ABSTRACT

This project aims to simulate and configure an IPsec site-to-site VPN using GNS3 (Graphical Network Simulator-3).

The network involves multiple network devices to establish a secure and encrypted connection between two remote sites.

The primary objectives include configuring IPsec protocols (such as ESP and AH), implementing secure tunnelling, ensuring data confidentiality, integrity, and authentication between the simulated sites.

INTRODUCTION

In the realm of modern networking, secure communication between geographically dispersed networks is indispensable. The advent of Virtual Private Networks (VPNs) has revolutionized the way organizations establish secure connections over public networks. Among these, the Internet Protocol Security (IPsec) protocol suite stands as a cornerstone for ensuring confidentiality, integrity, and authenticity in data transmission across networks.

This project endeavours to explore and implement an IPsec site-to-site VPN utilizing GNS3.

The objective is to replicate a secure communication channel between multiple remote sites over a simulated network infrastructure.

The introduction will focus on the following key points:

Significance of Secure Communication: Discussing the importance of secure communication between remote networks in contemporary networking scenarios, highlighting the risks associated with unsecured data transmission and the need for robust security measures.

Role of IPsec in Network Security: Providing an overview of the IPsec protocol suite, emphasizing its fundamental role in establishing Virtual Private Networks, and explaining its mechanisms for encryption, authentication, and key management.

GNS3 as a Simulation Platform: Introducing GNS3 as the chosen platform for network emulation, highlighting its capabilities in replicating real-world network scenarios and its suitability for simulating IPsec-based VPN deployments.

Objectives of the Project: Outlining the specific aims and objectives of the project, including the establishment of secure site-to-site communication using IPsec protocols within the GNS3 environment.

This introduction sets the stage by highlighting the importance of secure communication, elucidating the significance of IPsec in network security, and establishing the context for the implementation of an IPsec site-to-site VPN using GNS3 as the simulation platform.

This introduction aims to provide a foundational understanding of the project's objectives, emphasizing the significance of secure communication and positioning IPsec within the context of network security. Adjust the content based on the depth and scope of your project.

PROBLEM STATEMENT

Problem statement: In today's interconnected digital landscape, the secure transmission of data between geographically dispersed networks stands as a critical necessity. However, establishing secure communication channels across untrusted networks poses a significant challenge. The need for a robust, reliable, and scalable solution to facilitate secure site-to-site communication while preserving data confidentiality, integrity, and authenticity remains a pertinent issue in network security.

Establishment of Secure Communication: Design and implement a secure and scalable infrastructure that allows multiple remote sites to communicate securely over an untrusted network such as the internet.

Ensuring Data Confidentiality and Integrity: Employ encryption techniques and authentication mechanisms to guarantee the confidentiality and integrity of transmitted data between interconnected sites.

This project seeks to explore the design, implementation, and testing of an IPsec site-to-site VPN using GNS3 as a simulation platform, addressing the challenges of secure communication between remote networks over untrusted environments while ensuring data confidentiality, integrity, and authenticity.

METHODOLOGY

1. Network Design and Topology Planning:

The network shown in the Fig- 1 is a simplified network depicting public and private network, and 3 branches.

2. Configuration of Virtual Network Devices:

The gateway routers R1 and R2 are configured in order to secure the private networks.

3.Configuration of IPsec Parameters:

Configure the chosen IPsec protocol i.e., Encapsulating Security Payload (ESP) on the routers, specifying encryption algorithms, authentication methods, and key management settings.

IKE (Internet Key Exchange) Configuration: Set up IKE for secure key exchange and negotiation between VPN peers.

4. Traffic of Interest:

Generate test traffic to simulate data transmission between the remote sites. The traffic could be from single subnet or multiple subnets.

5.Analysing the packets:

Capture the packets on various links to show encryption of packets arriving from traffic of interest.

This methodology outlines the step-by-step approach used to design, configure, test, and implementation of an IPsec site-to-site VPN using GNS3 as the simulation platform.

SOFTWARE TERMINALS

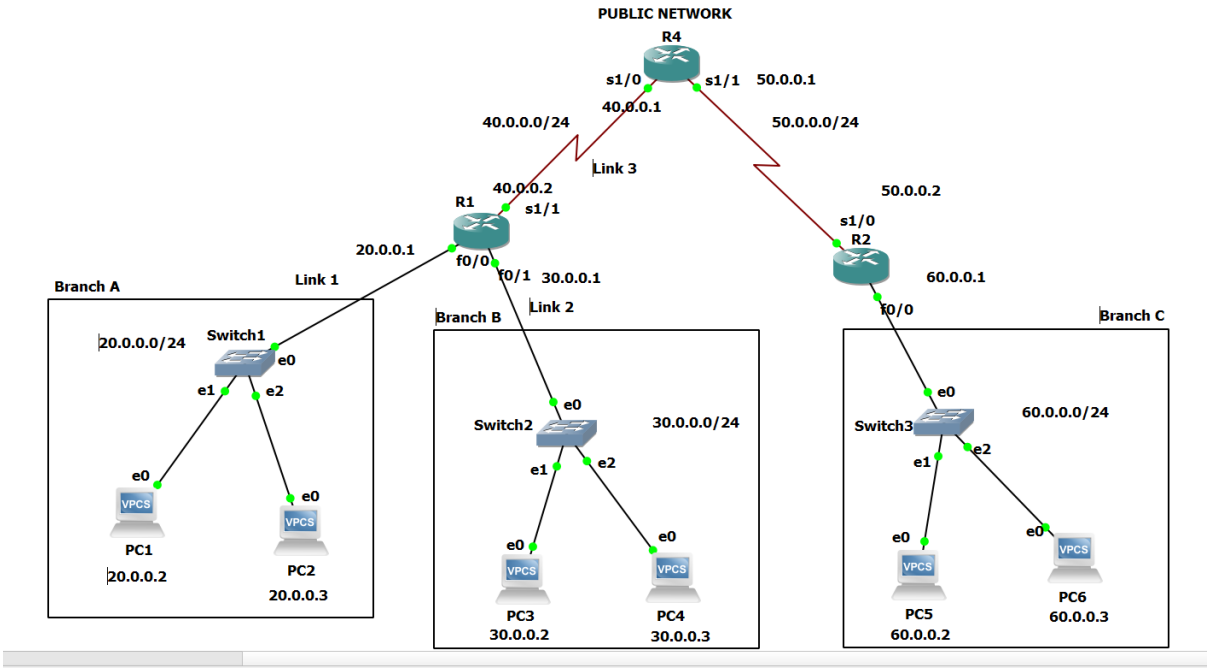

Fig – 1: GNS3 terminal.

R2 represents public network, R1 and R2 are gateway routers to the private network Branch A, Branch B and Branch C respectively.

There are 2 protocols for Internet protocol security,

1) Authentication Header (AH)
2) Encapsulating Security Payload (ESP)

ESP protocol provides source authentication, data integrity, and confidentiality. As AH doesn't provide confidentiality which is crucial in this technological world, ESP is widely used.

Routers need to agree upon some of the parameters to encrypt and decrypt the packets. Those are,

1) Type of encryption
2) Type of hashing
3) Type of integrity check
4) Key
5) Traffic

To configure the gateway routers from Fig -1, we have used Secure Hashing Algorithm (SHA), Advanced Encryption Standard (AES),

Hash based Message Authentication Code (HMAC) for integrity check and pre shared keys.

Fig – 2 and Fig -3 shows the commands for configuring the respective terminals and also the parameters discussed above.

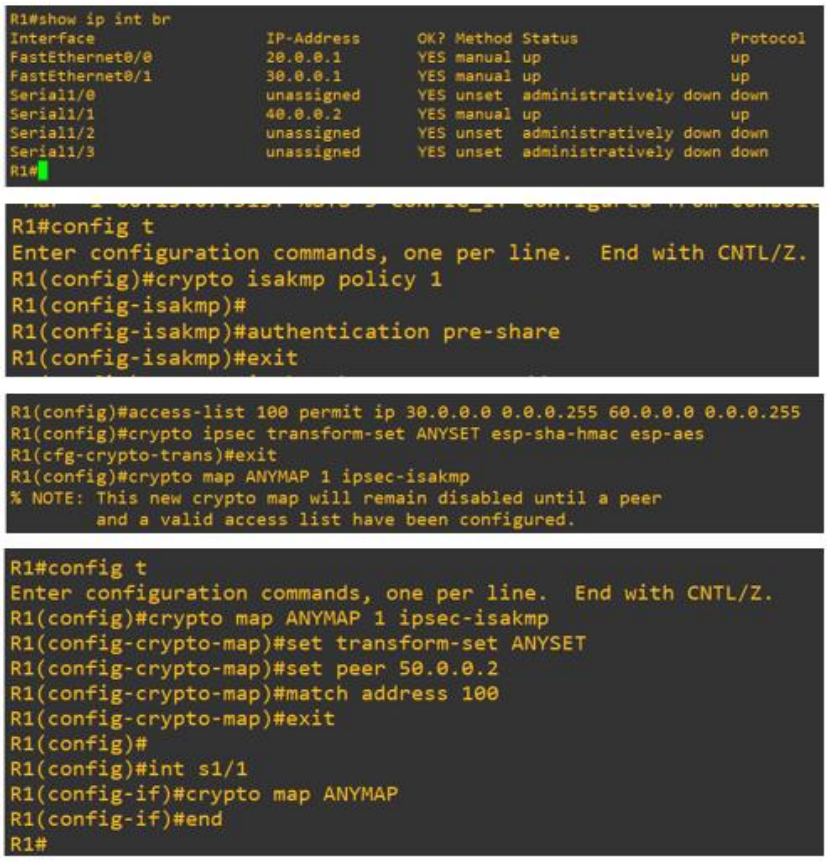

Fig – 2: Configuring of Router1.

```
R2#show ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            60.0.0.1        YES manual up                    up
FastEthernet0/1            unassigned      YES unset  administratively down down
Serial1/0                  50.0.0.2        YES manual up                    up
Serial1/1                  unassigned      YES unset  administratively down down
Serial1/2                  unassigned      YES unset  administratively down down
Serial1/3                  unassigned      YES unset  administratively down down
R2#
```

```
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#crypto isakmp policy 1
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#exit
R2(config)#crypto isakmp key ANYKEY address 40.0.0.2
R2(config)#access-list 100 permit ip 60.0.0.0 0.0.0.255 30.0.0.0 0.0.0.255
R2(config)#crypto ipsec transform-set ANYSET esa-sha-hmac esp-aes
                                          ^
% Invalid input detected at '^' marker.

R2(config)#crypto ipsec transform-set ANYSET esp-sha-hmac esp-aes
R2(cfg-crypto-trans)#exit
R2(config)#crypto map ANYMAP 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
       and a valid access list have been configured.
```

```
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#crypto map ANYMAP 1 ipsec-isakmp
R2(config-crypto-map)#set transform-set ANYSET
R2(config-crypto-map)#set peer 40.0.0.2
R2(config-crypto-map)#match address 100
R2(config-crypto-map)#exit
R2(config)#
R2(config)#int s1/0
R2(config-if)#crypto map ANYMAP
R2(config-if)#end
```

Fig – 3: Configuring of Router2.

```
R4#show ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES NVRAM  administratively down down
FastEthernet0/1            unassigned      YES NVRAM  administratively down down
Serial1/0                  40.0.0.1        YES NVRAM  up                    down
Serial1/1                  50.0.0.1        YES NVRAM  up                    down
Serial1/2                  unassigned      YES NVRAM  administratively down down
Serial1/3                  unassigned      YES NVRAM  administratively down down
R4#
```

Fig – 4: Configuring of Router4.

```
R1#
R1#show access-list
Extended IP access list 100
    10 permit ip 30.0.0.0 0.0.0.255 60.0.0.0 0.0.0.255 (110 matches)
R1#
```

Fig – 5: Access-list.

From the figure 2 ,3 and 5, we understand that the defined traffic of interest is between the networks 30.0.0.0/24 and 60.0.0.0/24, where in PC3 and PC4 lies, and the packets from these PC's will be encrypted in the public network.

The network 20.0.0.0/24 doesn't lie in the interest of traffic and packets sourced from the network will not be encrypted in the public network.

```
PC1> ping 60.0.0.2
84 bytes from 60.0.0.2 icmp_seq=1 ttl=61 time=91.077 ms
84 bytes from 60.0.0.2 icmp_seq=2 ttl=61 time=92.536 ms
84 bytes from 60.0.0.2 icmp_seq=3 ttl=61 time=92.842 ms
84 bytes from 60.0.0.2 icmp_seq=4 ttl=61 time=93.777 ms
84 bytes from 60.0.0.2 icmp_seq=5 ttl=61 time=90.765 ms
```

Fig – 6: ping operation from PC1

```
PC3> ping 60.0.0.2
84 bytes from 60.0.0.2 icmp_seq=1 ttl=62 time=92.188 ms
84 bytes from 60.0.0.2 icmp_seq=2 ttl=62 time=90.839 ms
84 bytes from 60.0.0.2 icmp_seq=3 ttl=62 time=76.073 ms
84 bytes from 60.0.0.2 icmp_seq=4 ttl=62 time=91.466 ms
84 bytes from 60.0.0.2 icmp_seq=5 ttl=62 time=91.890 ms
```

Fig – 7: ping operation from PC3

Figures 6 and 7 shows console of 2 PCs with successful ping operation, one from network 30.0.0.0/24 [PC3] and another from 20.0.0.0/24 [PC1]

Wireshark packets:

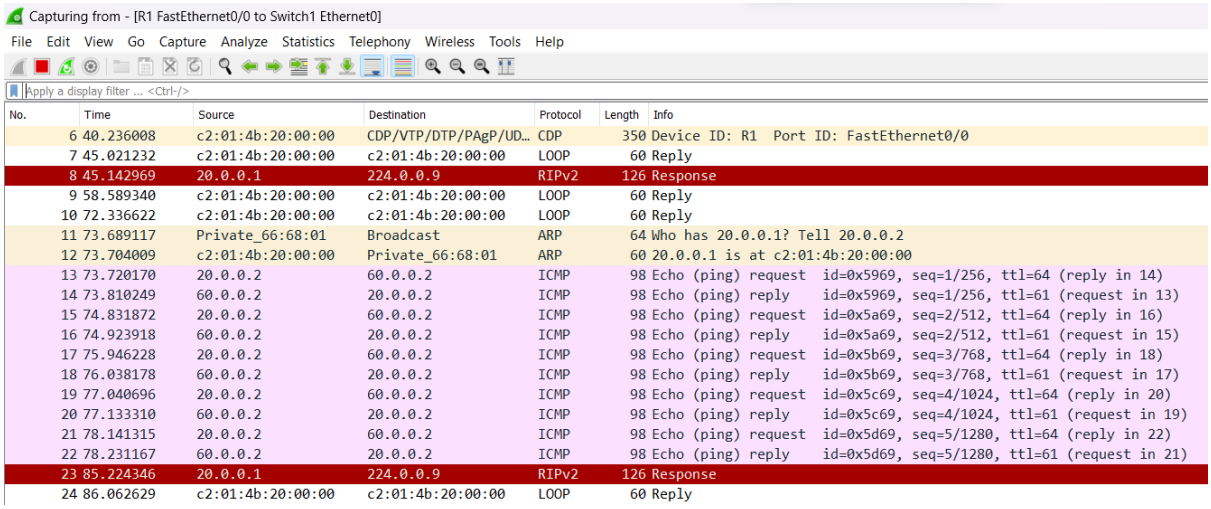

Fig – 8: Ping from PC1 to PC5.

Packet captured from link 1, from Branch A.

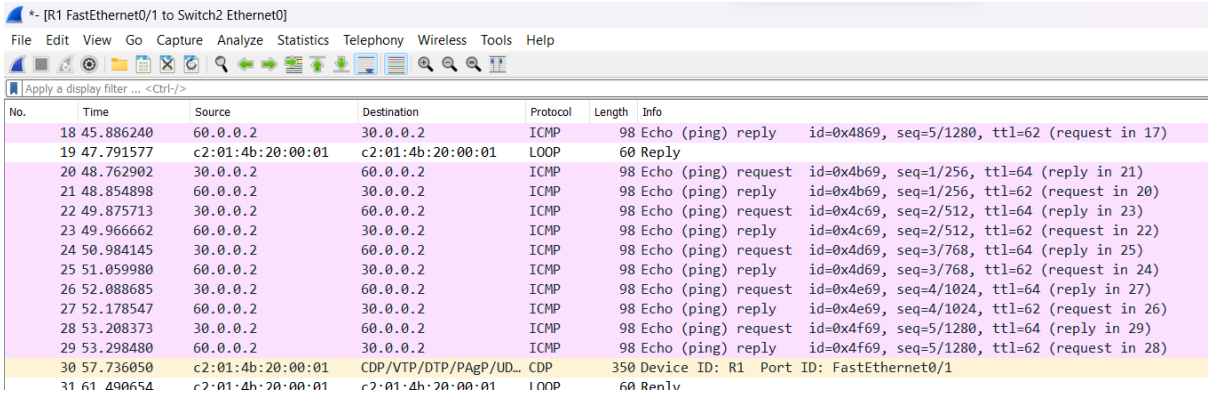

Fig – 9: Ping from PC3 to PC5, before gateway router.

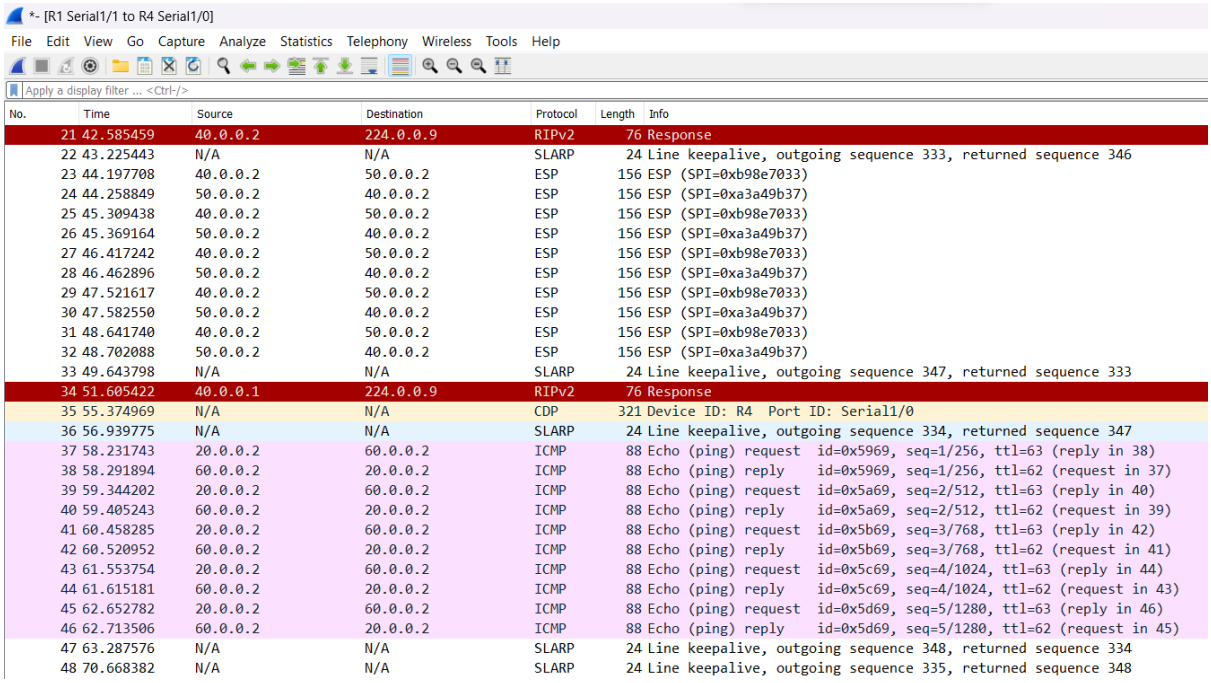

Fig – 10: Packets captured after gateway router from both PC1 and PC3.

Figure 10 shows packets captured from 2 set of ping operations. The first set is from PC3[Branch B], and second set is from PC1[Branch A]. we can observe that the packets from specified traffic are only encrypted before sending them to the public network.

The details like source and destination IP address, the protocol used are hidden by the ESP protocol.

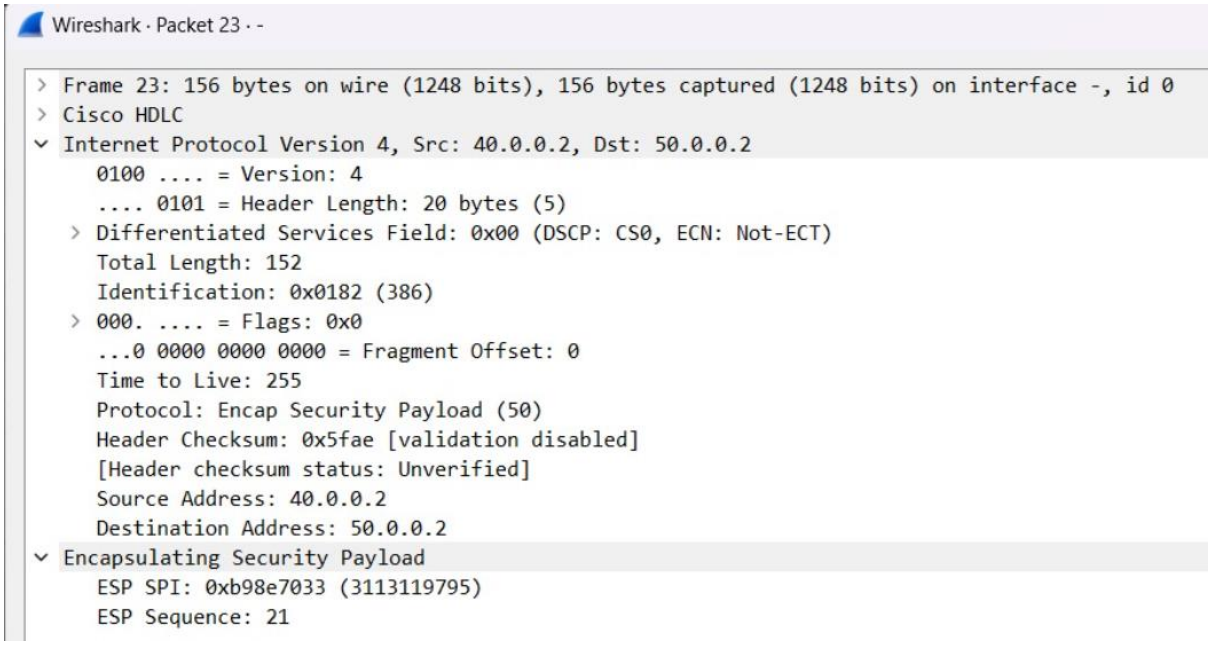

Fig – 11: Encrypted packet.

On opening the ESP packet, we can see the protocol number of ESP is 50, with the header file of 20 bytes.

```
R1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 2
        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
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
R1#
```

Fig – 12: List of isakmp policies (internet security association key management protocol)

```
R1#show crypto ipsec sa

interface: Serial1/1
    Crypto map tag: ANYMAP, local addr 40.0.0.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (30.0.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (60.0.0.0/255.255.255.0/0/0)
   current_peer 50.0.0.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 25, #pkts encrypt: 25, #pkts digest: 25
    #pkts decaps: 25, #pkts decrypt: 25, #pkts verify: 25
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 60, #recv errors 0

     local crypto endpt.: 40.0.0.2, remote crypto endpt.: 60.0.0.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial1/1
     current outbound spi: 0x0(0)
```

Fig:13 show crypto ipsec sa (internet protocol security association)

```
PC4> ping 60.0.0.3 -P 6 -p 1234
Connect   1234@60.0.0.3 seq=1 ttl=62 time=105.124 ms
SendData  1234@60.0.0.3 seq=1 ttl=62 time=105.092 ms
Close     1234@60.0.0.3 seq=1 ttl=62 time=120.021 ms
Connect   1234@60.0.0.3 seq=2 ttl=62 time=105.263 ms
SendData  1234@60.0.0.3 seq=2 ttl=62 time=105.816 ms
Close     1234@60.0.0.3 seq=2 ttl=62 time=119.107 ms
Connect   1234@60.0.0.3 seq=3 ttl=62 time=104.966 ms
SendData  1234@60.0.0.3 seq=3 ttl=62 time=105.473 ms
Close     1234@60.0.0.3 seq=3 ttl=62 time=120.513 ms
Connect   1234@60.0.0.3 seq=4 ttl=62 time=104.612 ms
SendData  1234@60.0.0.3 seq=4 ttl=62 time=106.520 ms
Close     1234@60.0.0.3 seq=4 ttl=62 time=119.894 ms
Connect   1234@60.0.0.3 seq=5 ttl=62 time=105.974 ms
SendData  1234@60.0.0.3 seq=5 ttl=62 time=106.036 ms
Close     1234@60.0.0.3 seq=5 ttl=62 time=119.255 ms

PC4> ping 60.0.0.3 -P 17 -p 1234
84 bytes from 60.0.0.3 udp_seq=1 ttl=62 time=91.545 ms
84 bytes from 60.0.0.3 udp_seq=2 ttl=62 time=91.113 ms
84 bytes from 60.0.0.3 udp_seq=3 ttl=62 time=90.080 ms
84 bytes from 60.0.0.3 udp_seq=4 ttl=62 time=91.214 ms
84 bytes from 60.0.0.3 udp_seq=5 ttl=62 time=90.530 ms
```

Fig 14: TCP and UDP pinging from branch B

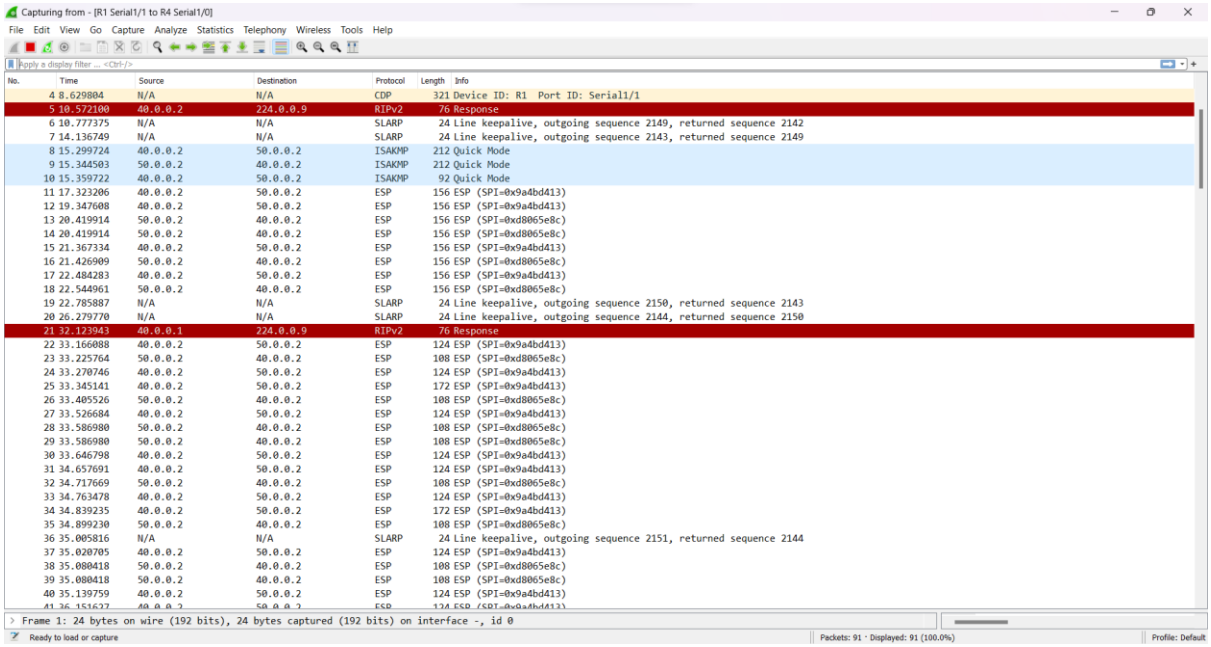

Fig 15: TCP and UDP pinging from PC4 to PC6

RESULTS

On performing the mentioned network simulation, we are able to verify the Secure connection between different PCs.

Data integrity, confidentiality and authentication is achieved.

FUTURE SCOPE

Challenges faced included ensuring compatibility among different devices, configuring correct IPsec parameters and handling and routing connectivity issues.