Laboratorium 2 – Implementacja nakładkowej sieci GRE IPSec VPN

Cele ćwiczenia

Celem ćwiczenia jest zaprojektowanie i implementacja wirtualnej sieci prywatnej (VPN) typu site-to-site w architekturze nakładkowej (ang. overlay) z wykorzystaniem urządzeń Cisco. Z uwagi na konieczność przenoszenia informacji rutingowych między lokalizacjami klienta, w pierwszym etapie ćwiczenia utworzony zostanie tunel GRE między urządzeniami brzegowymi klienta (bramami VPN). Następnie, w drugim etapie, ruch przesyłany w tunelu GRE zostanie zabezpieczony korzystając z mechanizmów IPSec. Utworzone zostaną dwa procesy rutingu OSPF: jeden obejmujący sieć dostawcy usług, drugi – sieci klienta w poszczególnych lokalizacjach.

Celami szczegółowymi ćwiczenia są:

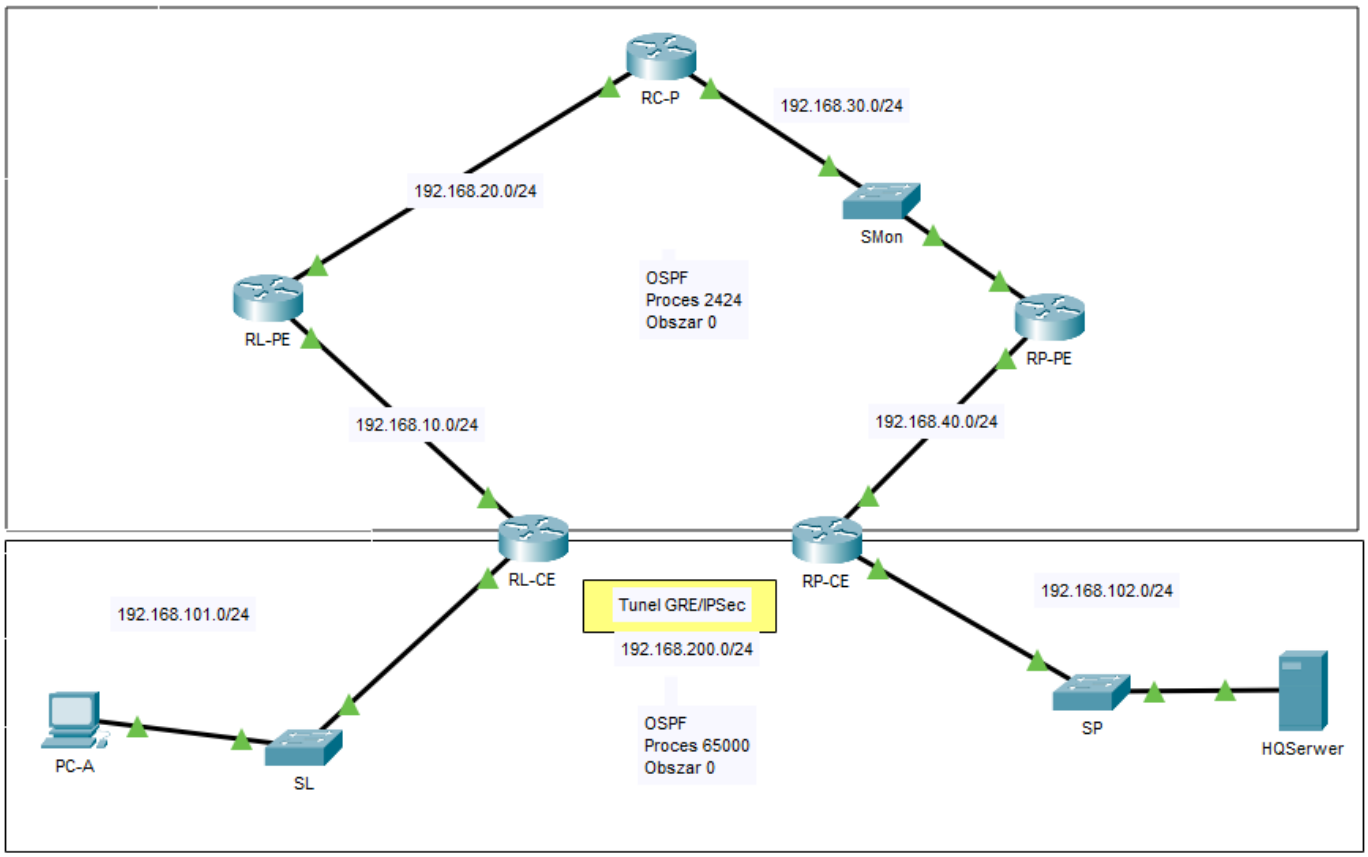
1. Konfiguracja rutingu OSPF w sieci operatora
2. Ustanowienie tunelu GRE między bramami VPN
3. Konfiguracja rutingu OSPF w sieci klienta
4. Zabezpieczenie ruchu klienta, przesyłanego przez sieć operatora, z wykorzystaniem mechanizmów IPSec
5. Zadanie opcjonalne: monitorowanie ruchu na przełączniku SMon.

Opis topologii logicznej i fizycznej sieci

1. Komputer PC-A o adresie IP 192.168.101.**2**/24 połączony łączem FastEthernet z portem FastEthernet 0/1 przełącznika SL
2. Port GigabitEthernet 0/1 przełącznika SL połączy z portem GigabitEthernet 0/1 rutera RL-CE o adresie 192.168.101.**1**/24
3. Port GigabitEthernet 0/0 rutera RL-CE o adresie 192.168.10.**1**/24 połączony z portem GigabitEthernet 0/0/1 rutera RL-PE o adresie 192.168.10.**2**/24

4. Port GigabitEthernet 0/0/0 rutera RL-PE o adresie 192.168.20.**1**/24 połączony z portem GigabitEthernet0/0/0 rutera RC-P o adresie 192.168.20.**2**/24
5. Port GigabitEthernet 0/0/1 rutera RC-P o adresie 192.168.30.**1**/24 połączony z portem GigabitEthernet 0/**1** przełącznika SMon
6. Port GigabitEthernet 0/2 przełącznika SMon połączony z portem GigabitEthernet 0/0/1 rutera RP-PE o adresie 192.168.30.**2**/24
7. Port GigabitEthernet 0/0/0 rutera RP-PE o adresie 192.168.40.**1**/24 połączony z portem GigabitEthernet 0/0 rutera RP-CE o adresie 192.168.40.**2**/24
8. Port GigabitEthernet 0/1 rutera RP-PE o adresie 192.168.102.**1**/24 połączony z portem GigabitEthernet 0/1 przełącznika SP
9. Sewer HQSerwer IP 192.168.102.**2**/24 połączony łączem FastEthernet z portem FastEthernet 0/1 przełącznika SP

Graficzną reprezentację opisanej topologii przedstawiono na poniższym rysunku



Przebieg ćwiczenia

Połączenie urządzeń zgodnie z topologią przedstawioną w poprzednim rozdziale

Nadanie adresów IP urządzeniom końcowym

1. Komputer PC-A
    a. Adres 192.168.101.2 z maską 24 bitową
    b. Adres bramy domyślnej: 192.168.101.1 z maską 24 bitową
2. Serwer HQSerwer
    a. Adres 192.168.102.2 z maską 24 bitową
    b. Adres bramy domyślnej: 192.168.102.1 z maską 24 bitową

Konfiguracja interfejsów sieciowych ruterów

1. Ruter RL-CE

```
RL-CE#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

RL-CE(config)#interface GigabitEthernet 0/0

RL-CE(config-if)#ip address 192.168.10.1 255.255.255.0

RL-CE(config-if)#no shutdown

RL-CE(config)#interface GigabitEthernet 0/1

RL-CE(config-if)#ip address 192.168.101.1 255.255.255.0

RL-CE(config-if)#no shutdown

RL-CE(config-if)#
```

2. Ruter RL-PE

```
RL-PE#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

RL-PE(config)#interface GigabitEthernet 0/0/1
```

```
RL-PE(config-if)#ip address 192.168.10.2 255.255.255.0
RL-PE(config-if)#no shutdown
RL-PE(config)#interface GigabitEthernet 0/0/0
RL-PE(config-if)#ip address 192.168.20.1 255.255.255.0
RL-PE(config-if)#no shutdown
RL-PE(config-if)#
```

3. Ruter RC-P

```
RC-P#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RC-P(config)#interface GigabitEthernet 0/0/0
RC-P(config-if)#ip address 192.168.20.2 255.255.255.0
RC-P(config-if)#no shutdown
RC-P(config)#interface GigabitEthernet 0/0/1
RC-P(config-if)#ip address 192.168.30.1 255.255.255.0
RC-P(config-if)#no shutdown
```

4. Ruter RP-PE

```
RP-PE#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RP-PE(config)#interface GigabitEthernet 0/0/1
RP-PE(config-if)#ip address 192.168.30.2 255.255.255.0
RP-PE(config-if)#no shutdown
RP-PE(config)#interface GigabitEthernet 0/0/0
```

```
RP-PE(config-if)#ip address 192.168.40.1 255.255.255.0

RP-PE(config-if)#no shutdown
```

5. Ruter RP-CE

```
RP-CE#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

RP-CE(config)#interface GigabitEthernet 0/0

RP-CE(config-if)#ip address 192.168.40.2 255.255.255.0

RP-CE(config-if)#no shutdown

RP-CE(config)#interface GigabitEthernet 0/1

RP-CE(config-if)#ip address 192.168.102.1 255.255.255.0

RP-CE(config-if)#no shutdown
```

Sprawdzenie poprawności konfiguracji interfejsów ruterów korzystając z polecenia:

```
Router#show ip interface brief
```

Konfiguracja protokołu rutingu OSPF w pojedynczym obszarze dla sieci operatora

Zakładamy, że sieci 192.168.10.0, 192.168.20.0, 192.168.30.0 oraz 192.168.40.0, wszystkie z maską 24 bitową, należą do sieci operatora. Protokołem rutingu dla sieci operatorskiej jest protokół OSPF. Przyjmij numer procesu2424. Zauważ, że różne numery procesów pozwolą na rozdzielenie rutingu na cześć operatora i klienta na ruterach brzegowych RL-CE oraz RP-CE (CE -ang. Customer Edge).

1. Ruter RL-CE

```
RL-PE(config)#router ospf 2424

RL-PE(config-router)#network 192.168.10.0 0.0.0.255 area 0

#Wazne: nie dodajemy sieci wewnętrznej 192.168.101.0. Dodamy ją
później, do innego procesu rutingu, po skonfigurowaniu
interfejsu tunelowego między RL-CE a RP-CE.
```

2. Ruter RL-PE

```
RL-PE(config)#router ospf 2424
RL-PE(config-router)#network 192.168.10.0 0.0.0.255 area 0
RL-PE(config-router)#network 192.168.20.0 0.0.0.255 area 0
```

3. Ruter RC-P

```
RC-P(config)#router ospf 2424
RC-P(config-router)#network 192.168.20.0 0.0.0.255 area 0
RC-P(config-router)#network 192.168.30.0 0.0.0.255 area 0
```

4. Ruter RP-PE

```
RP-PE(config)#router ospf 2424
RP-PE(config-router)#network 192.168.30.0 0.0.0.255 area 0
RP-PE(config-router)#network 192.168.40.0 0.0.0.255 area 0
```

5. Ruter RP-CE

```
RP-PE(config)#router ospf 2424
RP-PE(config-router)#network 192.168.40.0 0.0.0.255 area 0
#Wazne: nie dodajemy sieci wewnętrznej 192.168.102.0. Dodamy ją
później, do innego procesu rutingu, po skonfigurowaniu
interfejsu tunelowego między RL-CE a RP-CE.
```

Sprawdzenie poprawności konfiguracji OSPF (przykład dla jednego rutera)

RC-P#show ip ospf neighbor

```
Neighbor ID     Pri   State           Dead Time   Address
Interface
```

```
192.168.20.1      1    FULL/BDR        00:00:39    192.168.20.1
GigabitEthernet0/0/0

192.168.40.1      1    FULL/DR         00:00:39    192.168.30.2
GigabitEthernet0/0/1
```

RC-P>show ip route

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B
- BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route


Gateway of last resort is not set


O 192.168.10.0/24 [110/2] via 192.168.20.1, 00:30:48,
GigabitEthernet0/0/0

192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.20.0/24 is directly connected, GigabitEthernet0/0/0

L 192.168.20.2/32 is directly connected, GigabitEthernet0/0/0

192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
```

```
C 192.168.30.0/24 is directly connected, GigabitEthernet0/0/1

L 192.168.30.1/32 is directly connected, GigabitEthernet0/0/1

O 192.168.40.0/24 [110/2] via 192.168.30.2, 00:30:33,
GigabitEthernet0/0/1
```

Sprawdzenie łączności między ruterami typu CE, tj. RL-CE i PE-CE

```
RL-CE>ping 192.168.40.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.40.2, timeout is 2
seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Sprawdzenie łączności między komputerem PC-A a serwerem HQSerwer

```
C:\>ping 192.168.102.2

Pinging 192.168.102.2 with 32 bytes of data:

Request timed out.

Request timed out.

Request timed out.

Request timed out.

Ping statistics for 192.168.102.2:

    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Wyjaśnij brak wzajemnej osiągalności hostów.

Konfiguracja interfejsu tunelowego GRE między ruterami CE, tj. RL-CE i RP-CE

1. Tunel GRE między urządzeniami brzegowymi klienta pozwoli na enkapsulowanie dowolnych treści wymienianych między lokalizacjami, tj. sieciami wewnętrznymi 192.168.101.0/24 oraz 192.168.102.0. Dotyczy to w rozważanym przypadku uaktualnień LSA protokołu OSPF, przesyłanych w pakietach LSU z grupowym adresem docelowym.
2. Skonfiguruj tunel GRE po stronie rutera RL-CE

```
RL-CE(config)#interface tunnel 65000

RL-CE(config-if)#

%LINK-5-CHANGED: Interface Tunnel65000, changed state to up

RL-CE(config-if)#ip address 192.168.200.1 255.255.255.0

RL-CE(config-if)#tunnel source gigabitEthernet 0/0

RL-CE(config-if)#tunnel destination 192.168.40.2

RL-CE(config-if)#

%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel65000,
changed state to up
```

3. Skonfiguruj tunel GRE po stronie rutera RP-CE

```
RP-CE(config)#interface tunnel 65000

RP-CE(config-if)#

%LINK-5-CHANGED: Interface Tunnel65000, changed state to up

RP-CE(config-if)#ip address 192.168.200.2 255.255.255.0

RP-CE(config-if)#tunnel source gigabitEthernet 0/0

RP-CE(config-if)#tunnel destination 192.168.10.1

RP-CE(config-if)#
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
changed state to up
```

4. Sprawdź łączność między końcówkami tunelu
5. Sprawdź łączność między komputerem PC-A a serwerem HQSerwer

Konfiguracja protokołu rutingu OSPF w pojedynczym obszarze dla sieci klienta

Zakładamy, że sieci 192.168.101.0 oraz 192.168.102.0, wszystkie z maską 24 bitową, są sieciami wewnętrznymi klienta. Protokołem rutingu dla sieci klienta jest protokół OSPF (tak jak w przypadku operatora). W celu rozróżnienia procesów rutingu na ruterach CE, przyjmij numer procesu 65000. Do procesu rutingu 65000 dodaj adres sieciowy tunelu GRE oraz sieci wewnętrzne klienta.

1. Ruter RL-CE

```
RL-CE(config)#router ospf 65000
RL-CE(config-router)#network 192.168.101.0 0.0.0.255 area 0
RL-CE(config-router)#network 192.168.200.0 0.0.0.255 area 0
```

2. Ruter RP-CE

```
RP-CE(config)#router ospf 65000
RP-CE(config-router)#network 192.168.102.0 0.0.0.255 area 0
RP-CE(config-router)#network 192.168.200.0 0.0.0.255 area 0
```

3. Sprawdź poprawność nawiązania relacji sąsiedztwa przez interfejs tunelowy

```
01:12:28: %OSPF-5-ADJCHG: Process 65000, Nbr 192.168.101.1 on
Tunnel65000 from LOADING to FULL, Loading Done
```

```
RP-CE#sh ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface
192.168.40.1 1 FULL/BDR 00:00:34 192.168.40.1 GigabitEthernet0/0
192.168.101.1 0 FULL/ - 00:00:30 192.168.200.1 Tunnel65000
```

Sprawdzenie łączności między komputerem PC-A a serwerem HQSerwer

```
C:\>ping 192.168.102.2


Pinging 192.168.102.2 with 32 bytes of data:


Reply from 192.168.102.2: bytes=32 time<1ms TTL=126

Reply from 192.168.102.2: bytes=32 time<1ms TTL=126

Reply from 192.168.102.2: bytes=32 time=1ms TTL=126

Reply from 192.168.102.2: bytes=32 time=10ms TTL=126


Ping statistics for 192.168.102.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

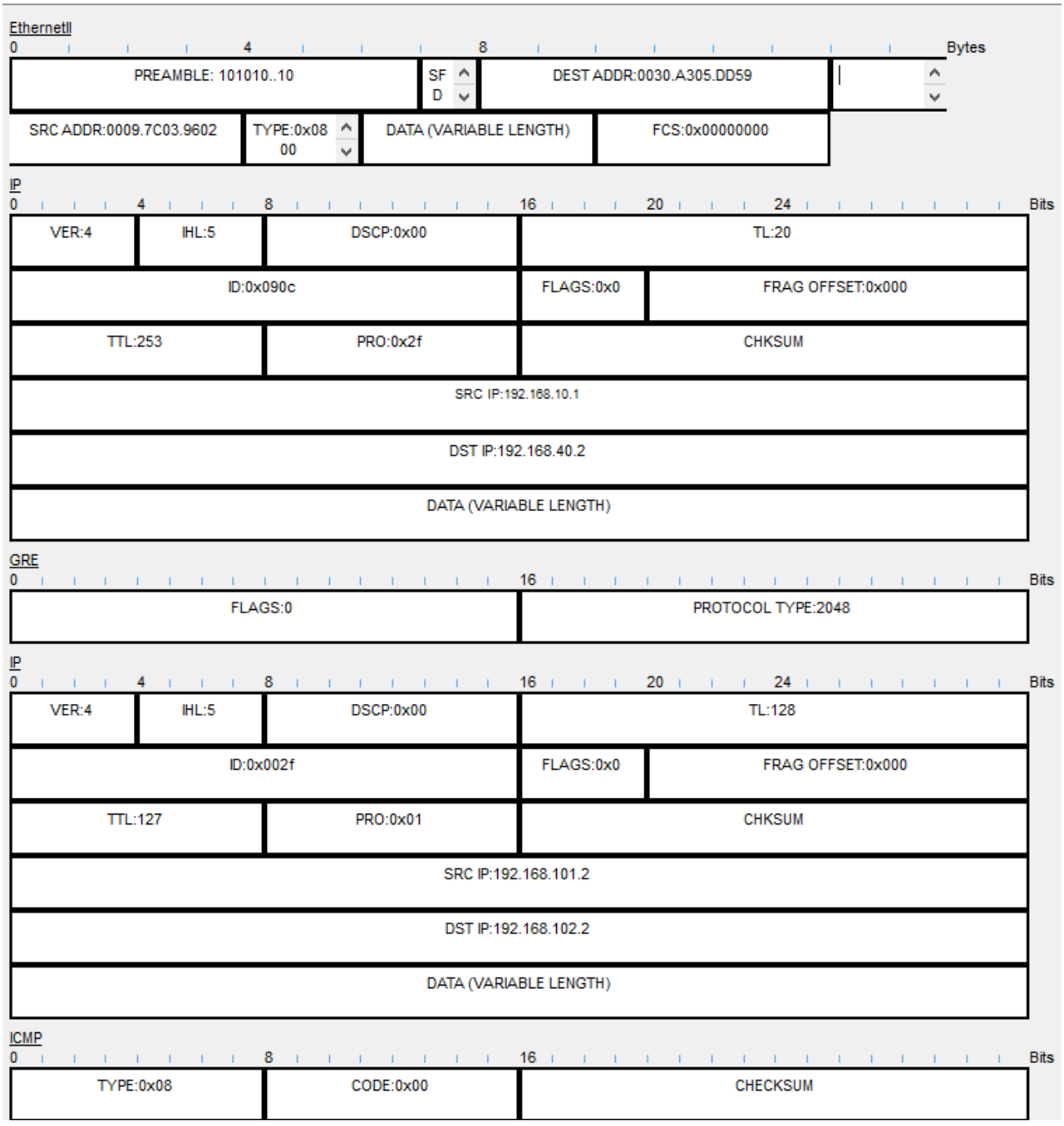
Sprawdzenie trasy między komputerem PC-A a serwerem HQSerwer

```
C:\>tracert 192.168.102.2

Tracing route to 192.168.102.2 over a maximum of 30 hops:

1  0 ms  0 ms  0 ms 192.168.101.1

2  0 ms  0 ms  0 ms 192.168.200.2

3  0 ms  10 ms  0 ms 192.168.102.2

Trace complete.
```

Analiza enkapsulacji trasy między komputerem PC-A a serwerem HQSerwer

Wykorzystaj program typu Wireshark lub wbudowaną funkcjonalność programu Cisco Packet Tracer do monitorowania ruchu przechodzącego przez przełącznik SMon.

Dla wygenerowanego na PC-A ruchu, wskutek polecenia ping 192.168.102.2, można zauważyć, że oryginalny pakiet IP z adresem źródłowym 192.168.101.1 i docelowym 192.168.102.2 jest enkapsulowany w pakiet GRE z dodatkowym nagłówkiem o adresie źródłowym 192.168.10.1 oraz docelowym 192.168.40.2 (odpowiednio początek i koniec tunelu GRE w sieci operatorskiej). Przykładowy zrzut ekranu prezentujący omówioną enkapsulację przedstawiono poniżej. Możemy zauważyć, że można odczytać oryginalne nagłówki IP:


Ethernetll
0
4
8
Bytes
PREAMBLE: 101010..10
SF
D
DEST ADDR:0030.A305.DD59
SRC ADDR:0009.7C03.9602
TYPE:0x08
00
DATA (VARIABLE LENGTH)
FCS:0x00000000
IP
0
4
8
16
20
24
Bits
VER:4
IHL:5
DSCP:0x00
TL:20
ID:0x090c
FLAGS:0x0
FRAG OFFSET:0x000
TTL:253
PRO:0x2f
CHKSUM
SRC IP:192.168.10.1
DST IP:192.168.40.2
DATA (VARIABLE LENGTH)
GRE
0
16
Bits
FLAGS:0
PROTOCOL TYPE:2048
IP
0
4
8
16
20
24
Bits
VER:4
IHL:5
DSCP:0x00
TL:128
ID:0x002f
FLAGS:0x0
FRAG OFFSET:0x000
TTL:127
PRO:0x01
CHKSUM
SRC IP:192.168.101.2
DST IP:192.168.102.2
DATA (VARIABLE LENGTH)
ICMP
0
8
16
Bits
TYPE:0x08
CODE:0x00
CHECKSUM

Zabezpieczanie ruchu przesyłanego w tunelu GRE mechanizmami IPSec

W celu zachowania poufności ruchu przesyłanego między lokalizacjami klienta pakiety z enkapsulacją GRE powinny być dodatkowo zabezpieczone mechanizmami IPSec, zapewniającymi, poza poufnością, także integralność i uwierzytelnianie stron.

Konfiguracja IPSec dla sieci VPN obejmuje dwa etapy: konfigurację parametrów IKE (ang .Internet Key Exchange) oraz konfigurację parametrów samego IPSec.

Implementacja IKE

1. Sprawdź dostępność polecenia:

```
RL-CE(config)#crypto isakmp enable

RP-CE(config)#crypto isakmp enable
```

2. Określ politykę ISAKMP (ang. Internet Security Association and Key Management Protocol) pomiędzy dwoma urządzeniami CE, tj. RL-CE i RP-CE. W ramach polityki określany jest proponowany mechanizm uwierzytelnienia, szyfrowania i algorytm generowania funkcji skrótu. Uzgadnianie tych parametrów to tzw. faza 1 IKE.

```
RL-CE(config)#crypto isakmp policy ?

  <1-10000>  Priority of protection suite

RL-CE(config)#crypto isakmp policy 10
```

3. Sprawdź dostępne polecenia w ramach konfiguracji ISAKMP (pojedynczego zestawu proponowanych parametrów):

```
RL-CE(config-isakmp)#?

authentication Set authentication method for protection suite

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
```

4. Jako metodę uwierzytelniania wybierz **pre-share**; jak algorytm kryptograficzny **aes 256**, jako algorytm funkcji skrótu **SHA**, do wymiany kluczy **grupę 5 Diffie-Hellman'a**, a czas obowiązywania parametrów na **1800 sekund**:

```
RL-CE(config-isakmp)#authentication pre-share
RL-CE(config-isakmp)#encryption ?
  3des  Three key triple DES
  aes   AES - Advanced Encryption Standard
  des   DES - Data Encryption Standard (56 bit keys).
RL-CE(config-isakmp)#encryption aes ?
  128  128 bit keys.
  192  192 bit keys.
  256  256 bit keys.
RL-CE(config-isakmp)#encryption aes 256
RL-CE(config-isakmp)#hash ?
  md5  Message Digest 5
  sha  Secure Hash Standard
RL-CE(config-isakmp)#hash sha
RL-CE(config-isakmp)#lifetime 1800
RL-CE(config-isakmp)#group ?
```

```
  1   Diffie-Hellman group 1
  2   Diffie-Hellman group 2
  5   Diffie-Hellman group 5
RL-CE(config-isakmp)#group 5
```

5. Upewnij się, że polityki dla ISAKMP są dokładnie takie same na obu urządzeniach:

```
RL-CE#sh crypto isakmp policy
Global IKE policy
Protection suite of priority 10
encryption algorithm: AES - Advanced Encryption Standard (256 bit
keys).
hash algorithm: Secure Hash Standard
authentication method: Pre-Shared Key
Diffie-Hellman group: #5 (1536 bit)
lifetime: 1800 seconds, no volume limit
RP-CE#sh crypto isakmp policy
Global IKE policy
Protection suite of priority 10
encryption algorithm: AES - Advanced Encryption Standard (256 bit
keys).
hash algorithm: Secure Hash Standard
authentication method: Pre-Shared Key
Diffie-Hellman group: #5 (1536 bit)
lifetime: 1800 seconds, no volume limit
```

6. Skonfiguruj klucze do uwierzytelniania stron. Zwróć uwagę na zastosowany adres IP rutera równorzędnego (ang. peer'a):

```
RP-CE(config)#crypto isakmp key AiTech address 192.168.10.1

RL-CE(config)#crypto isakmp key AiTech address 192.168.40.2
```

7. Określ parametry asocjacji bezpieczeństwa

```
RP-CE(config)#crypto ipsec transform-set RLCE_RPCE esp-aes 256
esp-sha-hmac

RL-CE(config)#crypto ipsec transform-set RLCE_RPCE esp-aes 256
esp-sha-hmac
```

8. Sprawdź znaczenie powyższych parametrów korzystając z dokumentacji urządzenia
9. Określenie ruchu zabezpieczanego określonymi powyżej parametrami IPSec. Zwróć uwagę, że w naszym przypadku będzie to ruch związany z pakietami GRE, w których z kolei przenoszony jest (**dlaczego?**) ruch IP między lokalizacjami.

```
RL-CE(config)#access-list 111 permit gre host 192.168.10.1 host
192.168.40.2

RP-CE(config)#access-list 111 permit gre host 192.168.40.2 host
192.168.10.1
```

10. Dla każdej z bram VPN (RL-CE oraz RP-CE) zdefiniuj mapowanie kryptograficzne, wiążące ruch podlegający zabezpieczeniu, miejsce do którego ma być ten ruch przesłany, oraz parametry asocjacji bezpieczeństwa.

```
RL-CE(config)#crypto map AiTech 10 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer

        and a valid access list have been configured.

RL-CE(config-crypto-map)#match address 111

RL-CE(config-crypto-map)#set peer 192.168.40.2
```

```
RL-CE(config-crypto-map)#set transform-set RLCE_RPCE

RL-CE(config-crypto-map)#exit

RP-CE(config)#crypto map AiTech 10 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer

RP-CE(config-crypto-map)#match address 111

RP-CE(config-crypto-map)#set peer 192.168.10.1

RP-CE(config-crypto-map)#set transform-set RLCE_RPCE

RP-CE(config-crypto-map)#exit
```

11. Nałóż skonfigurowaną politykę bezpieczeństwa na interfejsy ruterów prowadzące w kierunku sieci operatora

```
RP- RP-CE(config-if)#crypto map AiTech

RL-CE(config-if)#crypto map AiTech
```

12. Zwróć uwagę na zachodzące zmiany:

```
RP-CE#
00:25:51: %OSPF-5-ADJCHG: Process 65000, Nbr 192.168.101.1 on
Tunnel65000 from FULL to DOWN, Neighbor Down: Dead timer expired

00:25:51: %OSPF-5-ADJCHG: Process 65000, Nbr 192.168.101.1 on
Tunnel65000 from FULL to DOWN, Neighbor Down: Interface down or
detached

00:25:56: %OSPF-5-ADJCHG: Process 65000, Nbr 192.168.101.1 on
Tunnel65000 from LOADING to FULL, Loading Done
```

13. Sprawdź, czy Twój ruch był przesyłany w bezpiecznym tunelu:

```
RP-CE#sh crypto ipsec sa

interface: GigabitEthernet0/0/0
```

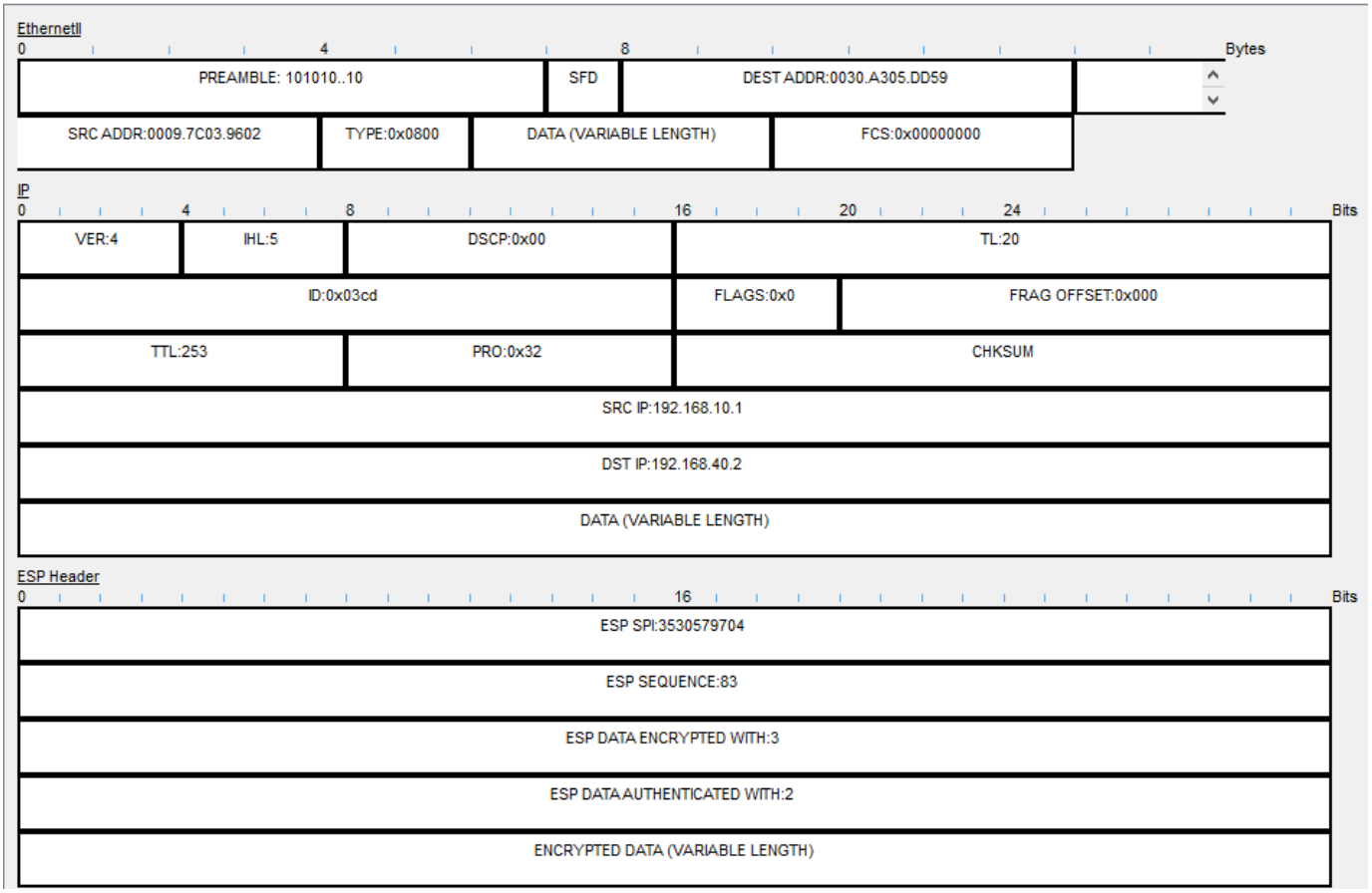
```
Crypto map tag: AiTech, local addr 192.168.40.2

protected vrf: (none)

local ident (addr/mask/prot/port):
(192.168.40.2/255.255.255.255/47/0)

remote ident (addr/mask/prot/port):
(192.168.10.1/255.255.255.255/47/0)

current_peer 192.168.10.1 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 31, #pkts encrypt: 31, #pkts digest: 0

#pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 0

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 192.168.40.2, remote crypto
endpt.:192.168.10.1

path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0

current outbound spi: 0xF46D9E8E(4100824718)

inbound esp sas:

spi: 0xD2705EF8(3530579704)

transform: esp-aes 256 esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2004, flow_id: FPGA:1, crypto map: AiTech
```

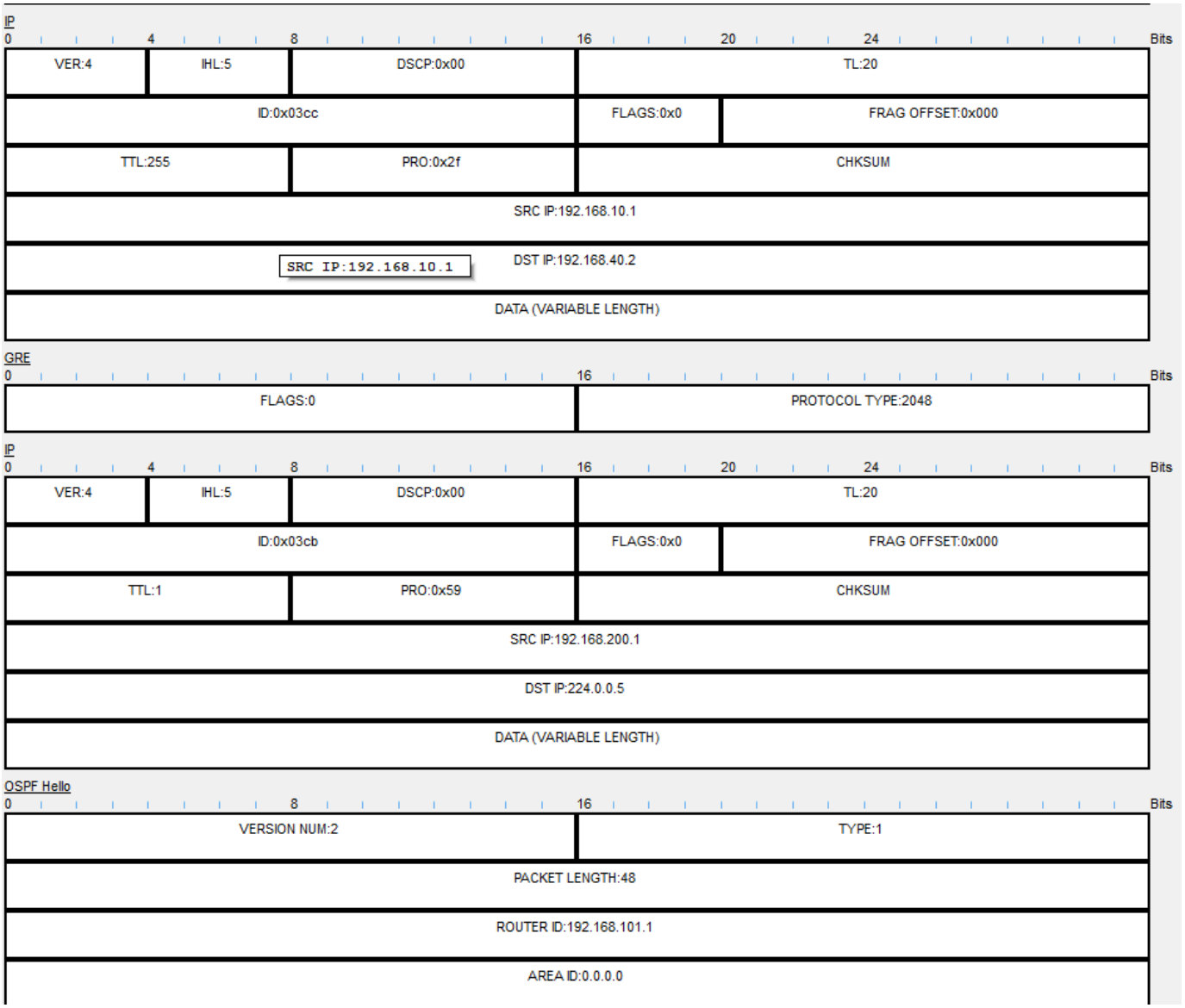
```
sa timing: remaining key lifetime (k/sec): (4525504/3390)

IV size: 16 bytes

replay detection support: N

Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0xF46D9E8E(4100824718)

transform: esp-aes 256 esp-sha-hmac ,

in use settings ={Tunnel, }

conn id: 2005, flow_id: FPGA:1, crypto map: AiTech

sa timing: remaining key lifetime (k/sec): (4525504/3390)

IV size: 16 bytes

replay detection support: N

Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

Analiza enkapsulacji trasy między komputerem PC-A a serwerem HQSerwer po zastosowaniu mechanizmów IPSec

Wykorzystaj program typu Wireshark lub wbudowaną funkcjonalność programu Cisco Packet Tracer do monitorowania ruchu przechodzącego przez przełącznik SMon.

Przykładowy zrzut ekranu prezentujący omówioną enkapsulację przedstawiono poniżej. Możemy zauważyć wielostopniową enkapsulację. Poświęć chwilę na szczegółową analizę procesu enkapsulacji.


EthernetII
0
4
8
Bytes
PREAMBLE: 101010..10
SFD
DEST ADDR:0030.A305.DD59
SRC ADDR:0009.7C03.9602
TYPE:0x0800
DATA (VARIABLE LENGTH)
FCS:0x00000000
IP
0
4
8
16
20
24
Bits
VER:4
IHL:5
DSCP:0x00
TL:20
ID:0x03cd
FLAGS:0x0
FRAG OFFSET:0x000
TTL:253
PRO:0x32
CHKSUM
SRC IP:192.168.10.1
DST IP:192.168.40.2
DATA (VARIABLE LENGTH)
ESP Header
0
16
Bits
ESP SPI:3530579704
ESP SEQUENCE:83
ESP DATA ENCRYPTED WITH:3
ESP DATA AUTHENTICATED WITH:2
ENCRYPTED DATA (VARIABLE LENGTH)


IP
0 4 8 16 20 24 Bits
VER:4
IHL:5
DSCP:0x00
TL:20
ID:0x03cc
FLAGS:0x0
FRAG OFFSET:0x000
TTL:255
PRO:0x2f
CHKSUM
SRC IP:192.168.10.1
SRC IP:192.168.10.1
DST IP:192.168.40.2
DATA (VARIABLE LENGTH)
GRE
0 16 Bits
FLAGS:0
PROTOCOL TYPE:2048
IP
0 4 8 16 20 24 Bits
VER:4
IHL:5
DSCP:0x00
TL:20
ID:0x03cb
FLAGS:0x0
FRAG OFFSET:0x000
TTL:1
PRO:0x59
CHKSUM
SRC IP:192.168.200.1
DST IP:224.0.0.5
DATA (VARIABLE LENGTH)
OSPF Hello
0 8 16 Bits
VERSION NUM:2
TYPE:1
PACKET LENGTH:48
ROUTER ID:192.168.101.1
AREA ID:0.0.0.0