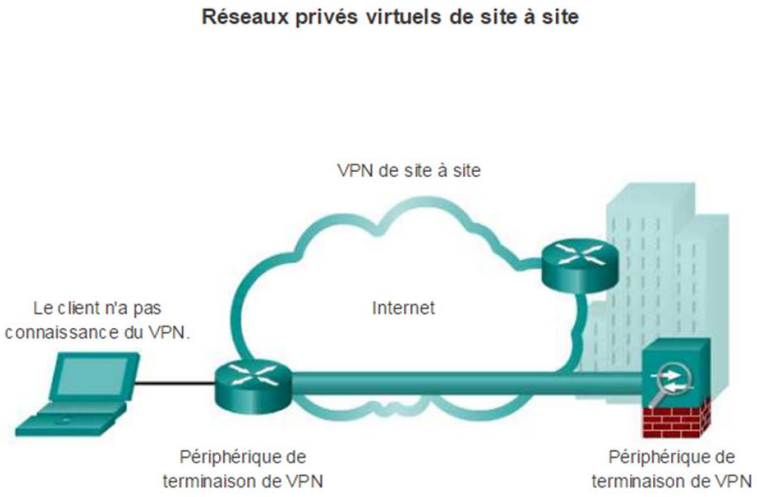
- Les VPNs connectent des éléments finaux, à l'exemple de deux bureaux distants, à travers un réseaux public pour créer une connexion logique.
- La connexion logique peut être établie à base de protocoles de couche 2 ou de couche 3.
- GRE, MPLS et IPsec sont des exemples de protocoles de couche 3.
- IPsec est une suite de protocoles ouverts utilisée pour assurer des services sécurisés sur un réseau IP.



Partie 8.1.2:
Les technologies VPN

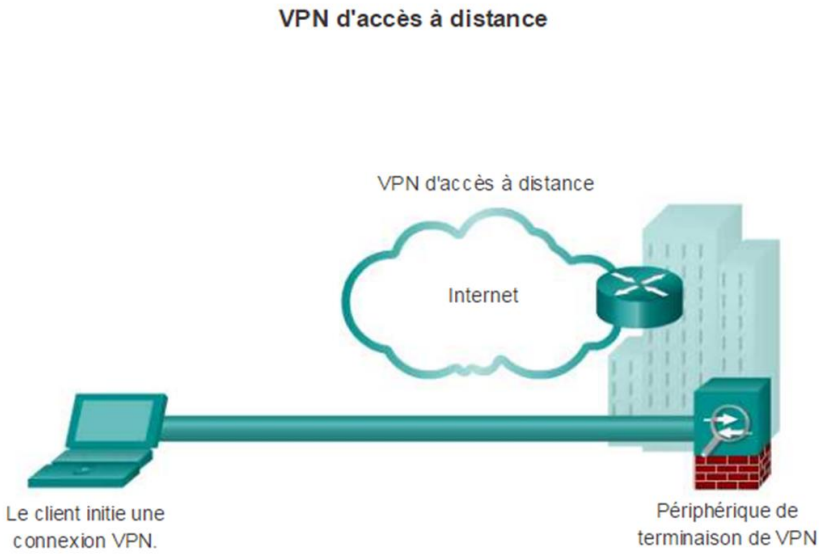
Deux types de VPNs

- Les VPN site à site connectent entre eux des réseaux entiers.
- Les hôtes internes n’ ont pas connaissance qu'un VPN existe.
- Les hôtes finaux envoient et reçoivent le trafic TCP/IP normal par l'intermédiaire d'une « passerelle » VPN.
- La passerelle VPN est responsable de l'encapsulation et du chiffrement de la totalité du trafic sortant issu d'un site spécifique.
- La passerelle VPN envoie ensuite ce trafic sur Internet par le biais d'un tunnel VPN jusqu'à une passerelle VPN homologue au niveau du site cible.
- Lors de la réception, la passerelle VPN homologue élimine les en-têtes, déchiffre le contenu et relaie le paquet vers l'hôte cible au sein de son réseau privé.



Deux types de VPNs

- Prend en charge les besoins en matière de télétravailleurs, d'utilisateurs mobiles, d'extranet et de trafic entre les clients et les entreprises.
- Prend en charge une architecture client-serveur, dans laquelle le client VPN (hôte distant) obtient un accès sécurisé au réseau de l'entreprise par l'intermédiaire d'un serveur VPN à la périphérie.
- Utilisé pour la connexion d'hôtes individuels devant accéder en toute sécurité au réseau de leur entreprise via Internet.
- Un logiciel client VPN doit être installé sur le périphérique final de l'utilisateur mobile.
- Lorsque l'hôte tente d'envoyer du trafic, le logiciel Client VPN encapsule et chiffre ce trafic. Les données chiffrées sont ensuite envoyées via Internet vers la passerelle VPN située à la périphérie du réseau cible.



Section 8.2: Composants et operations de VPN IPsec

À l’issue de ce section, vous devez être en mesure de :

- Décrire le protocole IPsec et ses fonctions basiques.
- Comparer les protocoles AH et ESP
- Décrire le protocole IKE

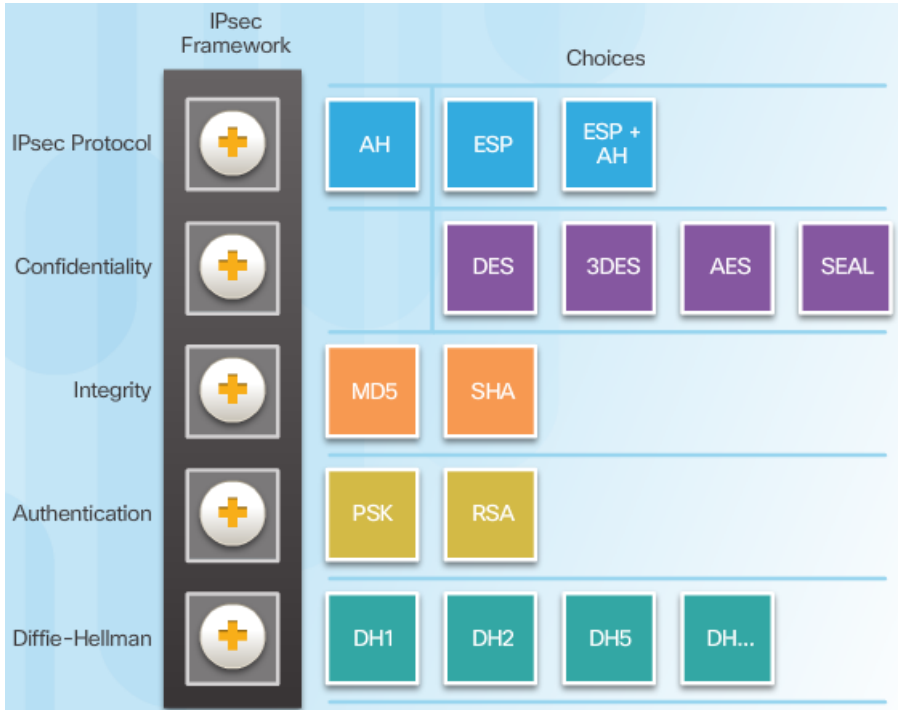
Topic 8.2.1:
Introduction à IPsec

Fonctions IPsec

- Définit comment un VPN peut être configuré de manière sécurisée à l'aide du protocole Internet (IP).
- IPsec est un cadre de standards ouverts qui compose en toutes lettres les règles pour des communications sécurisées.
- N'est lié à aucun algorithme de chiffrement, d'authentification et de sécurité spécifique, ni à aucune technologie d'utilisation de clés.
- Le protocole IPsec se base sur des algorithmes existants pour mettre en œuvre des communications sécurisées..
- Fonctionne au niveau de la couche réseau, en protégeant et en authentifiant les paquets IP entre les équipements IPsec participants (homologues).
- Sécurise un chemin entre une paire de passerelles, une paire d'hôtes ou une passerelle et un hôte.
- Les implémentations du protocole IPsec possèdent un en-tête de couche 3 en texte clair, et ce, afin d'éviter tout problème de routage.
- Fonctionne sur l'ensemble des protocoles de couche 2, tels qu'Ethernet, ATM ou Frame Relay.

Les caractéristiques du protocole IPsec

- Les caractéristiques du protocole IPsec peuvent se résumer comme suit :
  - Le protocole IPsec est un cadre de normes ouvertes qui est indépendant de l'algorithme.
  - Le protocole IPsec permet la confidentialité, l'intégrité et l'authentification de la source des données.
  - IPsec agit comme la couche réseau, qui protège et authentifie les paquets IP.



Services de sécurité IPsec

- Confidentialité (chiffrement) – chiffre les données avant de les transmettre à travers le réseau
- Intégrité des données – il vérifie que ces données n'ont pas été modifiées durant leur transfert, Si une quelconque altération est détectée, le paquet est supprimé.
- Authentification – vérifie l'identité de la source des données envoyées, garantit que la connexion est réalisée avec le partenaire de communication souhaité, IPsec utilise le mécanisme IKE (Internet Key Exchange) pour authentifier les utilisateurs et les périphériques qui peuvent effectuer des communications indépendantes.
- Protection anti-rejeu – détecte et rejete des paquets rediffusés, ce qui contribue à empêcher l'usurpation

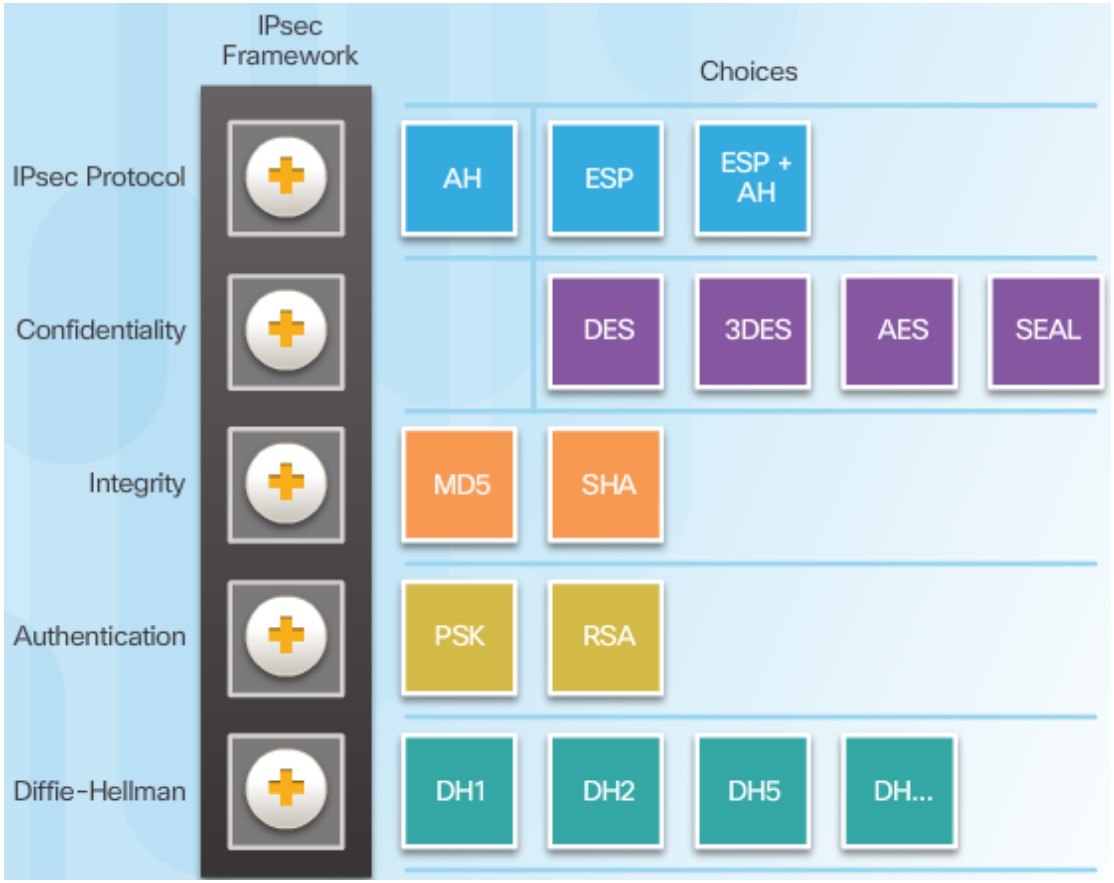
- CIA: Confidentialité, Intégrité et Authentification

Technologies IPsec

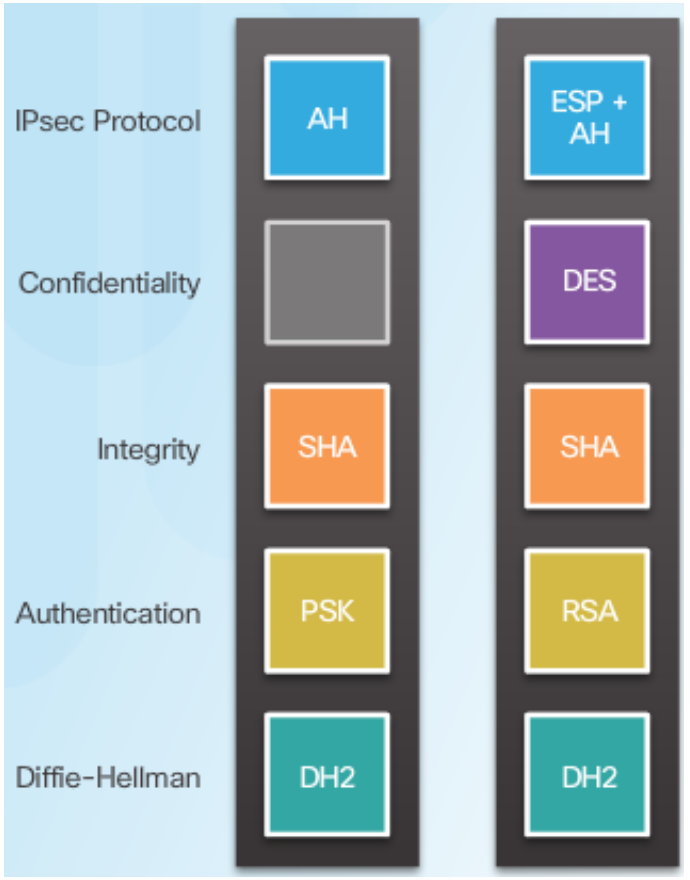
- IPsec est un standard IETF (RFC 2401-2412) qui définit comment un VPN peut être sécurisé à travers un réseau IP.
- IPsec protège et authentifie les paquets IP entre la source et la destination.
- IPsec peut virtuellement protéger tout trafic de la couche 4 jusqu'à la couche 7.
- En utilisant le framework IPsec , on bénéficie des fonctions de sécurité suivantes :
  - Confidentialité à base du cryptage.
  - Intégrité à base du hashage
  - L'authentification en utilisant Internet Key Exchange (IKE)
  - Sécuriser l'échange de clés avec l'utilisation de Diffie-Hellman DH

IPsec Technologies

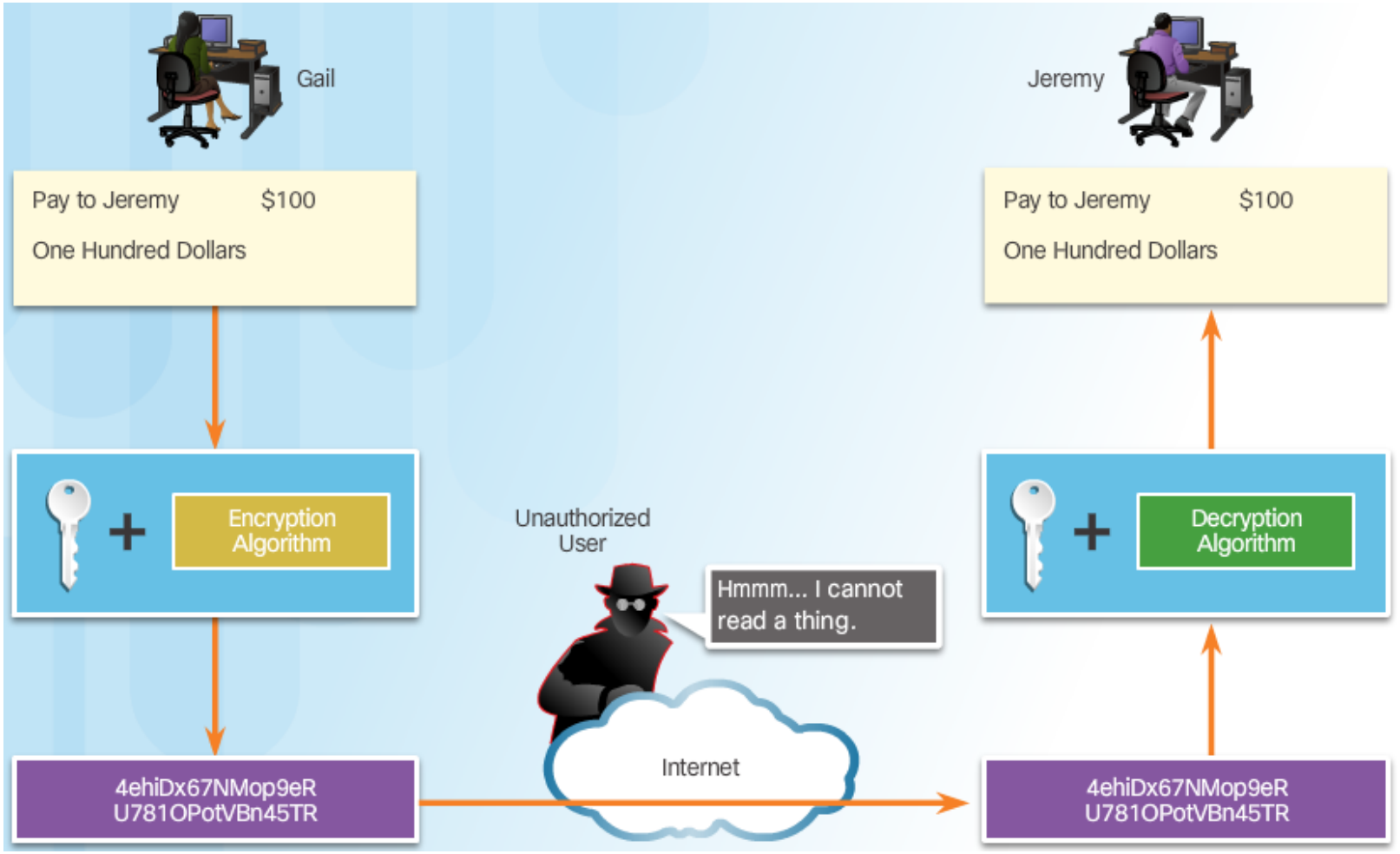
IPsec Framework



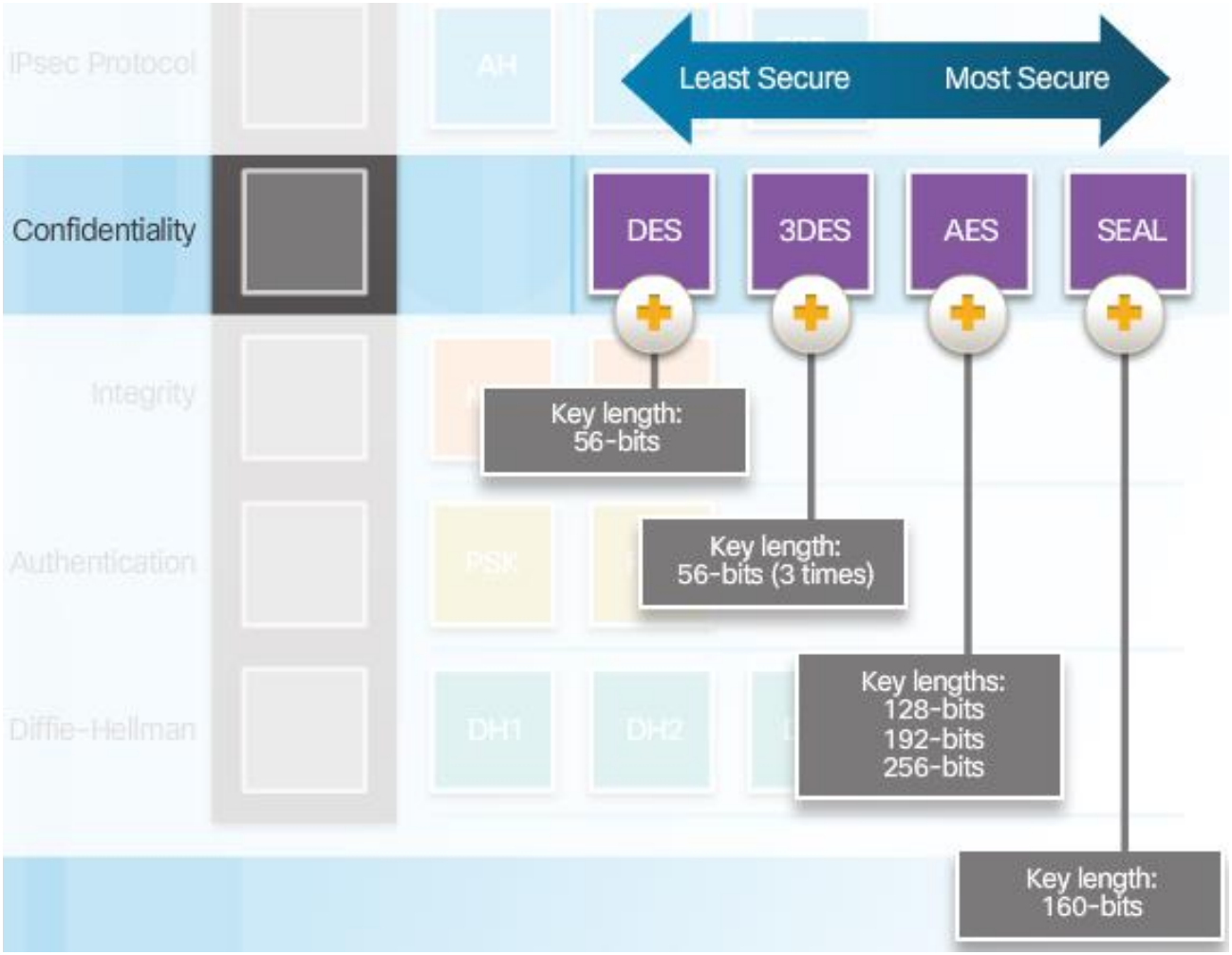
IPsec Implementation Examples



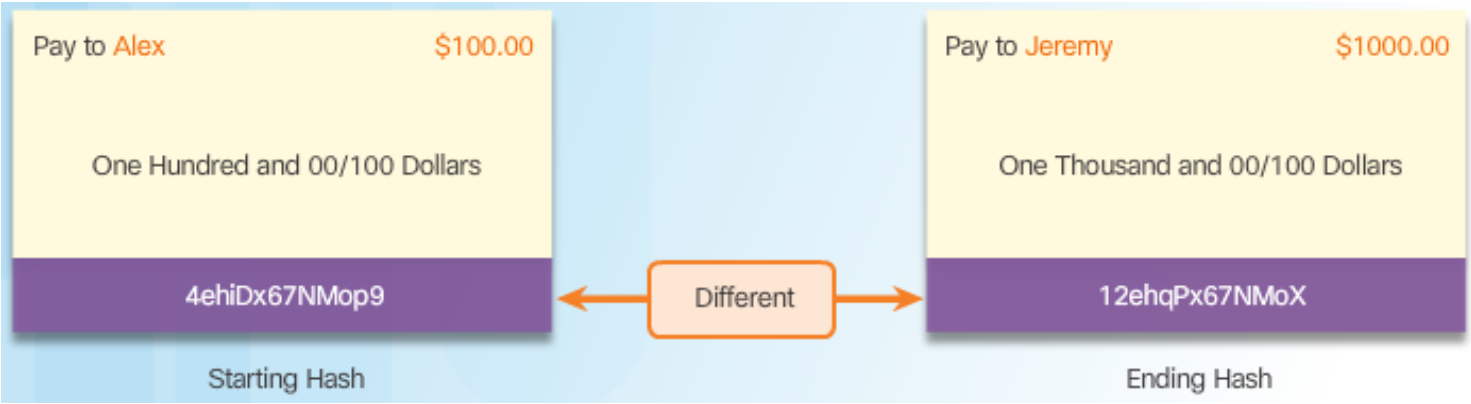
La confidentialité

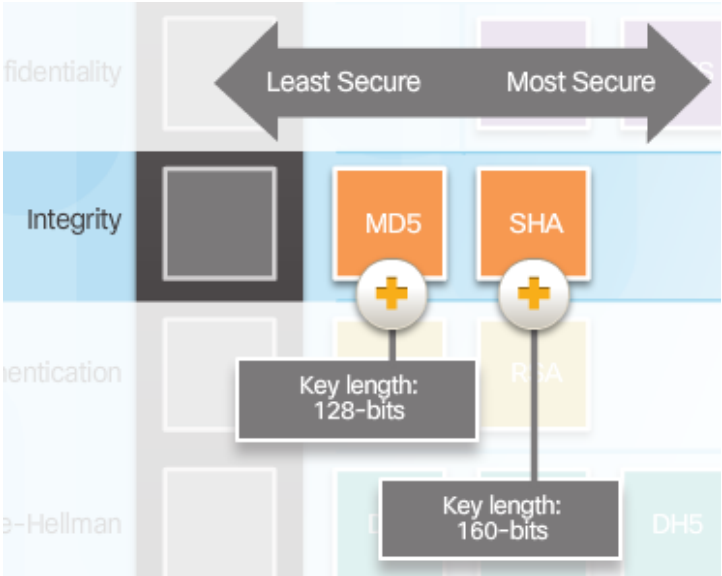


La confidentialité (Suite)

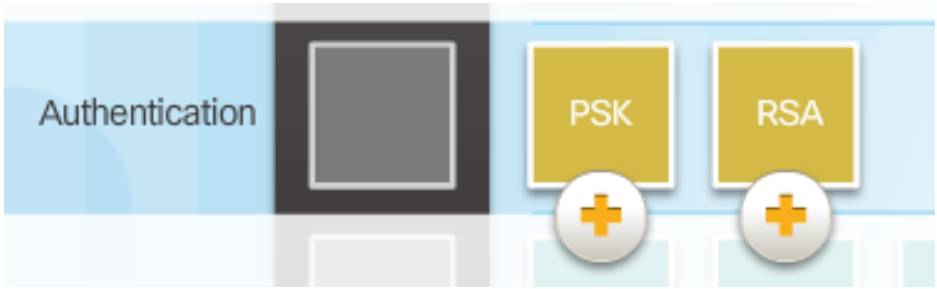


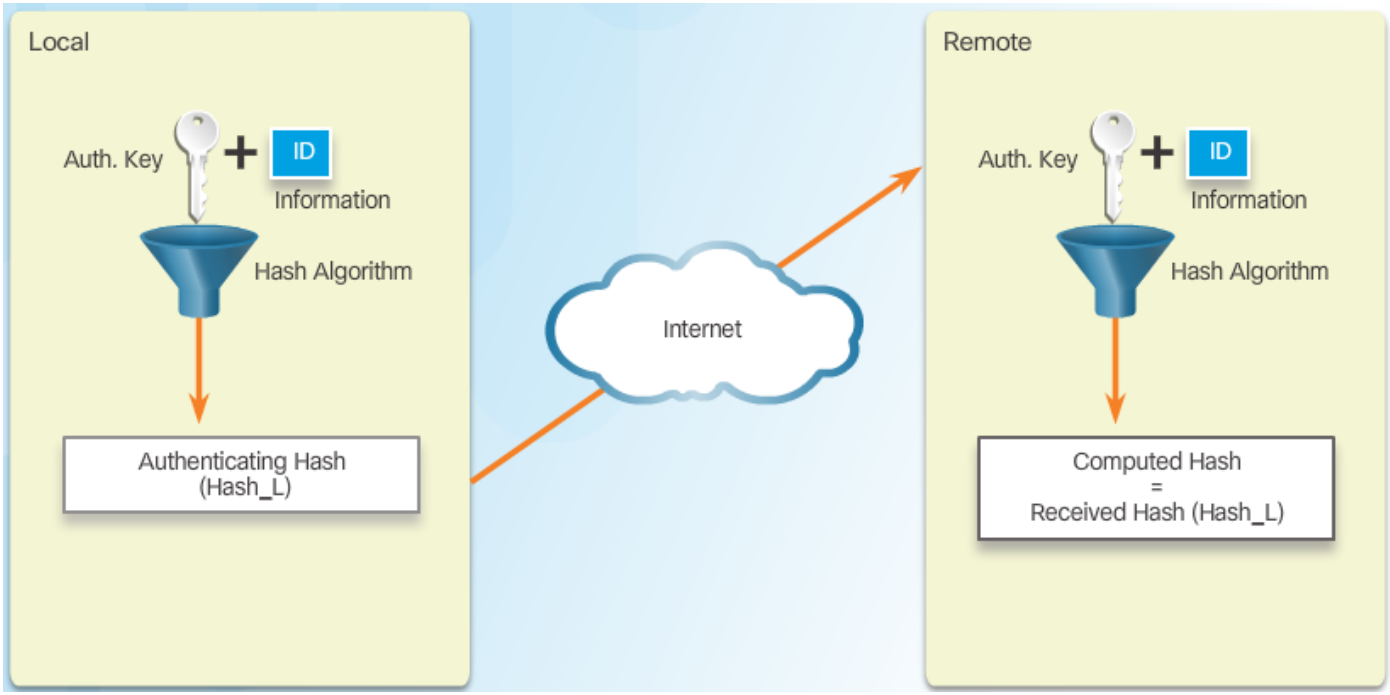
L’intégrité



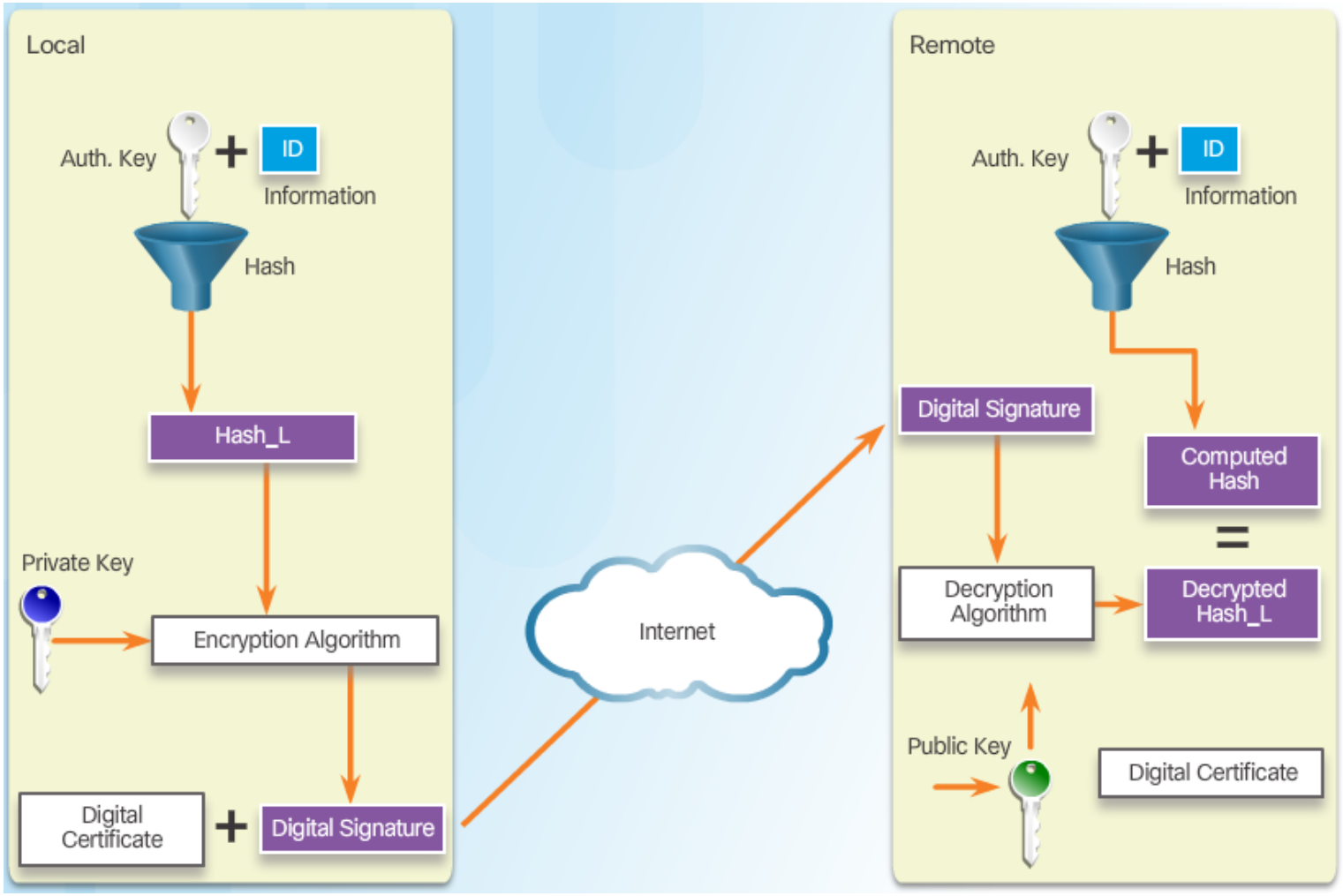


L’authentification

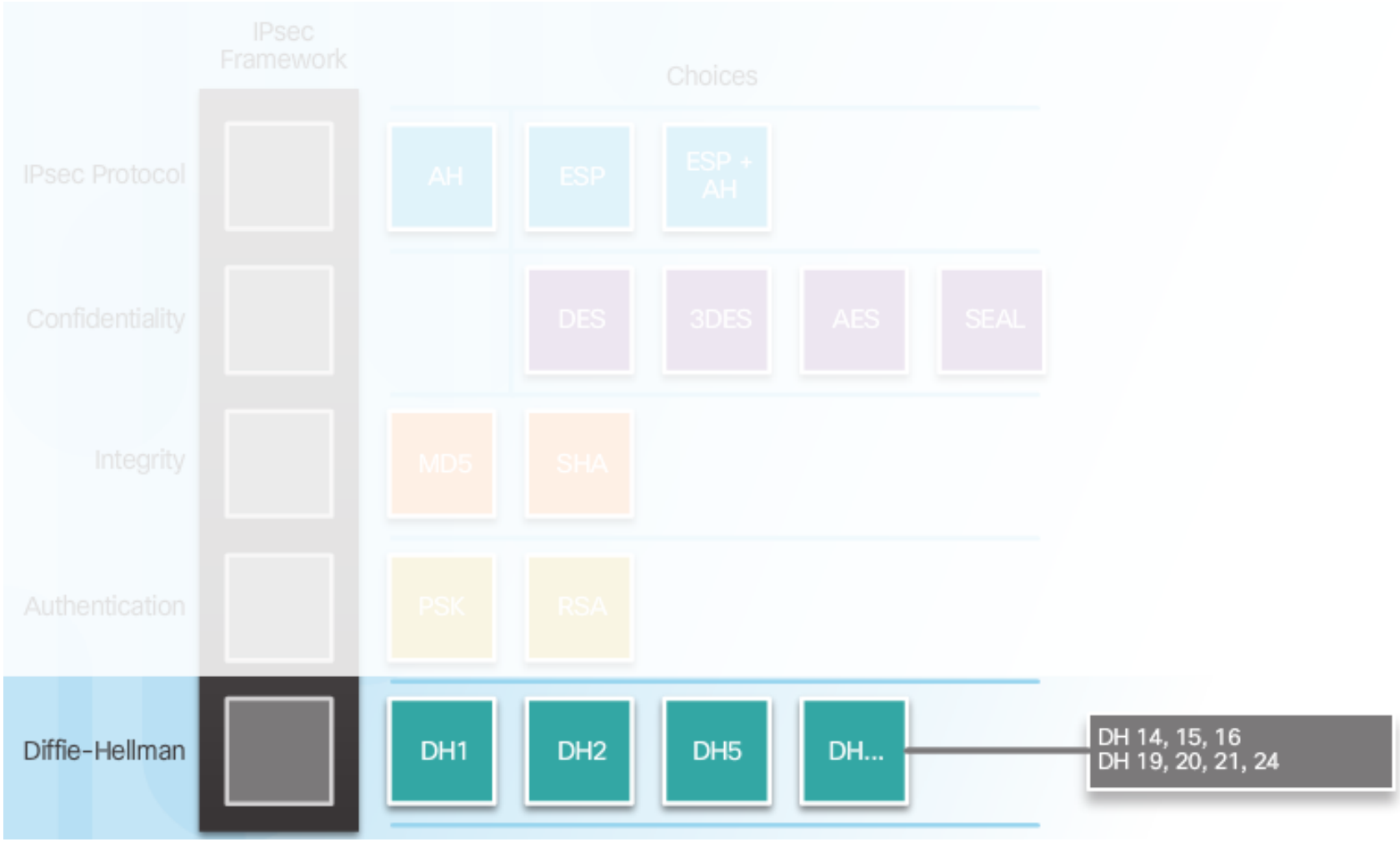




L’authentification (Suite)

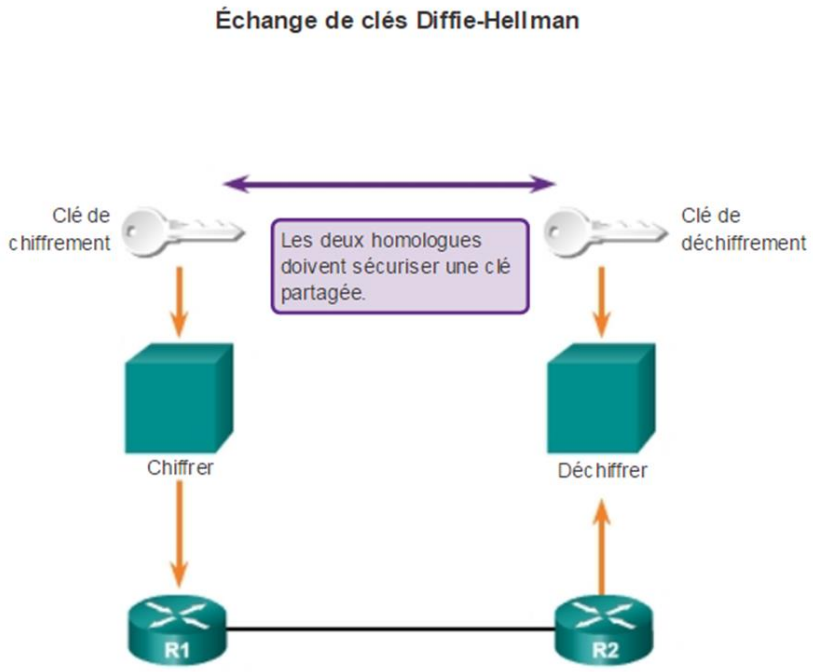


Échange sécurisé de clé



Échange de clés Diffie-Hellman

- L'algorithme DH (Diffie-Hellman) est une méthode d'échange sécurisé des clés utilisées pour chiffrer des données.
- L'algorithme DH spécifie une méthode d'échange de clé publique qui permet à deux homologues d'établir une clé secrète partagée qu'ils sont les seuls à connaître, bien qu'ils communiquent sur un canal non sécurisé.
- Le système DH fait aujourd'hui partie de la norme IPsec.
- Les algorithmes de chiffrement tels que DES, 3DES et AES, ainsi que les algorithmes de hachage MD5 et SHA-1 nécessitent une clé secrète partagée.

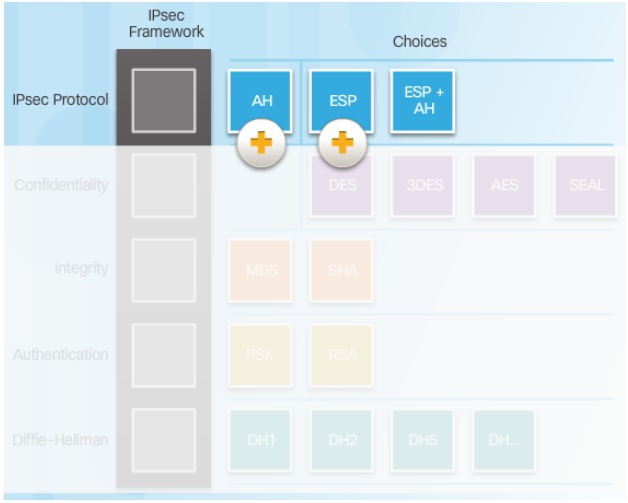


Les groupes Diffie-Helman

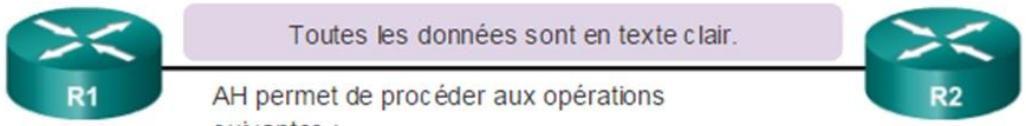
Diffie-Hellman Group	Description
Diffie-Hellman Group 1	768-bit group
Diffie-Hellman Group 2	1024-bit group
Diffie-Hellman Group 5	1536-bit group
Diffie-Hellman Group 14	2048-bit group
Diffie-Hellman Group 15	3072-bit group
Diffie-Hellman Group 19	256-bit elliptic curve group
Diffie-Hellman Group 20	384-bit elliptic curve group
Diffie-Hellman Group 21	521-bit elliptic curve group
Diffie-Hellman Group 24	2048-bit, 256 bit subgroup

Topic 8.2.2:
Les protocoles IPsec

Vue sur le protocole IPsec



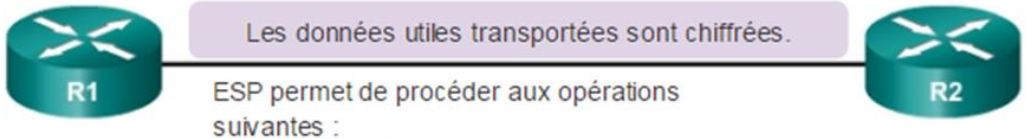
En-tête d'authentification



AH permet de procéder aux opérations suivantes :

- Authentification
- Intégrité

Encapsulation Security Payload

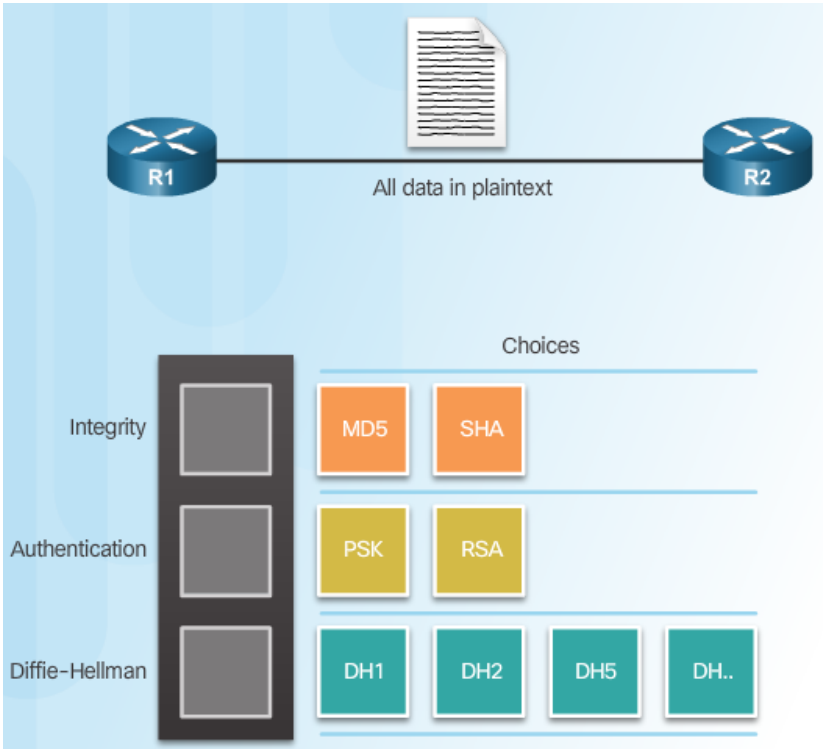


ESP permet de procéder aux opérations suivantes :

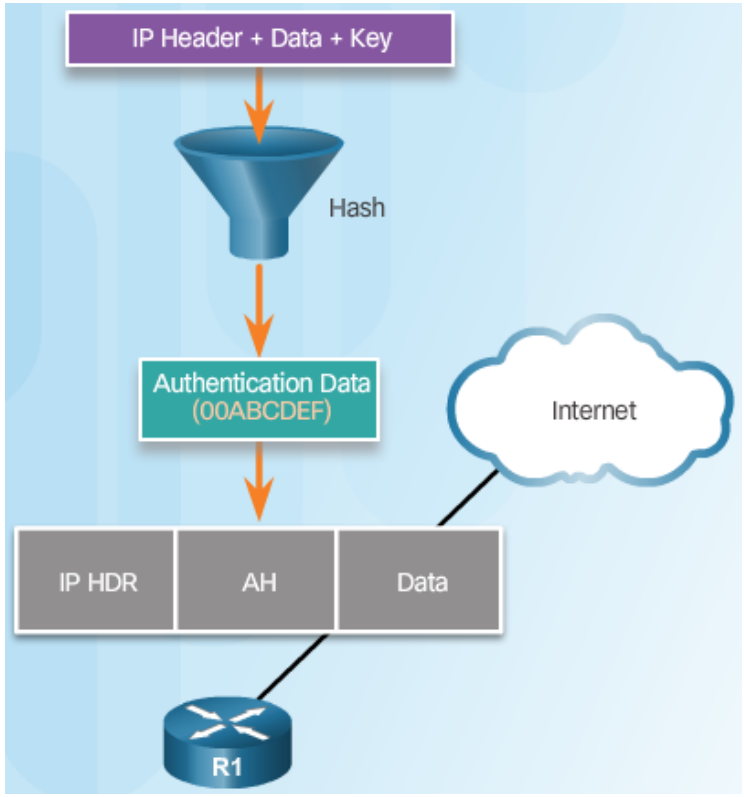
- Chiffrement
- Authentification
- Intégrité

Authentication Header (AH)

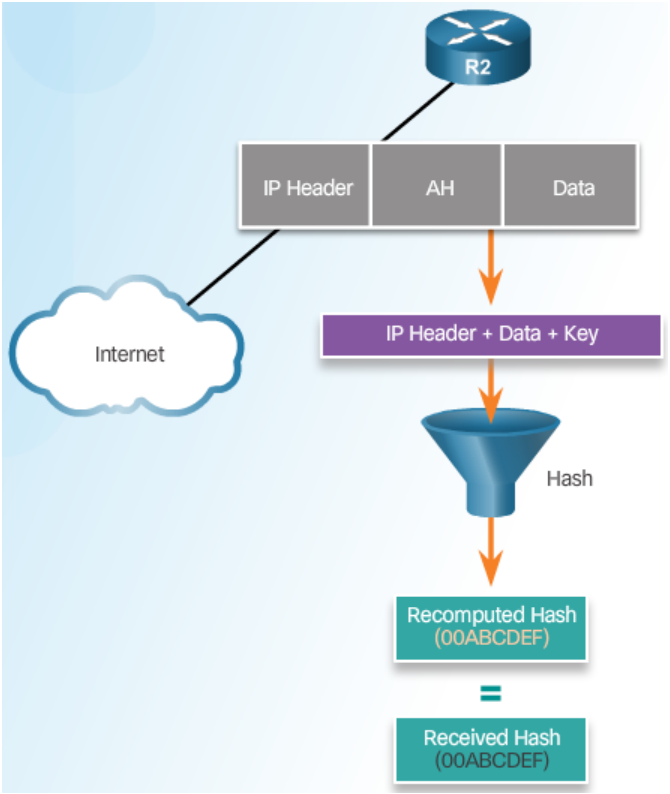
- En-tête d'authentification Protocole approprié à utiliser lorsque la confidentialité n'est pas requise ou autorisée.
- Permet l'authentification et l'intégrité des données des paquets IP qui sont transmis entre deux systèmes.
- Ne permet pas la confidentialité des données (chiffrement) des paquets.



Authentication Header (Cont.)



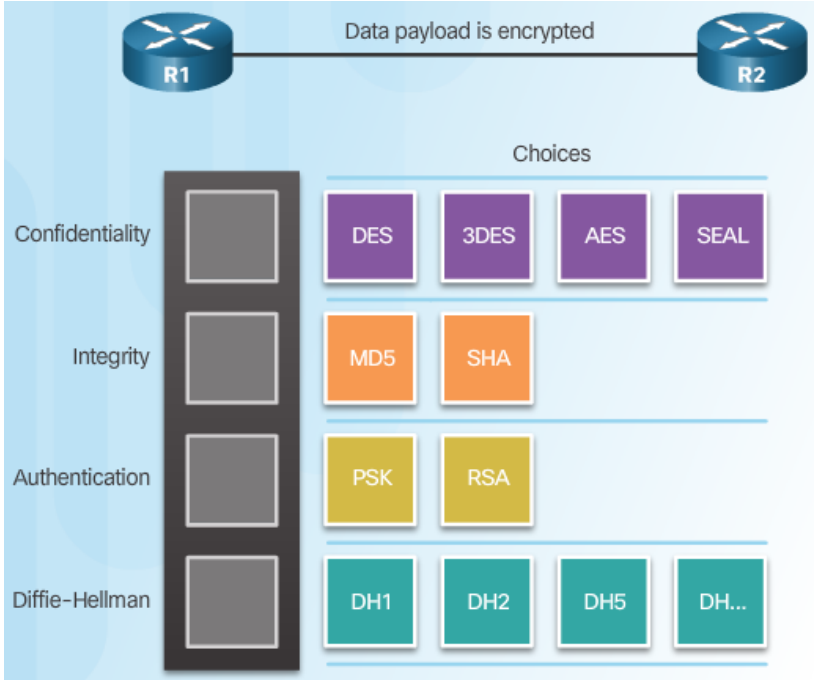
R1 génère un hash et le transmet à R2



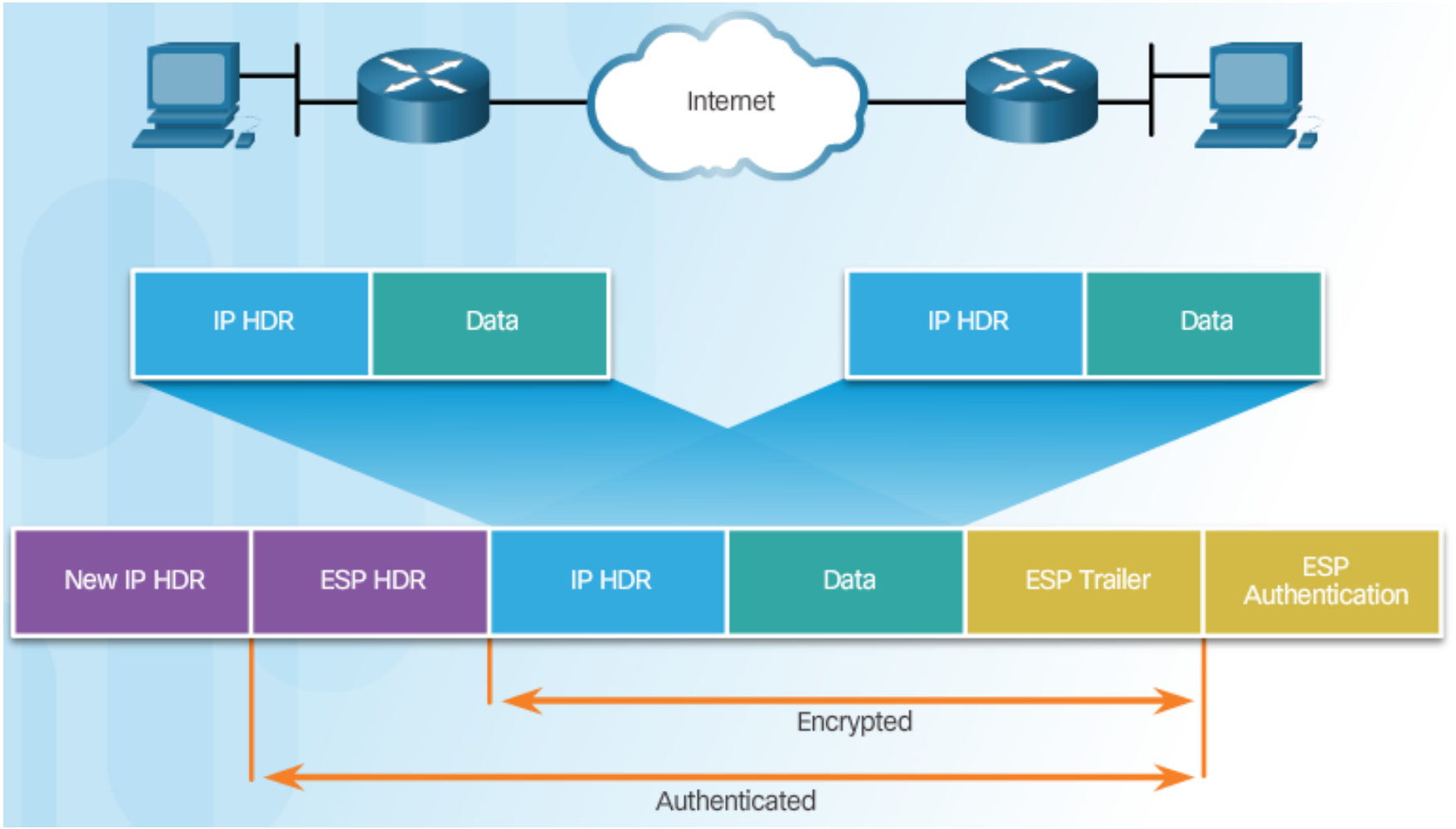
R2 recalcule le hash et le compare à celui reçu

ESP (Encapsulating Security Payload)

- Protocole de sécurité permettant la confidentialité et l'authentification grâce au chiffrement du paquet IP.
- ESP authentifie le paquet IP interne et l'en-tête ESP.
- Le hashage et l'authentification sont facultatives dans ESP, au minimum, l'un d'eux doit être sélectionné.

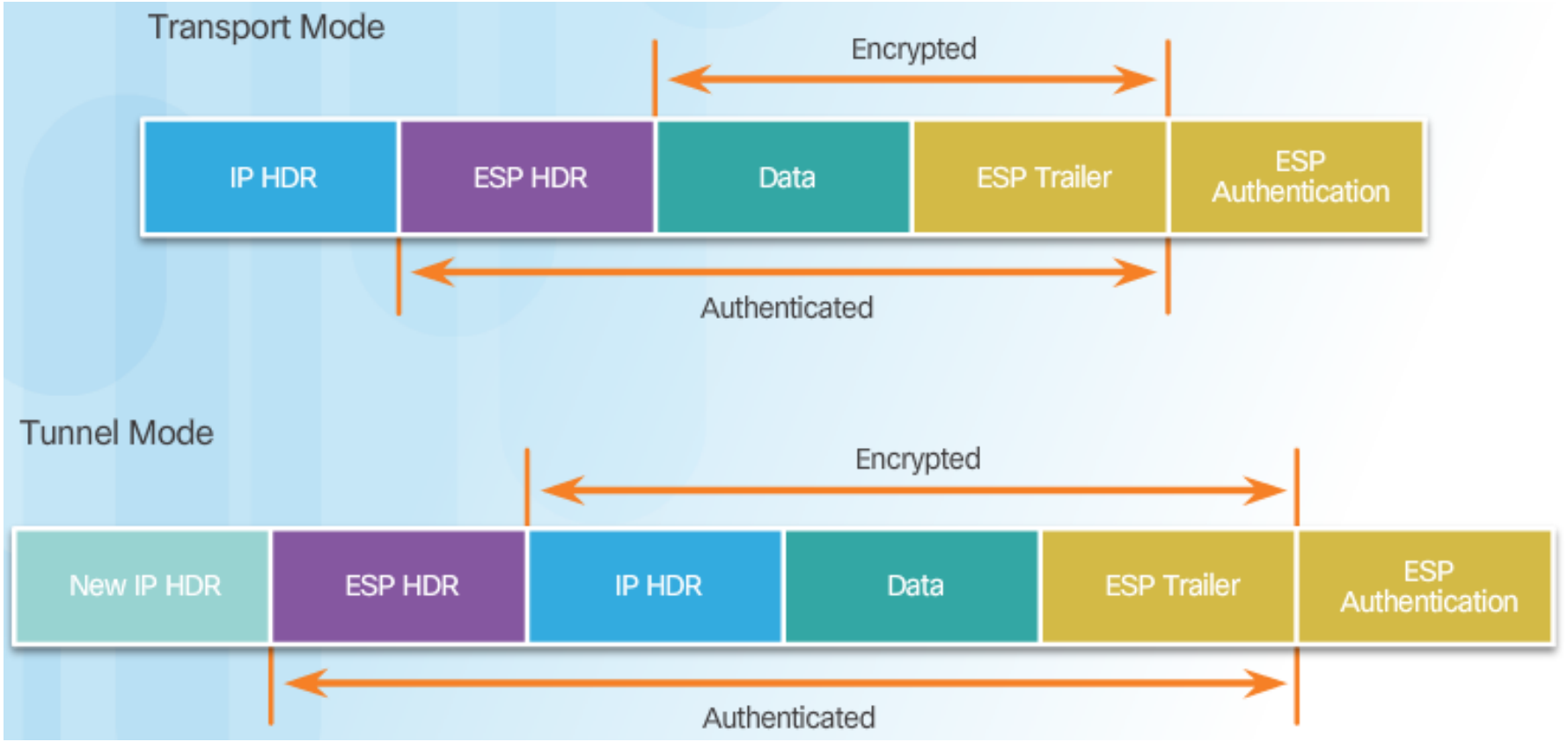


ESP crypte et authentifie



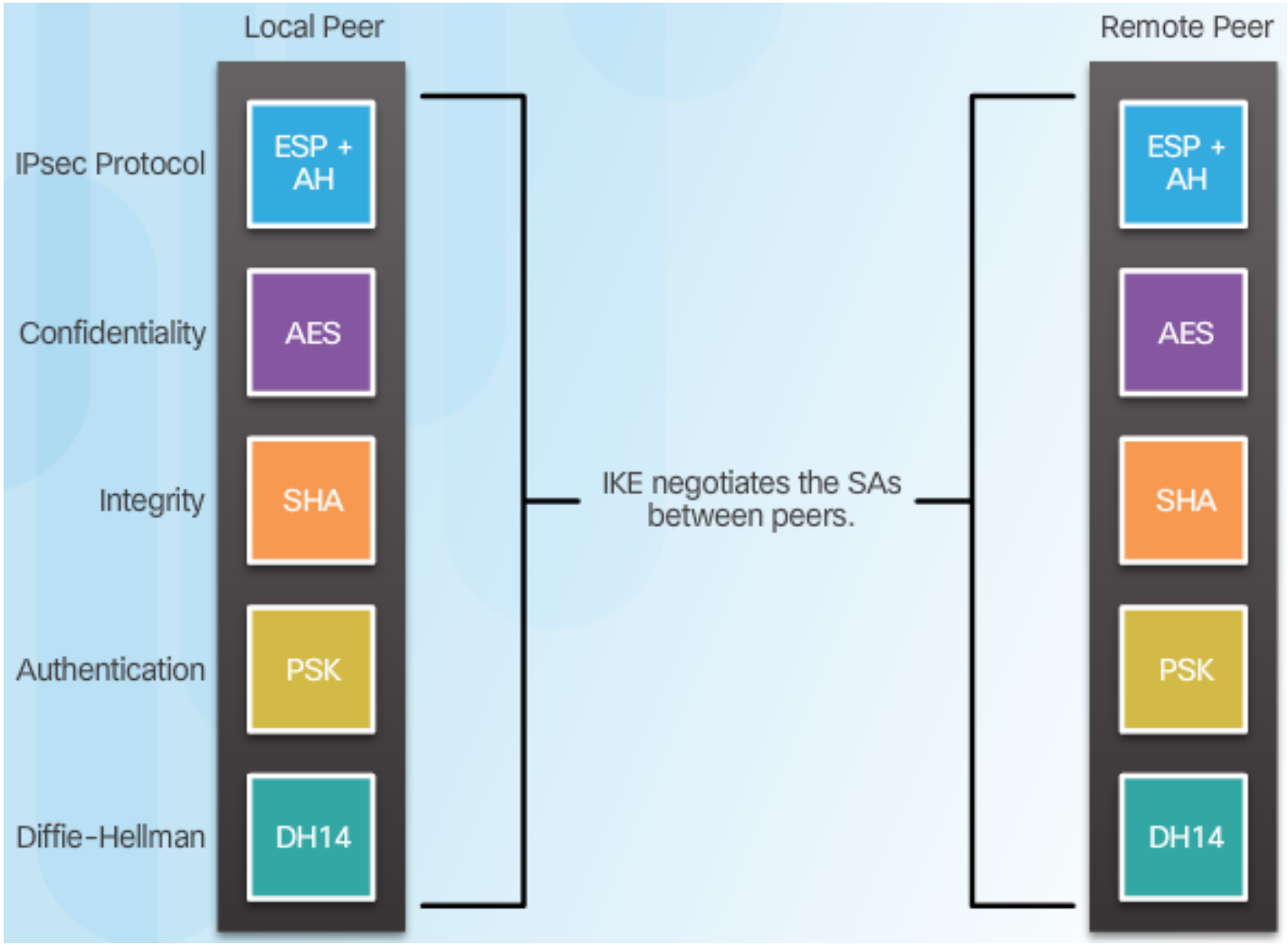
Les modes ESP : Transport ou Tunnel

Apply ESP and AH in Two Modes

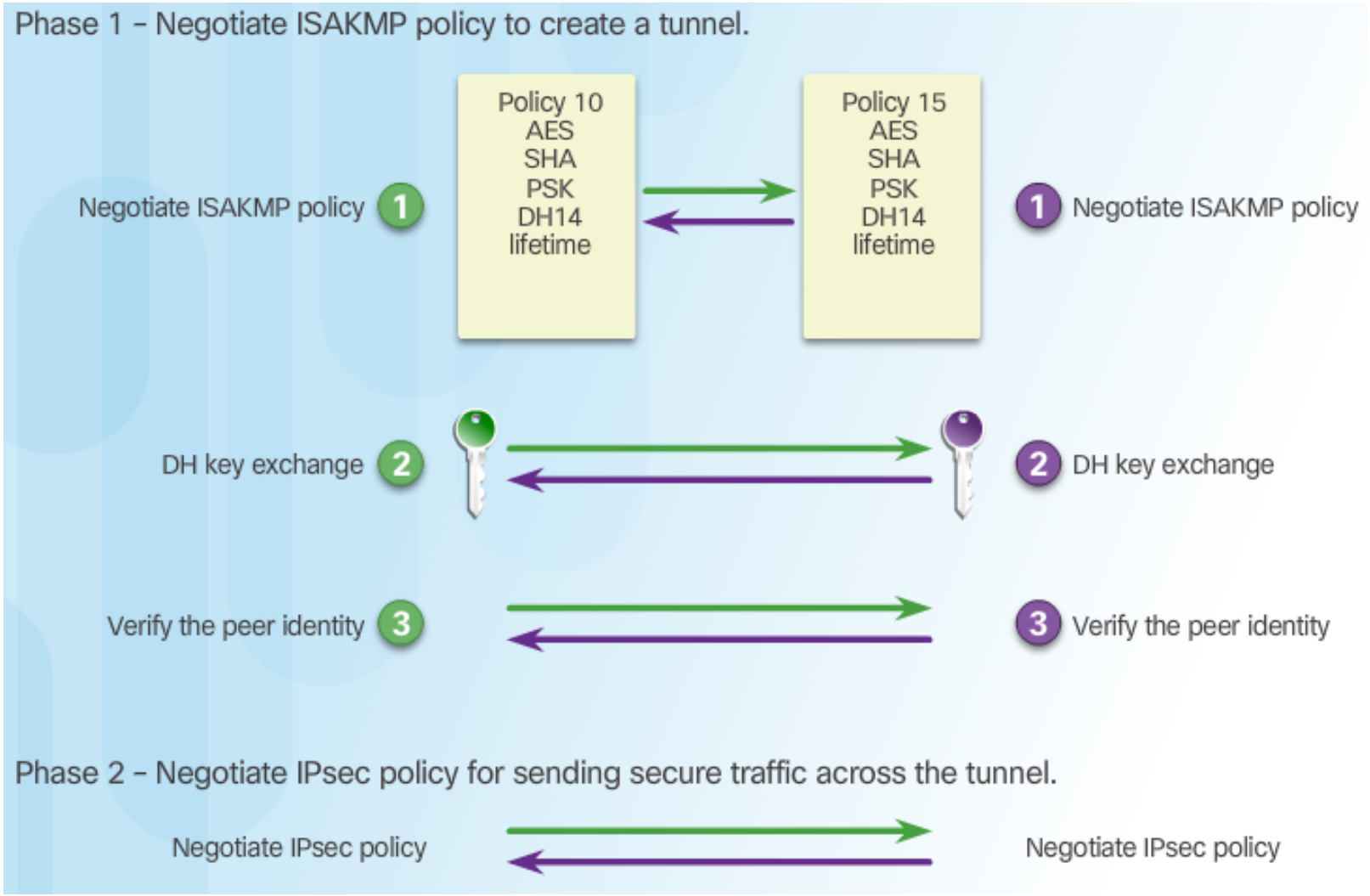


Topic 8.2.3:
Internet Key Exchange

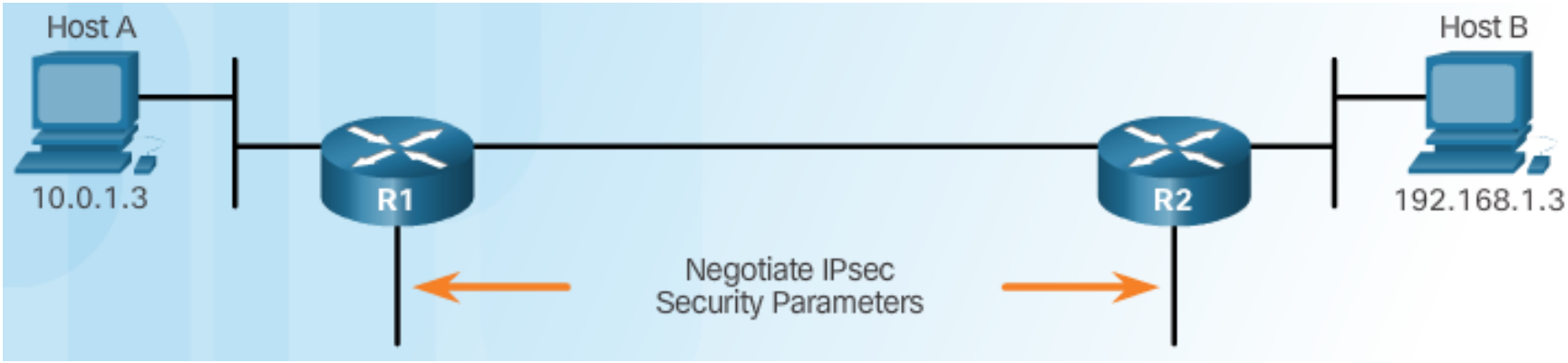
The IKE Protocol



Négotiation de clé : Phase 1 and 2



Phase 2: Negotiation des SA (Security Association)



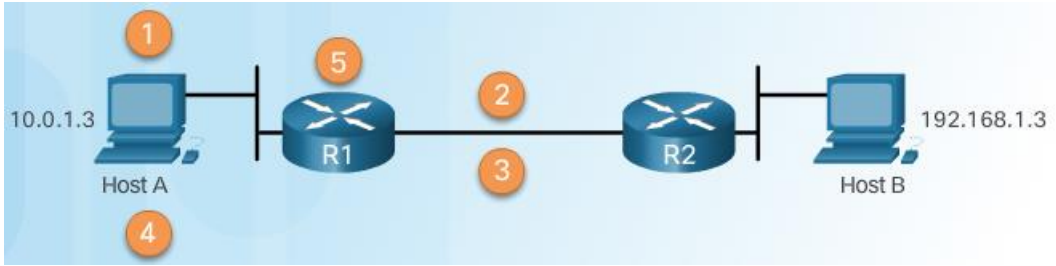
Section 8.3: Implementing Site-to-Site IPsec VPNs with CLI

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.

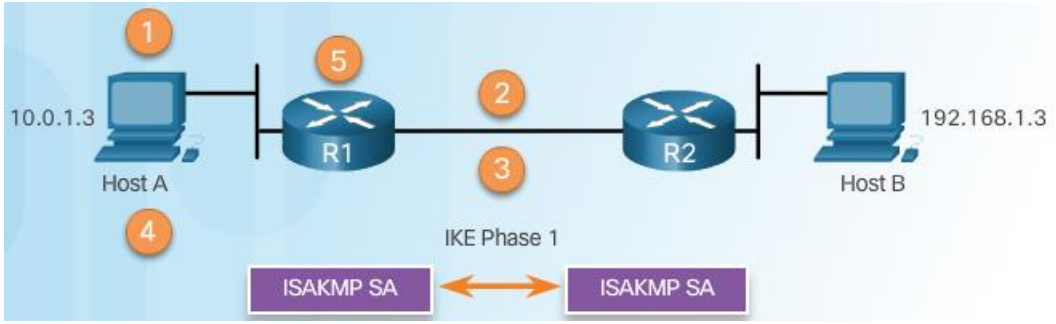
Topic 8.3.1:
Configuring a Site-to-Site IPsec VPN

Négotiation IPsec

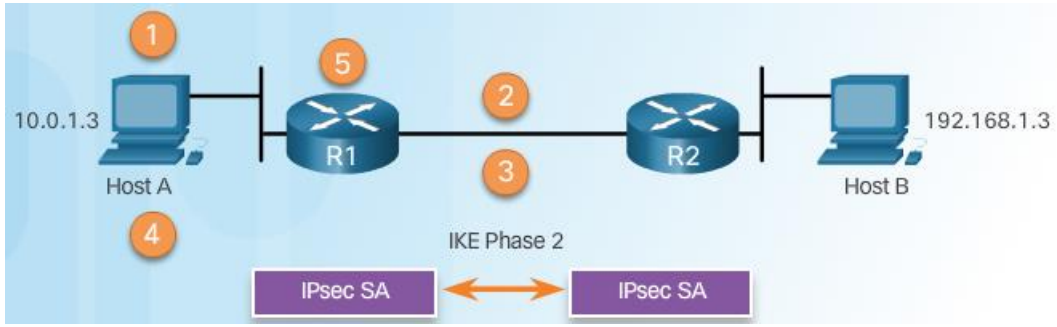


Step 1 - Host A sends interesting traffic to Host B.

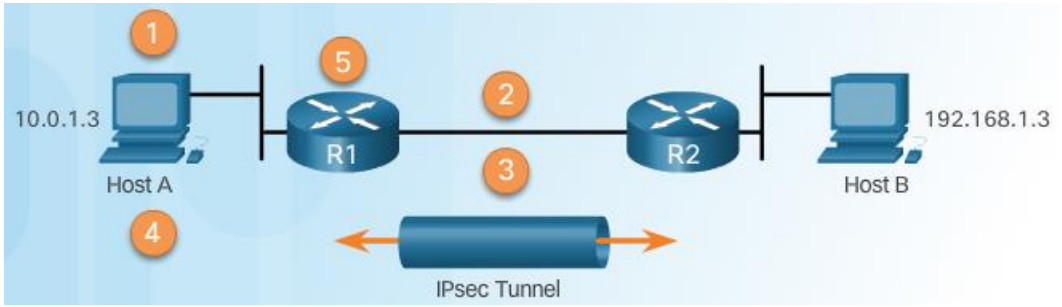
Step 2 - R1 and R2 negotiate an IKE Phase 1 session.



Step 3 - R1 and R2 negotiate an IKE Phase 2 session.

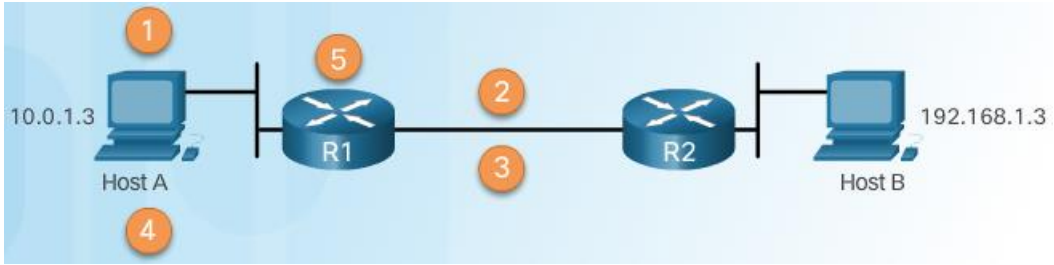


IPsec Negotiation (Cont.)



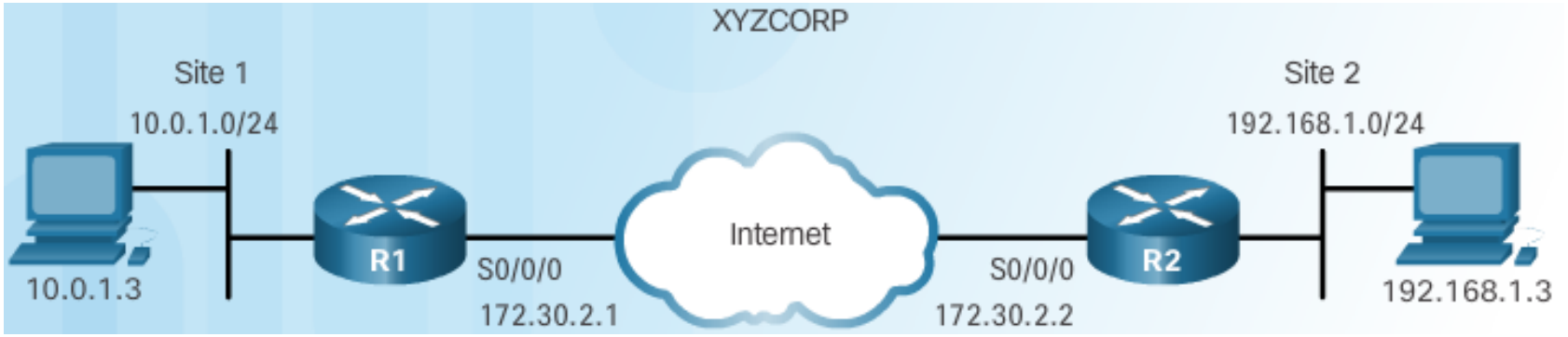
Step 4 - Information is exchanged via IPsec tunnel.

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

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
```

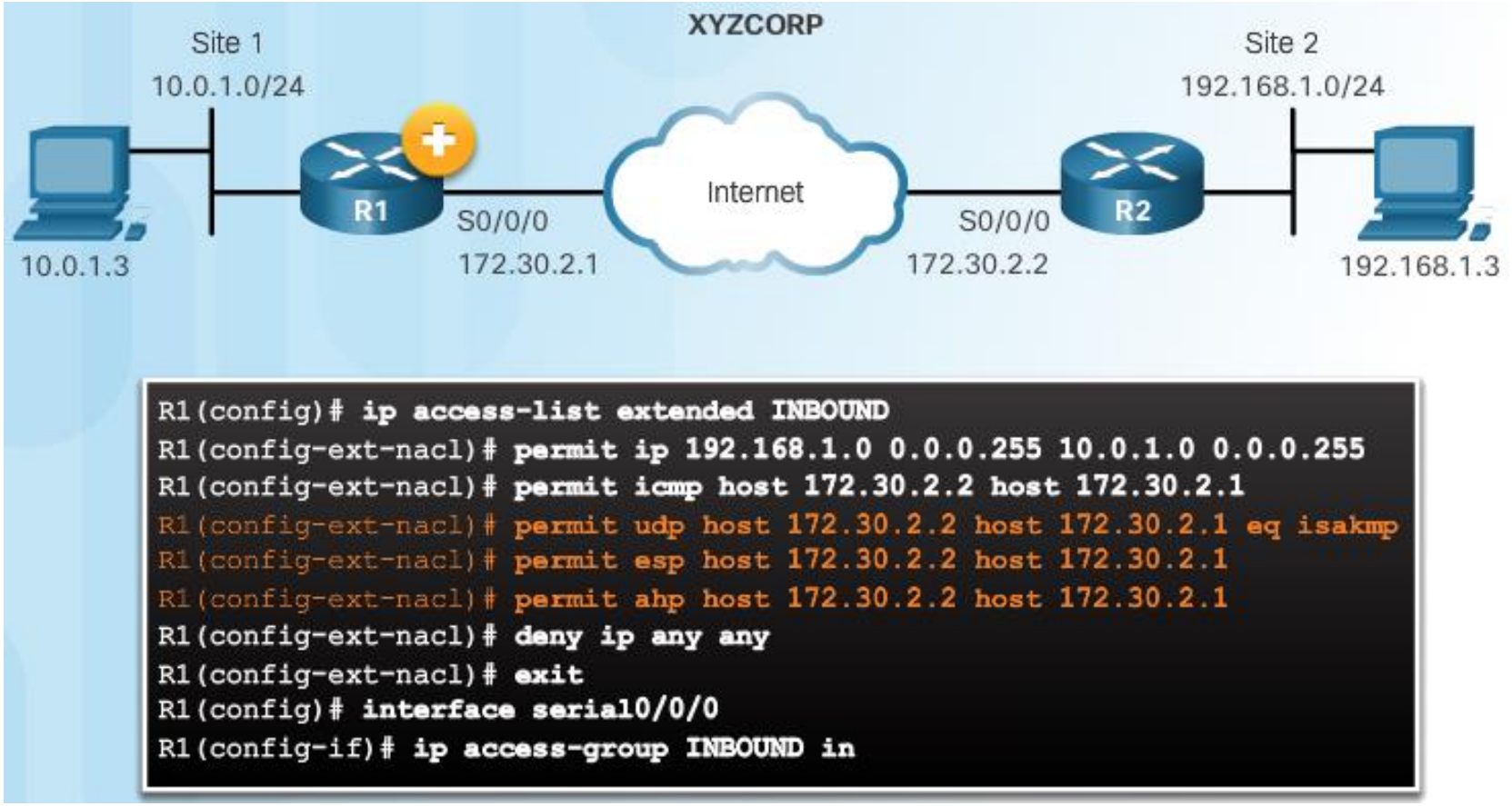
Permit AH Traffic

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

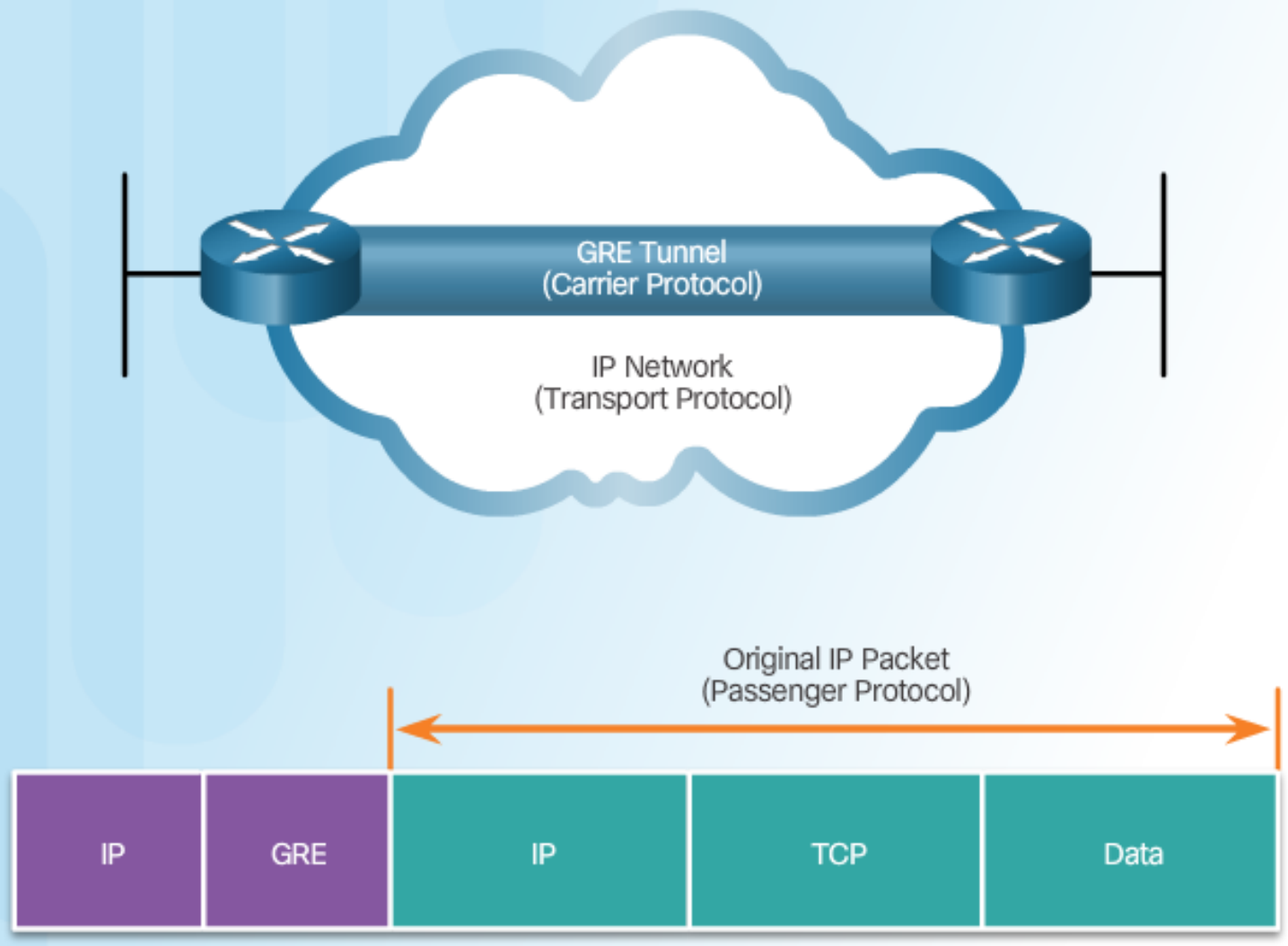
ACL Syntax for IPsec Traffic

Existing ACL Configurations (Cont.)

Permitting Traffic for IPsec Negotiations

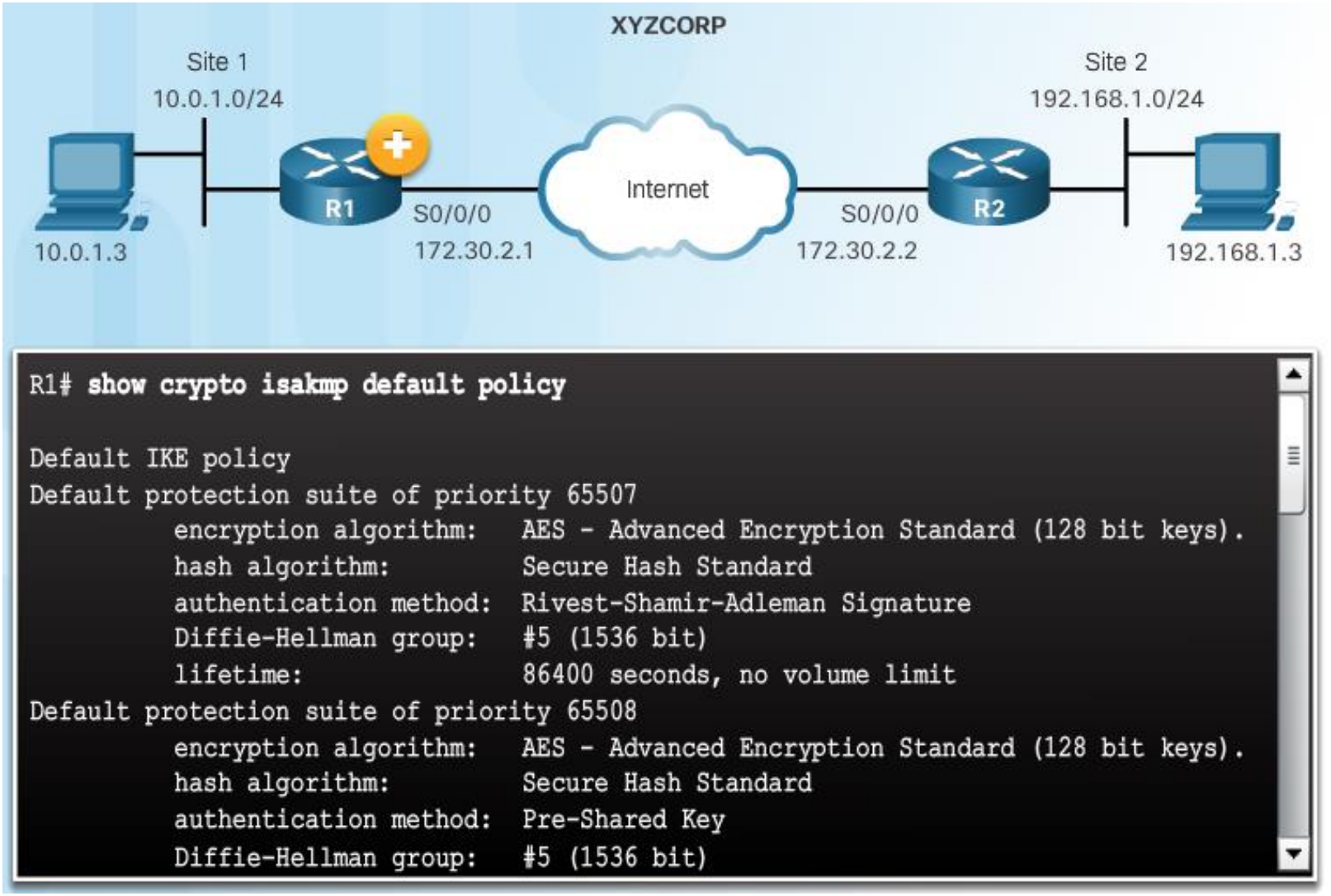


Introduction to GRE Tunnels



Topic 8.3.2: ISAKMP Policy

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#
```

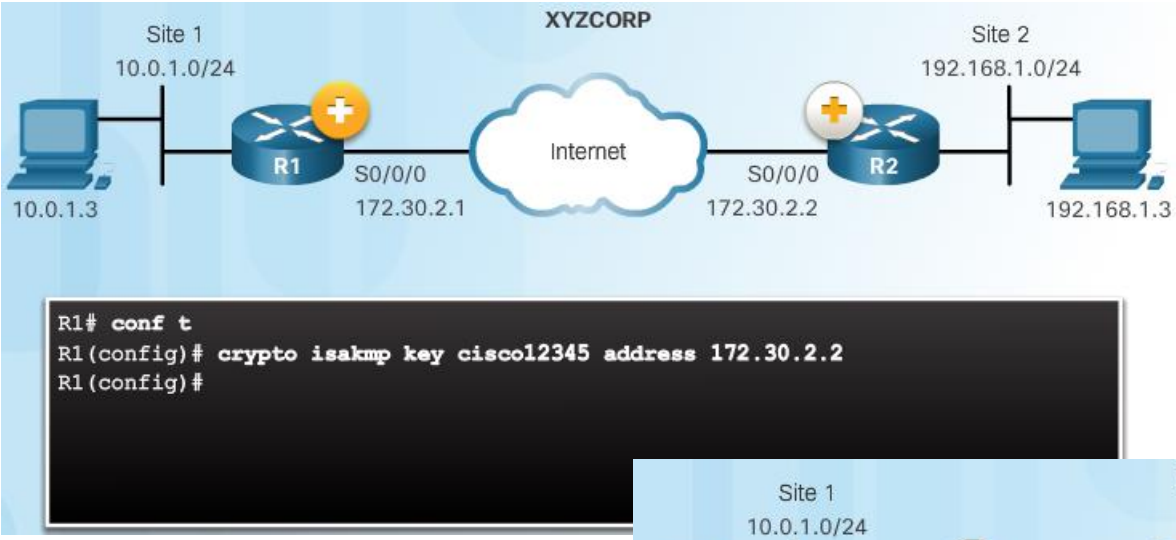
Configuring a Pre-Shared Key

The `crypto isakmp key` Command

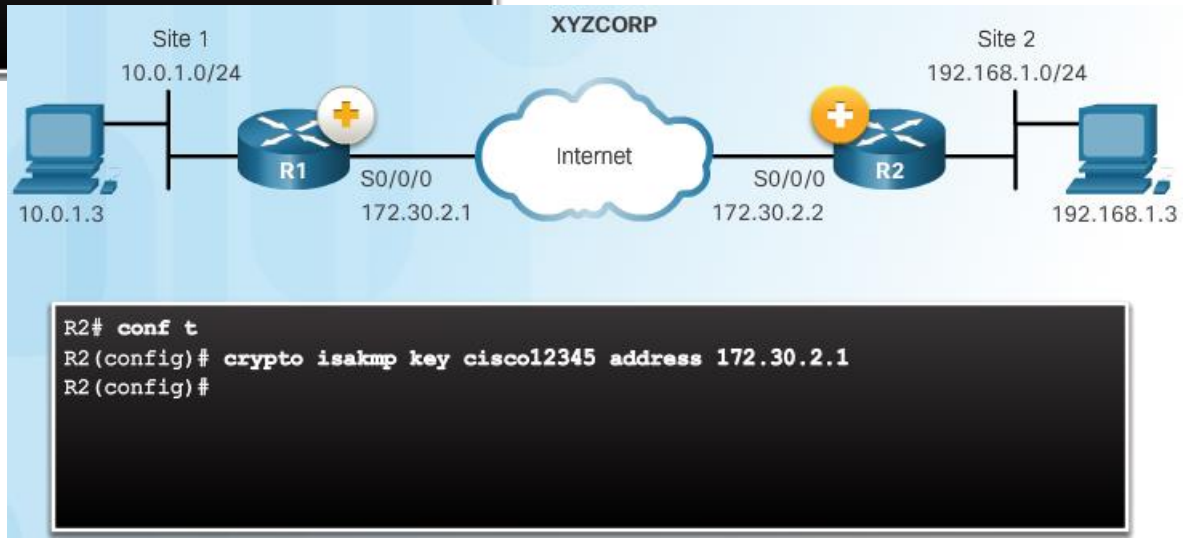
```
Router(config)#
crypto isakmp key keystring address peer-address

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)#
```

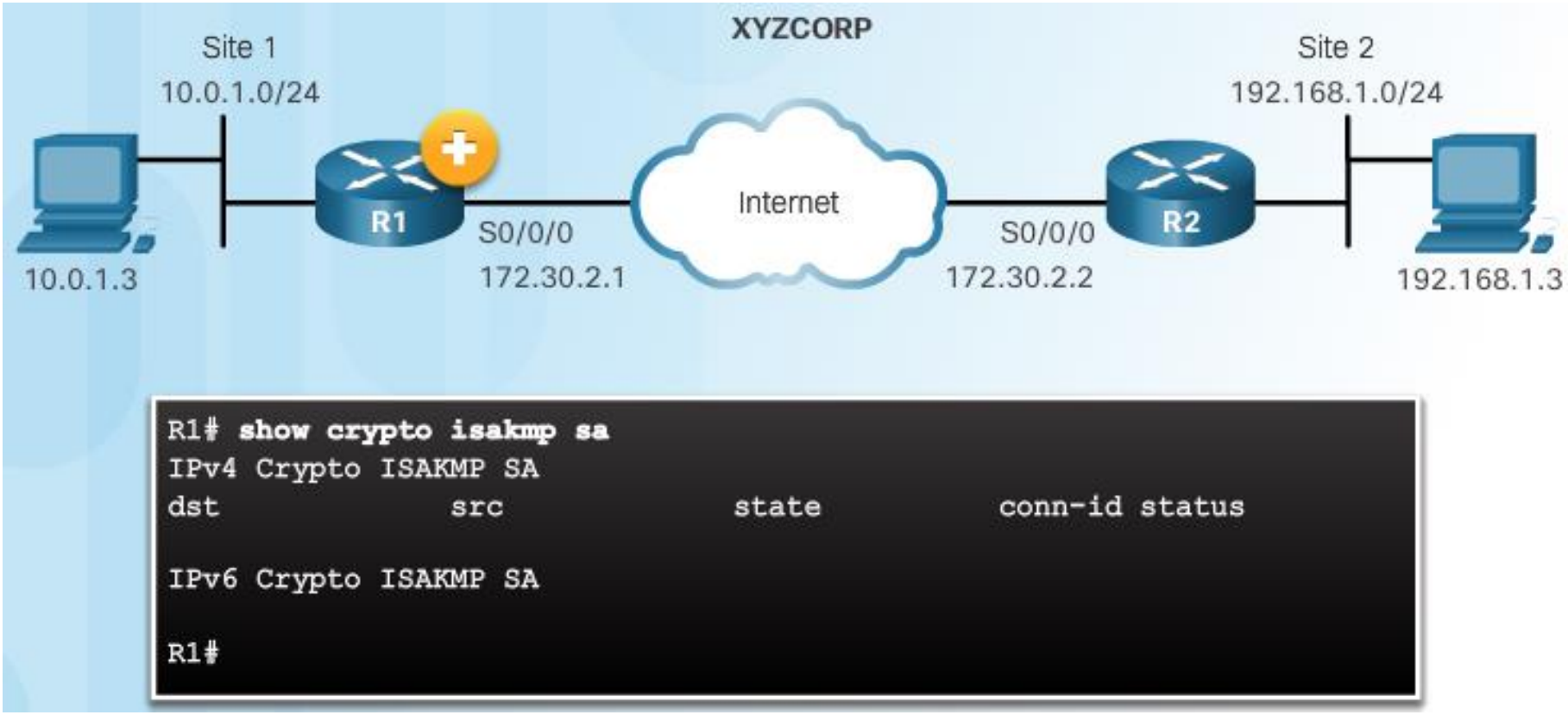



```
R2# conf t
R2(config)# crypto isakmp key cisco12345 address 172.30.2.1
R2(config)#
```

Topic 8.3.3:
IPsec Policy

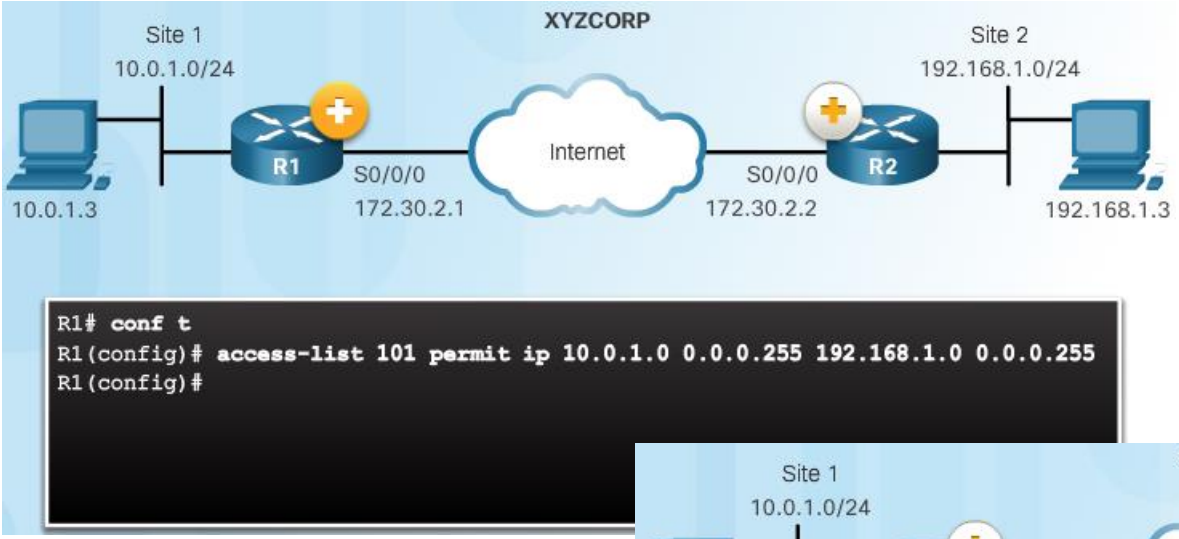
Define Interesting Traffic

The IKE Phase 1 Tunnel Does Not Exist Yet

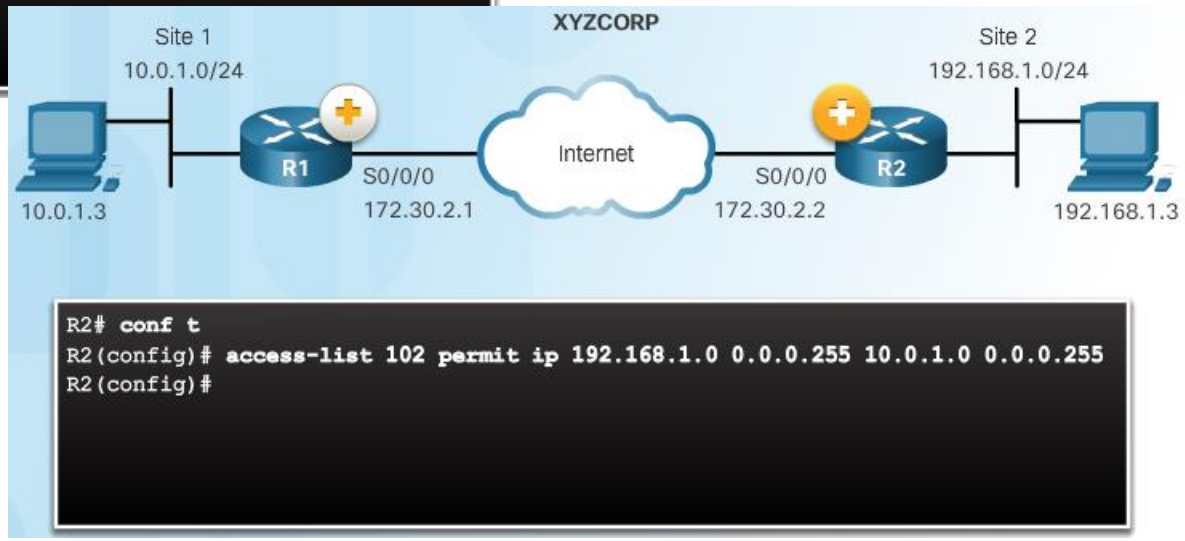


Define Interesting Traffic (Cont.)

Configure an ACL to Define Interesting Traffic



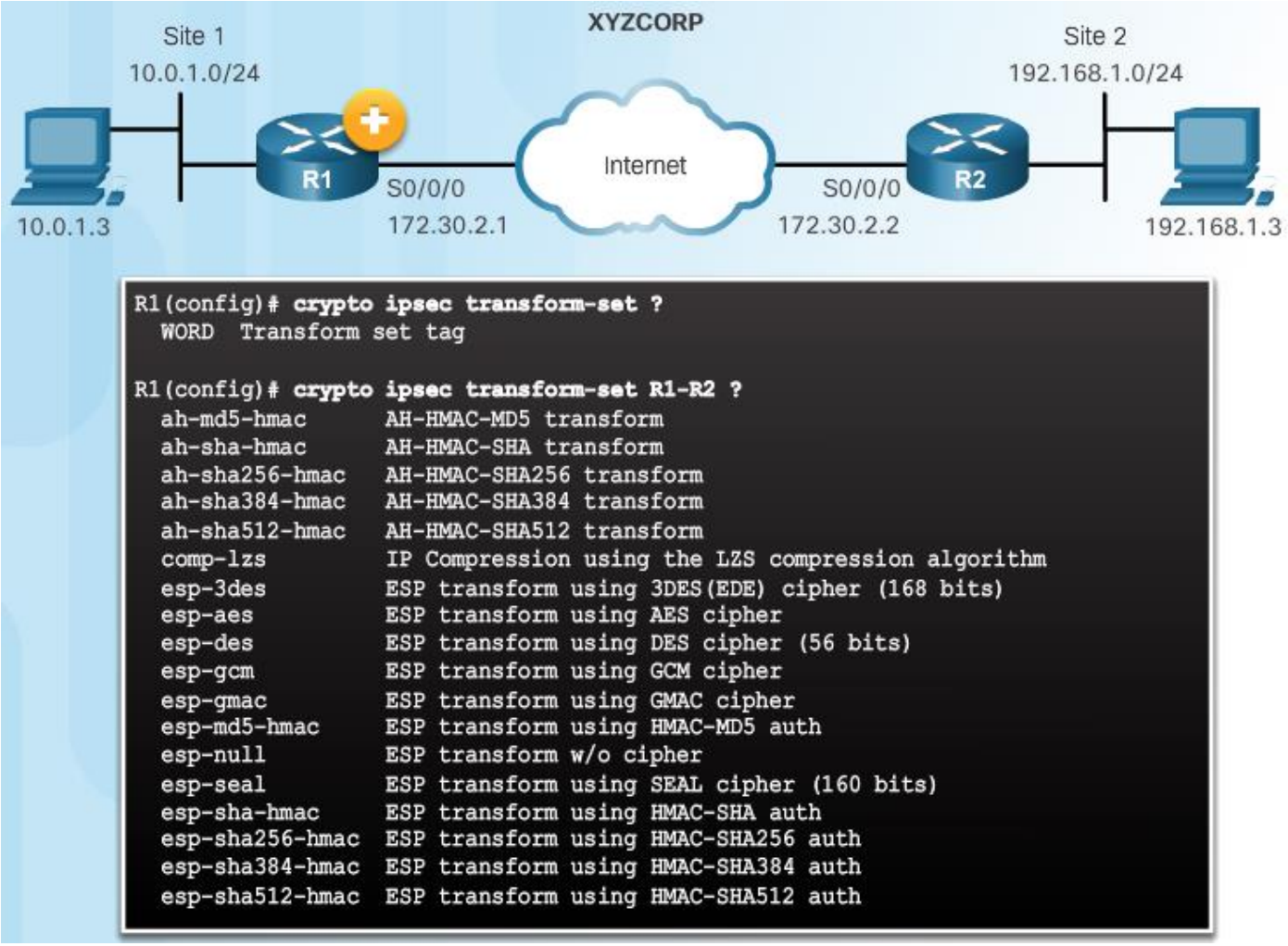

```
R1# conf t
R1(config)# access-list 101 permit ip 10.0.1.0 0.0.0.255 192.168.1.0 0.0.0.255
R1(config)#
```




```
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)#
```

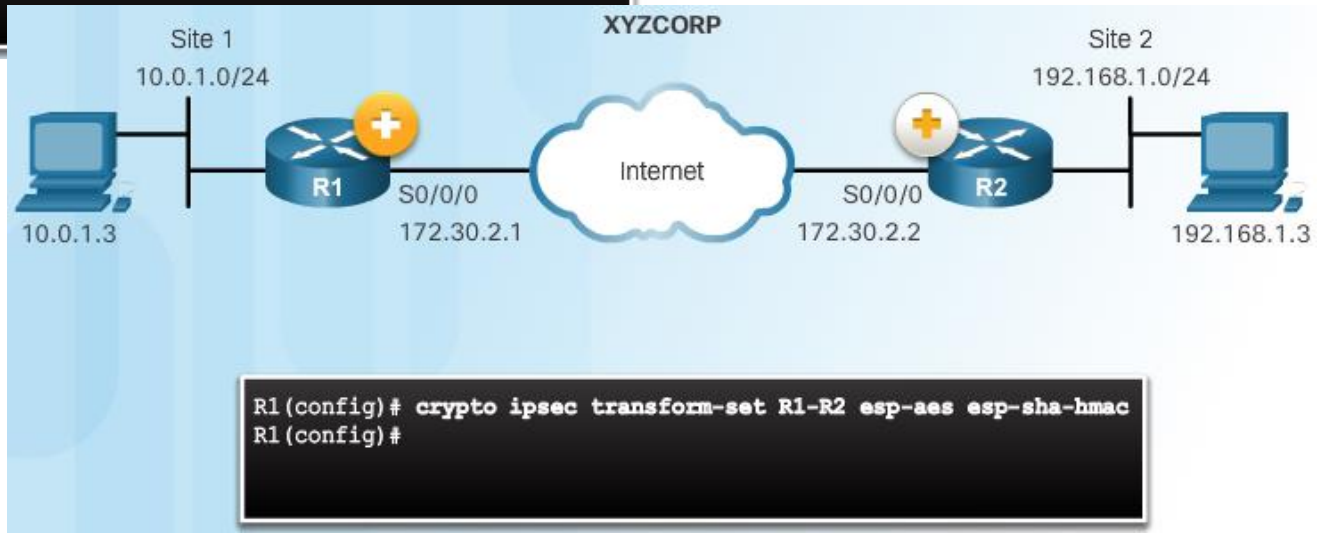
Configure IPsec Transform Set

The `crypto ipsec transform-set` Command



Configure IPsec Transform Set (Cont.)

The `crypto ipsec transform-set` Command



Topic 8.3.4: Crypto Map

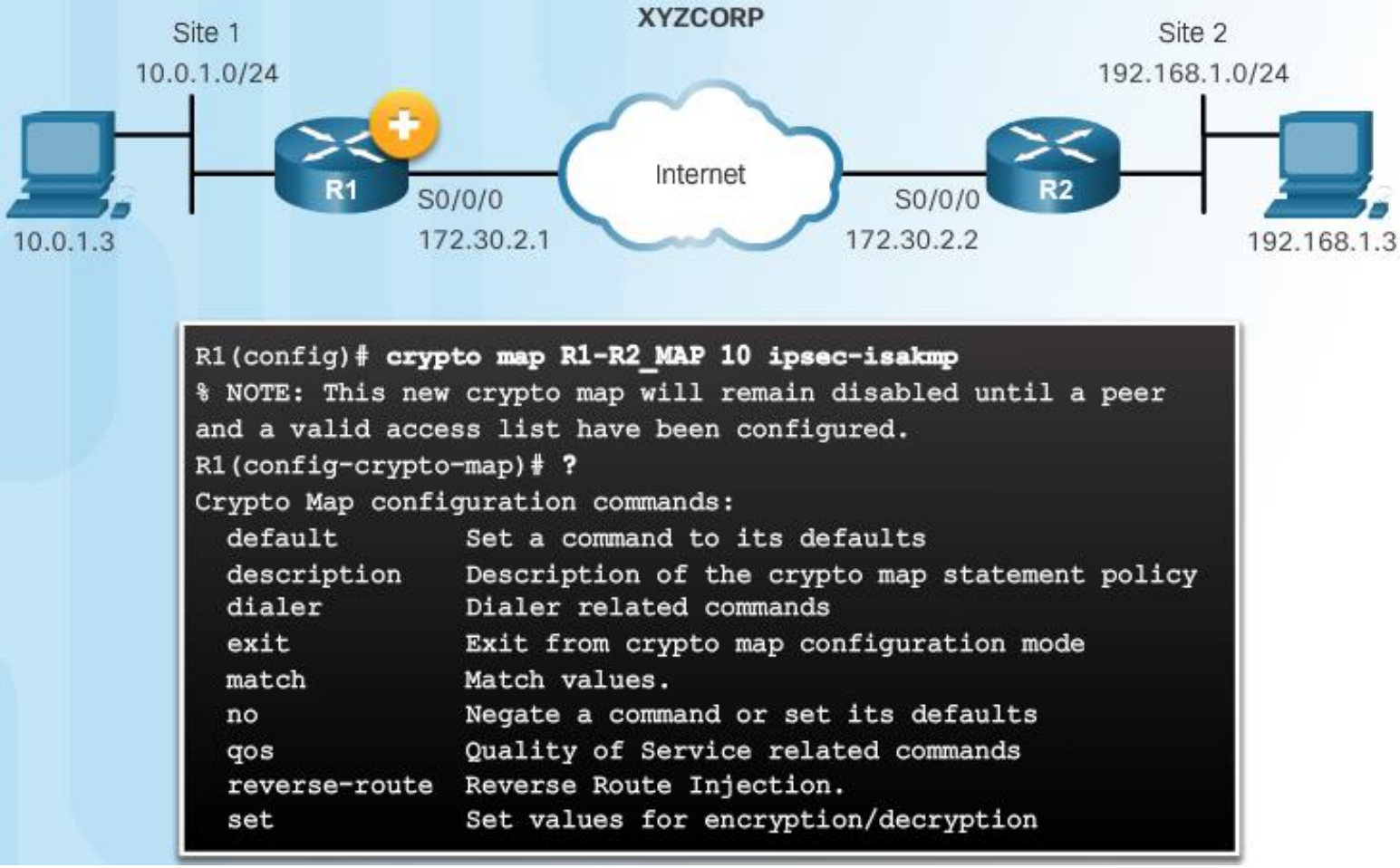
Syntax to Configure a Crypto Map

```
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



XYZCORP Crypto Map Configuration

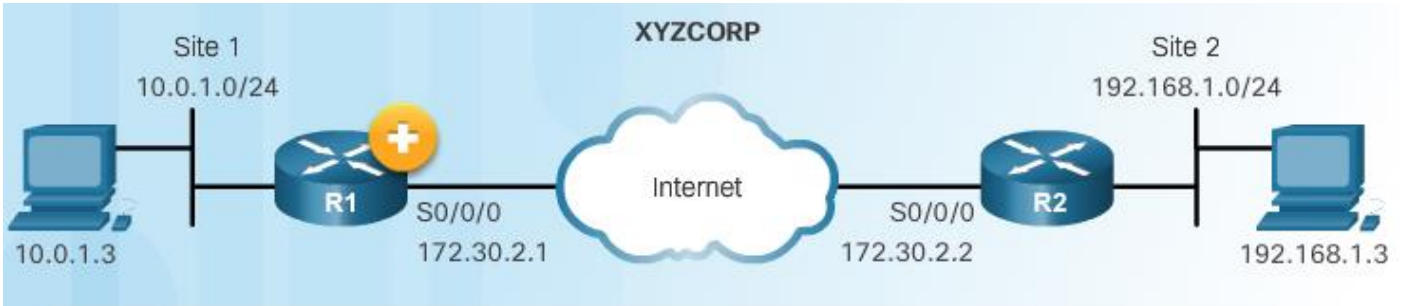
Crypto Map Configuration:


```
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:




```
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#
```

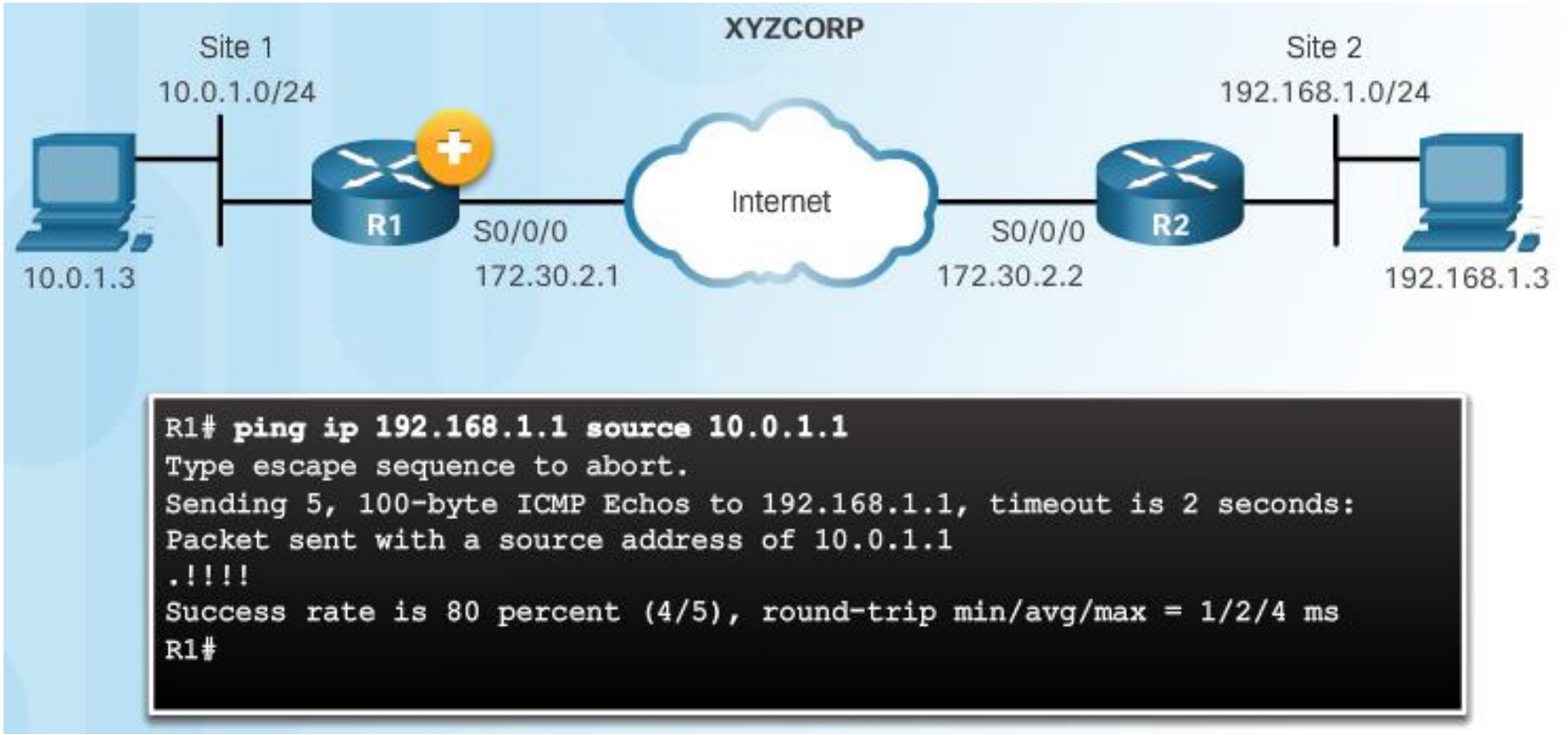
Apply the Crypto Map


```
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




```
R1# ping ip 192.168.1.1 source 10.0.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet sent with a source address of 10.0.1.1
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms
R1#
```

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
```

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.

Thank you.

Cisco Networking Academy

Mind Wide Open