Université Libre de Bruxelles

Communication networks : protocols and architectures
ELEC-H417

Lab 4 - VPN

Group D :

Bienfait Alexandre 513930
Boistel Julien 440915
Humblet Raphaël 514085
Mutkowski Philippe 494470

Teacher :

Dricot Jean-Michel

Teaching Assistant :

Chassagne Aurélien

December 2023

Academic year 2023-2024

Contents

1 Introduction

The goal of this lab will be to set up a L3 (IP-in-IP) VPN between Router 1 and Router 2 (from Brussels to Paris) and understand the IPSec options and phase 1 and 2 negociations.

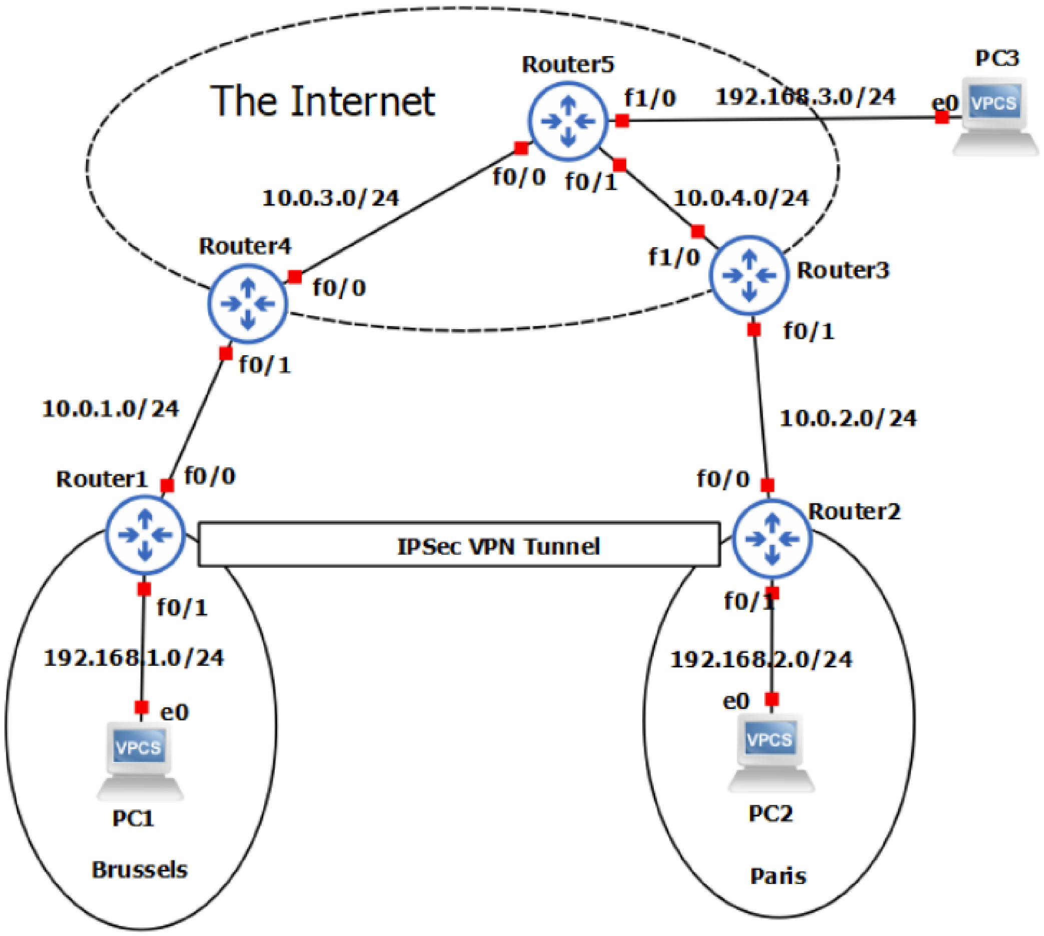

Figure 1: Initial topology

Here is the initial topology that will be used for the lab.

2 Mission 1: Traffic Observation

In this mission, the objective is to check whether all routers and PCs are correctly configured. This is done by sending a ping from PC1 (192.168.1.2) to PC3 (192.168.3.2). And from PC1 to PC2 (192.168.2.2).

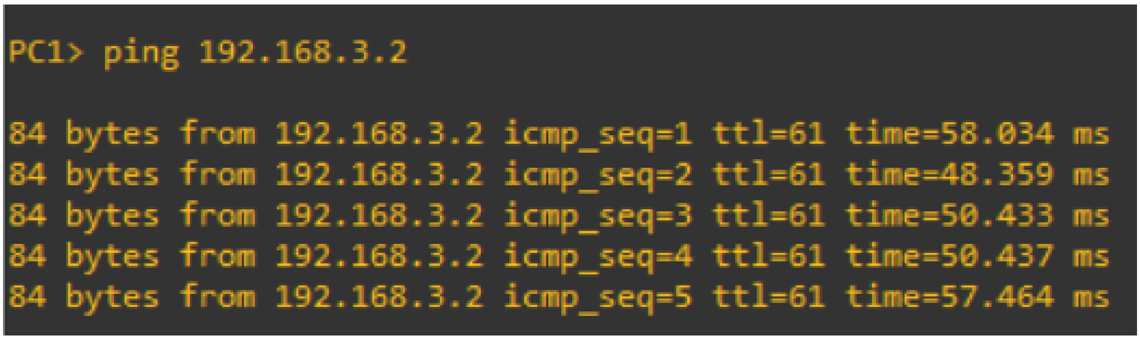

Figure 2: Ping from PC1 to PC3

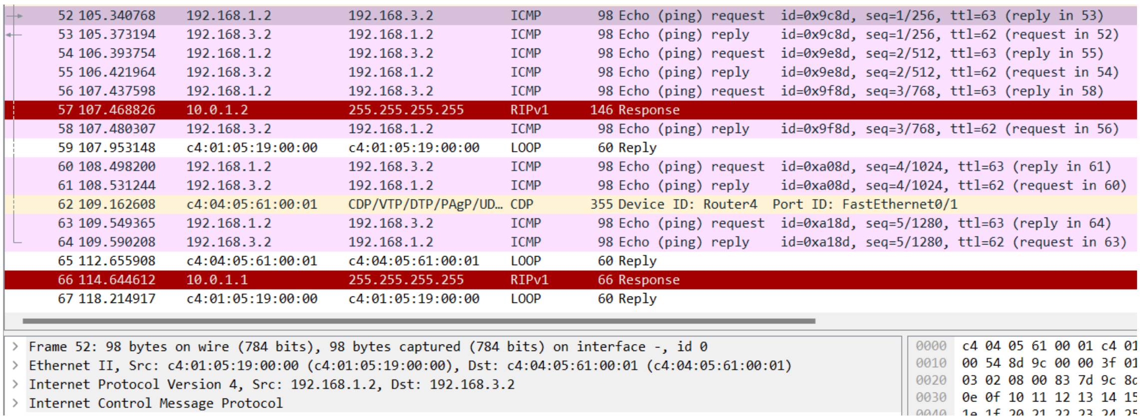

Figure 3: Capture Shark between R1 and R4

The figures 2 and 3 show that the communication between PC1 and PC3 works well. The wireshark capture shows the packets through the Router 1 - Router 4 link. For the moment, everything works as in the previous labs.

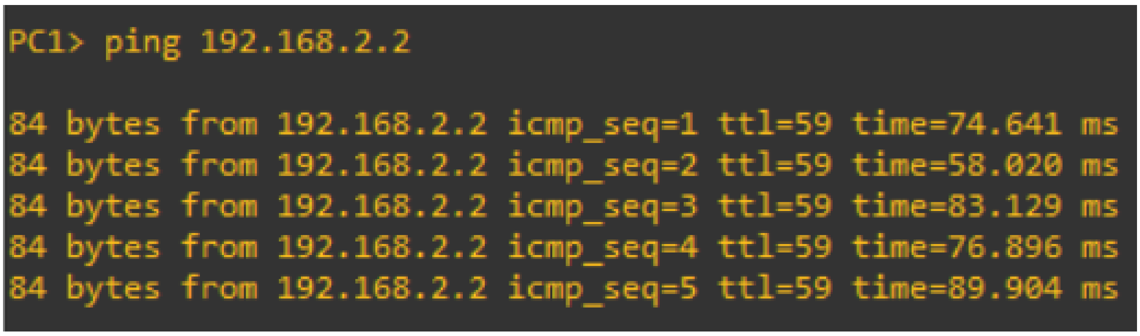

Figure 4: Ping between PC1 and PC2

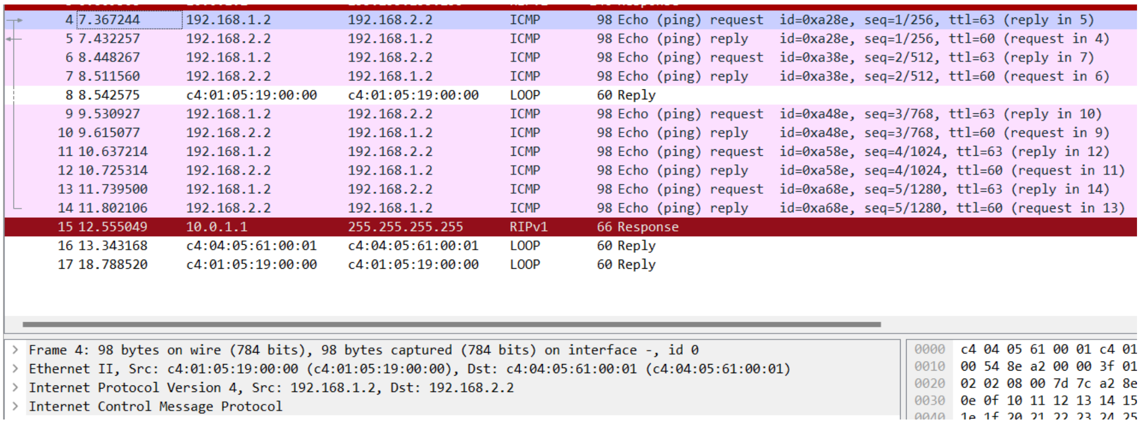

Figure 5: Capture Shark between R1 and R4

As it can be seen in figures 4 and 5, it is the same from PC1 to PC2. The traffic is thus normal for PC1 to PC3 and PC1 to PC2 messages.

3 Mission 2: Site-to-Site IPSec VPN

The objective of this mission is to set up the IPSec VPN tunnel beetween Router 1 and Router 2.

Both Router 1 and Router 2 needs to be configured but here, only the description of Router 1 configuration will be explained because Router 2's configuration is very similar.

The configuration of a router for Site-to-Site IPSec VPN is composed of 2 phases: IKE and Crypto transformation and access control.

3.1 IPSec Phase 1 - IKE

In this phase, the IKE policy will be defined for the router. The IKE negotiates an SA (Security Association) with the peer by authenticating. This is reflected by means of a ISAKMP (Internet Security Association and Key Management Protocol) phase 1 policy.

This L3 VPN (IPSec) will use the following IKE (Internet Key Exchange) policy: `AES-256` encryption algorithm, the `SHA1` hash algorithm and the group 2 with a lifetime of 86400 seconds.

At this phase, the policy is not yet related to a specific peer, it only describes the parameters that are in use for encryption, HMAC, key exchange etc.

Note that several policies can be described, and they will all be tried one by one until one actually works with the remote peer (here router 2). Here, only one policy has been described, so this won't be the case.

To finish phase 1, a pre-shared password, here `notredieuAurel` has to be set for the destination (router 2 thus 10.0.2.1).

A similar configuration has been done for Router 2 (only the destination changes to 10.0.1.2).

When a packet subject to crypto transformation is deteted. Phase 1 looks at the destination, extract the password/certificate for that destination from the local database and tries each policy one after one to try to establish a Phase 1 with the remote peer (Router 2). When a policy is IPSec IKE accepted, a SA (IPSec Security Association) is created.

3.2 ISAKMP Phase 2 - Crypto transformation and access control

Phase 2 concerns the IPSec configuration and is composed of different steps:

- Create an extended ACL (Access Control List) to determine the packets that are subject to transformation. It allows a separation between normal and VPN traffic.
- Create IPSec Transform to configure how packets will be ciphered, MAC'ed, etc.
- Create a Crypto Map to link the destination to a transform method and filter it with the ACL.
- Apply the crypto map to the public interface to tell the router to analyse each packet passing by that interface for a possible crypto transformation.

3.2.1 Create extended ACL

First, the access list is created and named VPN-TRAFFIC. Then add the networks (for Router 1) 192.168.1.0/24 to 192.168.2.0/24 to this ACL. The traffic in this line will then be subject to tagging and processing in the pipeline VPN-TRAFFIC.

```
>>> ip access-list extended VPN-TRAFFIC
>>> permit ip  192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
```

3.2.2 Create IPSec Transform

A transformation set is created. It just tells how the packets will be encrypted and decrypted (AES and SHA1).

```
>>> crypto ipsec transform-set MYTS esp-aes esp-sha-hmac
```

3.2.3 Create Crypto Map

The Crypto map connects the previously defined ISAKMP, apply the transform-set MYTS (defined in 3.2.2) and set the peer/endpoint of the tunnel (10.0.2.1-Router2 for Router 1).

```
>>> crypto map CMAP 10 ipsec-isakmp
>>> set peer 10.0.2.1
>>> set transform-set MYTS
>>> match address VPN-TRAFFIC
```

This last step will trigger Phase 1 to authenticate and negotiate a session key between the two tunnel peers.

3.2.4 Apply Crypto Map

Finally, the crypto map is applied to the network interface (fastEthernet 0/0 for both Router 1 and 2). with the command:

```
>>> crypto map CMAP
```

3.3 Confirmation of configuration

Figures 6 and 7 show that the ISAKMP has been successfully configured and activated for both Router 1 and 2.

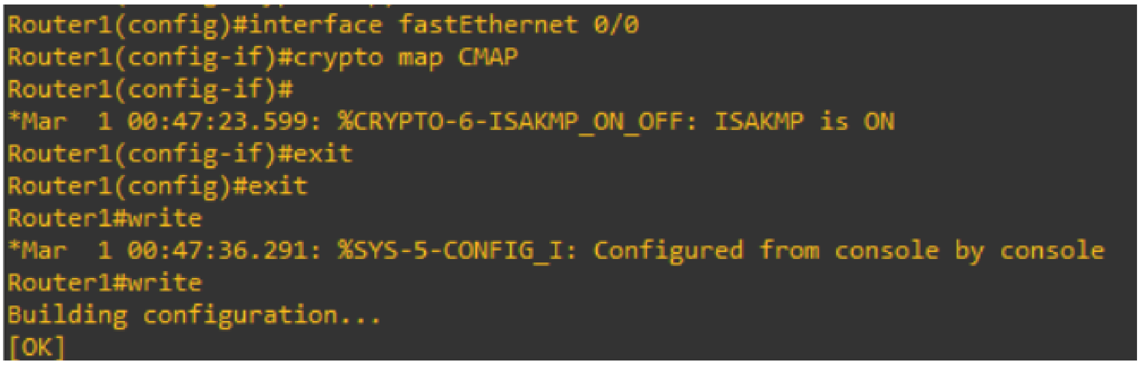

Figure 6: Confirmation that R1 has correctly been configured

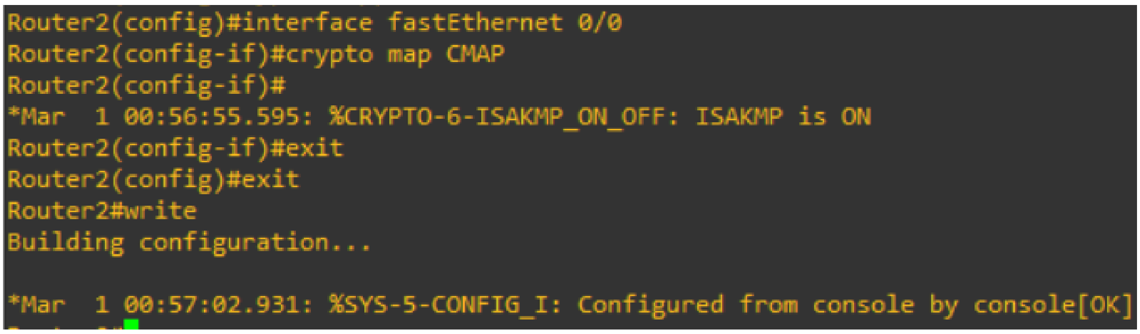

Figure 7: Confirmation that R2 has correctly been configured

4 Mission 3: Validate

4.1 Pinging from PC1 to PC3

Figure 8 shows a ping from PC1 to PC3. The pinging is successful and normal, it is not affected at all by the Site-to-Site VPN configuration. Which is normal because the PC3 is not a destination marked.

1023	3483.980594	192.168.1.2	192.168.3.2	ICMP	98 Echo (ping) request id=0x379c, seq=1/256, ttl=63 (reply in 1024)
1024	3484.033402	192.168.3.2	192.168.1.2	ICMP	98 Echo (ping) reply id=0x379c, seq=1/256, ttl=62 (request in 1023)
1025	3484.992476	c4:01:05:19:00:00	c4:01:05:19:00:00	LOOP	60 Reply
1026	3485.057595	192.168.1.2	192.168.3.2	ICMP	98 Echo (ping) request id=0x389c, seq=2/512, ttl=63 (reply in 1027)
1027	3485.112197	192.168.3.2	192.168.1.2	ICMP	98 Echo (ping) reply id=0x389c, seq=2/512, ttl=62 (request in 1026)
1028	3486.137427	192.168.1.2	192.168.3.2	ICMP	98 Echo (ping) request id=0x399c, seq=3/768, ttl=63 (reply in 1029)
1029	3486.189127	192.168.3.2	192.168.1.2	ICMP	98 Echo (ping) reply id=0x399c, seq=3/768, ttl=62 (request in 1028)
1030	3486.850705	10.0.1.2	255.255.255.255	RIPv1	146 Response
1031	3487.146113	c4:04:05:61:00:01	c4:04:05:61:00:01	LOOP	60 Reply
1032	3487.228510	192.168.1.2	192.168.3.2	ICMP	98 Echo (ping) request id=0x3a9c, seq=4/1024, ttl=63 (reply in 1033)
1033	3487.297292	192.168.3.2	192.168.1.2	ICMP	98 Echo (ping) reply id=0x3a9c, seq=4/1024, ttl=62 (request in 1032)
1034	3488.314503	192.168.1.2	192.168.3.2	ICMP	98 Echo (ping) request id=0x3b9c, seq=5/1280, ttl=63 (reply in 1035)
1035	3488.364442	192.168.3.2	192.168.1.2	ICMP	98 Echo (ping) reply id=0x3b9c, seq=5/1280, ttl=62 (request in 1034)
1036	3490.724257	10.0.1.1	255.255.255.255	RIPv1	66 Response
1037	3496.044919	c4:01:05:19:00:00	c4:01:05:19:00:00	LOOP	60 Reply
1038	3498.078803	c4:04:05:61:00:01	c4:04:05:61:00:01	LOOP	60 Reply

```
> Frame 1023: 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
```

```
0000  c4 04 05 61 00 01 c4 01
0010  00 54 9c 37 00 00 3f 01
0020  03 02 08 00 e8 6e 37 9c
0030  0e 0f 10 11 12 13 14 15
0040  1e 1f 20 21 22 23 24 25
```

Figure 8: Capture of the ping from PC1 to PC3 on the R1-R4 line

4.2 Pinging from PC1 to PC2

As it can be seen in figures 9 and 10, the pinging from PC1 to PC2 works and the packets are encapsulated in IPSec ESP. Which means that the Site-to-Site VPN works well. The fact that the reply also works show that both router have been correctly configured.

```
PC1> ping 192.168.2.2

84 bytes from 192.168.2.2 icmp_seq=1 ttl=62 time=101.977 ms
84 bytes from 192.168.2.2 icmp_seq=2 ttl=62 time=110.959 ms
84 bytes from 192.168.2.2 icmp_seq=3 ttl=62 time=90.413 ms
84 bytes from 192.168.2.2 icmp_seq=4 ttl=62 time=106.516 ms
84 bytes from 192.168.2.2 icmp_seq=5 ttl=62 time=96.610 ms
```

Figure 9: Ping from PC1 to PC2

```
 4 2.511665  10.0.1.1           10.0.2.1           ESP      166 ESP (SPI=0x226db3d9)
 5 2.610910  10.0.2.1           10.0.1.1           ESP      166 ESP (SPI=0xc91127c5)
 6 3.540040  c4:04:05:61:00:01  c4:04:05:61:00:01  LOOP      60 Reply
 7 3.635085  10.0.1.1           10.0.2.1           ESP      166 ESP (SPI=0x226db3d9)
 8 3.716761  10.0.2.1           10.0.1.1           ESP      166 ESP (SPI=0xc91127c5)
 9 4.737402  10.0.1.1           10.0.2.1           ESP      166 ESP (SPI=0x226db3d9)
10 4.823162  10.0.2.1           10.0.1.1           ESP      166 ESP (SPI=0xc91127c5)
11 5.469577  10.0.1.1           255.255.255.255    RIPv1     66 Response
12 5.844767  10.0.1.1           10.0.2.1           ESP      166 ESP (SPI=0x226db3d9)
13 5.926981  10.0.2.1           10.0.1.1           ESP      166 ESP (SPI=0xc91127c5)
14 6.947443  10.0.1.1           10.0.2.1           ESP      166 ESP (SPI=0x226db3d9)
15 7.042504  10.0.2.1           10.0.1.1           ESP      166 ESP (SPI=0xc91127c5)

> Frame 4: 166 bytes on wire (1328 bits), 166 bytes captured (1328 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: 10.0.1.1, Dst: 10.0.2.1
v Encapsulating Security Payload
    ESP SPI: 0x226db3d9 (577614809)
    ESP Sequence: 15
```

Figure 10: Capture of the ping from PC1 to PC2 on the R1-R4 line

4.3 Router 1 - ISAKMP check

```
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
```

Figure 11: Configuration of the ISAKMP policy

```
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
```

Figure 12: Router 1: Configuration of ISAKMP SA and Peers

4.4 Router 1 - IPSec SA check

```
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: 19, #pkts encrypt: 19, #pkts digest: 19
    #pkts decaps: 19, #pkts decrypt: 19, #pkts verify: 19
    #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: 0x226DB3D9(577614809)

     inbound esp sas:
      spi: 0xC91127C5(3373344709)
        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): (4415280/3126)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x226DB3D9(577614809)
        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): (4415280/3083)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

Figure 13: Router 1: IPSec SA configuration

5 Conclusion

The completion of the lab tasks demonstrates the successful establishment of a Site-to-Site IPSec VPN between Router 1 and Router 2. The configured IPSec policies, including ISAKMP Phase 1 and IPSec Phase 2, were validated through ping tests between PC1 and PC2. The Wireshark captures confirm that the communication is encrypted using the specified algorithms and security associations.

Additionally, the observation of PC1 to PC3 communication, unaffected by the VPN configuration, reinforces the proper segmentation of VPN and non-VPN traffic. The thorough examination of ISAKMP and IPSec Security Associations on Router 1 provides insights into the established connections and their parameters, further validating the correct configuration.

In conclusion, the successful implementation of the Site-to-Site IPSec VPN enhances the security of communication between the routers, ensuring confidentiality, integrity, and authenticity of the transmitted data. The thorough validation process, including network captures and router configuration checks, contributes to the overall reliability of the VPN setup.