Cisco Networking Academy
Mind Wide Open

Implementacja Wirtualnych Sieci Prywatnych (VPN)

Zawartość wykładu

1.0 Wprowadzenie

1.1 VPNy

1.2 Składniki i działanie IPsec VPN

1.3 Implementacja tunelu Site-to-Site IPsec VPN przy użyciu CLI

1.4 Podsumowanie

Rozdział 1.1: VPNy

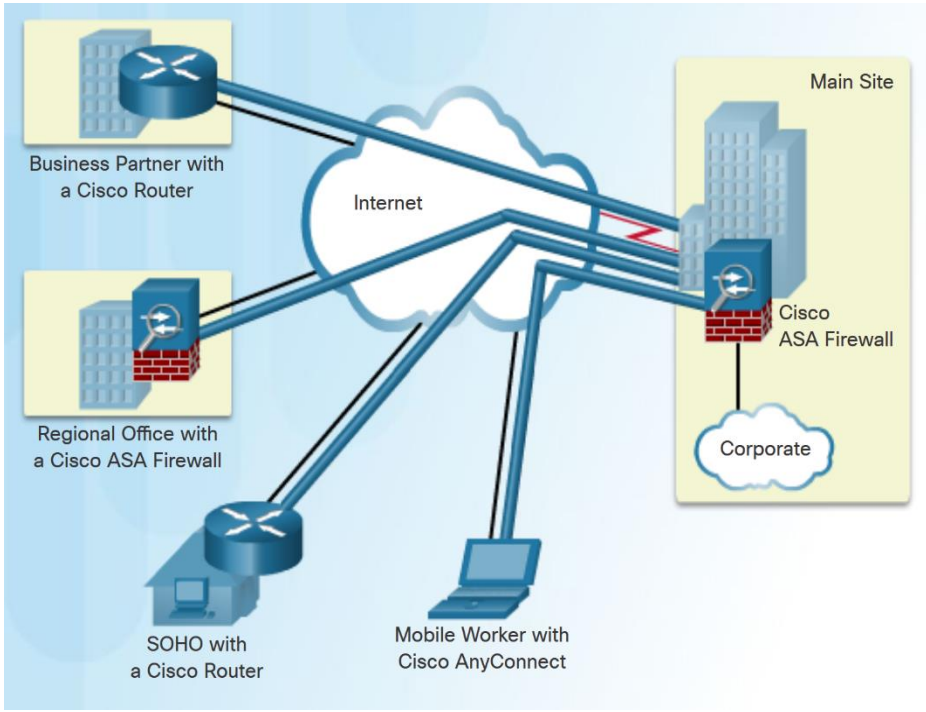
Po zakończeniu tej sekcji powinieneś być w stanie:

- Opisać sieci VPN oraz ich zalety.
- Porównać sieci VPN typu site-to-site i oraz zdalny VPN

Temat 1.1.1: Przegląd VPN

Wprowadzenie do sieci VPN

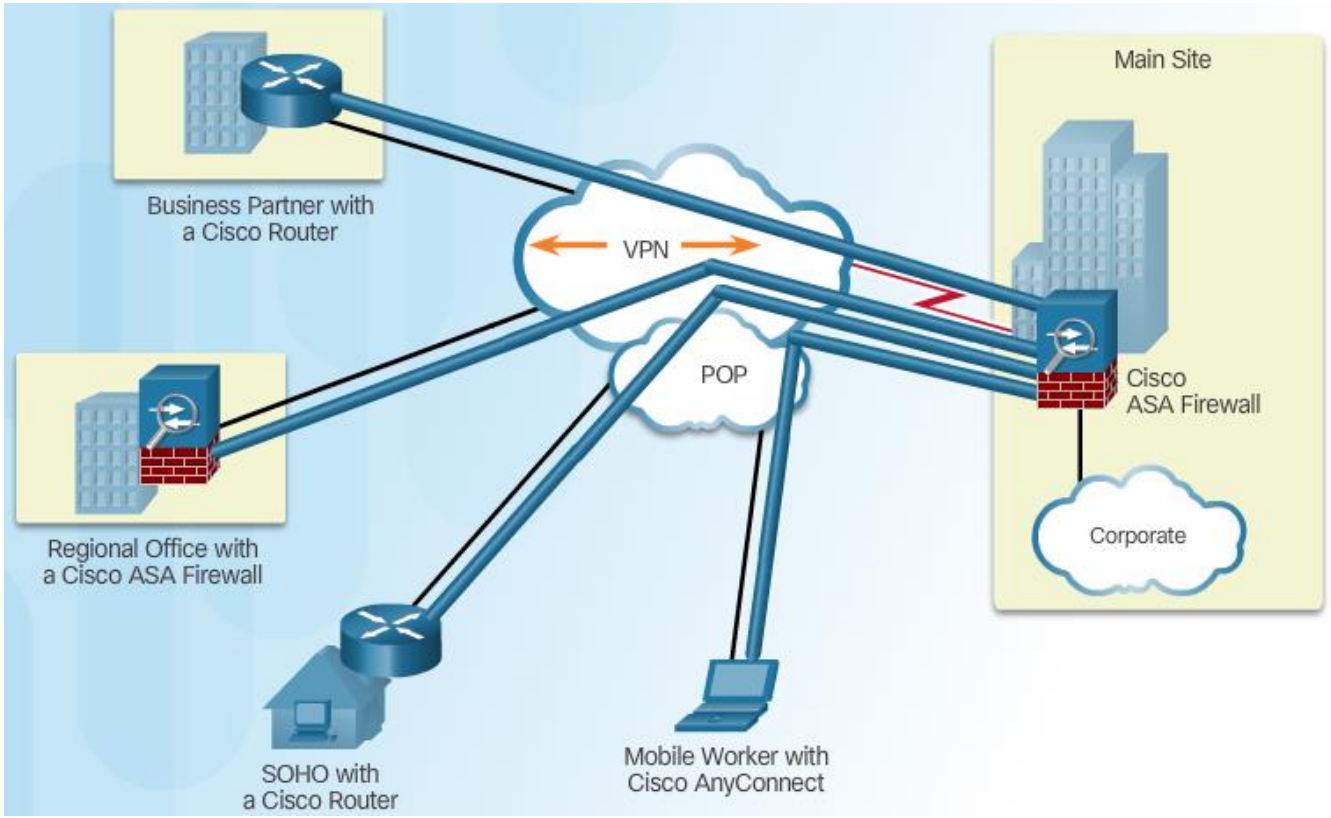
- VPN to prywatna sieć tworzona jako tunel poprzez sieć publiczną, zwykle Internet.
- Bezpieczna implementacja sieci VPN z szyfrowaniem, na przykład sieci VPN IPsec, jest zwykle określana jako wirtualna sieć prywatna.
- Aby wdrożyć VPN, niezbędna jest brama VPN - może to być router, zapora lub urządzenie Cisco Adaptive Security Appliance (ASA).



Wprowadzenie do sieci VPN

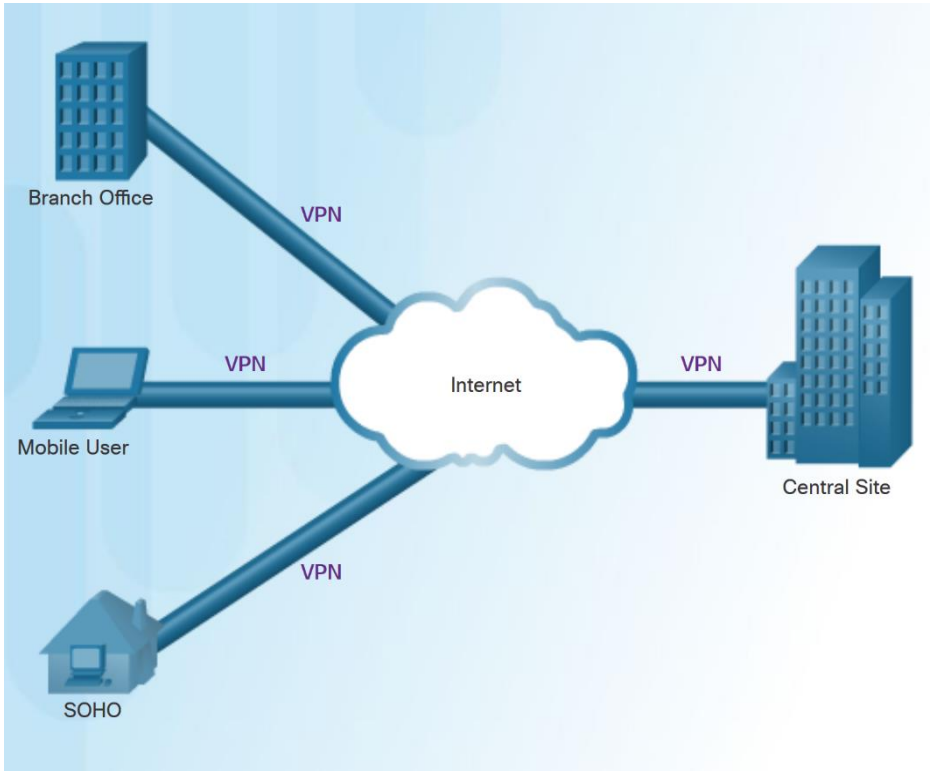
Zalety stosowania sieci VPN:

- Oszczędność kosztów
- Bezpieczeństwo
- Skalowalność
- Kompatybilność

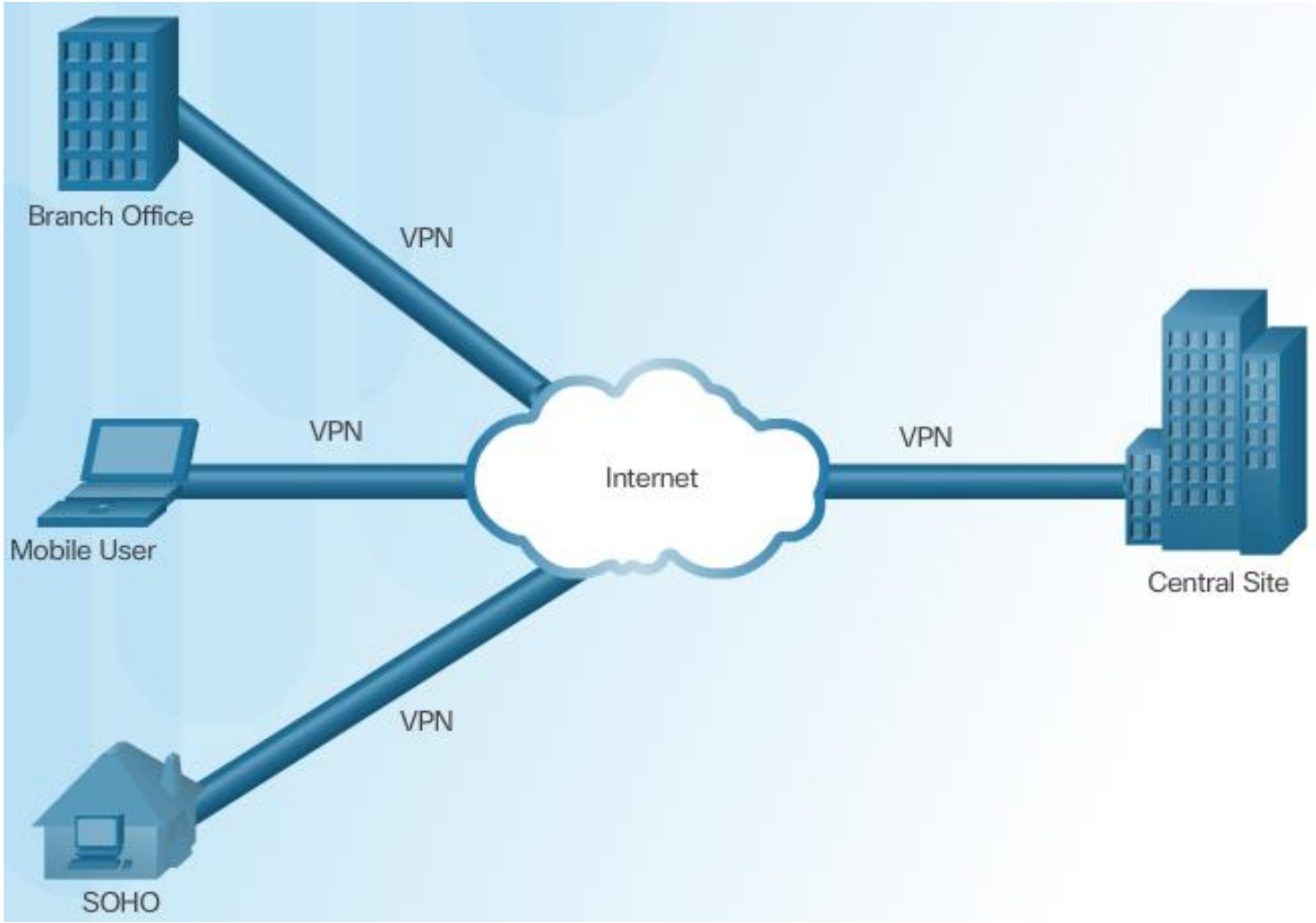


Zalety sieci VPN

- Zalety VPN obejmują następujące elementy:
  - **Oszczędność** - VPN umożliwiają organizacjom korzystanie z opłacalnych, wysokoprzepustowych technologii, takich jak DSL, do łączenia zdalnych biur i zdalnych użytkowników z siedzibą główną firmy.
  - **Skalowalność** - organizacje mogą dodawać nowe połączenia VPN bez znaczącej rozbudowy infrastruktury.
  - **Zgodność z technologią szerokopasmową** – Umożliwia pracownikom mobilnym i telepracownikom na korzystanie z szybkiej, szerokopasmowej łączności.
  - **Bezpieczeństwo** - VPNy mogą korzystać z zaawansowanych protokołów szyfrowania i uwierzytelniania.

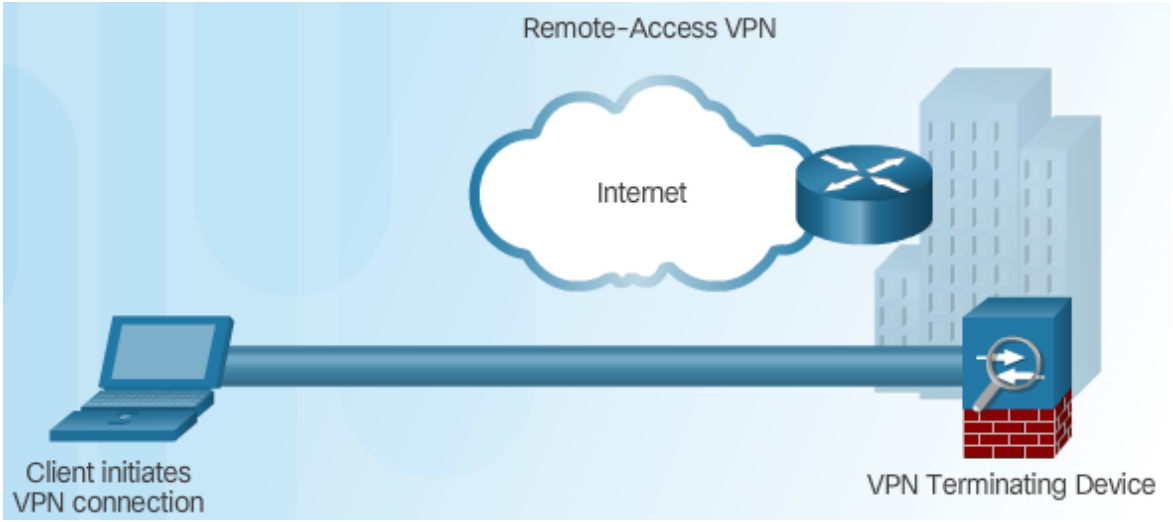


IPsec VPN warstwy 3



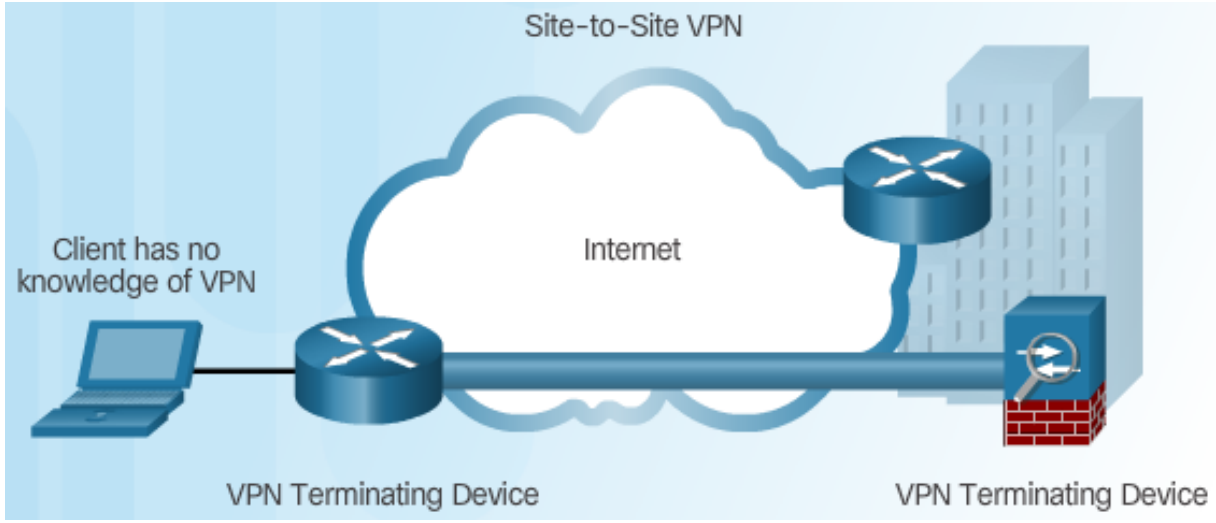
Temat 1.1.2: Technologie VPN

Dwa typy sieci VPN

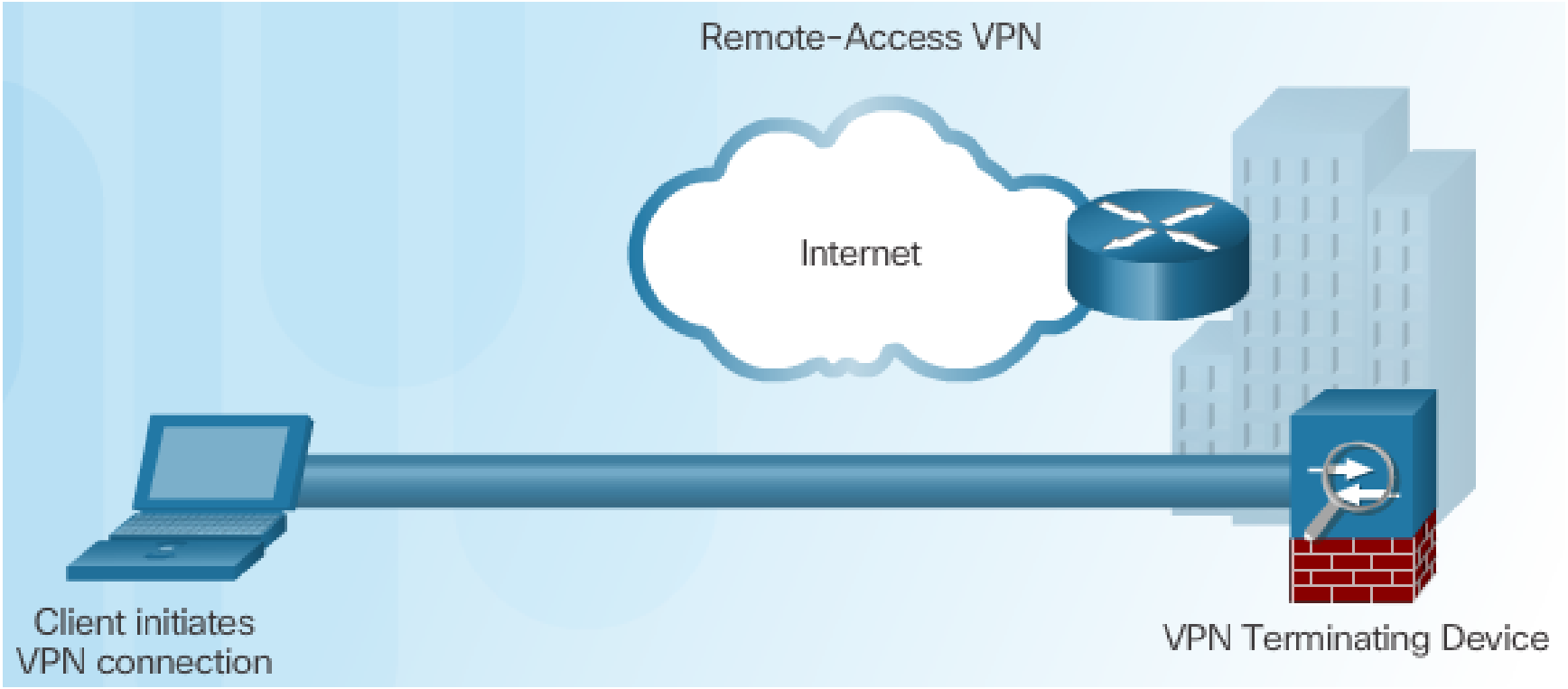


Zdalny VPN

Site-to-Site VPN

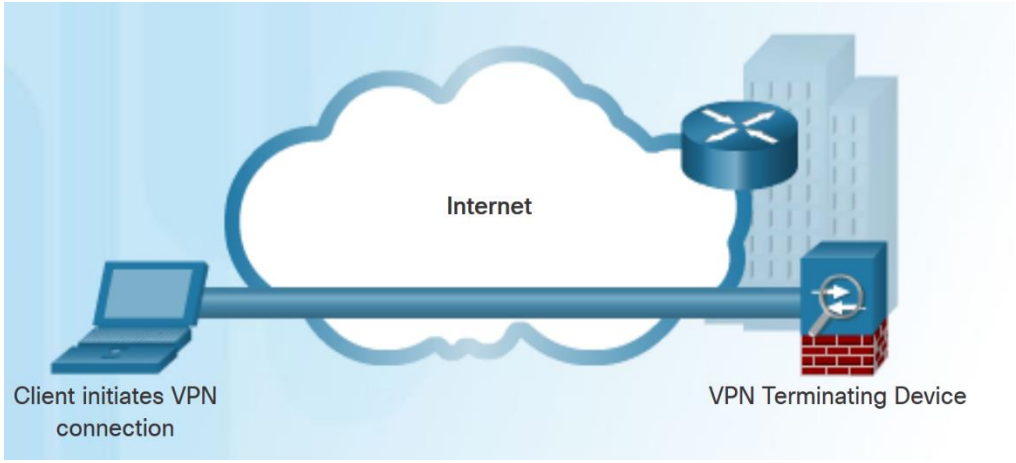


Składniki zdalnego VPN

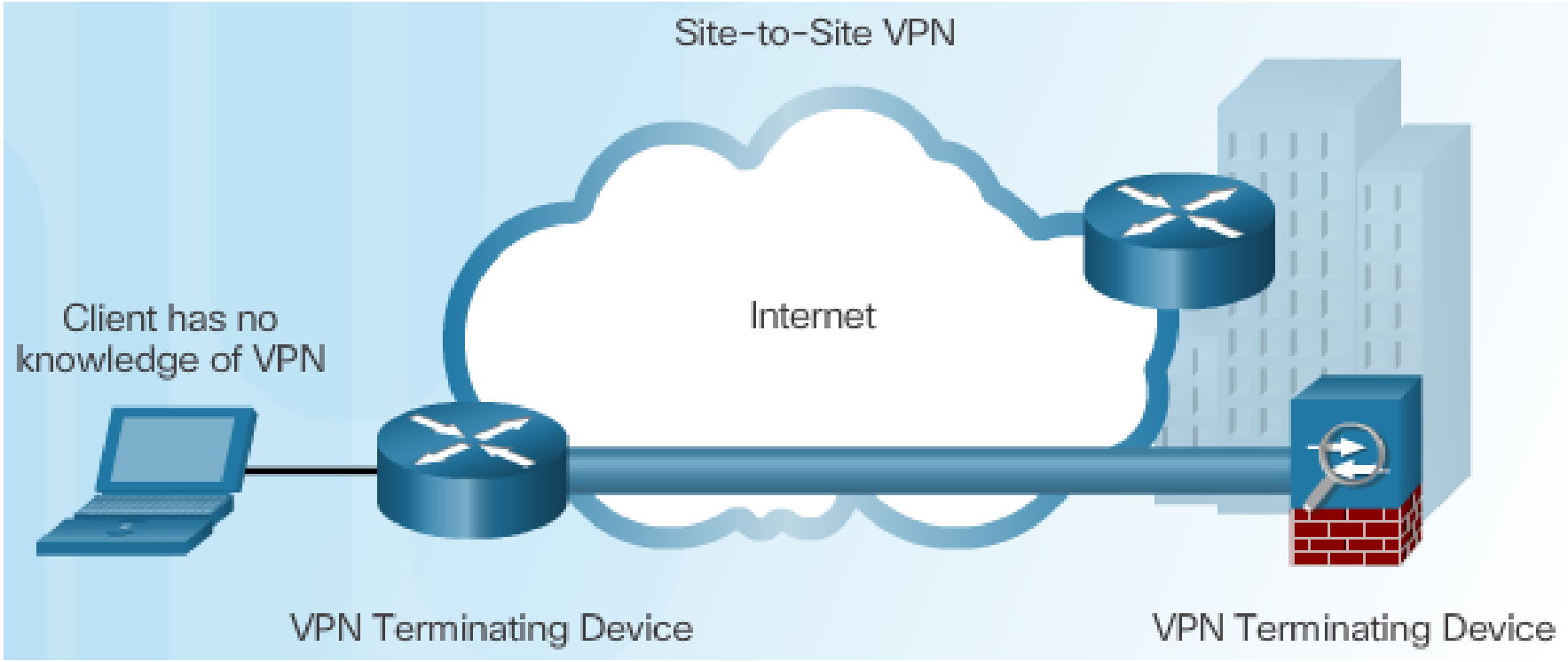


Zdalny dostęp VPN

- Zdalny dostęp VPN wspiera potrzeby telepracowników, użytkowników mobilnych i ruchu ekstranetowego.
- Umożliwia dynamiczną zmianę informacji. Może być włączany i wyłączany.
- Służy do łączenia poszczególnych hostów, które muszą bezpiecznie uzyskać dostęp do sieci firmowej poprzez Internet.
- Oprogramowanie klienckie VPN może wymagać zainstalowania na urządzeniu końcowym użytkownika mobilnego.

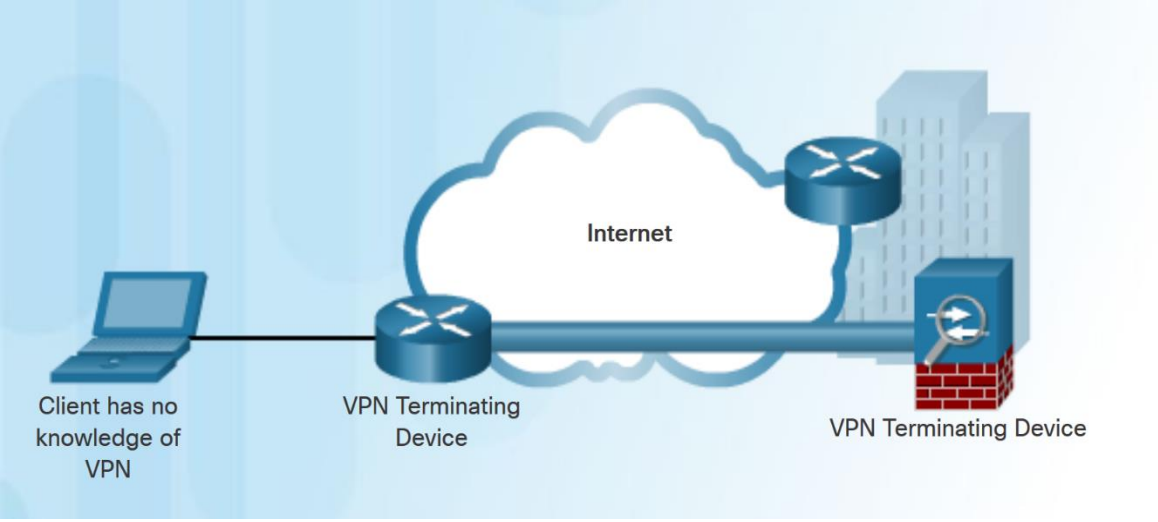


Składniki Site-to-Site VPN



Site-to-Site VPN

- Sieci site-to-site VPN łączą ze sobą całe sieci, na przykład łączą sieć oddziałów firmy z siecią centrali firmy.
- W sieci site-to-site VPN hosty końcowe wysyłają i odbierają normalny ruch TCP / IP przez „bramę” VPN.
- Brama VPN jest odpowiedzialna za hermetyzację i szyfrowanie ruchu wychodzącego.



Rozdział 1.2: Składniki i działanie IPsec VPN

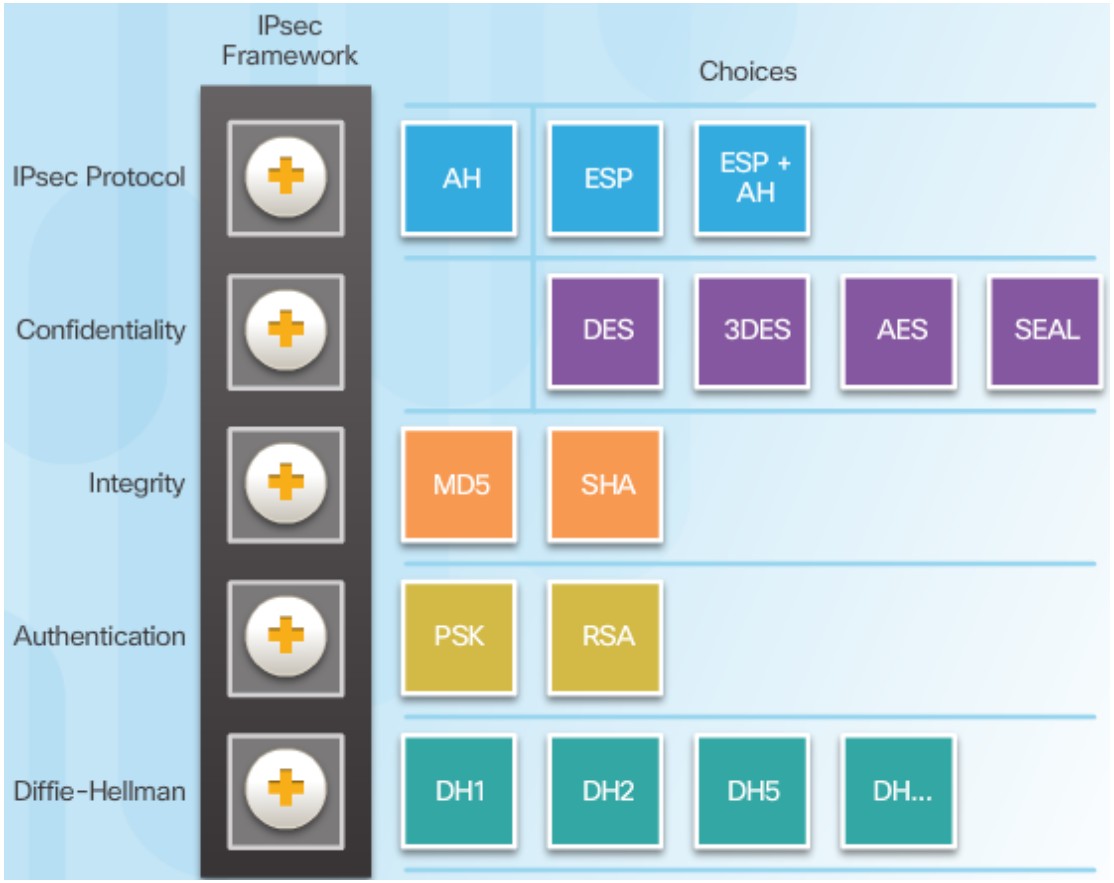
Po zakończeniu tej sekcji powinieneś być w stanie:

- Opiszać protokół IPsec i jego podstawowe funkcje.
- Porównać protokoły AH i ESP.
- Opisać protokół IKE.

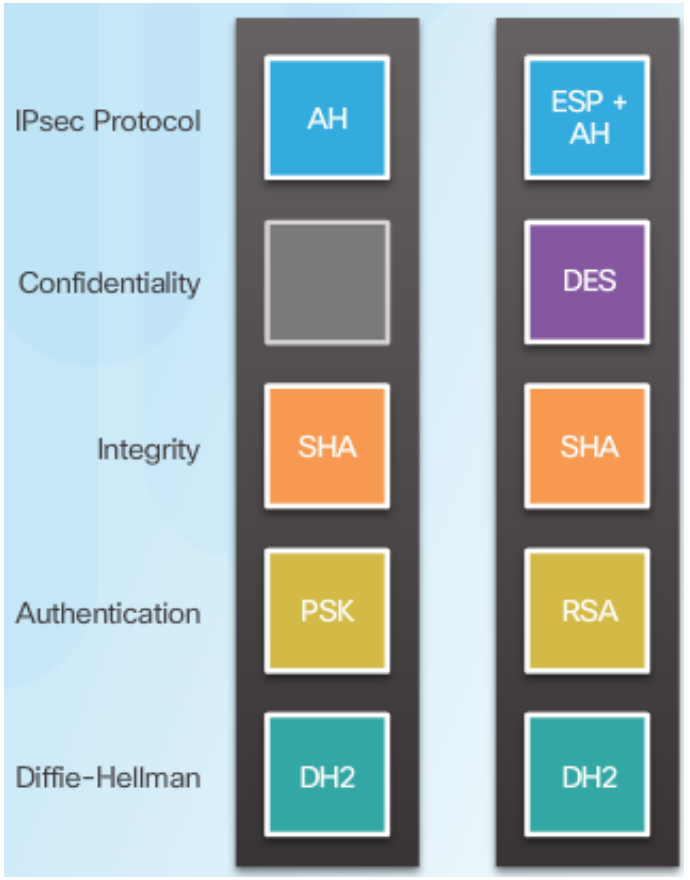
Temat 1.2.1:
Wprowadzenie do IPsec

Technologie IPsec

Framework IPsec

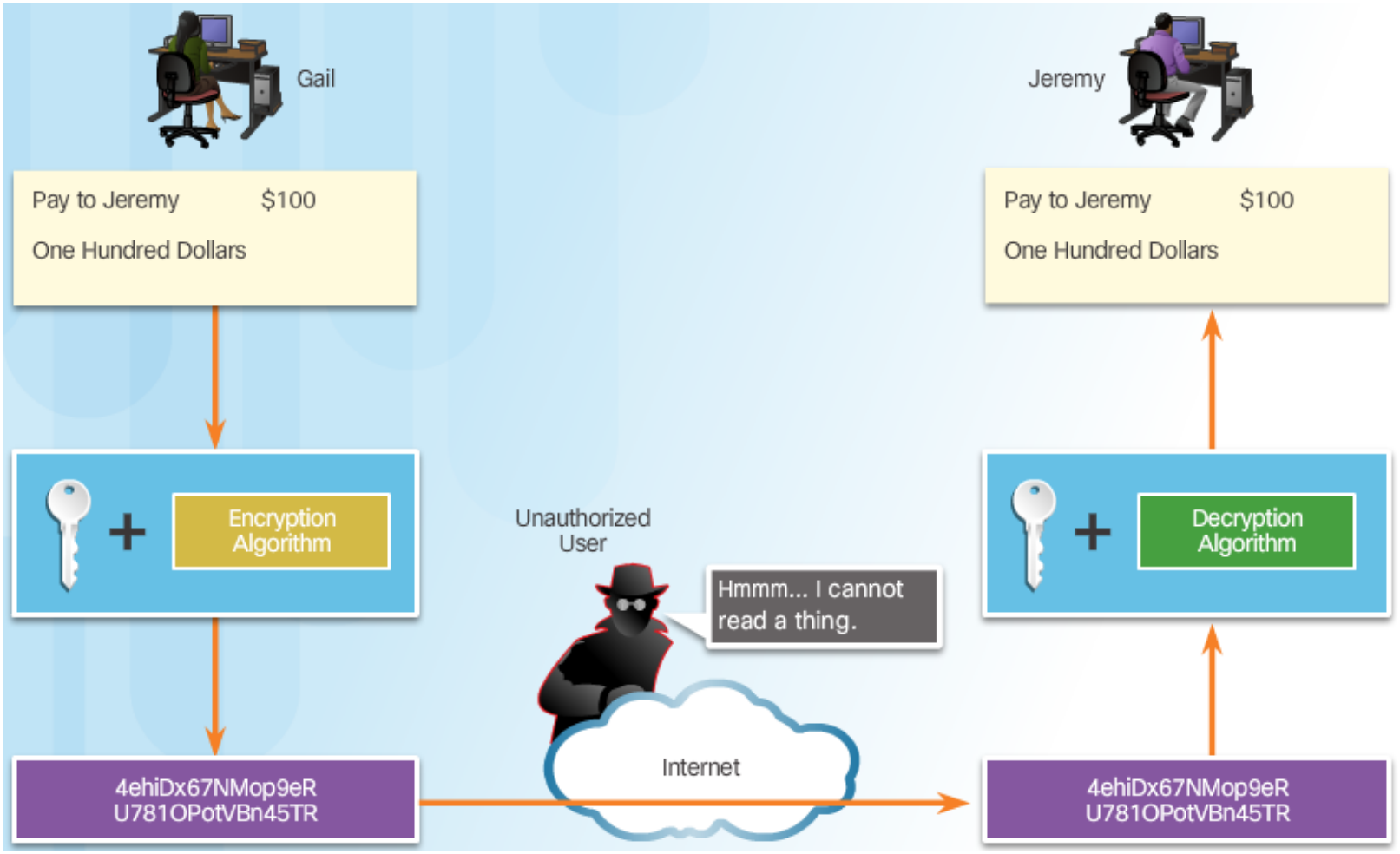


Przykłady implementacji IPSec



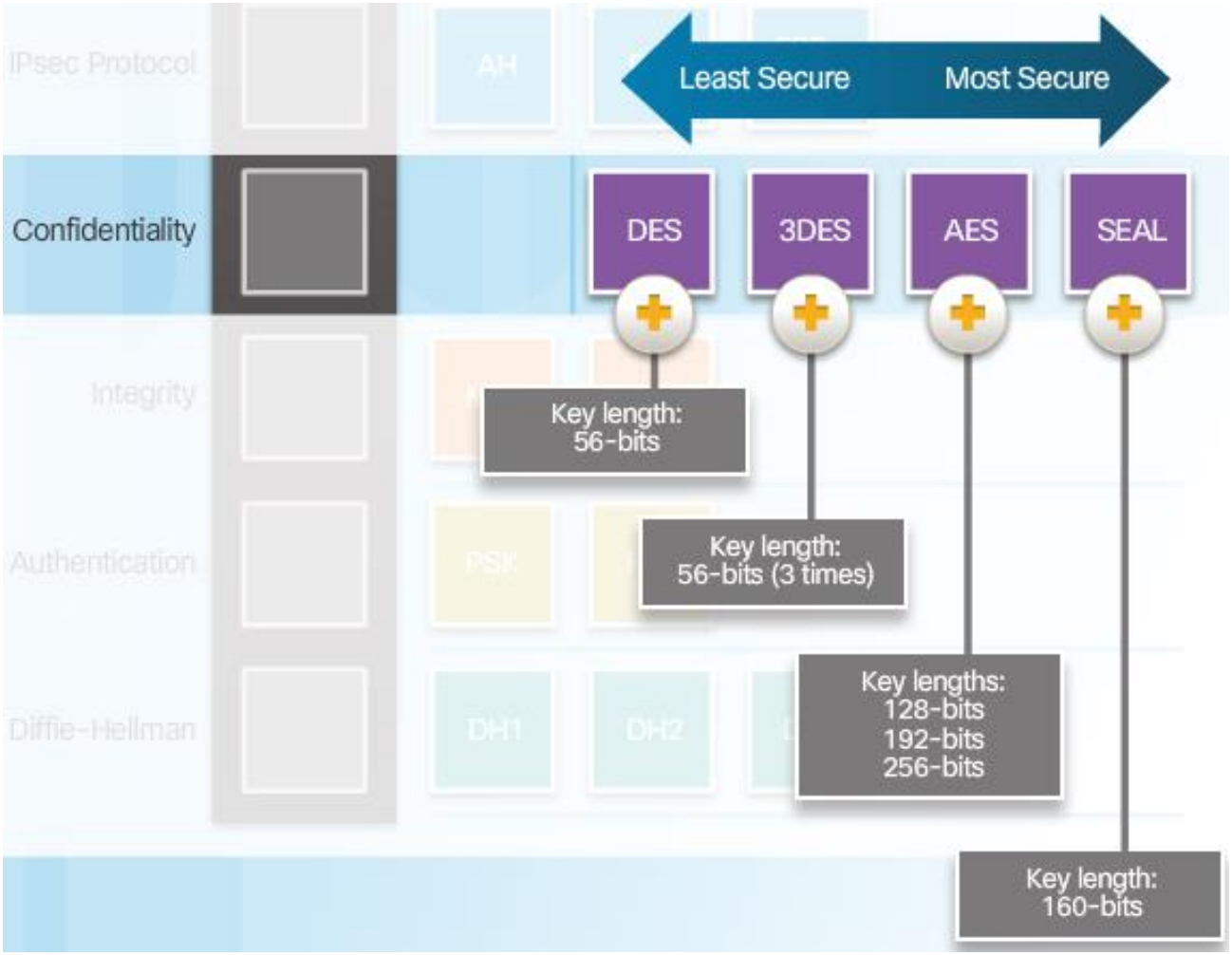
Poufność

Poufność z szyfrowaniem:



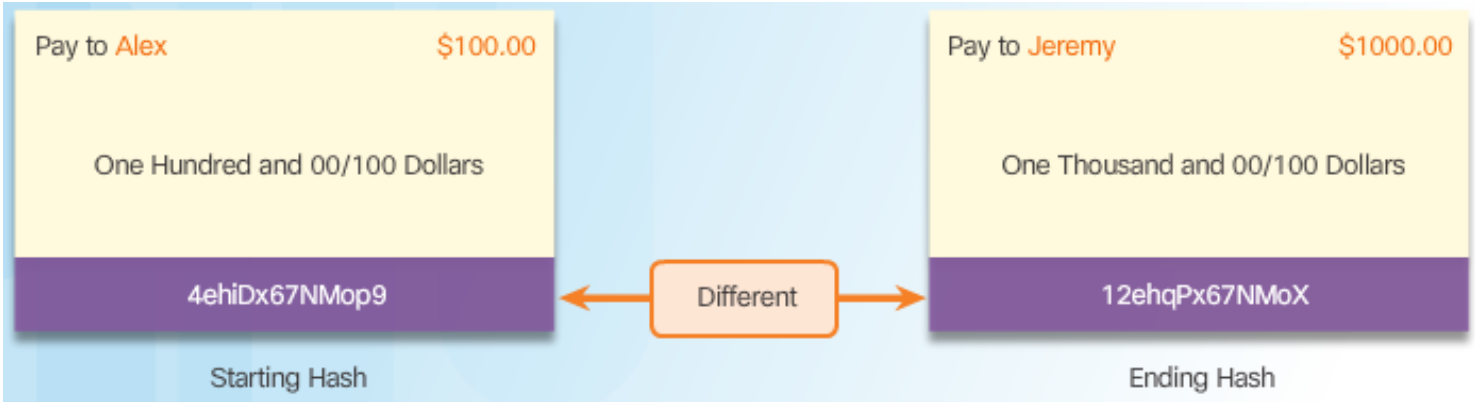
Poufność (Cont.)

Algorytmy szyfrujące:

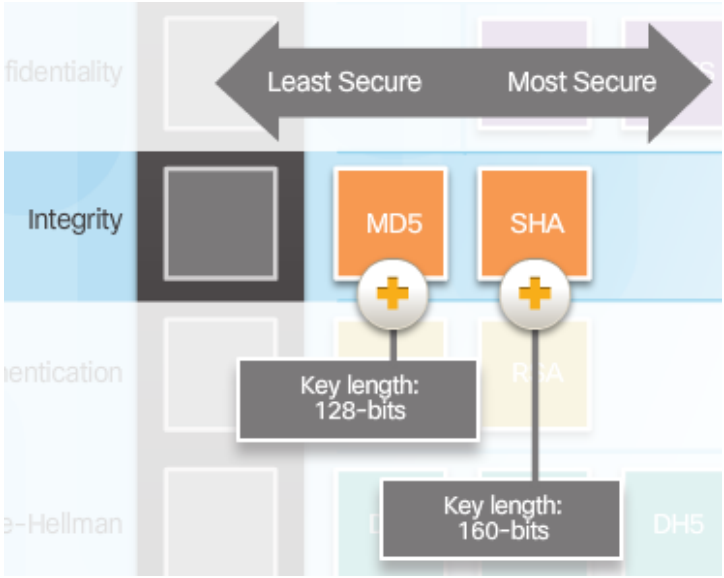


Integralność

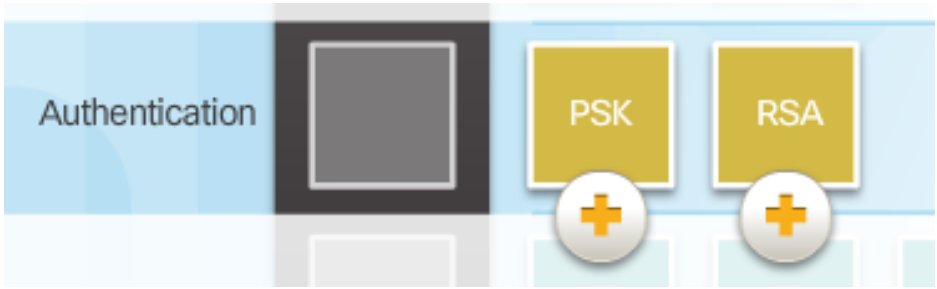
Algorytmy hashujące



Bezpieczeństwo algorytmów hashujących

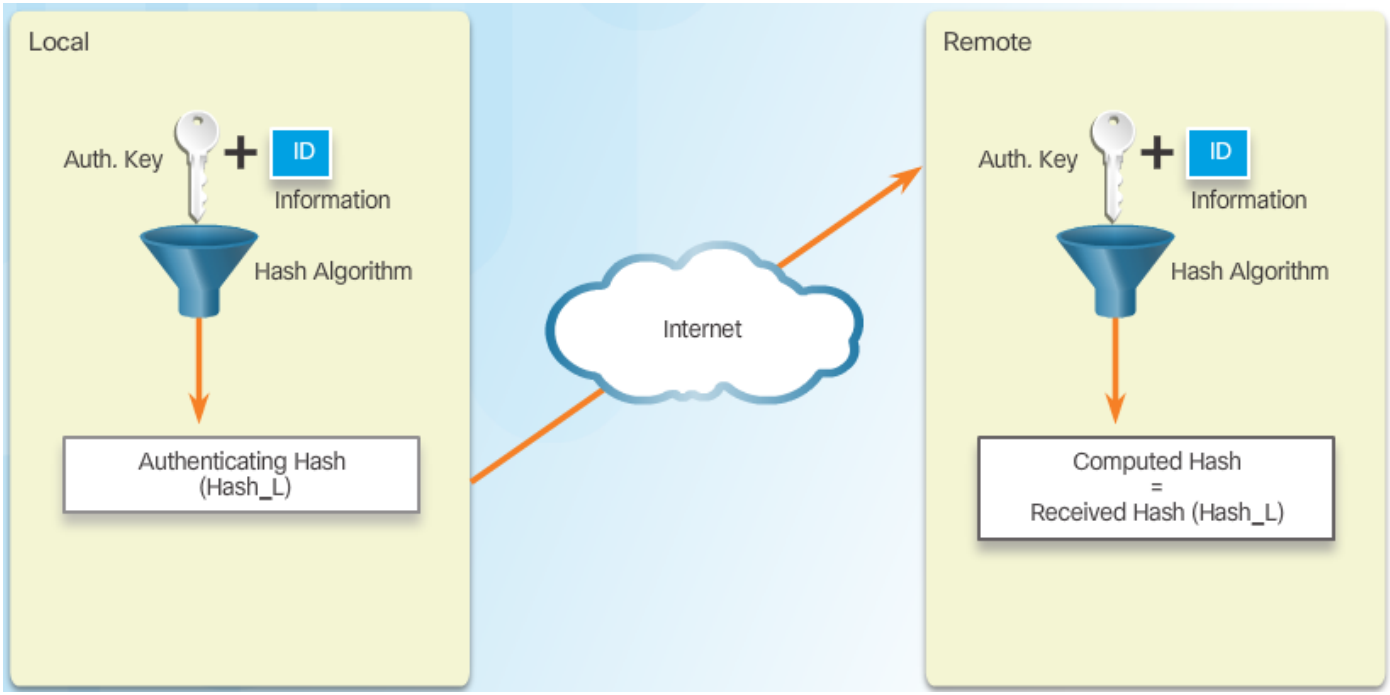


Uwierzytelnianie



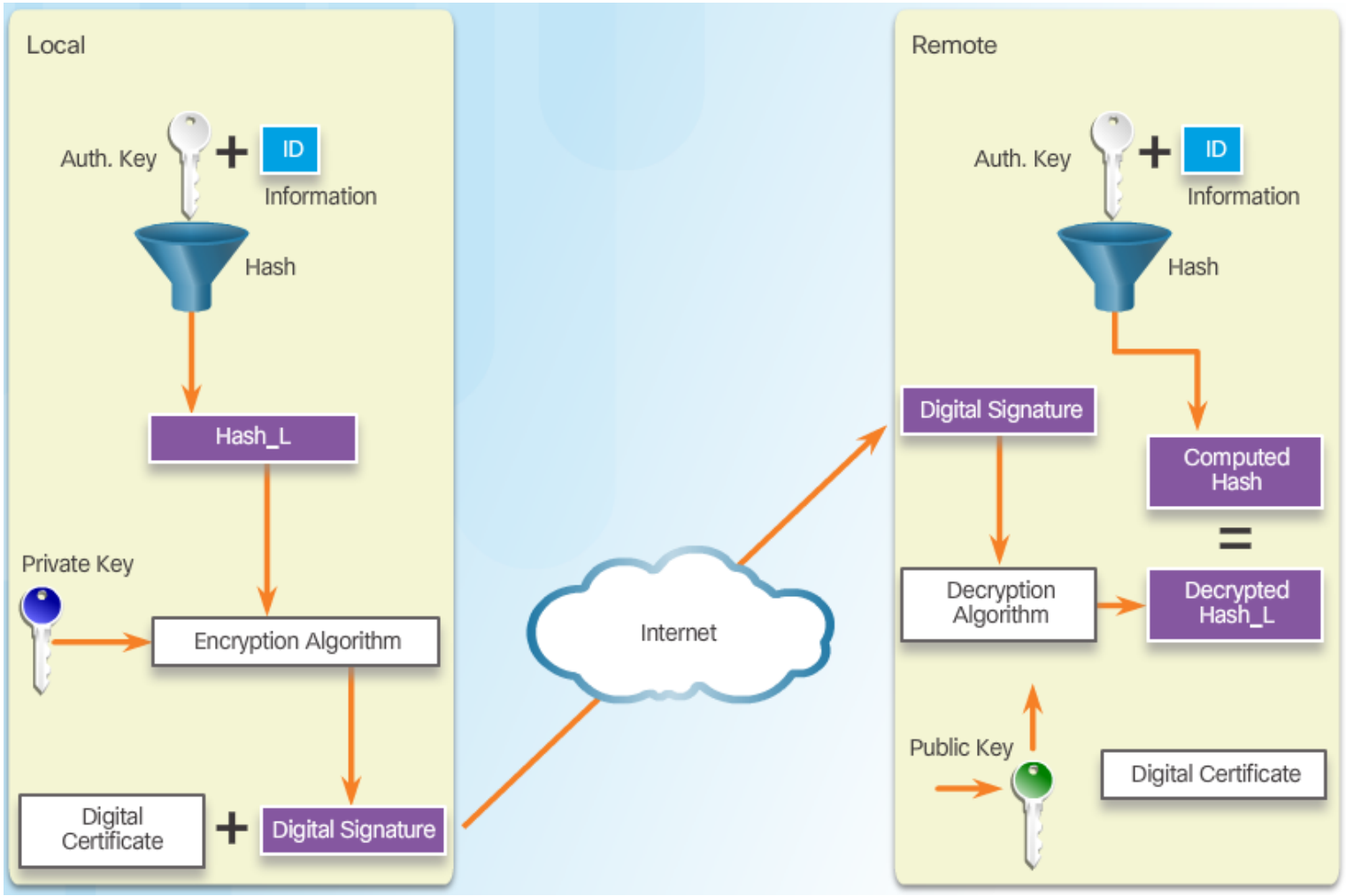
Metody uwierzytelniania węzłów

PSK



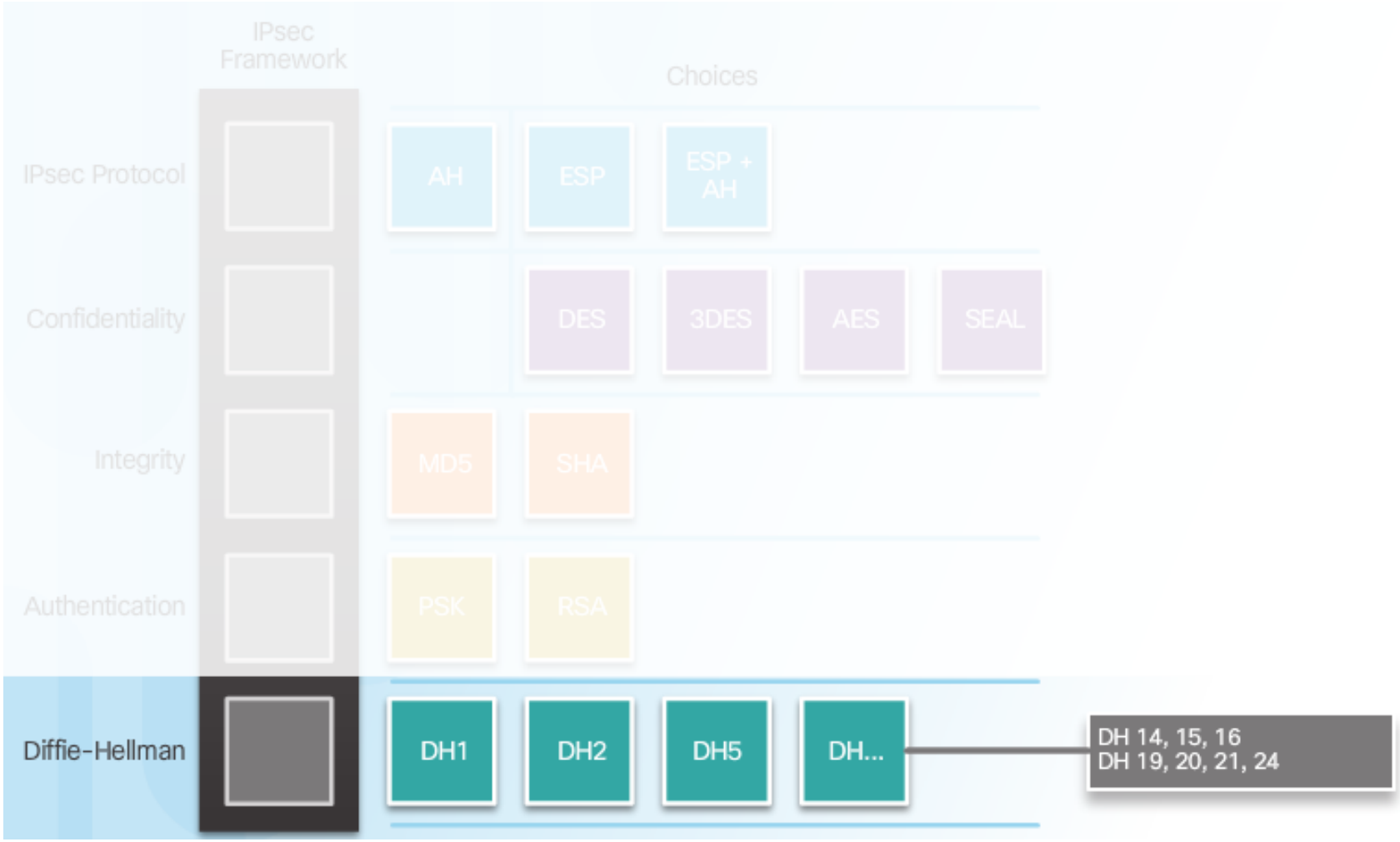
Uwierzytelnianie (Cont.)

RSA



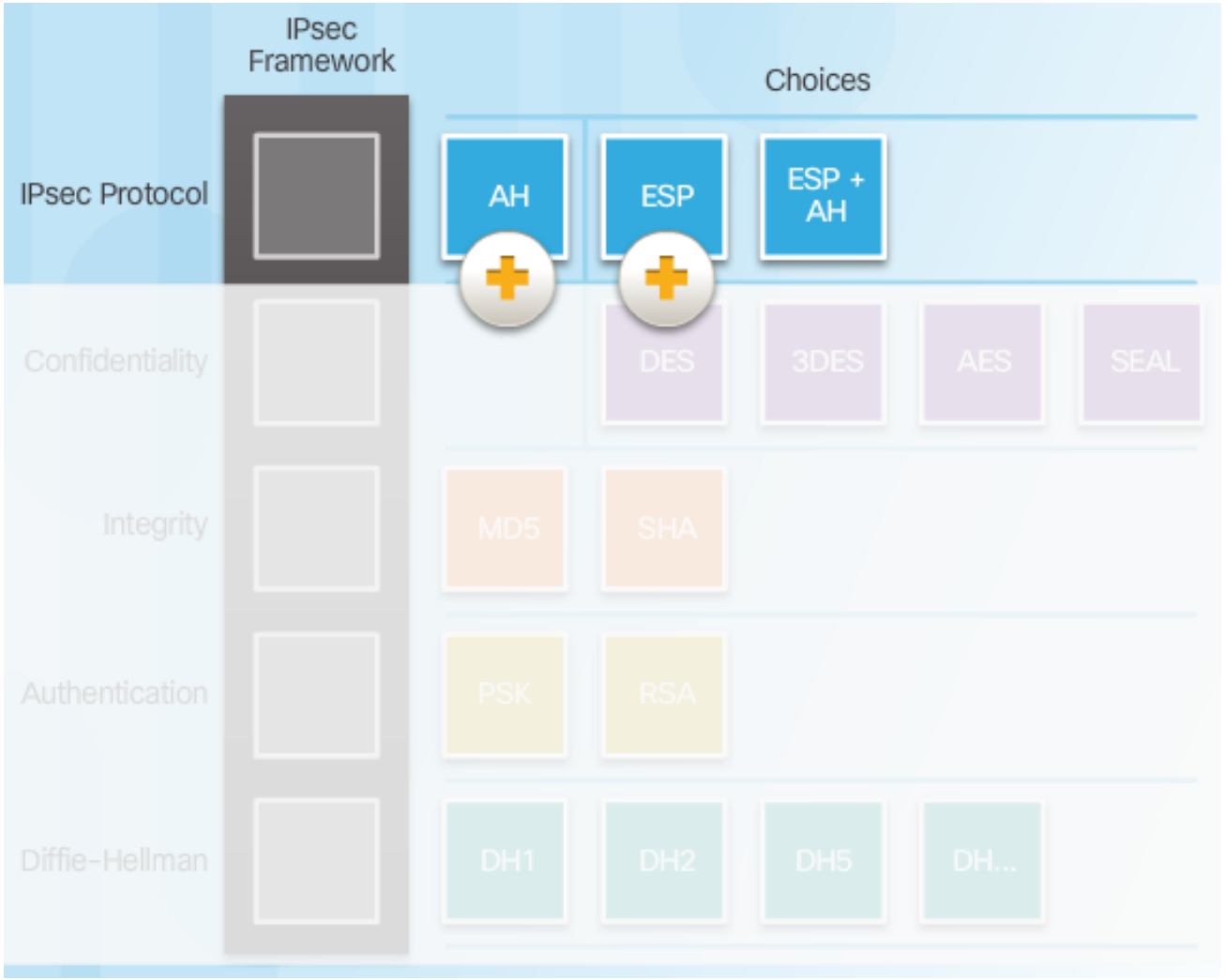
Bezpieczna wymiana kluczy

Wymiana kluczy Diffie-Hellman’a



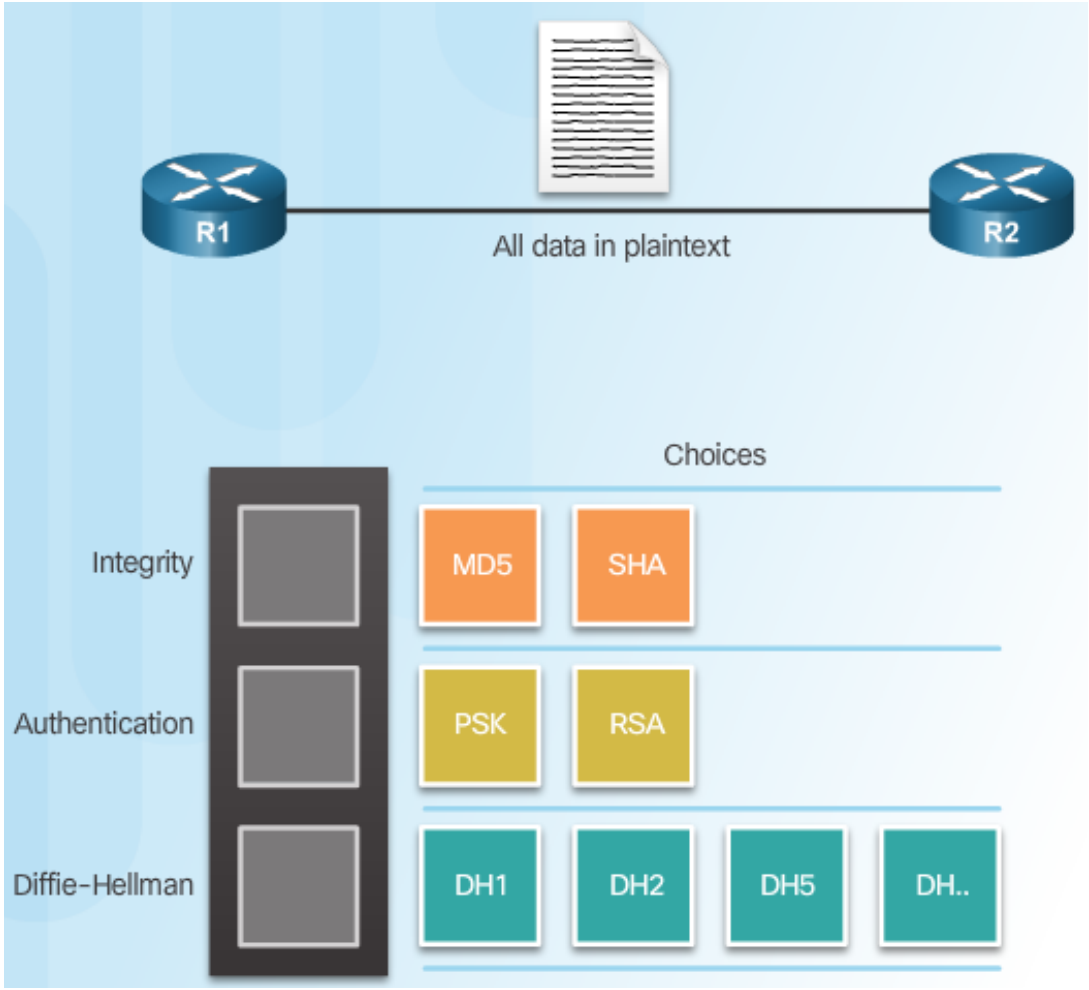
Temat 1.2.2: Protokoły IPSec

Przegląd protokołów IPSec

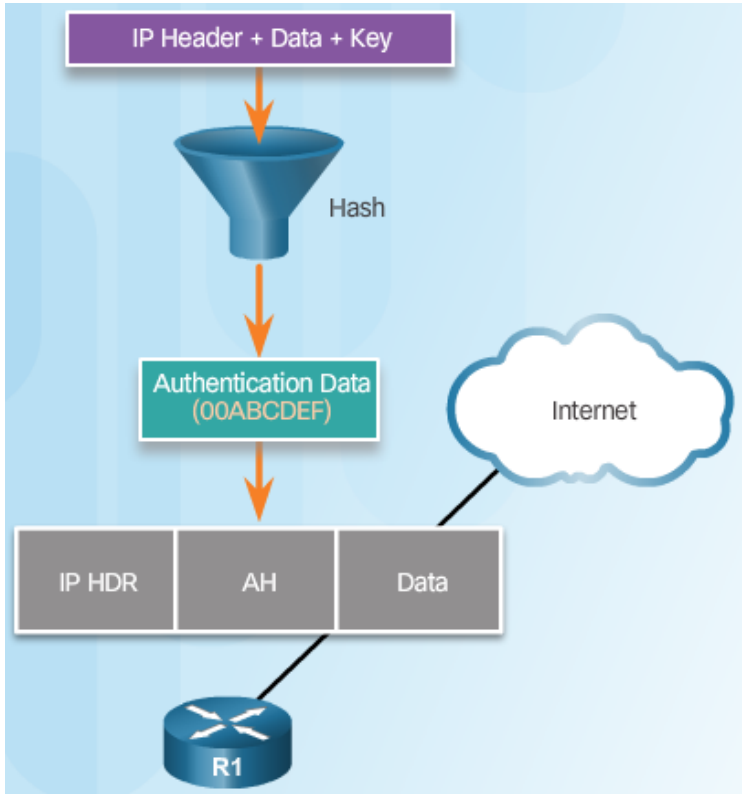


Authentication Header

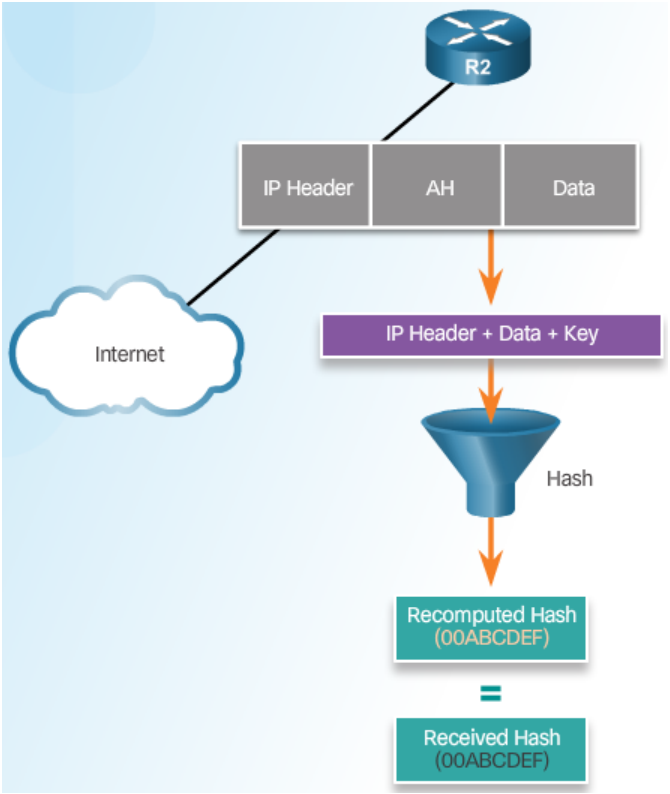
Protokoły AH



Authentication Header (Cont.)

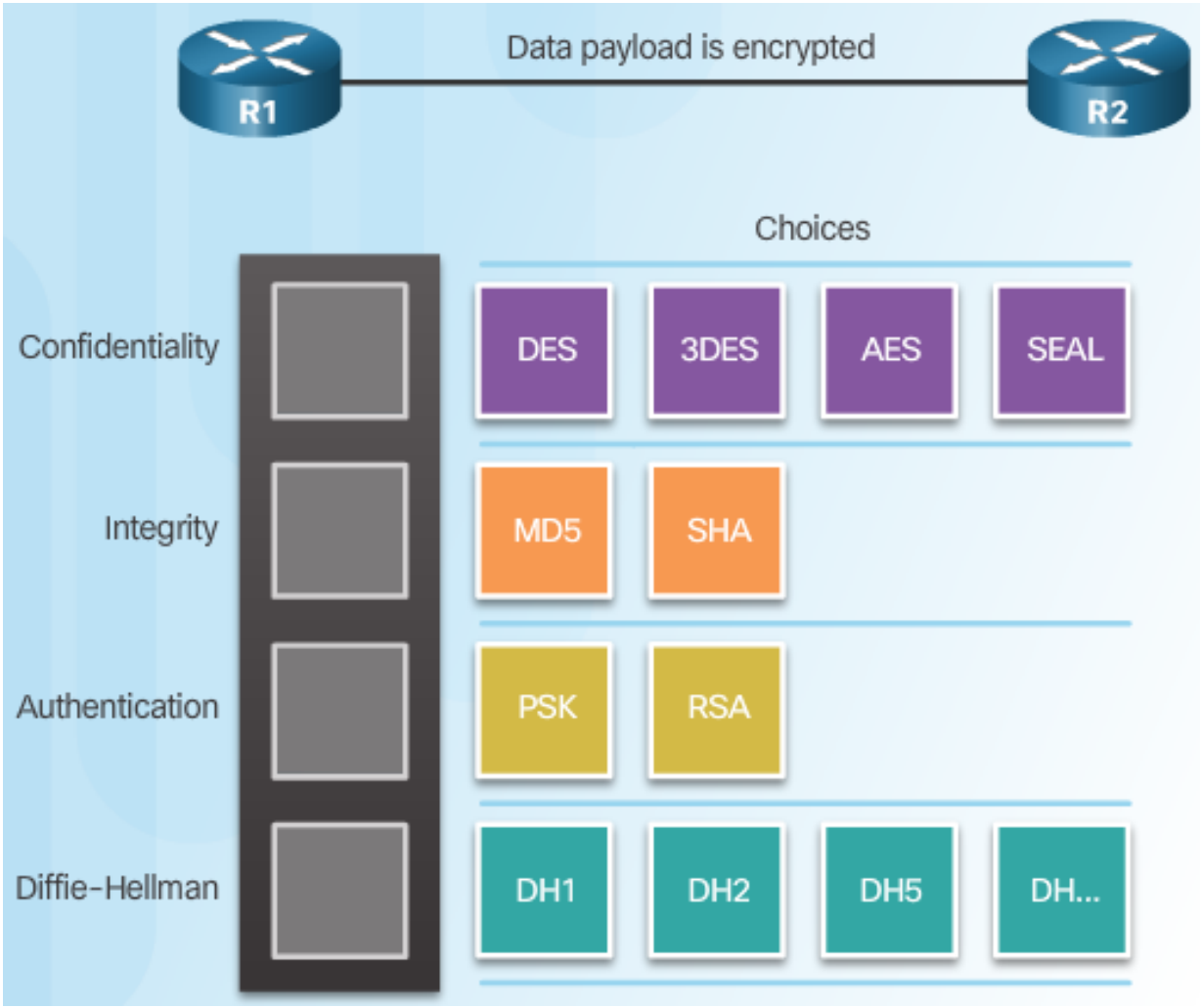


Router generuje hash i przesyła go to węzła

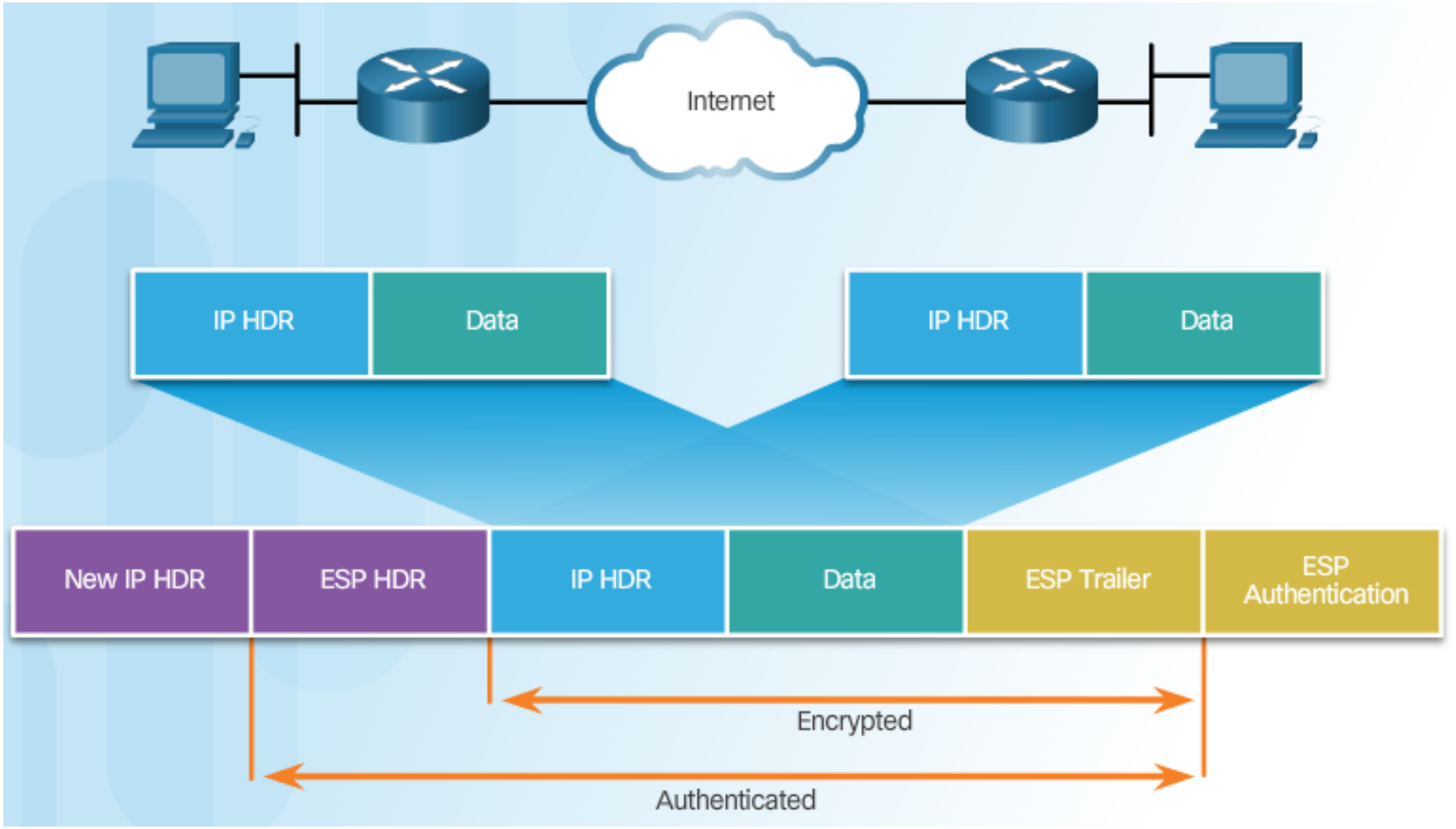


Węzeł (router) porównuje obliczony hash z tym otrzymanym

ESP

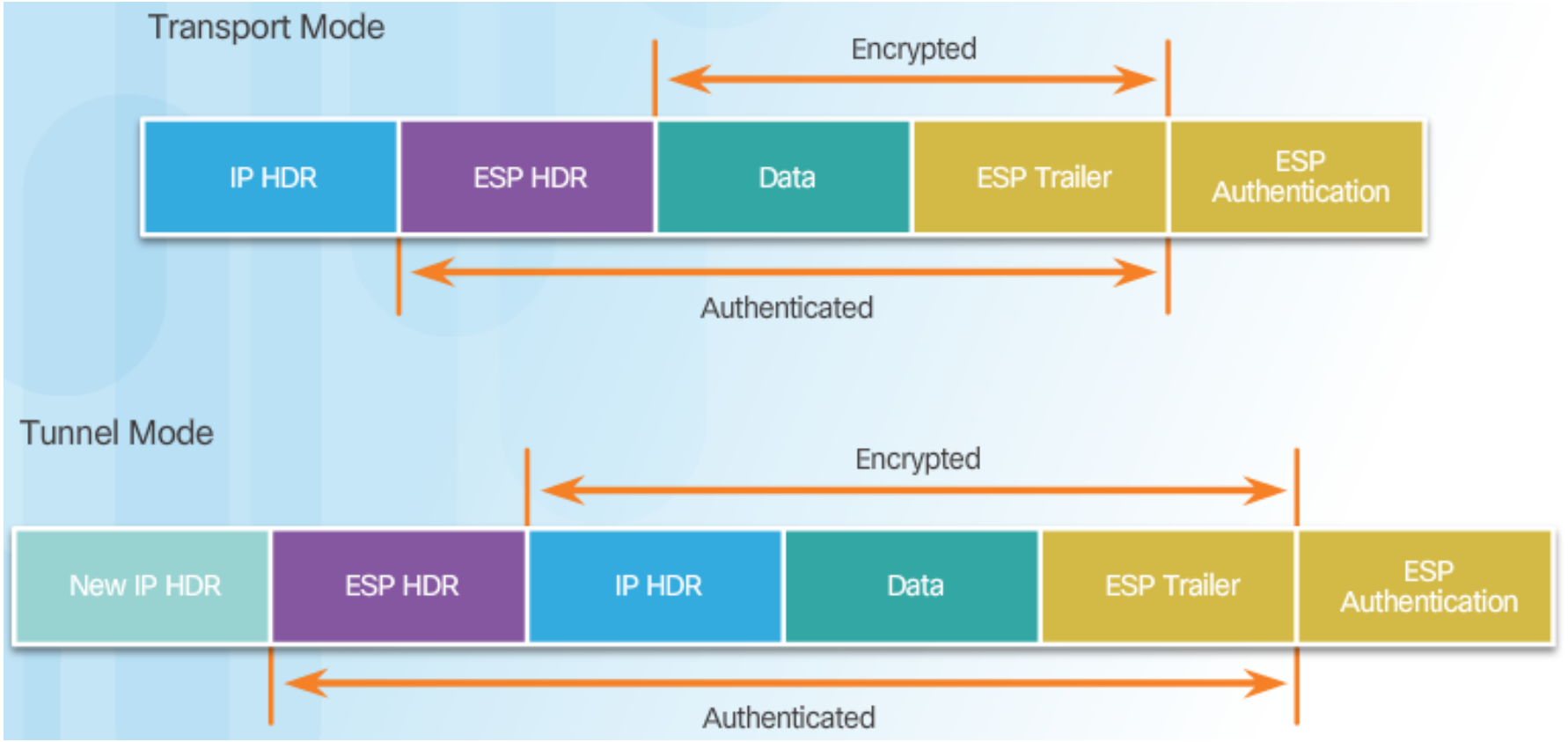


ESP szyfruje i uwierzytelnia



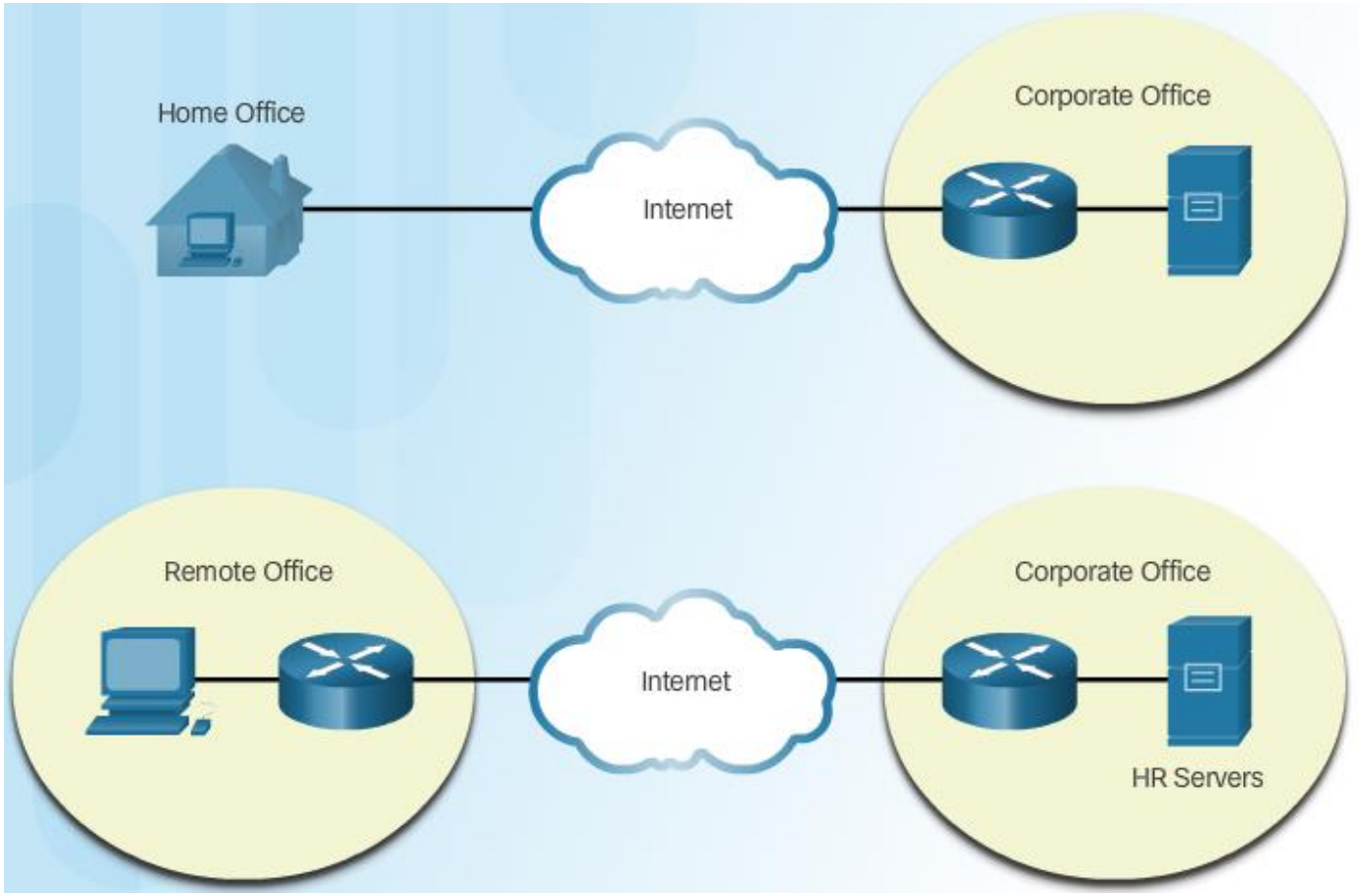
Tryby Transport oraz Tunnel

Używanie ESP oraz AH w dwóch trybach



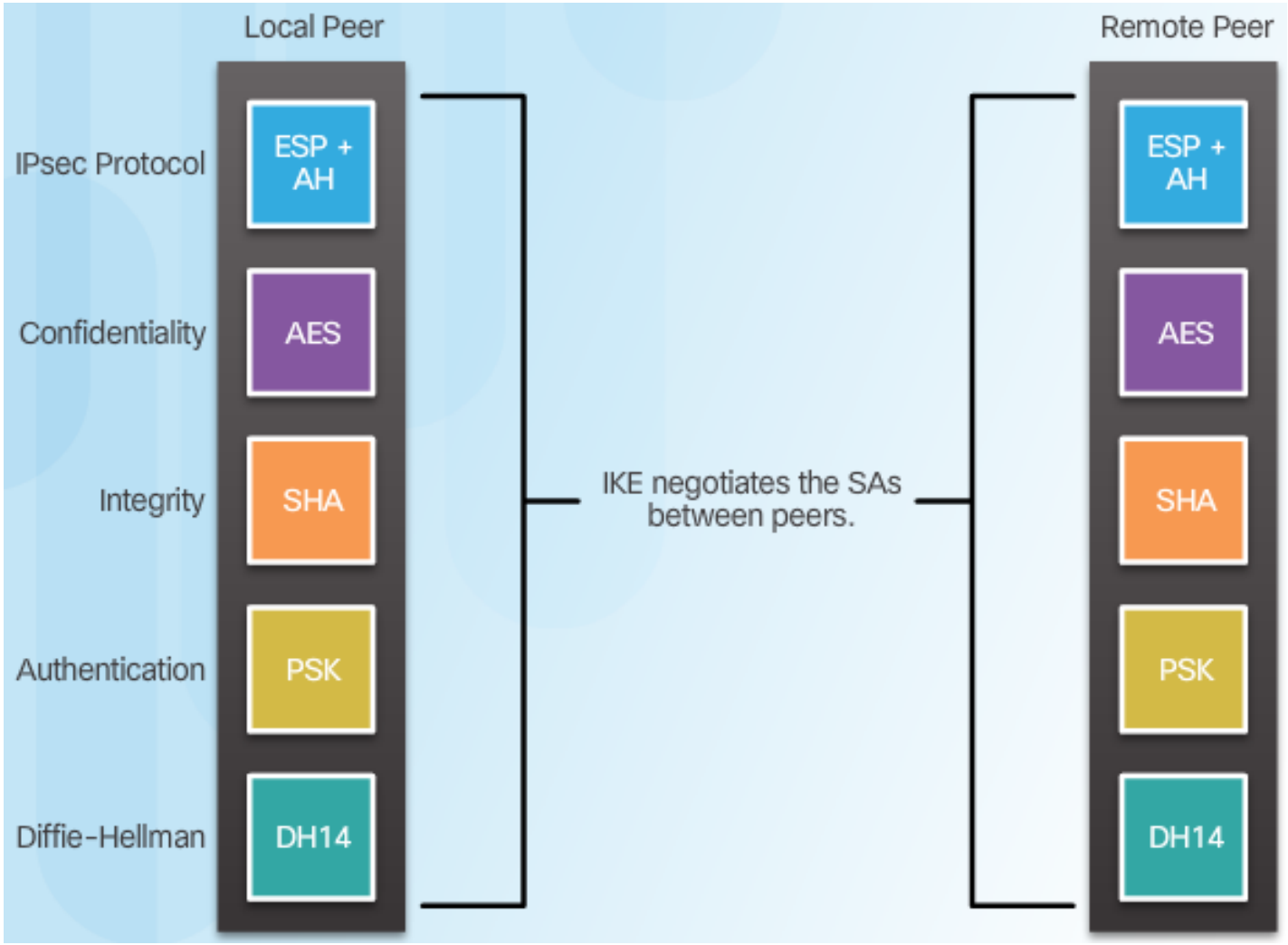
Tryby Transport oraz Tunnel (Cont.)

ESP Tunnel Mode

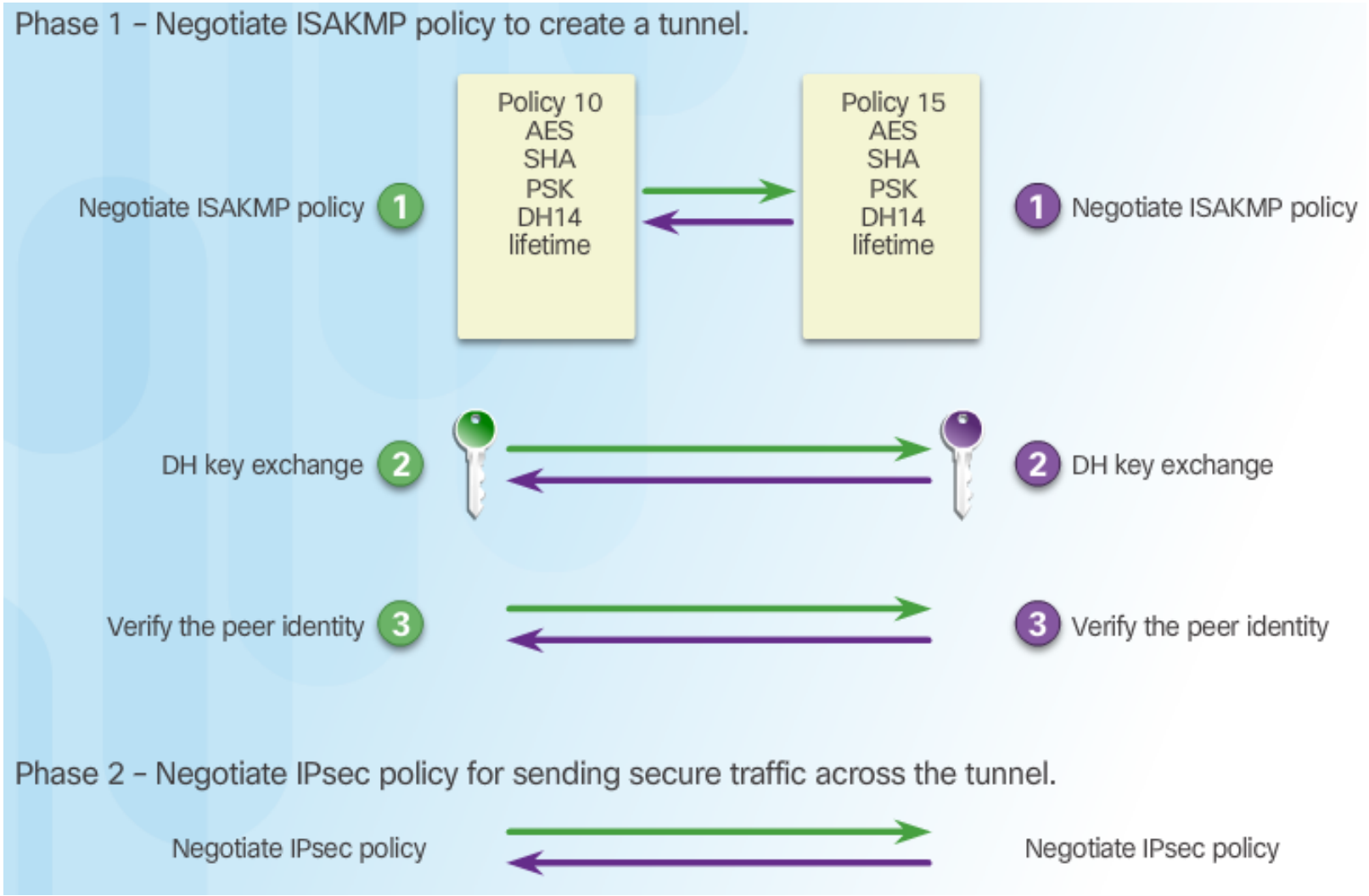


Temat 1.2.3:
Internet Key Exchange

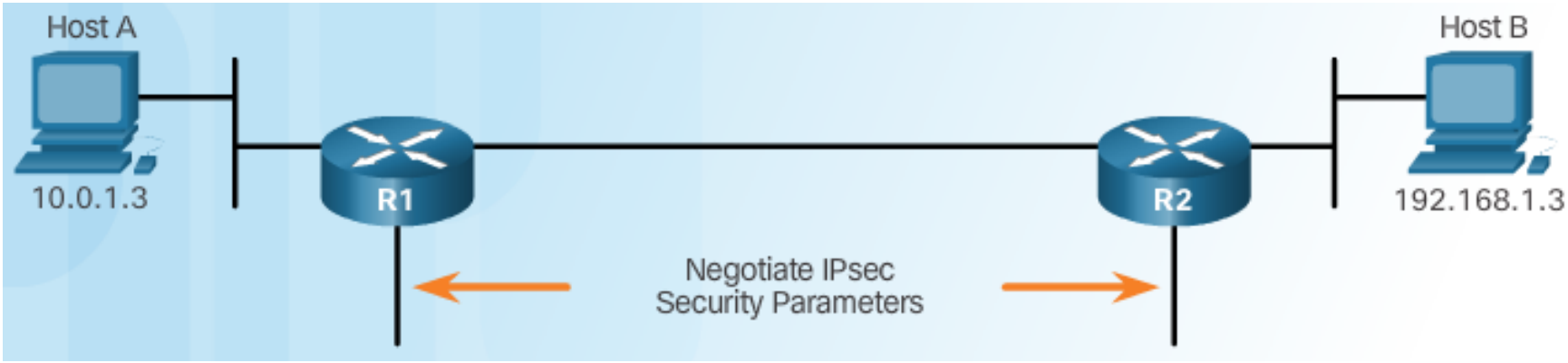
Protokół IKE



Faza 1 i 2 negocjacji klucza



Faza 2: Negocjacja SA



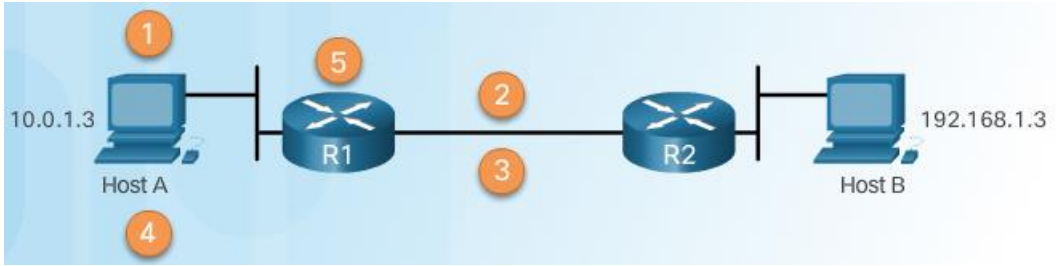
Rozdział 1.3: Implementacja Site-to-Site IPsec VPN z użyciem CLI

Po zakończeniu tej sekcji powinieneś być w stanie:

- Opisać negocjację IPsec i pięć kroków konfiguracji IPsec.
- Skonfigurować politykę ISAKMP.
- Skonfigurować zasady IPsec.
- Skonfigurować i zastosować crypto mapę.
- Sprawdzić działanie VPN IPsec.

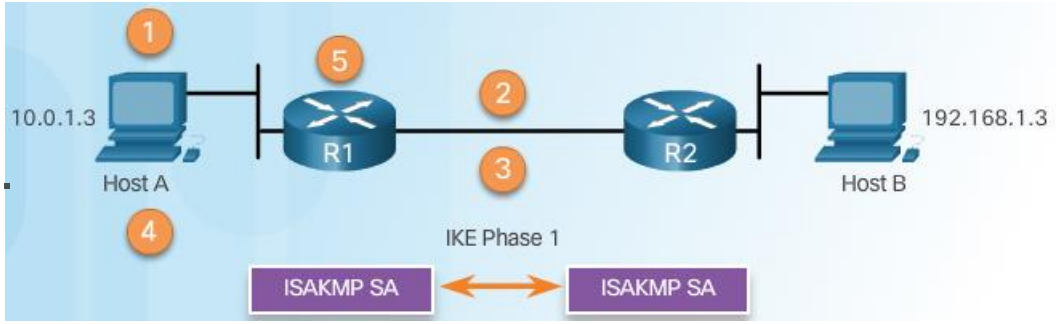
Temat 1.3.1:
Konfiguracja Site-to-Site IPsec VPN

Negocjacja IPsec

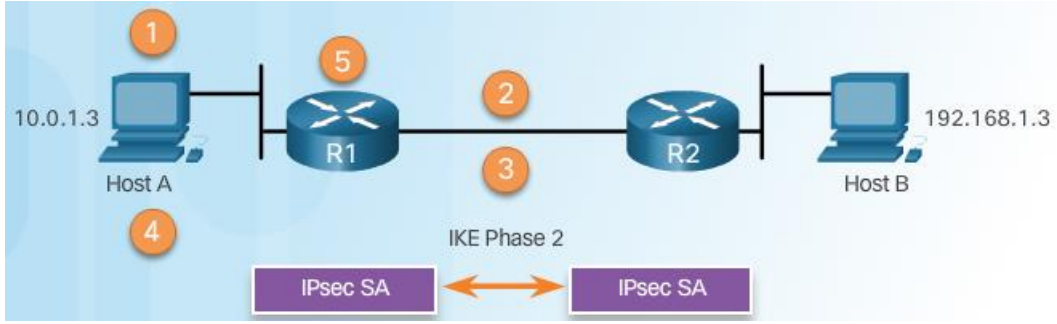


Negocjacja IPsec VPN: Krok 1 - Host A wysyła wiadomości do Hosta B.

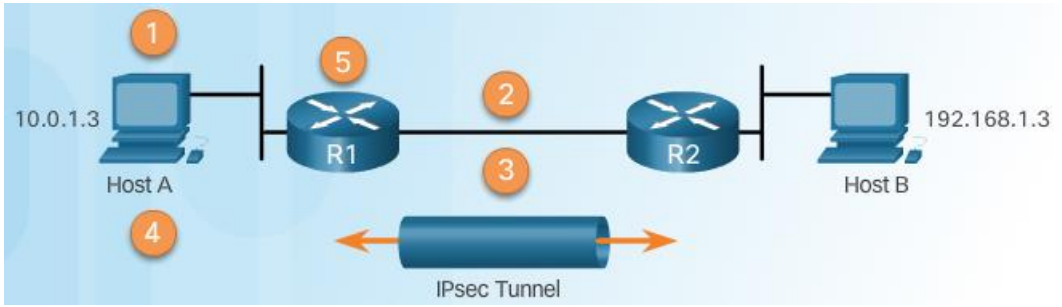
Negocjacja IPsec VPN: Krok 2 - R1 oraz R2 negocjują Fazę 1 sesji IKE.



Negocjacja IPsec VPN: Krok 3 - R1 oraz R2 negocjują Fazę 2 sesji IKE.

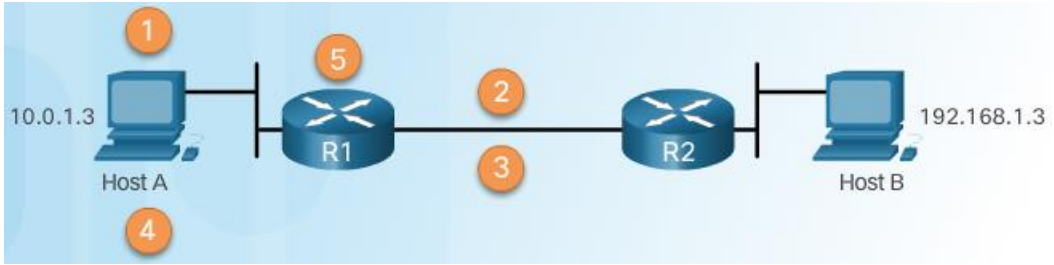


Negocjacja IPsec (Cont.)



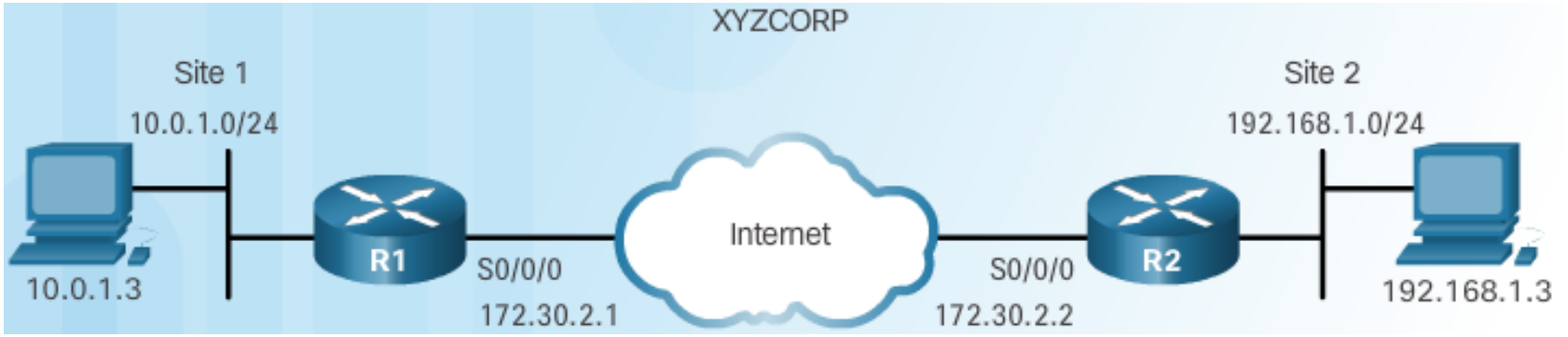
Negocjacja IPsec VPN: Krok 4 – Informacje wymieniane są poprzez tunel IPsec.

Negocjacja IPsec VPN: Krok 5 – Tunel Ipsec jest zamykany.



Topologia Site-to-Site IPsec VPN

Zadania konfiguracyjne IPsec VPN



Polityka bezpieczeństwa XYZCORP	Zadania konfiguracyjne
Szyfruj ruch z wykorzystaniem AES 256 i SHA	1. Skonfiguruj politykę ISAKMP dla Fazy 1 IKE
Uwierzytelnianie PSK	2. Skonfiguruj politykę IPsec dla Fazy 2 IKE
Wymiana kluczy z grupą DH 24	3. Skonfiguruj crypto mapę dla polityki IPsec
Lifetime dla tunelu ISAKMP 1 godzina	4. Zastosuj politykę IPsec
Tunel IPsec używa ESP z lifetime 15-min.	5. Zweryfikuj działanie tunelu IPsec

Konfiguracja ACL

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
```

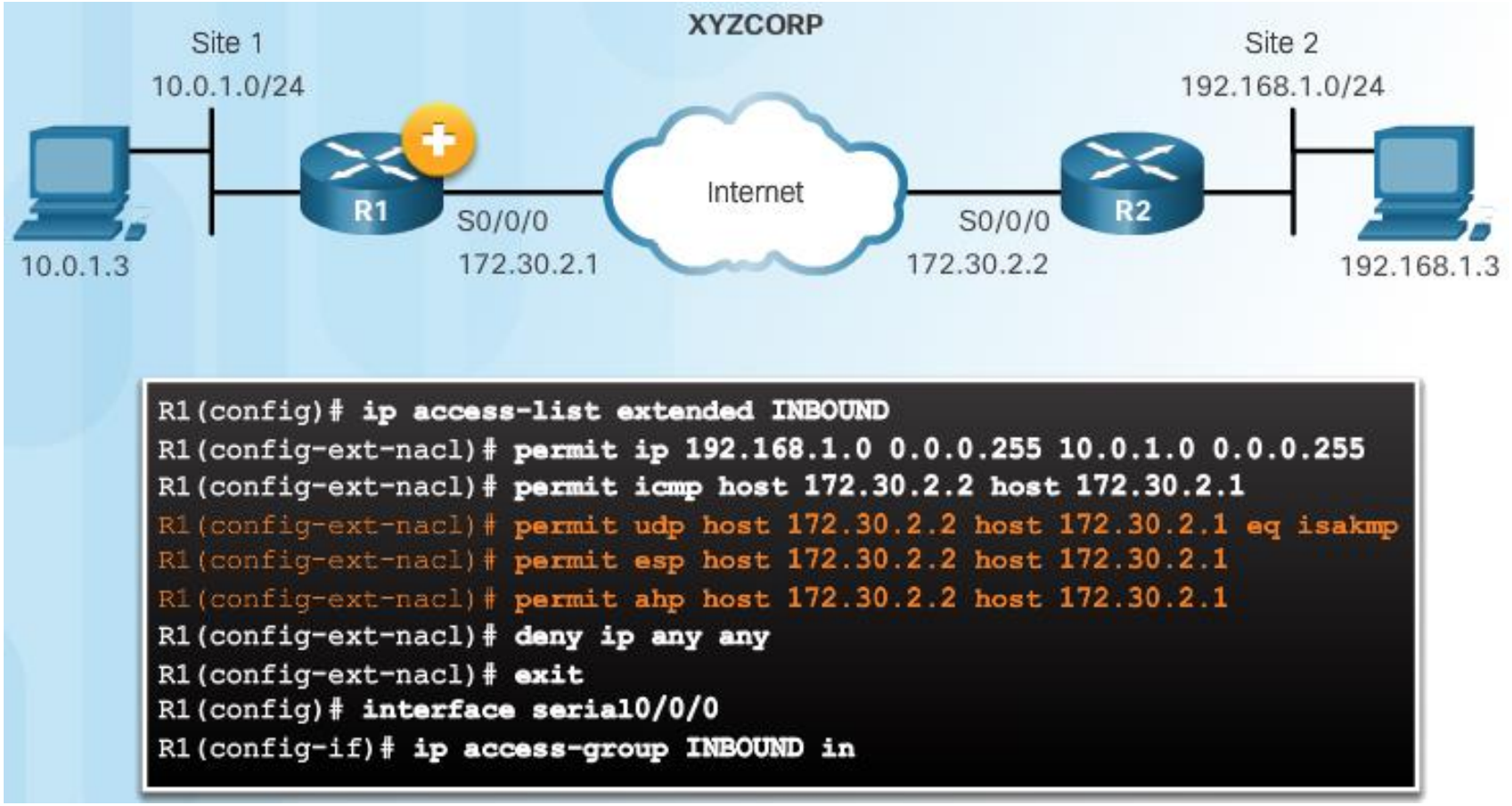
Permit AH Traffic

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

Składnia poleceń dla ruchu IPsec

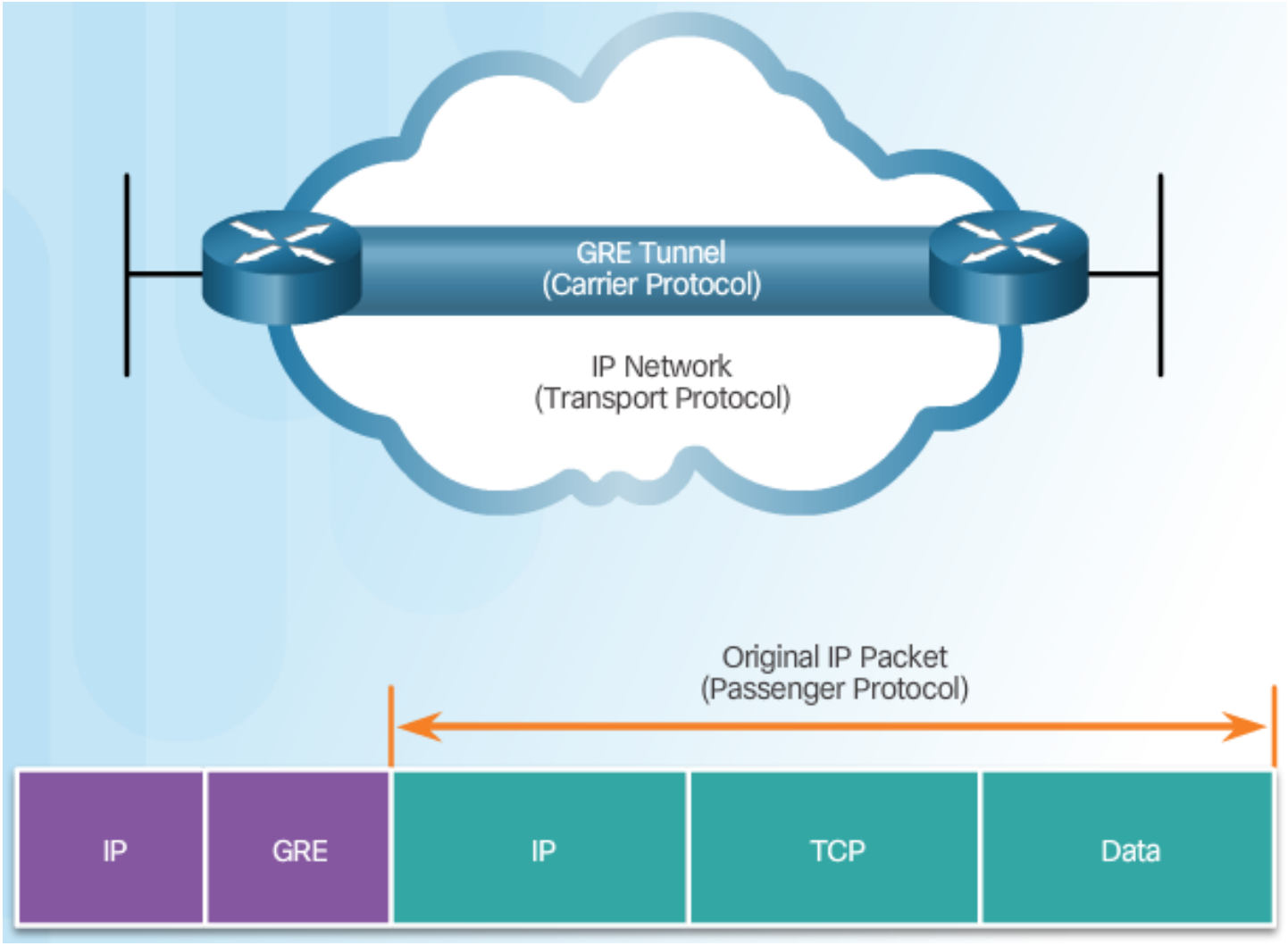
Konfiguracja ACL (Cont.)

Permitting Traffic for IPsec Negotiations

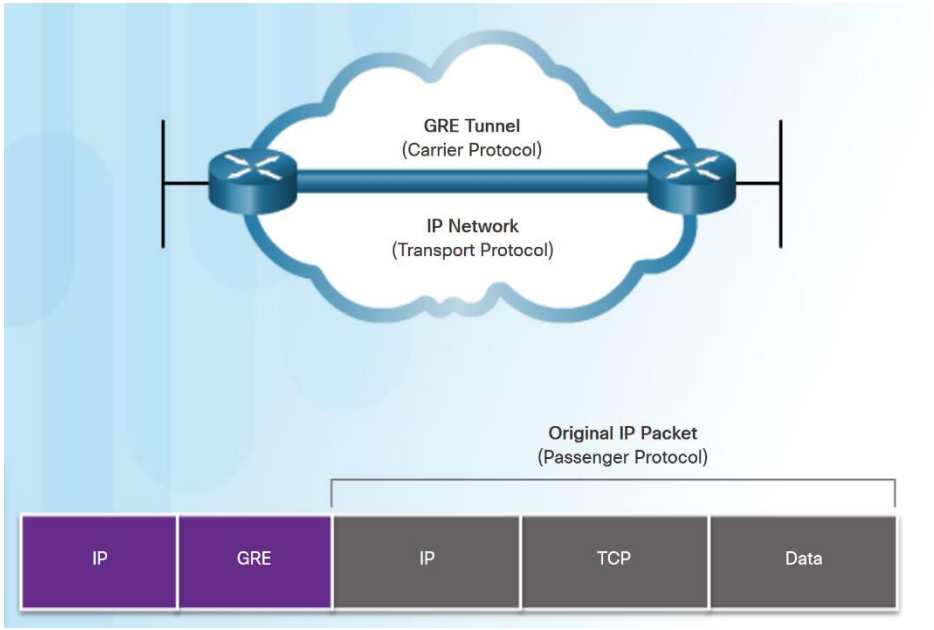


Temat 1.3.2: Tunele GRE

Wprowadzenie do tuneli GRE



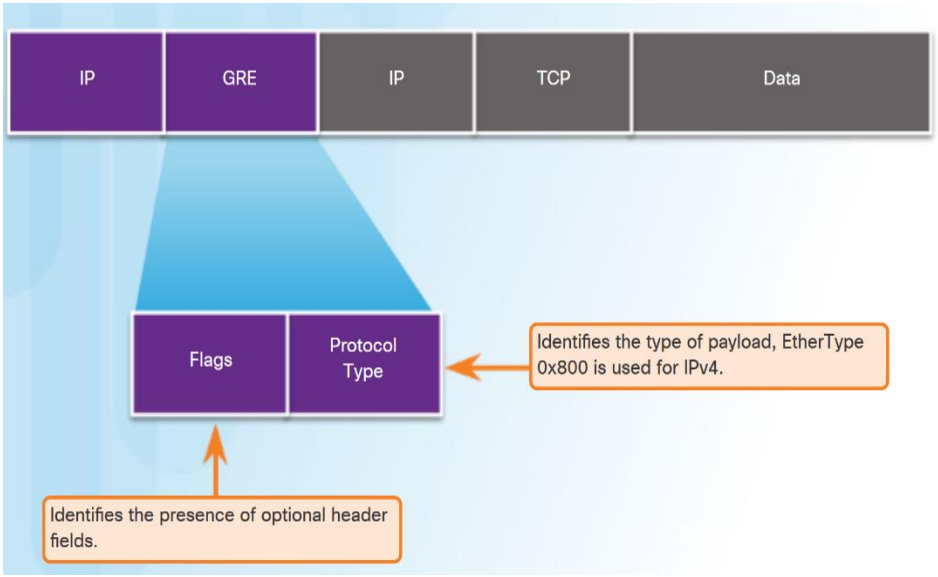
Wprowadzenie do tuneli GRE



- Generic Routing Encapsulation (GRE) jest niezabezpieczonym protokołem tunelowania VPN typu site-to-site.
- Opracowany przez Cisco.
- GRE zarządza transportem ruchu wieloprotokołowego i ruchu multicast między dwoma lub większą liczbą urządzeń (lokalizacji)
- Interfejs tunelowy obsługuje :

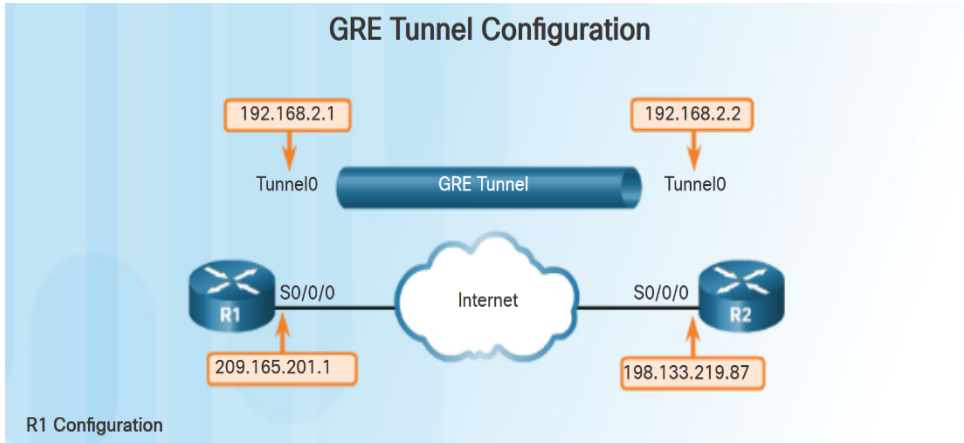
  Protokół enkapsulowany - lub protokół pasażera, taki jak IPv4, IPv6.
  Protokół enkapsulacji - lub protokół przewoźnika, taki jak GRE.
  Protokół transportowy, taki jak IP.

Charakterystyka GRE



- GRE jest zdefiniowany jako standard IETF (RFC 2784).
- W zewnętrznym nagłówku IP, liczba 47 jest używana w polu protokołu.
- Enkapsulacja GRE wykorzystuje pole typu protokołu w nagłówku GRE w celu obsługi enkapsulacji dowolnego protokołu warstwy 3 OSI.
- GRE jest bezstanowy.
- GRE nie zawiera żadnych silnych mechanizmów bezpieczeństwa.
- Nagłówek GRE wraz z nagłówkiem tunelowania IP tworzy co najmniej 24 bajty dodatkowego narzutu dla tunelowanych pakietów.

Konfiguracja GRE



R1 Configuration

```
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
```

```
R2(config)# interface Tunnel0
R2(config-if)# tunnel mode gre ip
R2(config-if)# ip address 192.168.2.2 255.255.255.0
R2(config-if)# tunnel source 198.133.219.87
R2(config-if)# tunnel destination 209.165.201.1
R2(config-if)# router ospf 1
R2(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

- Pięć kroków konfiguracji tunelu GRE:

  Krok 1. Utwórz interfejs tunelu za pomocą polecenia **interface tunnel** *number* .
  Krok 2. Skonfiguruj adres IP interfejsu tunelu. (Zwykle adres prywatny)
  Krok 3. Określ adres IP źródła tunelu.
  Krok 4. Określ adres docelowy IP tunelu.
  Krok 5. (Opcjonalnie) Określ tryb tunelu GRE jako tryb pracy interfejsu tunelu.

Weryfikacja GRE

- Użycie polecenia **show ip interface brief** w celu weryfikacji czy interfejs tunelu jest w stanie **up**.
- Użycie polecenia **show interface tunnel** w celu weryfikacji stanu tunelu.
- Użycie polecenia **show ip ospf neighbor** w celu weryfikacji czy sąsiedztwo w ramach protokołu OSPF zostało ustanowione przez interfejs tunelowy.

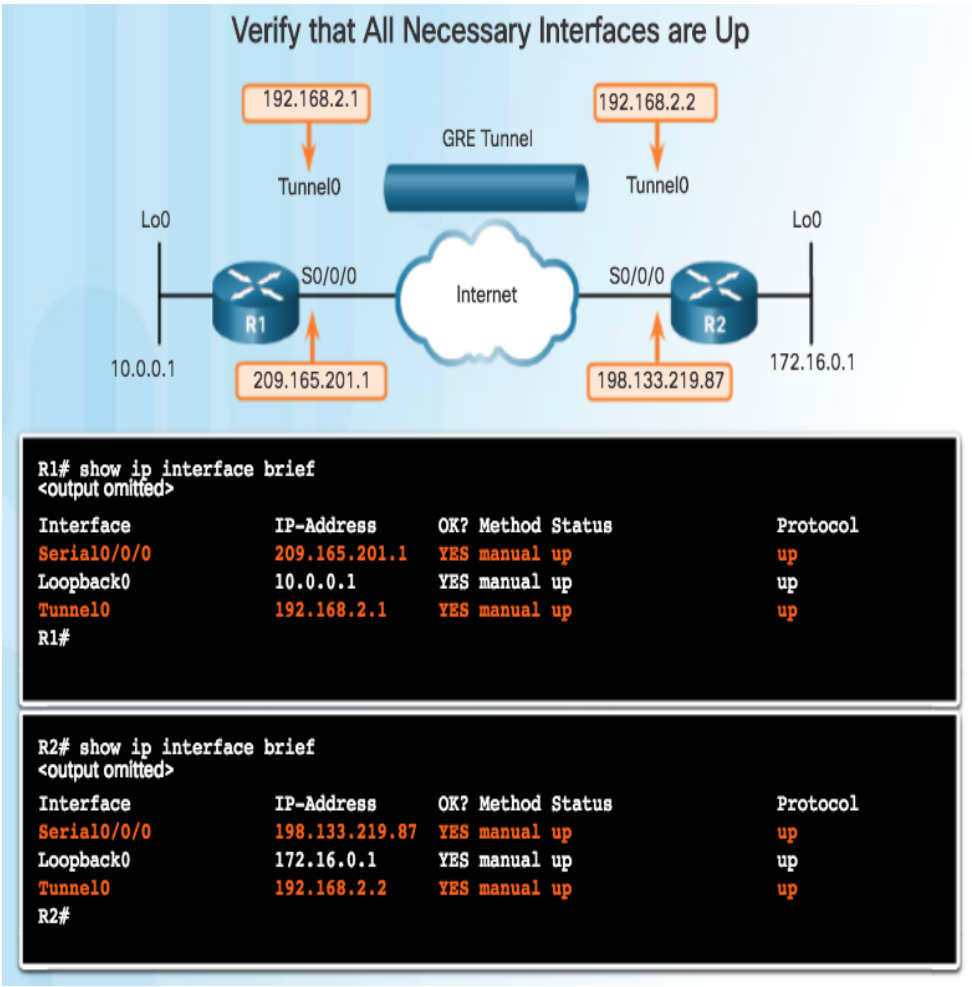
```
R1# show ip interface brief | include Tunnel

Tunnel0            192.168.2.1     YES manual up      up
```

```
R1# show interface Tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.2.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 209.165.201.1, destination 209.165.201.2
  Tunnel protocol/transport GRE/IP
<output omitted>
```

```
R1# show ip ospf neighbor

Neighbor ID     Pri State       Dead Time  Address     Interface
209.165.201.2   0   FULL/  -    00:00:37   192.168.2.2   Tunnel0
```

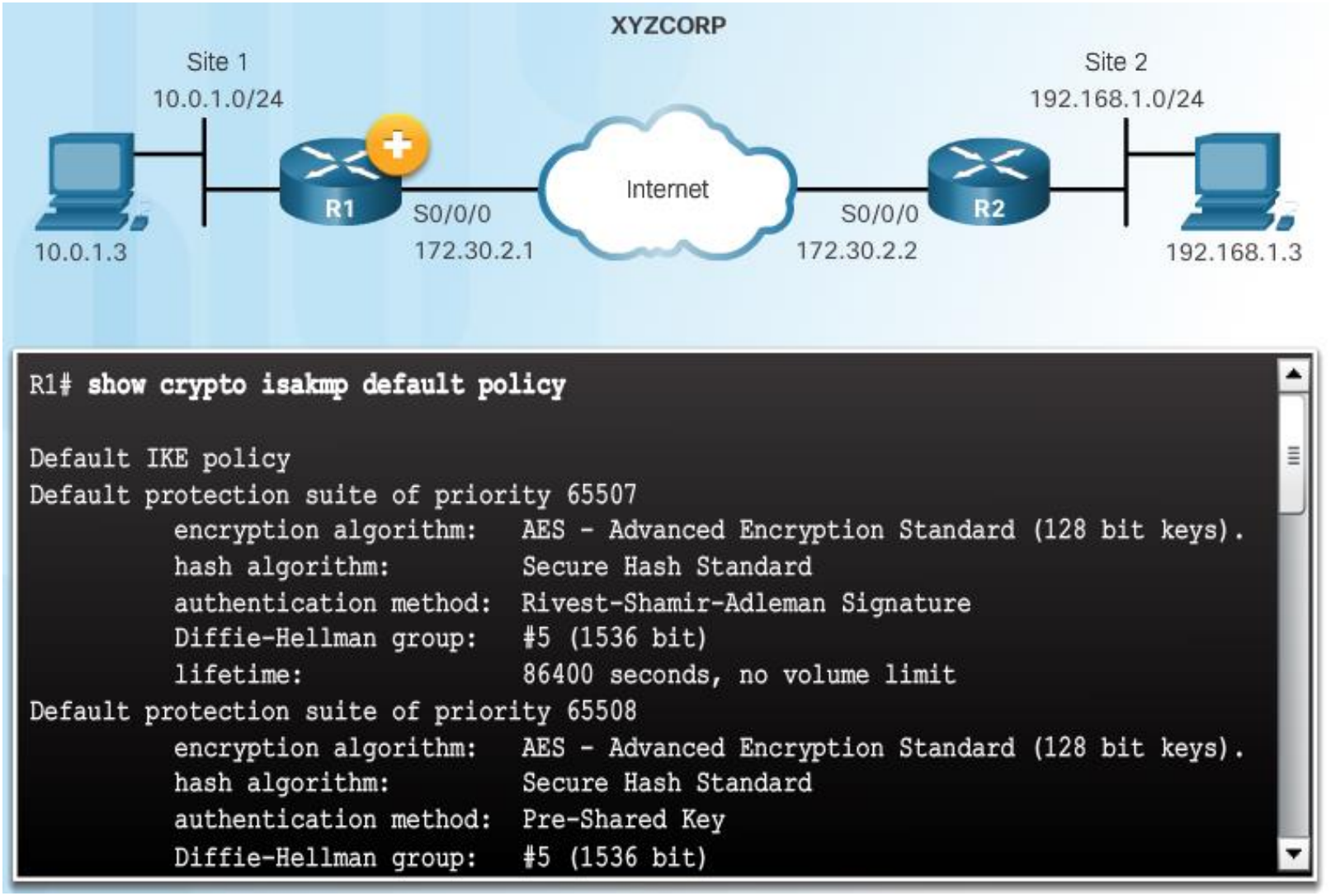
Rozwiązywanie problemów z tunelem GRE

- Problemy z GRE są zwykle spowodowane następującymi rzeczami:
  - Adresy IP interfejsu tunelu nie są w tej samej sieci lub maski podsieci nie pasują. Użyj polecenia **show ip interface brief**.
  - Interfejsy dla źródła tunelu i / lub miejsca docelowego nie są skonfigurowane z poprawnym adresem IP lub są wyłączone. Użyj polecenia **show ip interface brief**.
  - Routing statyczny lub dynamiczny nie jest poprawnie skonfigurowany. Użyj **show ip route** lub **show ip ospf neighbour**.



Temat 1.3.3: ISAKMP Policy

Domyślne polityki ISAKMP




```
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)
```

Konfiguracja nowej polityki ISAKMP


```
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
```

Konfiguracja polityki ISAKMP dla XYZCORP


```
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#
```

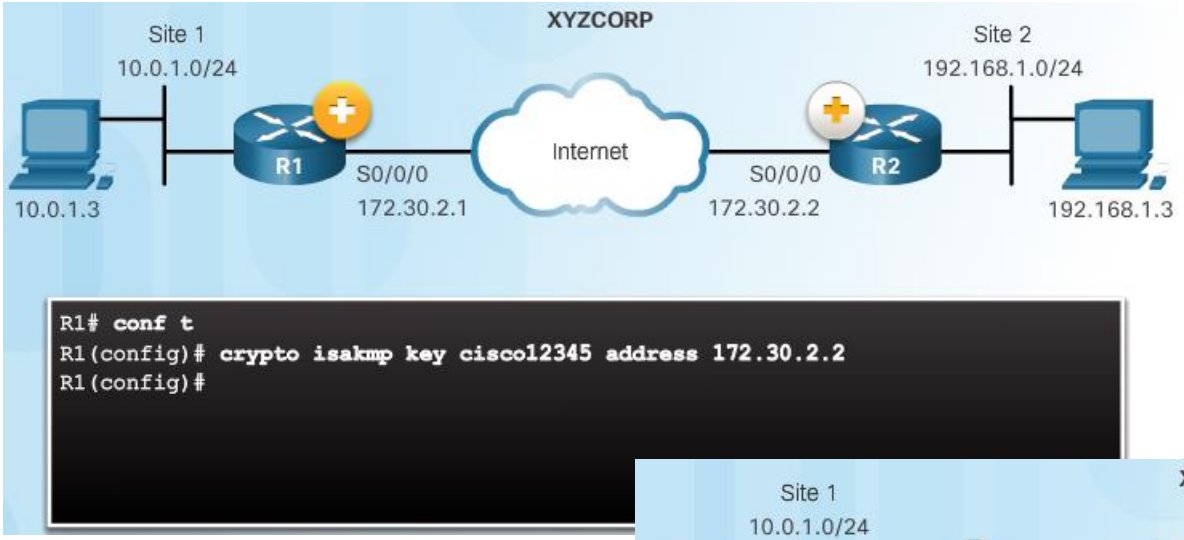
Konfiguracja współdzielonego klucza

Polecenie `crypto isakmp key`

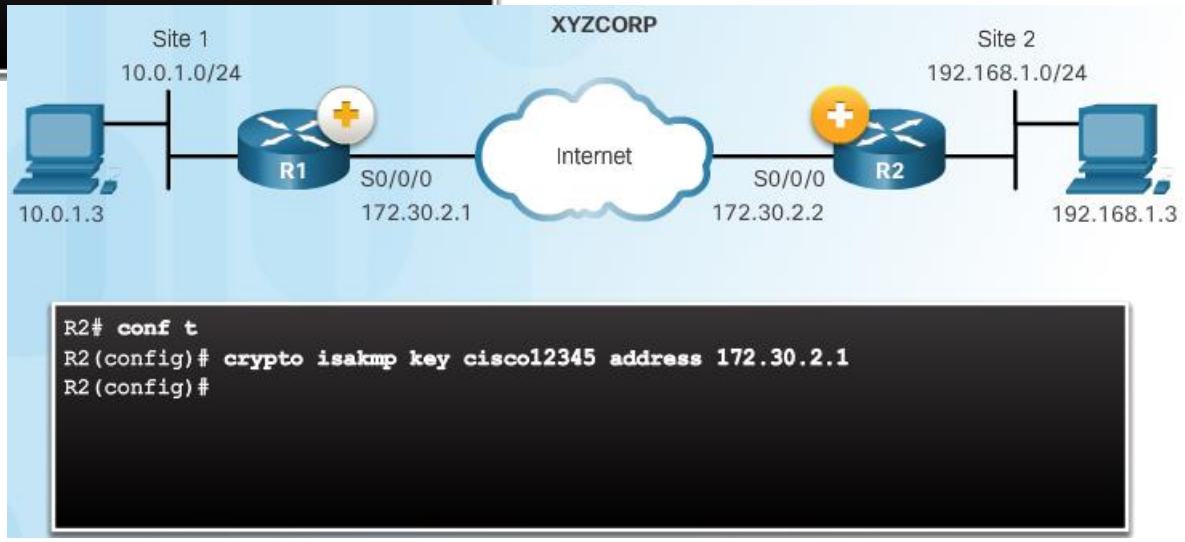
```
Router(config)#
crypto isakmp key keystring address peer-address

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

Konfiguracja współdzielonego klucza (Cont.)

Konfiguracja współdzielonego klucza




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

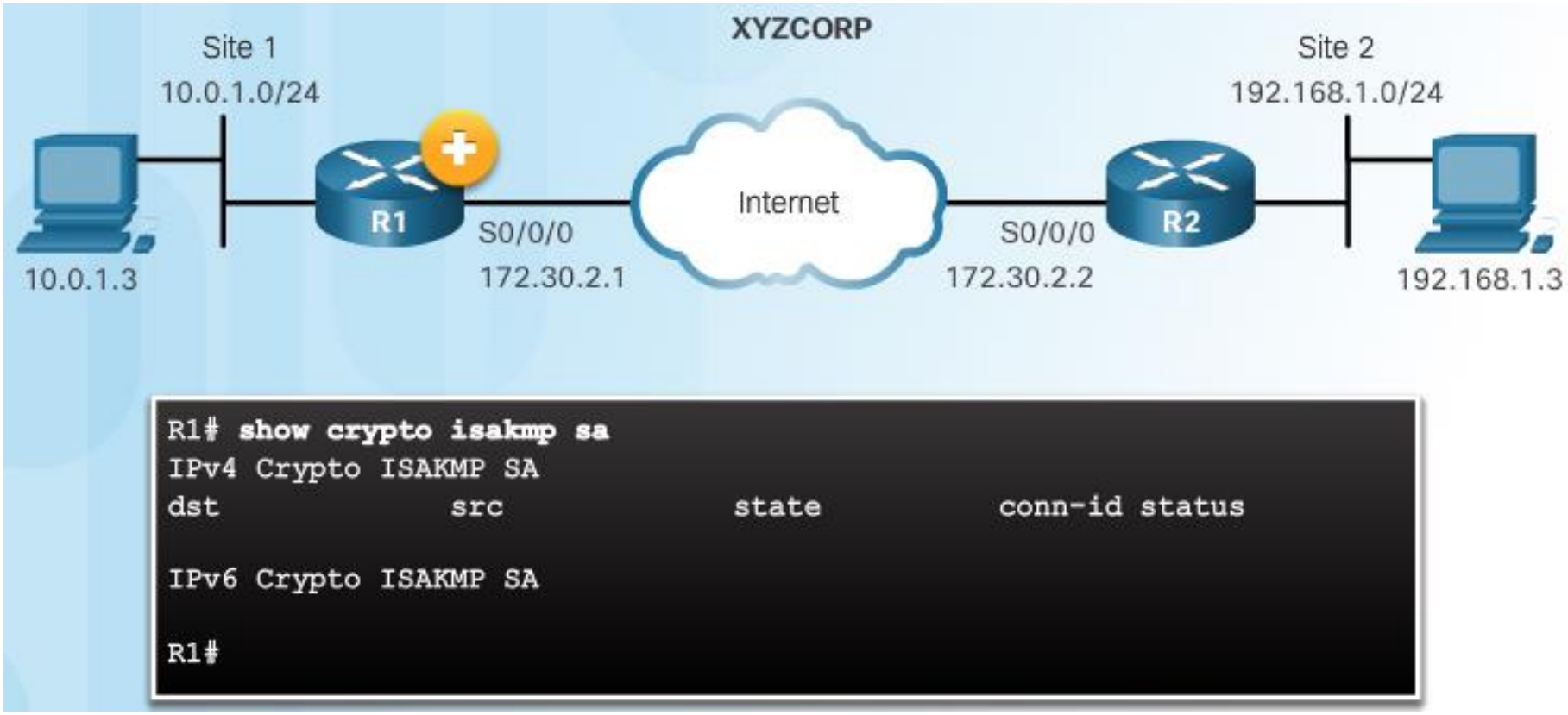



```
R2# conf t
R2(config)# crypto isakmp key cisco12345 address 172.30.2.1
R2(config)#
```

Temat 1.3.4:
IPsec Policy

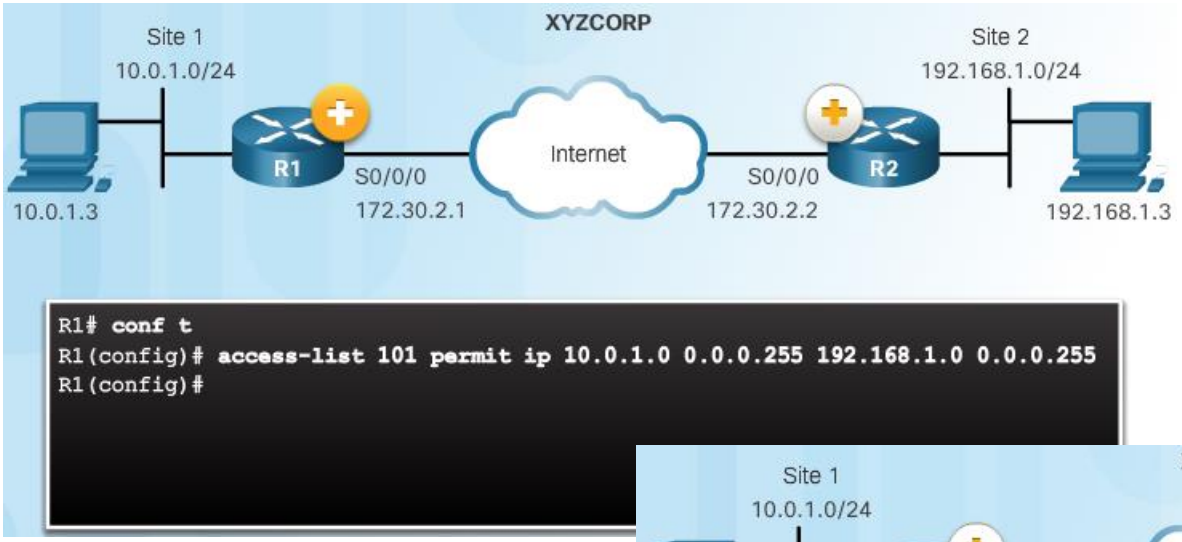
Definiowanie interesującego nas ruchu

Faza 1 IKE tunelu jeszcze nie istnieje

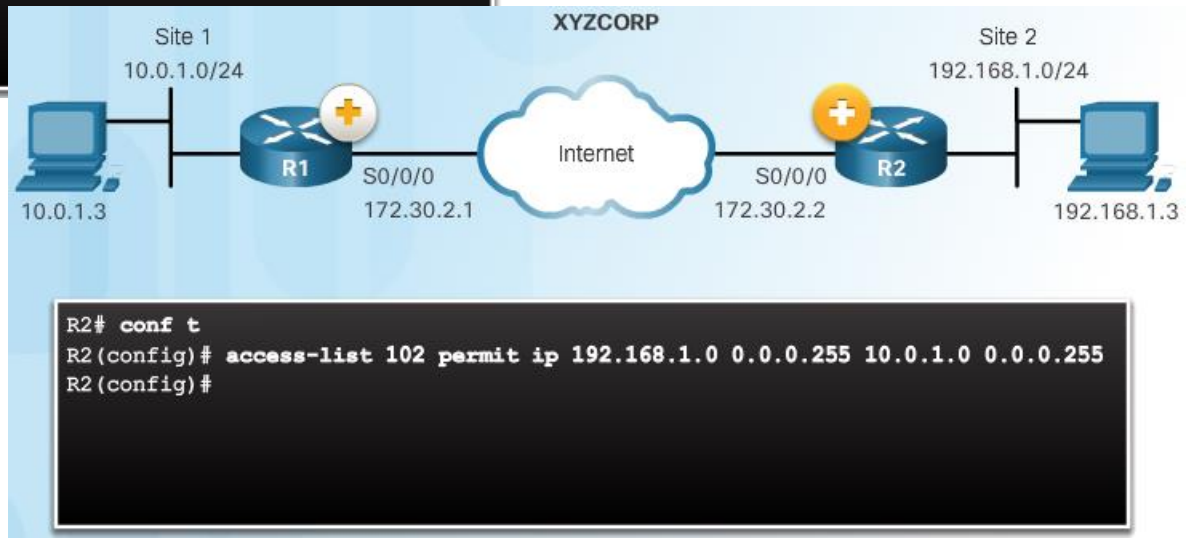


Definiowanie interesującego nas ruchu (Cont.)

Konfiguracja ACL w celu zdefiniowania interesującego nas ruchu




```
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)#
```

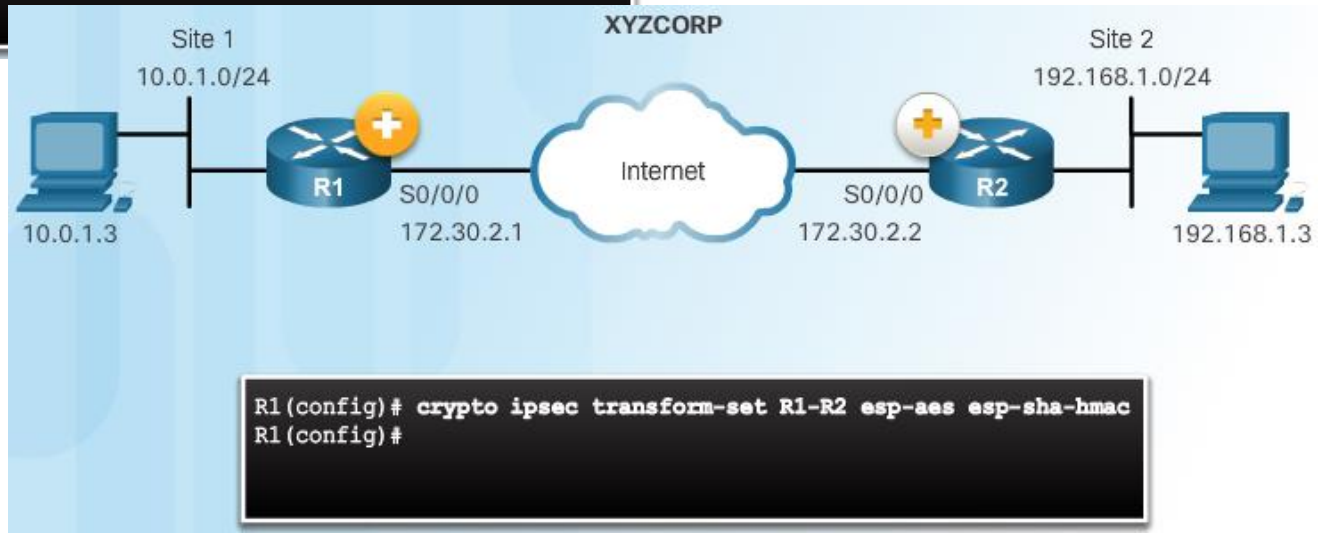
Konfiguracja IPsec Transform Set

Polecenie `crypto ipsec transform-set`


```
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
```

Konfiguracja IPsec Transform Set (Cont.)

Polecenie `crypto ipsec transform-set`



Temat 1.3.5: Crypto Mapa

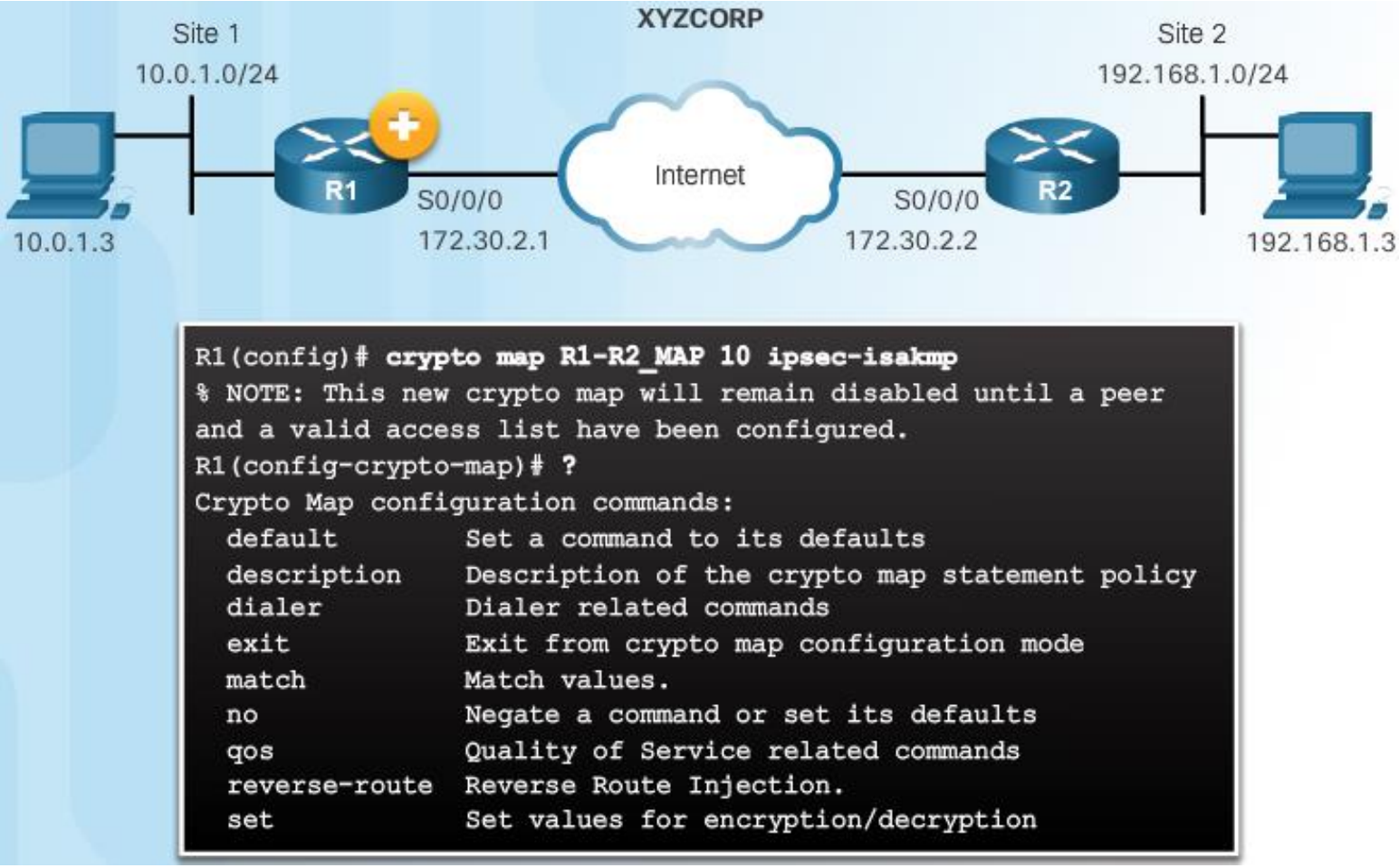
Składnia polecenia do konfiguracji Crypto Mapy

```
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

Składnia polecenia do konfiguracji Crypto Mapy

Polecenia konfiguracyjne Crypto mapy



Konfiguracja Crypto Mapy dla XYZCORP

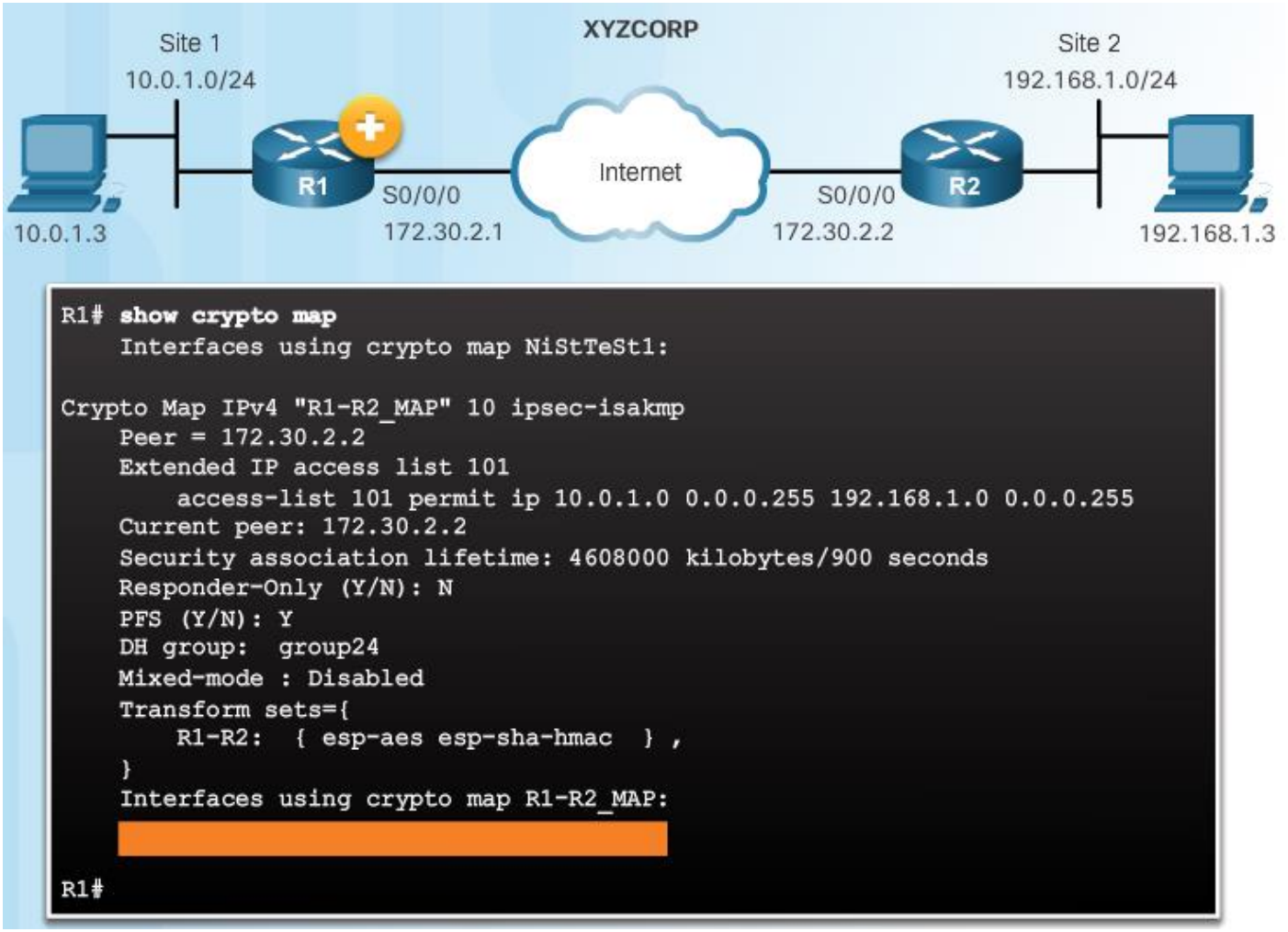
Konfiguracja Crypto Mapy:


```
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)#
```

Konfiguracja Crypto Mapy dla XYZCORP (Cont.)

Crypto Map Configuration:



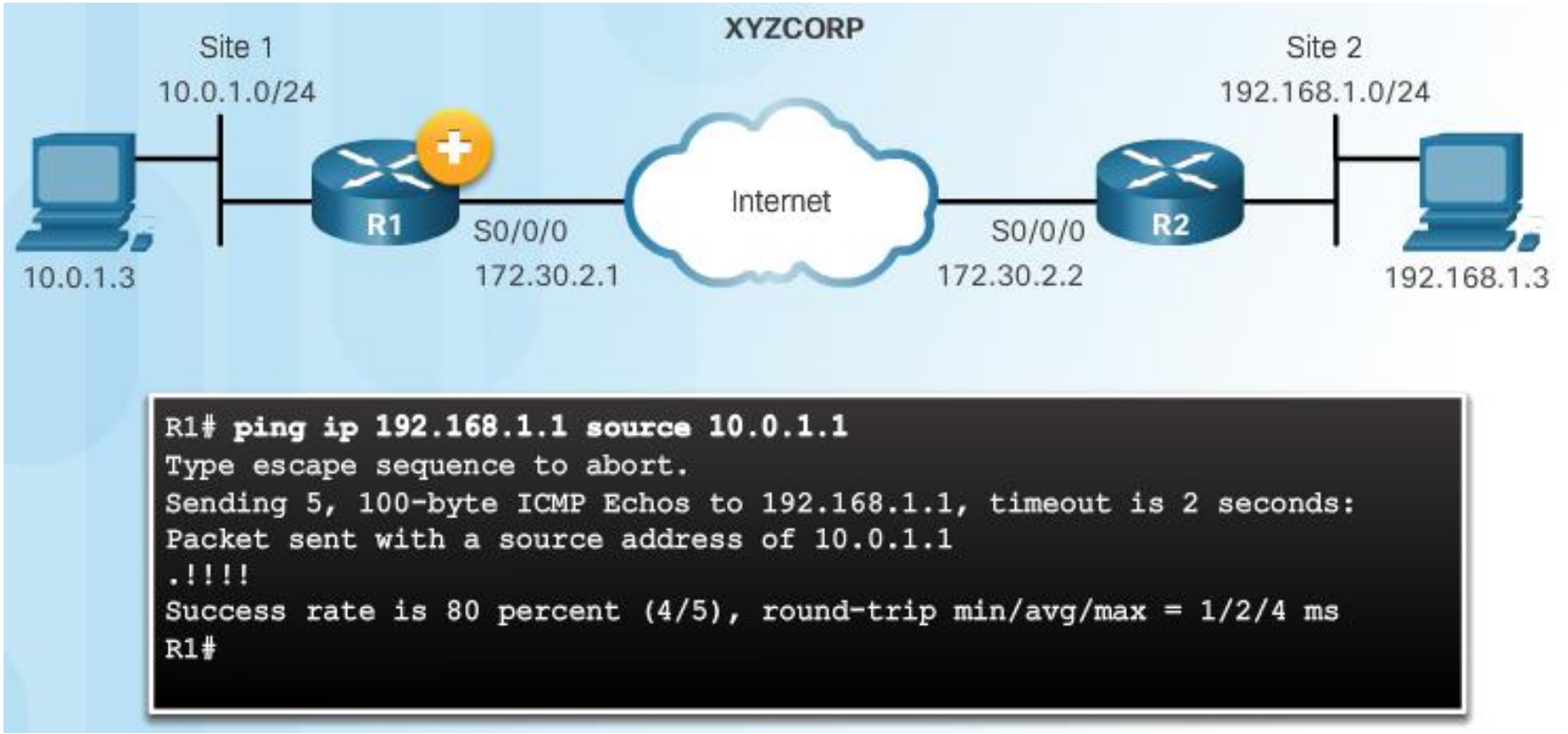
Użycie Crypto Mapy


```
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
```

Temat 1.3.6:
IPsec VPN

Przesyłanie ruchu przez tunel

Użyj rozszerzonego polecenia ping w celu przesłania ruchu przez tunel



Weryfikacja tuneli ISAKMP i IPsec

Weryfikacja aktywności tunelu ISAKMP


```
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#
```

Weryfikacja tuneli ISAKMP i IPsec (Cont.)

Weryfikacja działania tunelu IPsec


```
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
```

Rozdział 1.4: Podsumowanie

Cele rozdziału:

- Wyjaśnienie celu stosowania VPN.
- Wyjaśnienie działania sieci VPN IPsec.
- Konfiguracja tunelu VPN IPsec site-to-site z uwierzytelnianiem za pomocą klucza współdzielonego z wykorzystaniem CLI.

Thank you.

Cisco Networking Academy

Mind Wide Open