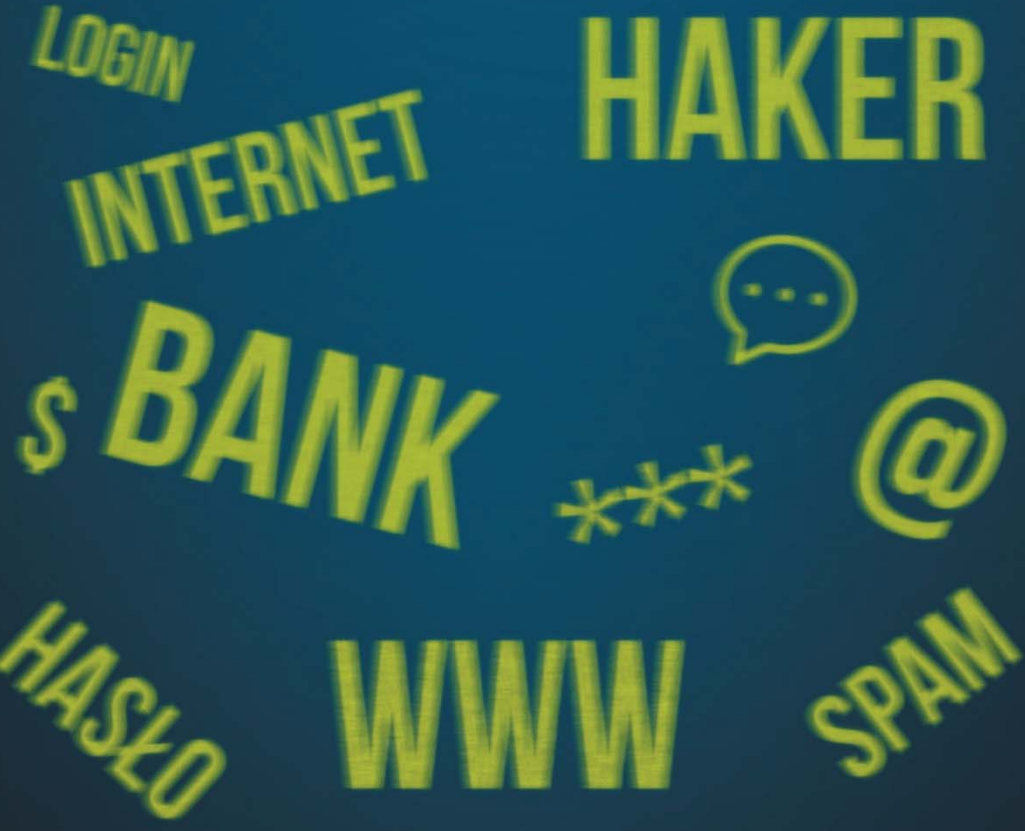


6 | TUNELOWANIE

6 TUNELOWANIE

Co to jest tunelowanie?

Tunelowanie to zestawienie połączenia między dwoma odległymi hostami tak, by stworzyć wrażenie, że są połączone bezpośrednio, przy założeniu, że sieć Internet nie zna protokołu, którym posługują się te hosty.

Rodzaje tunelowania:

- GRE,
- IPsec,

Co to jest sieć VPN?

VPN (*ang.* ***Virtual Private Network***) to usługa umożliwiająca połączenie między dwoma odległymi miejscami w Internecie poprzez wirtualny i szyfrowany tunel. VPN zapewnia bezpieczeństwo Twoich służbowych lub prywatnych przesyłanych danych, w trakcie korzystania z otwartych publicznych sieci Wi-Fi, z sieci w hotelach, a także w trakcie podróży służbowych.

Rodzaje sieci VPN:

- Site-to-Site
- Remote Access VPN

Sieć VPN typu **Site-to-Site** jest tworzona, gdy urządzenia zewnętrzne po obu stronach połączenia VPN znają konfigurację VPN.

Sieć VPN pozostaje statyczna, a hosty wewnętrzne nie mają wiedzy, że VPN istnieje. Hosty końcowe wysyłają i odbierają normalny ruch TCP/IP przez bramki VPN. Bramka VPN jest odpowiedzialna za inkapsulację i szyfrowanie ruchu wychodzącego dla całego ruchu z określonego miejsca.

Sieć VPN typu **Remote access** obsługuje potrzeby telepracowników, użytkowników mobilnych i extranetu, ruchu konsument – biznes. Jest tworzona, gdy informacje o VPN nie są statycznie skonfigurowane, lecz dynamicznie zmieniają się, a VPN może być włączany i wyłączany. VPN zdalnego dostępu obsługuje architekturę klient/serwer, w której klient VPN (zdalny) uzyskuje bezpieczny dostęp do sieci firmowej za pośrednictwem urządzenia serwer VPN na brzegu sieci.

Sieci VPN zdalnego dostępu są używane do łączenia poszczególnych hostów, które muszą uzyskać dostęp do ich sieci firmowej bezpiecznie przez Internet.

6.1 Tunelowanie oparte na protokole GRE

6.1.1 Protokół GRE

Tunelowanie oparte na **GRE** (*ang.* ***Generic Routing Encapsulation***) pozwala na przesyłanie poprzez tunel VPN, danych z wykorzystaniem specjalnego protokołu **GRE**. Protokół **GRE** został opracowany przez firmę Cisco.

Tunel VPN z wykorzystaniem protokołu **GRE** pozwala na zaszyfrowanie całego tunelu łączącego dwa oddzielne hosty i przesyłanie w nim danych za pomocą dynamicznych protokołów routingu.

W tym przypadku szyfrowany jest cały tunel a nie tylko dane, które się w nim znajdują. Pozwala to na ukrycie ruchu przesyłanego wewnątrz sieci prywatnej i przez Internet. Osoby postronne nie mogą zobaczyć tras lub protokołów jakie są wykorzystywane *wewnątrz sieci prywatnej VPN.*

6.1.2 Konfigurowanie sieci Site-to-Site za pomocą GRE

Aby skonfigurować sieć Site-to-Site przy użyciu GRE użyj poleceń zaprezentowanych w tabeli.

Polecenie	Opis
show interface tunnel *tunnel_name*	Weryfikacja stanu tunelu
tunnel mode gre ip	Ustawia tryb interfejsu jako GRE poprzez IP
tunnel source *ip_address*	Ustawia adres źródłowy tunelu
tunnel destination *ip_address*	Ustawia adres docelowy tunelu
ip address *ip_address mask*	Ustawia adres i maskę tunelu

Tabela 6.1 Polecenia służące do konfiguracji VPN GRE.

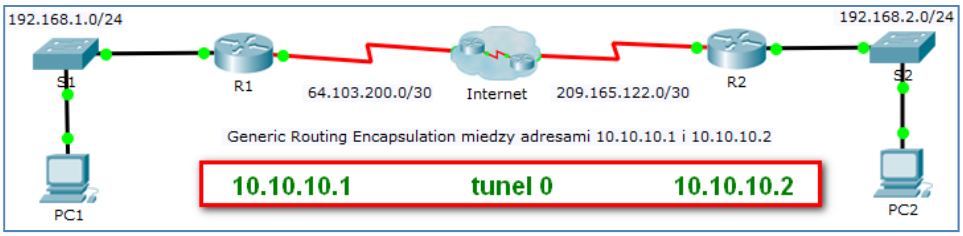
Przykładowe pliki
p6-1-2.pkt

Założenia:

- Adresy IP interfejsów są już skonfigurowane w całej sieci.
- Routing statyczny został skonfigurowany w sieci Internet.

Dla poniższej topologii sieciowej oraz tabeli adresacji, wykonaj następujące czynności, dla obu routerów brzegowych:

- Utwórz interfejs tunelu przy użyciu polecenia **interface**.
- Określ źródłowy adres IP tunelu.
- Określ docelowy adres IP tunelu.
- Skonfiguruj adres IP dla interfejsów tunelu.
- Określ tryb tunelu GRE jako tryb interfejsu tunelu. Tryb tunelu GRE jest domyślnym trybem interfejsu dla oprogramowania Cisco IOS.
- Sprawdź stan tunelu.



Rysunek 6.1 Przykładowa topologia tunelu 0.

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	G0/0	192.168.1.1	255.255.255.0	nie dotyczy
	S0/0/0	64.103.200.2	255.255.255.252	nie dotyczy
	Tunnel 0	10.10.10.1	255.255.255.252	nie dotyczy
R2	G0/0	192.168.2.1	255.255.255.0	nie dotyczy
	S0/0/0	209.165.122.2	255.255.255.252	nie dotyczy
	Tunnel 0	10.10.10.2	255.255.255.252	nie dotyczy
PC1	Fa0	192.168.1.2	255.255.255.0	192.168.1.1
PC1	Fa0	192.168.2.2	255.255.255.0	192.168.2.1

Tabela 6.2 Tabela adresacji.

Krok 1. Tworzenie tunelu i jego konfiguracja w routerze R1

Aby skonfigurować tunel w R1 z adresem wirtualnym **10.10.10.1** (na brzegu tunelu ustaw źródło i przeznaczenie) wykonaj następujące polecenia:

```
R1(config)# interface tunnel 0
R1(config-if)# ip address 10.10.10.1 255.255.255.252
R1(config-if)# tunnel source s0/0/0
R1(config-if)# tunnel destination 209.165.122.2
R1(config-if)# tunnel mode gre ip
R1(config-if)# no shutdown
```

```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
R1(config)#
R1(config)#
R1(config)#interface tunnel 0

R1(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up

R1(config-if)#ip address 10.10.10.1 255.255.255.252
R1(config-if)#tunnel source s0/0/0
R1(config-if)#tunnel destination 209.165.122.2
R1(config-if)#tunnel mode gre ip
R1(config-if)#no shutdown
```

Rysunek 6.2 Konfiguracja tunelu w R1.

Krok 2. konfigurowanie tunelu w routerze R2

Aby skonfigurować tunel w R2 z adresem wirtualnym **10.10.10.2** (na brzegu tunelu ustaw źródło i przeznaczenie) wykonaj następujące polecenia:

```
R2(config)# interface tunnel 0
R2(config-if)# ip address 10.10.10.2 255.255.255.252
R2(config-if)# tunnel source s0/0/0
R2(config-if)# tunnel destination 64.103.200.2
R2(config-if)# tunnel mode gre ip
R2(config-if)# no shutdown
```

```
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface tunnel 0

R2(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up

R2(config-if)#ip address 10.10.10.2 255.255.255.252
R2(config-if)#tunnel source s0/0/0
R2(config-if)#tunnel destination 64.103.200.2
R2(config-if)#tunnel mode gre ip
R2(config-if)#no shutdown
```

Rysunek 6.3 Konfiguracja tunelu w R2.

Krok 3. Skonfiguruj trasy dla ruchu między sieciami z adresami prywatnymi

Wykonaj trasy pomiędzy sieciami 192.168.X.X wykorzystujące następne przeskoki do sieci 10.10.10.0/30.

```
R1(config)# ip route 192.168.2.0 255.255.255.0 10.10.10.2
```

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip route 192.168.2.0 255.255.255.0 10.10.10.2
R1(config)#
```

Rysunek 6.4 Konfiguracja trasy w R1.

```
R2(config)# ip route 192.168.1.0 255.255.255.0 10.10.10.1
```

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip route 192.168.1.0 255.255.255.0 10.10.10.1
R2(config)#
```

Rysunek 6.5 Konfiguracja trasy w R2.

Wykonaj także trasę domyślną wykorzystującą przeskok do Serial 0/0/0.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/0
```

```
R1(config)#ip route 0.0.0.0 0.0.0.0 Serial0/0/0
%Default route without gateway, if not a point-to-point
interface, may impact performance
R1(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up
```

Rysunek 6.6 Konfiguracja trasy domyślnej w R1.

```
R2(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/0
```

```
R2(config)#ip route 0.0.0.0 0.0.0.0 Serial0/0/0
%Default route without gateway, if not a point-to-point
interface, may impact performance
R2(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed
state to up
```

Rysunek 6.7 Konfiguracja trasy domyślnej w R2.

Krok 4. Wykonaj weryfikację komunikacji między komputerami PC1 i PC2

Wykonaj polecenie **tracert** z **PC1** do **PC2**.

```
C:\>tracert 192.168.2.2

Tracing route to 192.168.2.2 over a maximum of 30 hops:

  1    1 ms      0 ms      0 ms      192.168.1.1
  2    2 ms      3 ms      2 ms      10.10.10.2
  3    10 ms     12 ms     14 ms     192.168.2.2

Trace complete.
```

Rysunek 6.8 Wynik polecenia tracert z PC1 do PC2.

```
C:\>tracert 192.168.1.2

Tracing route to 192.168.1.2 over a maximum of 30 hops:

  1    0 ms      1 ms      0 ms      192.168.2.1
  2    2 ms      2 ms      2 ms      10.10.10.1
  3    11 ms     3 ms      10 ms     192.168.1.2

Trace complete.
```

Rysunek 6.9 Wynik polecenia tracert z PC2 do PC1.

Tunelowanie pomiędzy sieciami prywatnymi 192.168.X.X odbywa się za pomocą adresów wirtualnych 10.10.10.X w tunelu GRE.

6.2 Tunelowanie za pomocą protokołu IPsec

6.2.1 Protokół IPsec

Tunelowanie za pomocą protokołu **IPsec (**ang. ***Internet Protocol Security***) stosuje mechanizmy kryptografii, które umożliwiają uwierzytelnianie oraz szyfrowanie, które gwarantują, że pakiety pochodzą od właściwego nadawcy oraz że nie zostały zmienione podczas transmisji. Szyfrowanie zapobiega przeglądaniu pakietów przez nieuprawnionych użytkowników.

6.2.2 Konfigurowanie sieci VPN Site-to-Site za pomocą IPsec

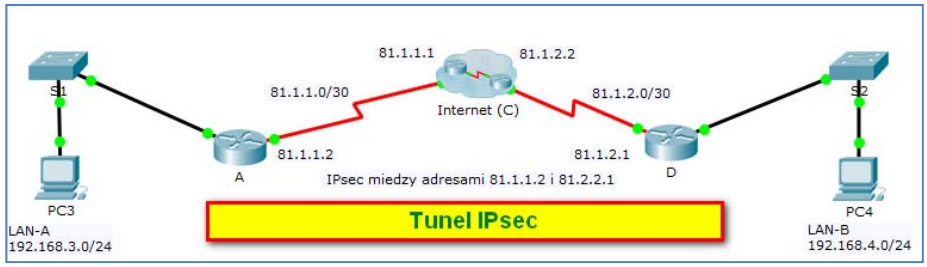
Przykładowe pliki
p6-2-2.pkt

Założenia:

- Adresy IP interfejsów są już skonfigurowane w całej sieci.
- Routing statyczny został skonfigurowany w sieci Internet.

Dla poniższej topologii sieciowej oraz tabeli adresacji, tabeli konfiguracji parametrów tabeli fazy 1 uwierzytelniania i szyfrowania, tabeli fazy 2 dla IPsec, wykonaj następujące czynności, dla obu routerów brzegowych:

- Dla poniższej topologii użyj routerów klasy **C2900**.
- Na wszystkich routerach ustaw hasło do trybu uprzywilejowanego: **cisco123**
- Aktywuj pakiet **securityk9** dla routerów brzegowych **A** i **D**
- Skonfiguruj listy ACL filtrujące ruch sieciowy dla **A** i **D**.
- Skonfiguruj parametry zasad zabezpieczeń (faza 1).
- Na **A, D** skonfiguruj zasadę zabezpieczeń (politykę, *ang.* ***policy***) szyfrowania **ISAKMP** o numerze **10** za pomocą klucza publicznego **cisco**. Użyj parametrów z tabeli **Parametry fazy 1 (zasady zabezpieczeń)**. Domyślne parametry nie muszą być konfigurowane, natomiast szyfrowanie, metoda wymiany klucza oraz metoda DH muszą.
- Na **A, D** skonfiguruj fazę 2 (patrz **Parametry fazy 2 dla IPsec**).
- Sprawdź stan tunelu.



Rysunek 6.10 Przykładowa topologia tunelu IPsec.

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
A	Gi0/0	192.168.3.1	255.255.255.0	192.168.3.1
	S0/0/0	**81.1.1.2**	255.255.255.252	nie dotyczy
	Internet (C) S0/0/0	**81.1.1.1**	255.255.255.252	nie dotyczy
D	Gi0/0	182.168.4.0	255.255.255.0	192.168.4.1
	S0/0/0	**81.1.2.1**	255.255.255.252	nie dotyczy
	Internet (C) S0/0/1	**81.1.1.2**	255.255.255.252	nie dotyczy
PC3	Fa0 (**LAN-A**)	192.168.3.2	255.255.255.0	192.168.3.1
PC4	Fa0 (**LAN-B**)	192.168.4.2	255.255.255.0	192.168.4.1

Tabela 6.3 Podstawowa adresacja topologii.

Parametry		**A i D**
Key distribution method	Manual or **ISAKMP**	**ISAKMP**
Encryption algorithm	**DES**, 3DES, or AES	**AES**
Hash algorithm	MD5 or **SHA-1**	**SHA-1**
Metoda uwierzytelniania	Pre-shared keys or **RSA**	**pre-share**
Key exchange	DH Group **1**, 2, or 5	**DH 2**
ISAKMP Key	-	**cisco**

Tabela 6.4 Parametry fazy 1 (zasady zabezpieczeń).

Parametry wypisane czcionką **wytłuszczoną** są domyślne. Pozostałe muszą zostać skonfigurowane.

Parametry	A	D
Transform Set	**VPN-SET**	**VPN-SET**
Peer Hostname	**D**	**A**
Peer IP Address	**81.1.2.1**	**81.1.1.2**
Crypto Map name	**VPN-MAP**	**VPN-MAP**
SA Establishment	**ipsec-isakmp**	**ipsec-isakmp**

Tabela 6.5 Parametry fazy 2 dla IPsec.

Połączenie VPN składa się z dwóch faz. W fazie pierwszej routery próbujące nawiązać połączenie wymieniają się kluczami. Wykorzystywany jest tu protokół IKE. Następuje uwierzytelnienie każdej strony. W fazie drugiej następuje ustanowienie parametrów szyfrowania tunelu docelowego. Parametry na obu końcach tunelu (w naszym przypadku na routerach A i C oraz C i D) muszą być takie same.

Krok 1. Aktywuj pakiet securityk9 w routerach A, D oraz C

Aktywuj moduł **securityk9** dla routera, zaakceptuj licencję, zapisz konfigurację oraz zrestartuj router.

```
A# conf t
A(config)# license boot module c2900 technology-package
securityk9
A(config)# end
A# copy running-config startup-config
A# reload

C# conf t
C(config)# license boot module c2900 technology-package
securityk9
C(config)# end
C# copy running-config startup-config
C# reload
```

```
D# conf t
D(config)# license boot module c2900 technology-package
securityk9
D(config)# end
D# copy running-config startup-config
D# reload
```

```
A(config)#license boot module c2900 technology-package securityk9
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE
LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR
USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE
FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE
BOUND
BY ALL THE TERMS SET FORTH HEREIN.
```

Rysunek 6.11 Aktywacja pakietu securityk9 w A.

Krok 2. Podstawowa konfiguracja routera A

```
enable
conf t
hostname A
interface GigabitEthernet 0/0
ip address 192.168.3.1 255.255.255.0
interface Serial0/0/0
ip address 81.1.1.2 255.255.255.252
crypto map VPN-MAP
ip route 0.0.0.0 0.0.0.0 81.1.1.1
```

```
A(config)#hostname A
A(config)#interface GigabitEthernet 0/0
A(config-if)#ip address 192.168.3.1  255.255.255.0
A(config-if)#interface Serial0/0/0
A(config-if)#ip address 81.1.1.2  255.255.255.252
A(config-if)#crypto map VPN-MAP
ERROR: Crypto Map with tag VPN-MAP does not exist.

A(config-if)#ip route 0.0.0.0  0.0.0.0  81.1.1.1
```

Rysunek 6.12 Podstawowa konfiguracja routera A.

Krok 2. Konfiguracja fazy pierwszej dla routera A

Musisz wpisać adres drugiego routera i metodę klucza (***Key distribution method***), który będzie wymieniany pomiędzy nimi oraz bramę domyślną**.**

```
ip route 0.0.0.0 0.0.0.0 81.1.1.1
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco address 81.1.1.1
crypto ipsec transform-set VPN-MAP esp-aes esp-sha-hmac
```

```
A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
A(config)#
A(config)#
A(config)#ip route 0.0.0.0   0.0.0.0   81.1.1.1
A(config)#crypto isakmp policy 1
A(config-isakmp)#authentication pre-share
A(config-isakmp)#crypto isakmp key cisco address 81.1.2.1
A pre-shared key for address mask 81.1.2.1 255.255.255.255
already exists!
A(config)#crypto ipsec transform-set VPN-MAP esp-aes esp-sha-hmac
A(config)#
```

Rysunek 6.13 Konfiguracja fazy 1 routera A.

Krok 3. Wykonaj konfigurację filtrowania ruchu na routerze A.

Skonfiguruj **ACL 110** w celu filtrowania ruchu z sieci **LAN-A** do sieci **LAN-B**. Pozwoli to przełączać ruch w IPsec VPN pomiędzy sieciami **LAN-A** i **LAN-B**. Pozostały ruch generowany z sieci LAN nie będzie szyfrowany. Pamiętaj o domyślnym wpisie **deny any any** na końcu ACL (którego nie musisz dodawać).

```
A(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255
192.168.4.0 0.0.0.255
```

```
A(config)#access-list 110 permit ip 192.168.3.0   0.0.0.255
192.168.4.0   0.0.0.255
A(config)#
```

Rysunek 6.14 Filtrowanie ruchu na routerze A.

Krok 4. Konfiguracja fazy drugiej dla routera A

Uwaga: Lista **ACL 110** jest konieczna do nawiązania połączenia pomiędzy dwoma sieciami lokalnymi.

```
crypto map VPN-MAP 1 ipsec-isakmp
set peer 81.1.2.1
set transform-set VPN-MAP
match address 110
```

```
A(config)#
A(config)#crypto map VPN-MAP 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
A(config-crypto-map)#set peer 81.1.2.1
A(config-crypto-map)#set transform-set VPN-MAP
A(config-crypto-map)#match address 110
A(config-crypto-map)#
```

Rysunek 6.15 Konfiguracja fazy 2 routera A.

Krok 5. Podstawowa konfiguracja routera D

```
enable
conf t
hostname D
interface GigabitEthernet 0/0
ip address 192.168.4.1 255.255.255.0
interface Serial0/0/0
ip address 81.1.2.1 255.255.255.252
crypto map VPN-MAP
ip route 0.0.0.0 0.0.0.0 81.1.2.2
```

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname D
D(config)#interface GigabitEthernet 0/0
D(config-if)#ip address 192.168.4.1  255.255.255.0
D(config-if)#interface Serial0/0/0
D(config-if)#ip address 81.1.2.1  255.255.255.252
D(config-if)#crypto map VPN-MAP
ERROR: Crypto Map with tag VPN-MAP does not exist.

D(config-if)#ip route 0.0.0.0  0.0.0.0  81.1.2.2
D(config)#
```

Rysunek 6.16 Podstawowa konfiguracja routera D.

Krok 6. Konfiguracja fazy pierwszej dla routera D

Musisz wpisać adres drugiego routera i metodę klucza (***Key distribution method***), który będzie wymieniany pomiędzy nimi oraz bramę domyślną**.**

```
ip route 0.0.0.0 0.0.0.0 81.1.2.2
crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco address 81.1.2.2
crypto ipsec transform-set VPN-MAP esp-aes esp-sha-hmac
```

```
D(config-if)#ip route 0.0.0.0  0.0.0.0  81.1.2.2
D(config)#
D(config)#
D(config)#crypto isakmp policy 1
D(config-isakmp)#authentication pre-share
D(config-isakmp)#crypto isakmp key cisco address 81.1.1.2
D(config)#crypto ipsec transform-set VPN-MAP esp-aes esp-sha-hmac
```

Rysunek 6.17 Konfiguracja fazy 1 routera D.

Krok 7. Wykonaj konfigurację filtrowania ruchu na routerze D.

Skonfiguruj **ACL 110** w celu filtrowania ruchu z sieci **LAN-B** do sieci **LAN-A**. Pozwoli to przełączać ruch w IPsec VPN pomiędzy sieciami **LAN-A** i **LAN-B**. Pozostały ruch generowany z sieci LAN nie będzie szyfrowany. Pamiętaj o domyślnym wpisie **deny any any** na końcu ACL (którego nie musisz dodawać).

```
D(config)# access-list 110 permit ip 192.168.4.0 0.0.0.255
192.168.3.0 0.0.0.255
```

```
D#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
D(config)#access-list 110 permit ip 192.168.4.0   0.0.0.255
192.168.3.0   0.0.0.255
```

Rysunek 6.18 Filtrowanie ruchu na routerze D.

Krok 8. Konfiguracja fazy drugiej dla routera D

Uwaga: Lista **ACL 110** jest konieczna do nawiązania połączenia pomiędzy dwoma sieciami lokalnymi.

```
crypto map VPN-MAP 1 ipsec-isakmp
set peer 81.1.1.2
```

```
set transform-set VPN-MAP
match address 110
```

```
D(config)#crypto map VPN-MAP 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
D(config-crypto-map)#set peer 81.1.1.2
D(config-crypto-map)#set transform-set VPN-MAP
D(config-crypto-map)#match address 110
```

Rysunek 6.19 Konfiguracja fazy 2 routera D.

Krok 9. Konfiguracja tras statycznych w routerze C

Na routerze C w chmurze Internet wykonaj konfiguracje tras statycznych za pomocą następujących poleceń:

```
ip route 192.168.4.0 255.255.255.0 81.1.2.1
ip route 192.168.3.0 255.255.255.0 81.1.1.2
```

```
C#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
C(config)#ip route 192.168.4.0 255.255.255.0 81.1.2.1
C(config)#ip route 192.168.3.0 255.255.255.0 81.1.1.2
C(config)#
```

Rysunek 6.20 Konfiguracja tras statycznych w routerze C.

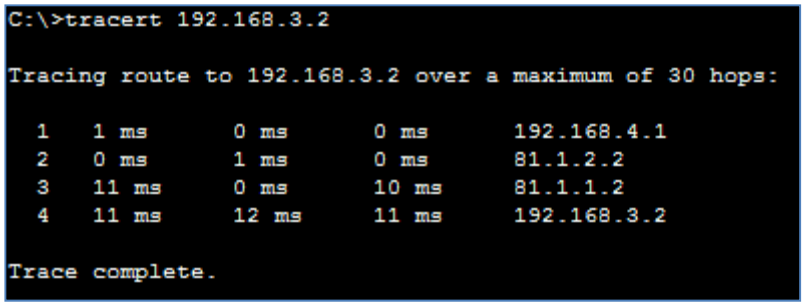
Krok 10. Zweryfikuj komunikację z PC3 do PC4 przez tunel IPsec.

Na komputerze **PC3** wykonaj polecenie **tracert 192.168.4.2 (do PC4)**.

```
C:\>tracert 192.168.4.2

Tracing route to 192.168.4.2 over a maximum of 30 hops:

  1    1 ms      0 ms      0 ms      192.168.3.1
  2    0 ms      0 ms      0 ms      81.1.1.1
  3    0 ms      10 ms     10 ms     81.1.2.1
  4    14 ms     12 ms     12 ms     192.168.4.2

Trace complete.
```

Rysunek 6.21 Weryfikacja tunelu IPsec.

Na komputerze **PC4** wykonaj polecenie **tracert 192.168.3.2 (do PC3)**.



Rysunek 6.22 Weryfikacja tunelu IPsec.

Pakiety testowe przechodzą przez adresy IP tunelu:

- od 81.1.1.1 do 81.1.2.1.
- od 81.1.2.2 do 81.1.1.2.