Communication Networks Protocol II

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

December 19 2021

1 Snapshot of the topology

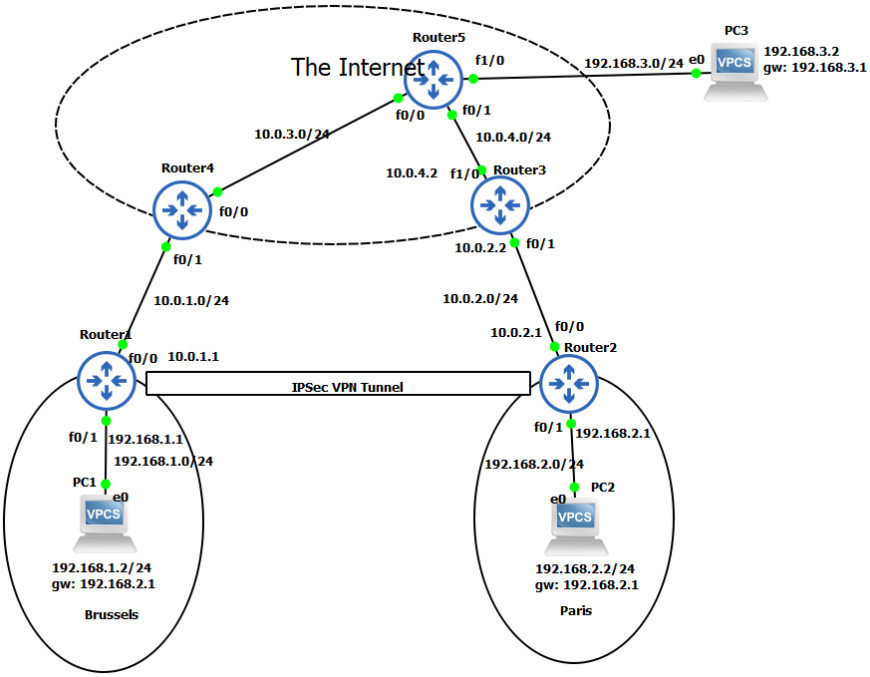

Figure 1: Lab 4 Topology

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

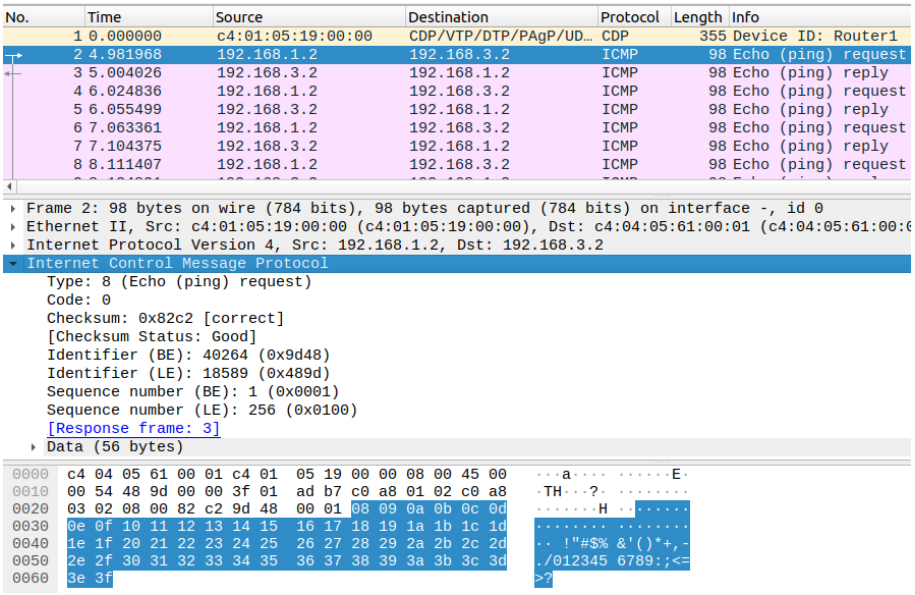

Figure 2: traffic logging between Router1 and Router4

2.2 Pinging PC2 from PC1

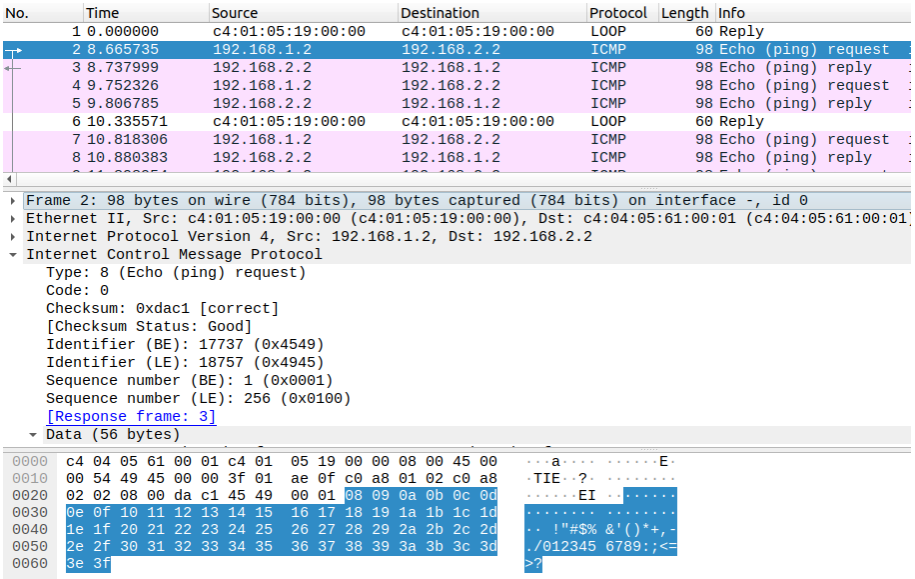

Figure 3: traffic logging between Router1 and Router4

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 lits) 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)

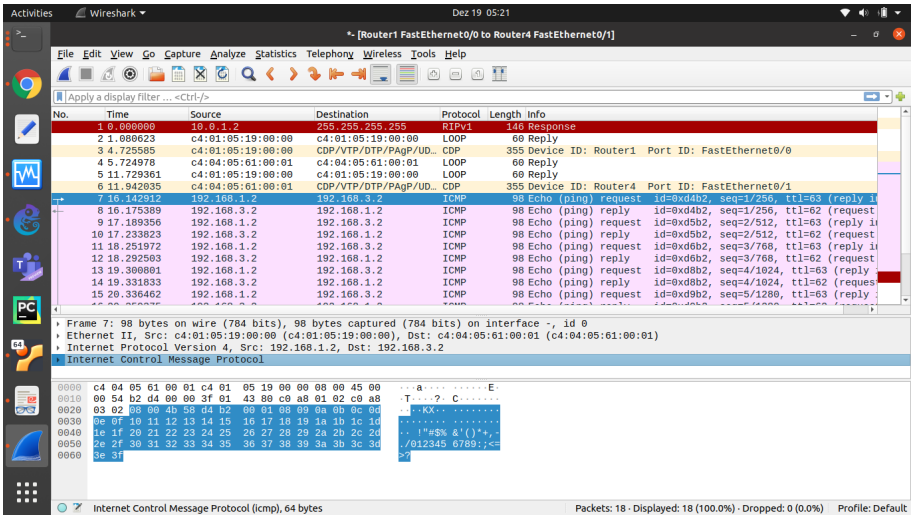

Figure 4: traffic logging between Router1 and Router4

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

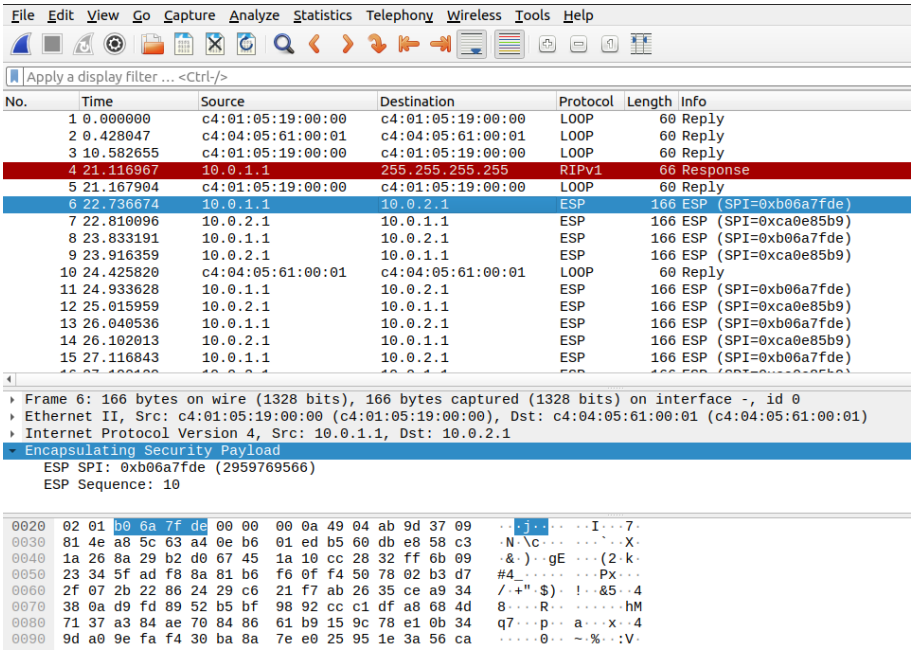

Figure 5: traffic logging between Router1 and Router4

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 snaphot 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 pcp 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 pcp sas:
```