

Communication Networks Protocol II

Mohamad Saab, Semilogo Ogungbure, Nicolas Gennart, Yiyu Wang,

December 19 2021

1 Snapshot of the topology

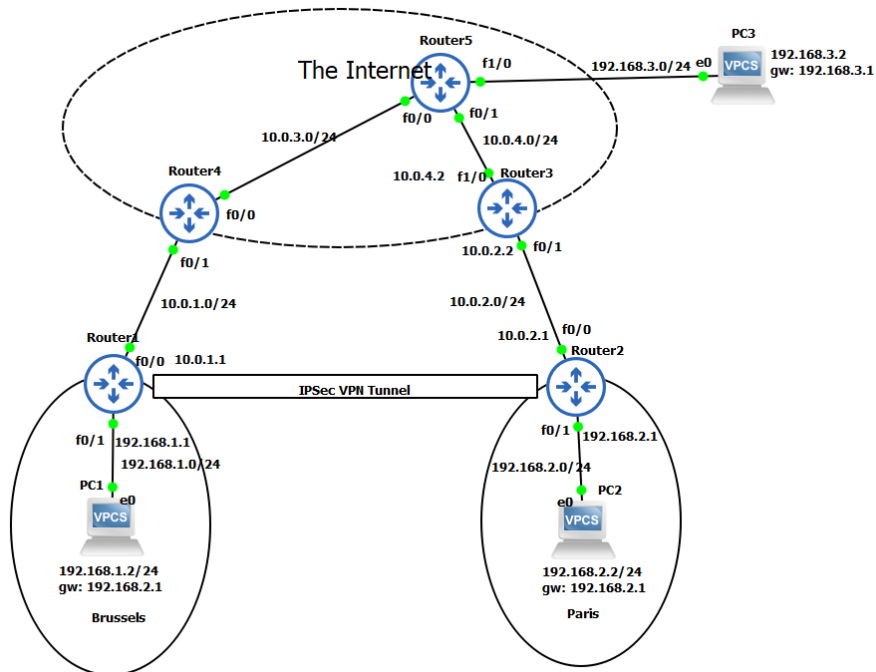


Figure 1: Lab 4 Topology

2 Mission 1

In this mission we only verify that the preconfigured topology works and we can ping pc2 and pc3 from pc1. We also see using wireshark that the traffic is in clear when capturing the path between router 1 and router 4 while pinging.

2.1 Pinging PC3 from PC1

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	c4:01:05:19:00:00	CDP/VTP/DTP/PAgP/UD...	CDP	355	Device ID: Router1
2	4.981968	192.168.1.2	192.168.3.2	ICMP	98	Echo (ping) request
3	5.004026	192.168.3.2	192.168.1.2	ICMP	98	Echo (ping) reply
4	6.024836	192.168.1.2	192.168.3.2	ICMP	98	Echo (ping) request
5	6.055499	192.168.3.2	192.168.1.2	ICMP	98	Echo (ping) reply
6	7.063361	192.168.1.2	192.168.3.2	ICMP	98	Echo (ping) request
7	7.104375	192.168.3.2	192.168.1.2	ICMP	98	Echo (ping) reply
8	8.111407	192.168.1.2	192.168.3.2	ICMP	98	Echo (ping) request

Frame 2: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Ethernet II, Src: c4:01:05:19:00:00 (c4:01:05:19:00:00), Dst: c4:04:05:61:00:01 (c4:04:05:61:00:01)
Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.3.2
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x82c2 [correct]
[Checksum Status: Good]
Identifier (BE): 40264 (0x9d48)
Identifier (LE): 18589 (0x489d)
Sequence number (BE): 1 (0x0001)
Sequence number (LE): 256 (0x0100)
[Response frame: 3]
Data (56 bytes)

0000	c4 04 05 61 00 01 c4 01 05 19 00 00 08 00 45 00	...a.....E
0010	00 54 48 9d 00 00 3f 01 ad b7 c0 a8 01 02 c0 a8	..TH...?.....
0020	03 02 08 00 82 c2 9d 48 00 01 08 09 0a 0b 0c 0dH.....
0030	0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d
0040	1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d	..!#\$%&'()*+,-
0050	2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d	./012345 6789:;<=
0060	3e 3f	>?

Figure 2: traffic logging between Router1 and Router4

2.2 Pinging PC2 from PC1

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	c4:01:05:19:00:00	c4:01:05:19:00:00	LOOP	60	Reply
2	8.665735	192.168.1.2	192.168.2.2	ICMP	98	Echo (ping) request
3	8.737999	192.168.2.2	192.168.1.2	ICMP	98	Echo (ping) reply
4	9.752326	192.168.1.2	192.168.2.2	ICMP	98	Echo (ping) request
5	9.806785	192.168.2.2	192.168.1.2	ICMP	98	Echo (ping) reply
6	10.335571	c4:01:05:19:00:00	c4:01:05:19:00:00	LOOP	60	Reply
7	10.818306	192.168.1.2	192.168.2.2	ICMP	98	Echo (ping) request
8	10.880383	192.168.2.2	192.168.1.2	ICMP	98	Echo (ping) reply

Frame 2: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Ethernet II, Src: c4:01:05:19:00:00 (c4:01:05:19:00:00), Dst: c4:04:05:61:00:01 (c4:04:05:61:00:01)
Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.2.2
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xdac1 [correct]
[Checksum Status: Good]
Identifier (BE): 17737 (0x4549)
Identifier (LE): 18757 (0x4945)
Sequence number (BE): 1 (0x0001)
Sequence number (LE): 256 (0x0100)
[Response frame: 3]
Data (56 bytes)

0000	c4 04 05 61 00 01 c4 01 05 19 00 00 08 00 45 00	...a.....E
0010	00 54 49 45 00 00 3f 01 ae 0f c0 a8 01 02 c0 a8	..TIE...?.....
0020	02 02 08 00 da c1 45 49 00 01 08 09 0a 0b 0c 0dEI.....
0030	0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d
0040	1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d	..!#\$%&'()*+,-
0050	2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d	./012345 6789:;<=
0060	3e 3f	>?

Figure 3: traffic logging between Router1 and Router4

3 Mission 2

In mission 2 we configure site to site ipsec vpn tunnel between the cisco routers 1 and 2. And below is the routers involved configuration.

Router 1 Configuration

```
hostname Router1
!
crypto isakmp policy 1
  encr aes
  authentication pre-share
  group 2
crypto isakmp key unicorn address 10.0.2.1
!
!
crypto ipsec transform-set MYTS esp-aes esp-sha-hmac
!
crypto map CMAP 10 ipsec-isakmp
  set peer 10.0.2.1
  set transform-set MYTS
  match address VPN-TRAFFIC
!
!
!
!
interface FastEthernet0/0
  ip address 10.0.1.1 255.255.255.0
  duplex auto
  speed auto
  crypto map CMAP
!
interface FastEthernet0/1
  ip address 192.168.1.1 255.255.255.0
  duplex auto
  speed auto
!
router rip
  network 10.0.0.0
  network 192.168.1.0
!
ip access-list extended VPN-TRAFFIC
  permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
!
```

Router 2 Configuration

```
hostname Router2
!
crypto isakmp policy 1
  encr aes
  authentication pre-share
```

```

group 2
crypto isakmp key unicorn address 10.0.1.1
!

crypto ipsec transform-set MYTS esp-aes esp-sha-hmac
!
crypto map CMAP 10 ipsec-isakmp
set peer 10.0.1.1
set transform-set MYTS
match address VPN-TRAFFIC
!
!
!
!
interface FastEthernet0/0
ip address 10.0.2.1 255.255.255.0
duplex auto
speed auto
crypto map CMAP
!
interface FastEthernet0/1
ip address 192.168.2.1 255.255.255.0
duplex auto
speed auto
!
router rip
network 10.0.0.0
network 192.168.2.0
!
ip access-list extended VPN-TRAFFIC
permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
!

```

Comments

After following the lab4 tutorial and applying similar configuration to the other tunnel end (router 2). We created successfully a site to site Ipsec vpn. We first selected the IKE policy as required to establish security association between two IPsec end points. Next we set the pre-shared password ("unicorn") for our destination. Then we move to phase 2 to configure how packets will be transformed. To configure IPsec we need to setup the following in order:

1. Create extended ACL (access control lists) to determine what packets are subject (or not) to transformation. This allows to separate between the normal traffic and the VPN traffic.
2. Create IPsec Transform to configure how packets will be ciphered, MAC'ed, etc..
3. Create Crypto Map to link a specific destination with a specific transform and filtered with the ACL (it is a glue of the previous steps)
4. Apply crypto map to the public interface to tell the router to analyze every packet passing by that interface for a possible crypto transformation.

4 Mission 3

4.1 Ping from PC1 to PC3 (no VPN tunnel)

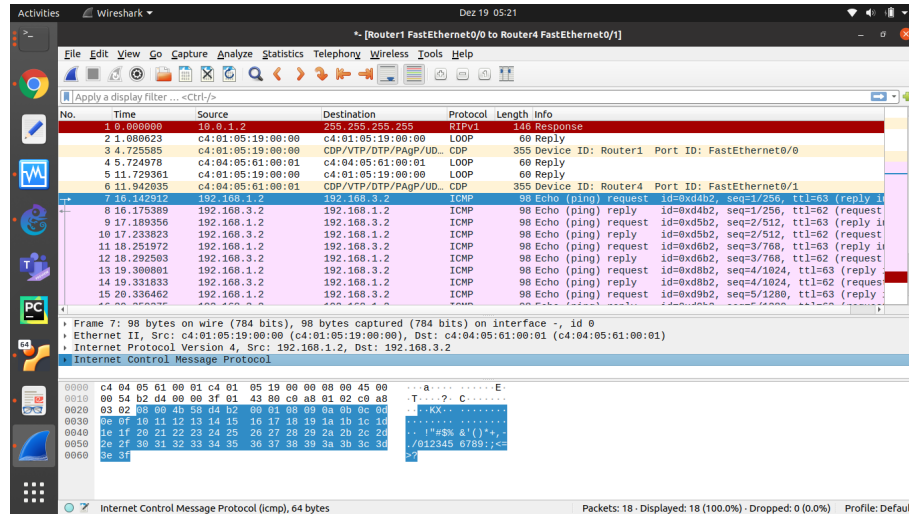


Figure 4: traffic logging between Router1 and Router4

4.2 Ping from PC1 to PC3 (VPN tunnel exist between the two ends)

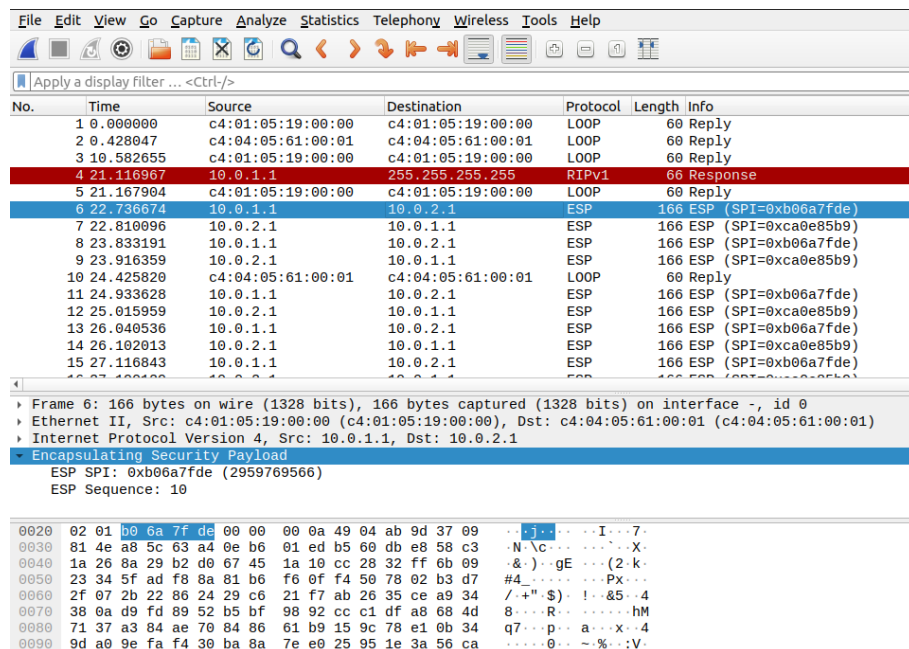


Figure 5: traffic logging between Router1 and Router4

Comments

We observe ICMP ping messages sent in clear when pinging from PC1 to PC3 as there is no ipsec vpn tunnel between these 2 ends. Whereas when pinging from PC1 to PC2 where we have an ipsec vpn tunnel in between, the packets are subject to the transform rule and are encapsulated in IPSec ESP. This is observed in the highlighted line in the wireshark snapshot above in figure 5.

4.3 Validation on the tunnel (IKE Policies, transformations)

```
Router1#show crypto isakmp policy
```

```
Global IKE policy
```

```
Protection suite of priority 1
```

```
  encryption algorithm: AES - Advanced Encryption Standard (128 bit keys).
```

```
  hash algorithm: Secure Hash Standard
```

```
  authentication method: Pre-Shared Key
```

```
  Diffie-Hellman group: #2 (1024 bit)
```

```
  lifetime: 86400 seconds, no volume limit
```

```
Default protection suite
```

```
  encryption algorithm: DES - Data Encryption Standard (56 bit keys).
```

```
  hash algorithm: Secure Hash Standard
```

```
  authentication method: Rivest-Shamir-Adleman Signature
```

```
  Diffie-Hellman group: #1 (768 bit)
```

```
  lifetime: 86400 seconds, no volume limit
```

```
Router1#show crypto isakmp sa
```

dst	src	state	conn-id	slot	status
10.0.2.1	10.0.1.1	QM_IDLE	1	0	ACTIVE

```
Router1#show crypto isakmp peers
```

```
Peer: 10.0.2.1 Port: 500 Local: 10.0.1.1
```

```
Phase1 id: 10.0.2.1
```

```
Router1#show crypto ipsec sa
```

```
interface: FastEthernet0/0
```

```
  Crypto map tag: CMAP, local addr 10.0.1.1
```

```
protected vrf: (none)
```

```
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
```

```
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
```

```
current_peer 10.0.2.1 port 500
```

```
  PERMIT, flags={origin_is_acl,}
```

```
  #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
```

```
  #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3
```

```
  #pkts compressed: 0, #pkts decompressed: 0
```

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

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

```
  #send errors 1, #recv errors 0
```

```
local crypto endpt.: 10.0.1.1, remote crypto endpt.: 10.0.2.1
```

```
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
```

```
current outbound spi: 0xB06A7FDE(2959769566)
```

inbound esp sas:
spi: 0xCA0E85B9(3389949369)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2001, flow_id: SW:1, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4440640/3043)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcg sas:

outbound esp sas:
spi: 0xB06A7FDE(2959769566)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2002, flow_id: SW:2, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4440640/3035)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcg sas: