



# COMPUTER SCIENCE & ENGINEERING DEPARTMENT

## REPORT (CSE 419)

### IPsec(secure Tunnel)

#### Submitted By:

|                      |  |
|----------------------|--|
| <b>Student Name:</b> | Yazan Fahad<br>Mohammed Alharbi<br>Bandar Almutairi<br>Meshal Mohammed<br>Hatem Alhamar<br>Abdulaziz aldughaim |
| <b>Student ID:</b>   | 2210003017<br>2210002589<br>2210001275<br>2210002799<br>2210001357<br>2210001954                               |
| <b>Term:</b>         | 2 <sup>rd</sup> term   |
| <b>Date:</b>         | April 26, 2025   |
| <b>Advisor:</b>      | Abdullah Alshammari  |

# Table of Contents

|   |    |
|---|----|
| 1. Introduction.....  | 5  |
| 2. Problem Statement.....   | 7  |
| 3. Background.....  | 8  |
| 4. Requirements and Specifications.....                                 | 10 |
| 5. System Design .....  | 11 |
| 5.1 Solution Concept.....   | 11 |
| 5.2. Architecture .....   | 12 |
| 5.3. Component Design .....   | 14 |
| 5.4. System Integration.....  | 15 |
| 5.5 Design Evaluation :.....  | 16 |
| 6. Implementation .....   | 18 |
| Network Scenario .....  | 19 |
| Internet Key Exchange .....   | 20 |
| ISAKMP Policy (Phase 1): .....  | 20 |
| Phase 2:.....   | 20 |
| ISAKMP Phase 1 Policy Parameters .....                                  | 21 |
| IPsec Phase 2 Policy Parameters.....                                    | 22 |
| Instructions .....  | 23 |
| Part 1: Configure IPsec Parameters on R1 .....                          | 23 |
| Step 1: Test connectivity.....  | 23 |
| Step 2: Enable the Security Technology package. ....                    | 23 |
| Step 3: Identify interesting traffic on R1.....                         | 23 |
| Step 4: Configure the IKE Phase 1 ISAKMP policy on R1. ....             | 24 |
| Step 5: Configure the IKE Phase 2 IPsec policy on R1. ....              | 24 |
| Step 6: Configure the crypto map on the outgoing interface. ....        | 25 |
| Part 2: Configure IPsec Parameters on R3 .....                          | 25 |
| Step 1: Enable the Security Technology package. ....                    | 25 |
| Step 2: Configure router R3 to support a site-to-site VPN with R1. .... | 25 |
| Step 3: Configure the IKE Phase 1 ISAKMP properties on R3. ....         | 25 |
| Step 4: Configure the IKE Phase 2 IPsec policy on R3. ....              | 26 |
| Step 5: Configure the crypto map on the outgoing interface. ....        | 26 |
| Part 3: Verify the IPsec VPN.....                                       | 27 |

|   |    |
|---|----|
| Step 1: Verify the tunnel prior to interesting traffic..... | 27 |
| Step 2: Create interesting traffic. ....                    | 27 |
| Step 3: Verify the tunnel after interesting traffic. ....   | 27 |
| Step 4: Create uninteresting traffic. ....                  | 27 |
| Step 5: Verify the tunnel.....                              | 27 |
| 7. Testing, Analysis, and Evaluation .....                  | 27 |
| 8. Issues .....   | 29 |
| 9. Engineering Tools and Standards .....                    | 31 |
| 10. Teamwork.....   | 32 |
| 11. Conclusions .....                                       | 42 |

## List Of Tables:

|  |    |
|--|----|
| Table 1-Addressing Table .....               | 19 |
| Table 2-ISAKMP Phase 1 .....                 | 21 |
| Table 3-IPsec Phase 2 .....                  | 22 |
| Table 4-System Analysis and Evaluation ..... | 29 |
| Table 5-Teamwork(Week1) .....                | 33 |
| Table 6-Teamwork(Week2) .....                | 34 |
| Table 7-Teamwork(Week3) .....                | 35 |
| Table 8-Teamwork(Week4) .....                | 36 |
| Table 9-Teamwork(Week5) .....                | 37 |
| Table 10-Teamwork(Week6) .....               | 38 |
| Table 11-Teamwork(Week7) .....               | 38 |
| Table 12-Teamwork(Week8) .....               | 39 |
| Table 13-Teamwork(Week9) .....               | 40 |
| Table 14-Teamwork(Week10) .....              | 41 |
| Table 15-Teamwork(Week11) .....              | 41 |

## List Of Figures:

|                                      |    |
|--------------------------------------|----|
| Figure 1-IPSec Tunnel .....          | 12 |
| Figure 2-VPN Client(Flowchart) ..... | 14 |
| Figure 3-Component Instraction ..... | 16 |
| Figure 4-IPSec VPN Tuunel .....      | 18 |
| Figure 5 ping Instruction.....       | 23 |
| Figure 6-Tracert Path .....          | 27 |

## 1. Introduction

This project is based on configuring and verifying a **Site-to-Site IPsec VPN** using **Cisco Packet Tracer**. A Site-to-Site VPN securely connects two distant networks over the internet, allowing devices from both sites to communicate as if they were on the same local network. In this setup, routers act as VPN gateways, establishing an encrypted tunnel between them to protect data transmission. The objective of the project is to simulate a real-world VPN environment between two sites (Router R1 and Router R3) by configuring key elements such as ISAKMP policies, IPsec transform sets, crypto maps, and applying them to router interfaces. By the end of this project, we aim to ensure private and secure communication across the public network, enhancing our understanding of VPN technologies and network security principles

### Why is it an issue?

As digital communication grows, so does the risk of cyber threats. The internet is inherently insecure—data sent over it can be intercepted, altered, or stolen. This makes securing sensitive information such as personal data, financial records, business communications, and government transactions a top priority.

According to IBM's 2023 Cost of a Data Breach Report, the **average global cost of a data breach** reached **\$4.45 million**, the highest in history. In addition, **Verizon's 2023 Data Breach Investigations Report** found that over **74% of data breaches involved human error, social engineering, or system misuse**, often due to poor encryption or unsecured connections. These statistics emphasize the urgent need for robust network security solutions like IPsec VPNs.

### How the Project Deals with the Issue:

This project provides a working model for implementing a Site-to-Site IPsec VPN, which ensures secure communication between two remote networks over an untrusted medium (the internet). By encrypting traffic using AES-256,

authenticating peers using pre-shared keys, and using access lists to define and limit the scope of encrypted traffic, the project offers a practical, cost-effective solution to:

- Prevent unauthorized access to sensitive internal resources.
- Guarantee the confidentiality, integrity, and authenticity of transmitted data.
- Demonstrate how security policies can be enforced at the network layer, reducing the risk of compromise.

### **Project Impact on Society:**

#### **Positive Impact:**

The implementation of secure tunnels enhances data protection, fostering trust among users and organizations. This leads to more robust remote work environments, allowing employees to collaborate safely from any location. Furthermore, businesses can maintain operational continuity and effectively collaborate without compromising security.

#### **Possible Negative Impact:**

Despite its benefits, there is a risk of misuse. If not managed properly, secure communication tools could be exploited by malicious actors to conceal illegal activities. Additionally, the complexity of such systems may lead to vulnerabilities if not adequately maintained, highlighting the need for ongoing vigilance and risk management in cybersecurity practices

## **2. Problem Statement**

### **The specific problem the project is trying to solve.**

The specific problem this project aims to solve is the vulnerability of data transmitted over untrusted networks, such as the Internet. As organizations increasingly rely on remote communication, sensitive information is at risk of interception and unauthorized access. Without proper security measures, data can be eavesdropped, tampered with, or compromised, leading to severe consequences, including financial loss, reputational damage, and regulatory penalties.

The lack of secure communication channels poses significant challenges for businesses, especially those with multiple sites or remote employees. The project seeks to address these issues by establishing a fully operational IPSec tunnel that encrypts and securely transmits data between specified endpoints. This solution not only protects sensitive information but also ensures that organizations can operate with confidence in a digital landscape fraught with cyber threats.

### 3. Background

#### Related Terminology and Concepts

1. **IPSec (Internet Protocol Security):** A suite of protocols designed to secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet in a communication session. IPSec is commonly used to create Virtual Private Networks (VPNs).
2. **VPN (Virtual Private Network):** A technology that creates a secure and encrypted connection over a less secure network, such as the Internet. VPNs are used to protect private web traffic from snooping, interference, and censorship.
3. **Encryption:** The process of converting information or data into a code to prevent unauthorized access. Encryption is a critical component of securing communications over the internet.
4. **Eavesdropping:** The act of secretly listening to private conversations or communications. In the context of data transmission, eavesdropping can lead to data breaches and unauthorized access.



## Existing Solutions

1. **Commercial VPN Services:** Numerous companies offer VPN services that utilize IPsec and other security protocols to protect user data. Examples include NordVPN, ExpressVPN, and Cisco AnyConnect. These solutions are widely used by individuals and organizations for secure remote access.
2. **Open-Source Solutions:** Tools like OpenVPN and StrongSwan provide robust, community-driven options for establishing secure tunnels. These solutions allow organizations to customize their security implementations according to their specific needs.
3. **Research and Development:** Ongoing academic and industry research focuses on improving the security and efficiency of IPsec implementations. Studies often explore new encryption algorithms, authentication methods, and the integration of machine learning for threat detection.
4. **Corporate Solutions:** Many organizations develop proprietary VPN solutions tailored to their infrastructure. These solutions often include additional features such as secure access controls, monitoring, and compliance with industry regulations.

## 4. Requirements and Specifications

### Functional user requirements

1. **Secure Data Transmission:** The system must ensure that all data transmitted through the IPSec tunnel is encrypted and protected from unauthorized access.
2. **User Authentication:** The system must provide robust user authentication mechanisms to verify the identity of users accessing the secure tunnel.
3. **Access Control:** The system must allow administrators to define and manage access rights for different users and groups to ensure secure communications.
4. **Multi-Endpoint Support:** The system must support secure connections between multiple endpoints, including remote users and different corporate sites.

### Non-Functional User Requirements

1. **Response Time:** The IPSec tunnel must establish connections in under 5 seconds for users to ensure a seamless experience.
2. **Scalability:** The system must support at least 100 concurrent users without performance degradation.
3. **Size:** The hardware solution (if applicable) should be compact enough to fit in standard server racks without requiring excessive space.

### Technical Specifications

1. **Encryption Standards:** The system must implement AES-256 encryption for data in transit, ensuring compliance with industry standards for secure communication.
2. **Authentication Protocols:** The system must support IKEv2 for key exchange and utilize X.509 certificates for user authentication.
3. **Throughput:** The IPSec tunnel must support a minimum throughput of 1 Gbps to accommodate high-volume data transfers.
4. **Latency:** The system should maintain latency below 100 ms for real-time applications, such as VoIP or video conferencing.

## 5. System Design

### 5.1 Solution Concept

#### General Approach

The project addresses the problem of insecure data transmission over untrusted networks by implementing an IPSec tunnel. This approach ensures that all data sent between remote users and corporate networks is encrypted and protected from eavesdropping and tampering. The solution leverages existing security protocols while incorporating custom features to enhance usability and performance.

#### Description of Used/Developed Algorithms

##### 1. Key Exchange Algorithm:

- **Diffie-Hellman (DH):** Used for securely exchanging cryptographic keys over a public channel. This algorithm enables both parties to generate a shared secret without transmitting it directly.

##### 2. Encryption Algorithm:

- **AES-256:** Advanced Encryption Standard with a key size of 256 bits is used for encrypting data packets transmitted over the tunnel.

##### 3. Authentication Algorithm:

- **HMAC-SHA-1:** Used for ensuring data integrity and authenticity of the transmitted packets by generating a unique hash based on the data and a secret key.

#### Alternative Approaches and Algorithms

- **SSL/TLS:** Another common approach for securing data transmission. While effective, it is generally more complex to implement in site-to-site communication compared to IPSec.
- **Comparison Criteria:**
  - **Security Level:** IPSec provides robust security features tailored for network-level protection.

- **Performance:** IPSec tends to have lower overhead compared to SSL/TLS in certain scenarios, making it suitable for high-volume data transfers.

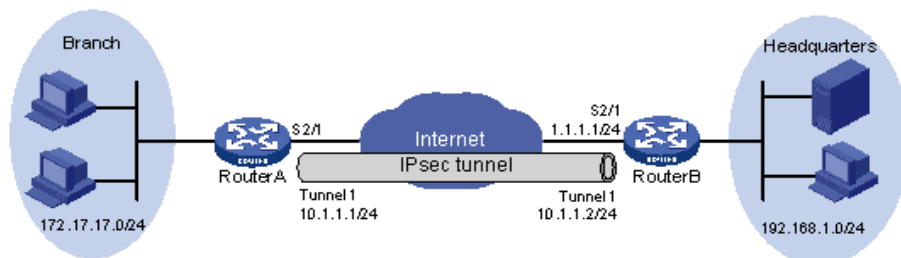
### Sub-function Identification

1. **Establish Connection**
2. **Authenticate User**
3. **Encrypt Data**
4. **Transmit Data**
5. **Log and Monitor Activity**

## 5.2. Architecture

### System Architecture and Components

The system architecture consists of a client-server model, where the client represents the remote user and the server is the IPSec tunnel.



*Figure 1-IPSec Tunnel*

## **Alternative Architectures**

- **Peer-to-Peer (P2P):** An alternative architecture where each node can act as both a client and a server. This can enhance redundancy but complicates management and security.
- **Comparison Criteria:**
  - **Scalability:** Client-server architecture scales well with centralized management.
  - **Security:** Centralized control in client-server architecture simplifies security policies.

## **Hardware vs. Software Components**

- **Hardware Components:**
  - VPN Server
  - Load Balancers
- **Software Components:**
  - VPN Client Software
  - Network Firewalls
  - IPSec Protocol Implementation
  - Logging and Monitoring Tools

## **Functions of Each Component**

1. **VPN Server:** Manages connections, encrypts data, and enforces security policies.
2. **Network Firewalls:** Filters traffic to protect the corporate network.
3. **Load Balancers:** Distributes incoming VPN connections to multiple servers for load management.

## 5.3. Component Design

### Custom vs. Off-the-Shelf

- **Custom Components:**
  - Justification: Tailored features that fit specific organizational needs (e.g., custom logging mechanisms).
- **Off-the-Shelf Components:**
  - Alternatives: Pre-built VPN solutions, commercial firewalls.
  - Comparison Criteria: Cost, support, feature set.

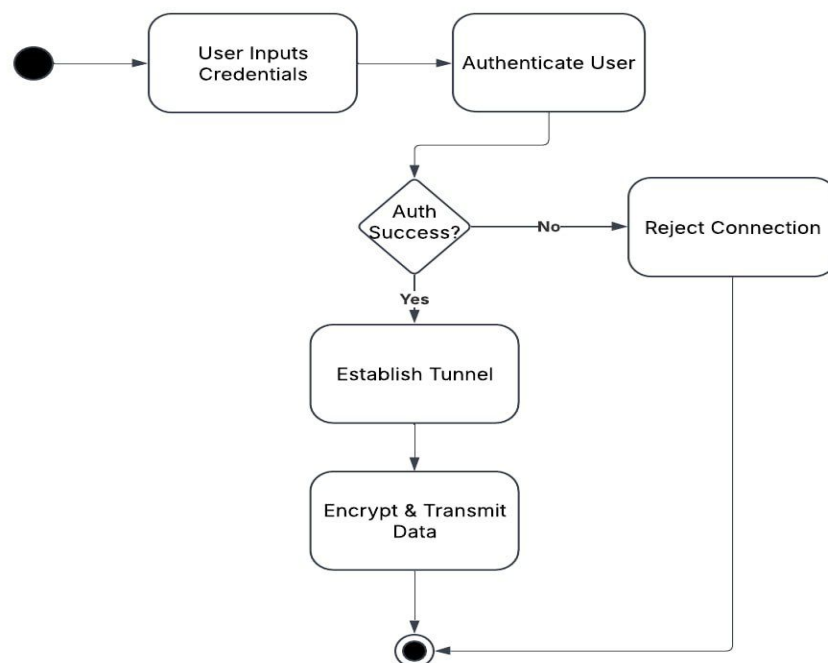
Custom components:

- Design and implementation, e.g. flow chart, state machine, pseudocode.
- Component design alternatives, comparison, and selection criteria.

### Custom Components Design and Implementation

#### 1. VPN Client:

- **Flowchart:**



*Figure 2-VPN Client(Flowchart)*

## 2. Logging Module:

- **State Machine:**

- States: Idle, Logging, Error Handling, End
- Transitions based on user actions and system events.

## 5.4. System Integration

### Standard Interfaces:

- **IPsec (Internet Protocol Security):** An industry-standard protocol suite used for securing IP communications by authenticating and encrypting each IP packet in a data stream.
- **ISAKMP/IKE (Internet Key Exchange):** A standard framework for establishing security associations and cryptographic keys in an IPsec environment.
- **ACLs (Access Control Lists):** A Cisco-standard feature to define "interesting traffic" for triggering the VPN.
- **Serial and Ethernet Interfaces:** Standard physical/logical interfaces used to connect routers and PCs in Packet Tracer.

**Using these standard interfaces ensures that the VPN tunnel could be realistically deployed on actual Cisco hardware or other compatible systems beyond the simulation environment.**

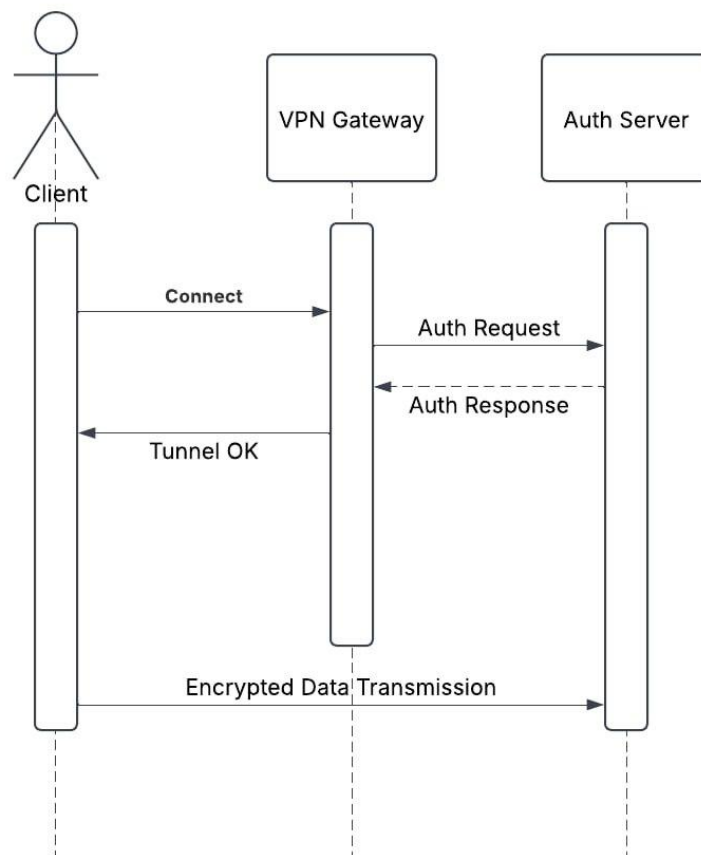
### Custom Interfaces

**custom configurations were manually applied:**

- **Custom Crypto Maps:** Tailored VPN configurations created using CLI commands (crypto map, transform-set) that matched specific security requirements for this scenario.

- **Manual Key Distribution:** A pre-shared key (vpnpa55) was manually configured instead of using automated key exchange via RSA or certificates.
- **Custom ACL Rules:** ACL 110 was customized to specifically define the traffic to be encrypted between R1 and R3.

## Component Interaction



*Figure 3-Component Instruction*

## 5.5 Design Evaluation :

### 1. Initial Design:

- The initial setup included basic IP addressing, static routing, and unencrypted communication.



- Focus was mainly on testing basic connectivity from PC-A to PC-C.
- No security or VPN components were implemented at this stage.

## 2. Final Design:

- **Security Package Enabled:** The design was enhanced by enabling the securityk9 package on R1 and R3 to support cryptographic features in Packet Tracer.
- **ISAKMP Phase 1:** Policies were added for Phase 1 negotiation, including AES 256 encryption, SHA-1 hashing, and DH Group 5 key exchange.
- **IPsec Phase 2:** A transform-set (VPN-SET) was created to define encryption/authentication for the actual data traffic.
- **Crypto Maps:** Crypto maps were introduced and applied to serial interfaces, binding IPsec settings to real traffic.
- **Access Control Lists:** ACL 110 was configured to define “interesting traffic” to trigger the VPN tunnel only between the two target LANs.

## Why the Design Changed:

- **Security Needs:** The initial model did not address encryption or security. To meet project objectives, IPsec had to be introduced.
- **Packet Tracer Limitations:** Certain advanced cryptographic methods (like DH Group 14 or SHA-256) are not supported in Packet Tracer. The design was adapted to use the highest supported options (e.g., DH Group 5).
- **Operational Clarity:** Intermediate testing revealed the importance of clearly separating interesting and non-interesting traffic. ACL adjustments and careful crypto map bindings were necessary for proper VPN operation.

- **Debugging and Testing:** Minor tweaks (e.g., reordering commands or checking ISAKMP key addresses) were made after testing, to ensure tunnel formation and data encryption occurred as expected.

## 6. Implementation

Configuring and Verifying a Site-to-Site IPsec VPN using CLI , we collaborated to configure and verify a site-to-site IPsec VPN between R1 and R3. Our goal was to establish a secure connection for transmitting sensitive information between the LANs of these routers through an unprotected network. Below, we document our process and the specific steps taken.

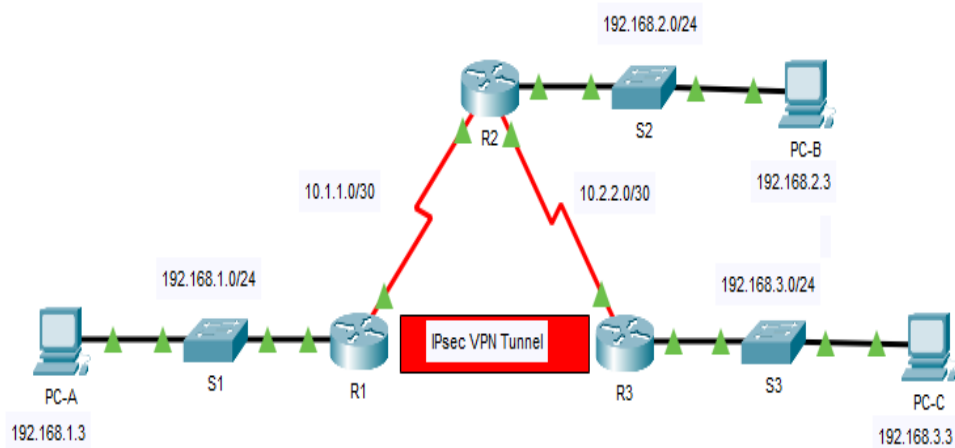


Figure 4-IPSec VPN Tunnel

### Addressing Table:

| Device | Interface | IP Address  | Subnet Mask     | Default Gateway | Switch Port |
|--------|-----------|-------------|-----------------|-----------------|-------------|
| R1     | G0/0      | 192.168.1.1 | 255.255.255.0   | N/A             | S1 F0/1     |
|        | S0/0/0    |             |                 |                 | N/A         |
| R1     | (DCE)     | 10.1.1.2    | 255.255.255.252 | N/A             |             |
| R2     | G0/0      | 192.168.2.1 | 255.255.255.0   | N/A             | S2 F0/2     |
| R2     | S0/0/0    | 10.1.1.1    | 255.255.255.252 | N/A             | N/A         |
|        | S0/0/1    |             |                 |                 | N/A         |
| R2     | (DCE)     | 10.2.2.1    | 255.255.255.252 | N/A             |             |
| R3     | G0/0      | 192.168.3.1 | 255.255.255.0   | N/A             | S3 F0/5     |
| R3     | S0/0/1    | 10.2.2.2    | 255.255.255.252 | N/A             | N/A         |
| PC-A   | NIC       | 192.168.1.3 | 255.255.255.0   | 192.168.1.1     | S1 F0/2     |
| PC-B   | NIC       | 192.168.2.3 | 255.255.255.0   | 192.168.2.1     | S2 F0/1     |
| PC-C   | NIC       | 192.168.3.3 | 255.255.255.0   | 192.168.3.1     | S3 F0/18    |

*Table 1-Addressing Table*

### Objectives

- Verify connectivity throughout the network.
- Configure R1 to support a site-to-site IPsec VPN with R3.

### Network Scenario

## **Internet Key Exchange**

A mechanism called Internet Key Exchange (IKE) is used to safely create and maintain encryption keys for virtual private networks (VPNs), especially in IPSec communications. By confirming both parties' identities and deciding on encryption algorithms to protect the data flow, IKE guarantees secure key exchange. In order to negotiate encryption keys and create a secure communication channel, it works in two stages.

**ISAKMP Policy (Phase 1):** In Phase 1, a secure, authenticated communication channel is established between the two parties using the Internet Security Association and Key Management Protocol (ISAKMP) policy. It specifies the specifications for the secure connection, including hash functions, encryption algorithms, and key exchange techniques. Establishing a secure tunnel for additional communication and authenticating the peers are the objectives.

**Phase 2:** The Transform-Set specifies the precise authentication and encryption techniques that will be applied to protect the actual data transit. In order to ensure that all parties use the same settings for data encryption and integrity, this phase negotiates the security parameters, including the hashing methods (like SHA) and encryption techniques (like AES).

### **The topology consists of three routers:**

- R1 and R3 serve as VPN endpoints.
- R2 acts as a pass-through device and does not participate in the VPN.

By implementing IPSec, we ensured secure communication at the network layer while protecting and authenticating IP packets between the peer routers.

## ISAKMP Phase 1 Policy Parameters

| Parameters                     | Parameter Options and Defaults | R1            | R3            |
|--------------------------------|--------------------------------|---------------|---------------|
| <b>Key Distribution Method</b> | Manual or <b>ISAKMP</b>        | <b>ISAKMP</b> | <b>ISAKMP</b> |
| <b>Encryption Algorithm</b>    | <b>DES</b> , 3DES, or AES      | AES 256       | AES 256       |
| <b>Hash Algorithm</b>          | MD5 or <b>SHA-1</b>            | <b>SHA-1</b>  | <b>SHA-1</b>  |
| <b>Authentication Method</b>   | Pre-shared keys or <b>RSA</b>  | pre-share     | pre-share     |
| <b>Key Exchange</b>            | DH Group 1, 2, or 5            | DH 5          | DH 5          |
| <b>IKE SA Lifetime</b>         | 86400 seconds or less          | <b>86400</b>  | <b>86400</b>  |
| <b>ISAKMP Key</b>              | Provided by user.              | vpnpa55       | vpnpa55       |

*Table 2-ISAKMP Phase 1*

**Note:** Bolded parameters are defaults. Only unbolded parameters must be explicitly configured.

### IPsec Phase 2 Policy Parameters

| Parameters                          | R1  | R3  |
|-------------------------------------|---|---|
| <b>Transform Set Name</b>           | VPN-SET   | VPN-SET   |
| <b>ESP Transform Encryption</b>     | esp-aes   | esp-aes   |
| <b>ESP Transform Authentication</b> | esp-sha-hmac  | esp-sha-hmac  |
| <b>Peer IP Address</b>              | 10.2.2.2  | 10.1.1.2  |
| <b>Traffic to be Encrypted</b>      | access-list 110 (source 192.168.1.0 dest 192.168.3.0) | access-list 110 (source 192.168.3.0 dest 192.168.1.0) |
| <b>Crypto Map Name</b>              | VPN-MAP   | VPN-MAP   |
| <b>SA Establishment</b>             | ipsec-isakmp  | ipsec-isakmp  |

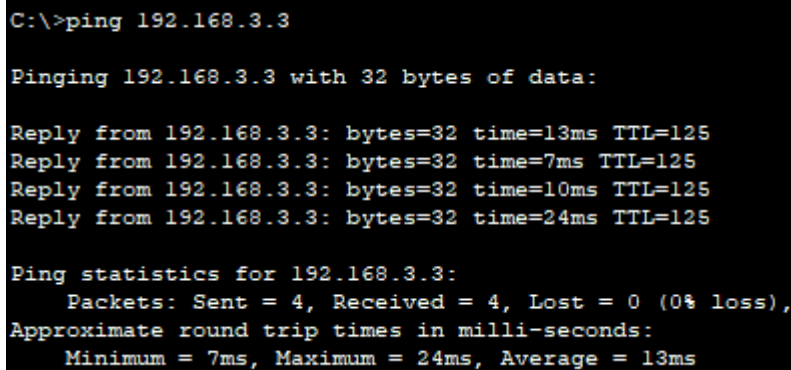
*Table 3-IPsec Phase 2*

## Instructions

### Part 1: Configure IPsec Parameters on R1

#### Step 1: Test connectivity.

We confirmed network reachability by pinging PC-C from PC-A.



```
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=13ms TTL=125
Reply from 192.168.3.3: bytes=32 time=7ms TTL=125
Reply from 192.168.3.3: bytes=32 time=10ms TTL=125
Reply from 192.168.3.3: bytes=32 time=24ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 24ms, Average = 13ms
```

*Figure 5 ping Instruction*

#### Step 2: Enable the Security Technology package.

- a. Executed the following command on R1:

```
R1(config)# license boot module c1900 technology-  
package securityk9
```

Accepted the end-user license agreement.

- b. Saved the running configuration and reloaded the router.  
c. Verified installation using:

```
R1# show version
```

#### Step 3: Identify interesting traffic on R1.

Configured ACL 110 to identify the traffic from the LAN on R1 to the LAN on R3 as interesting. This interesting traffic will trigger the IPsec VPN to be implemented when there is traffic between the R1 to R3 LANs. All other traffic sourced from the LANs will not be encrypted. Because of the implicit **deny all**, there is no need to configure a **deny Ip any** statement.

```
R1(config)# access-list 110 permit ip 192.168.1.0
0.0.0.255 192.168.3.0 0.0.0.255
```

#### **Step 4: Configure the IKE Phase 1 ISAKMP policy on R1.**

Configured the **crypto ISAKMP policy 10** properties on R1 along with the shared crypto key **vpnpa55**. Referring to the ISAKMP Phase 1 table for the specific parameters to configure. Default values do not have to be configured. Therefore, only the encryption method, key exchange method, and DH method must be configured.

**Note:** The highest DH group currently supported by Packet Tracer is group 5. In a production network, we would configure at least DH 14.

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 5
R1(config-isakmp)# exit
R1(config)# crypto isakmp key vpnpa55 address
10.2.2.2
```

#### **Step 5: Configure the IKE Phase 2 IPsec policy on R1.**

- a. Created the transform-set VPN-SET to use **esp-aes** and **esp-sha-hmac**.

```
R1(config)# crypto ipsec transform-set VPN-SET esp-
aes esp-sha-hmac
```

- b. Created and configured the crypto map VPN-MAP that binds all the Phase 2 parameters together. Using sequence number 10 and identifying it as an ipsec-isakmp map.

```
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
```



```
R1(config-crypto-map)# description VPN connection to
R3

R1(config-crypto-map)# set peer 10.2.2.2

R1(config-crypto-map)# set transform-set VPN-SET

R1(config-crypto-map)# match address 110

R1(config-crypto-map)# exit
```

### **Step 6: Configure the crypto map on the outgoing interface.**

Applied the **VPN-MAP** crypto map to the outgoing Serial 0/0/0 interface.

```
R1(config)# interface s0/0/0

R1(config-if) # crypto map VPN-MAP
```

## **Part 2: Configure IPsec Parameters on R3**

### **Step 1: Enable the Security Technology package.**

Verified package installation on R3 with:

```
R3# show version
```

Enabled it if necessary and reloaded R3.

### **Step 2: Configure router R3 to support a site-to-site VPN with R1.**

Configured reciprocating parameters on R3. Configured ACL 110 to identify the traffic from the LAN on R3 to the LAN on R1 as interesting.

```
R3(config)# access-list 110 permit ip 192.168.3.0
0.0.0.255 192.168.1.0 0.0.0.255
```

### **Step 3: Configure the IKE Phase 1 ISAKMP properties on R3.**

Configured the crypto ISAKMP policy 10 properties on R3 along with the shared crypto key **vpnpa55**.

```
R3(config)# crypto isakmp policy 10

R3(config-isakmp)# encryption aes 256

R3(config-isakmp)# authentication pre-share
```

```
R3(config-isakmp)# group 5
R3(config-isakmp)# exit
```

Defined the pre-shared key:

```
R3(config)# crypto isakmp key vpnpa55 address
10.1.1.2
```

#### **Step 4: Configure the IKE Phase 2 IPsec policy on R3.**

- a. Created the transform-set VPN-SET to use **esp-aes** and **esp-sha-hmac**.

```
R3(config)# crypto ipsec transform-set VPN-SET esp-
aes esp-sha-hmac
```

- b. Created and configured the crypto map VPN-MAP to bind all the Phase 2 parameters together. Using sequence number 10 and identify it as an ipsec-isakmp map.

```
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)# description VPN connection to
R1
R3(config-crypto-map)# set peer 10.1.1.2
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit
```

#### **Step 5: Configure the crypto map on the outgoing interface.**

Applied the VPN-MAP crypto map to the outgoing Serial 0/0/1 interface.

```
R3(config)# interface s0/0/1
R3(config-if)# crypto map VPN-MAP
```

### Part 3: Verify the IPsec VPN

#### Step 1: Verify the tunnel prior to interesting traffic.

Checked the initial IPsec statistics:

```
R1# show crypto ipsec sa
```

#### Step 2: Create interesting traffic.

Initiated traffic by pinging PC-C from PC-A.

#### Step 3: Verify the tunnel after interesting traffic.

Re-ran:

```
R1# show crypto ipsec sa
```

Observed packet counts increasing, indicating a working VPN.

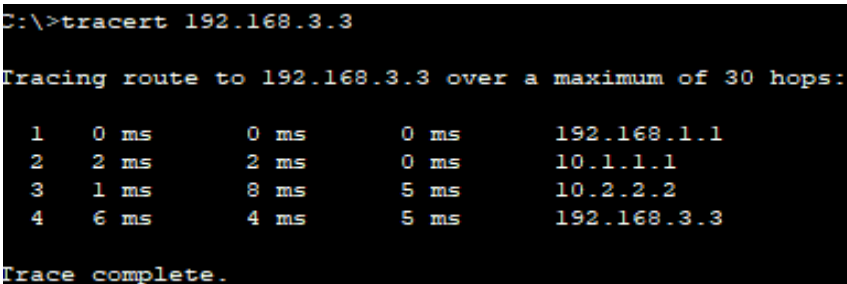
#### Step 4: Create uninteresting traffic.

Pinging PC-B from PC-A did not trigger encryption.

#### Step 5: Verify the tunnel.

Confirmed that uninteresting traffic was not encrypted by checking:

```
R1# show crypto ipsec sa
```



```
C:\>tracert 192.168.3.3

Tracing route to 192.168.3.3 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms   192.168.1.1
  1  2 ms    2 ms    0 ms   10.1.1.1
  2  1 ms    8 ms    5 ms   10.2.2.2
  3  6 ms    4 ms    5 ms   192.168.3.3

Trace complete.
```

*Figure 6-Tracert Path*

## 7. Testing, Analysis, and Evaluation

### Testing Methodology and Results

To determine whether the VPN tunnel was operational and met all requirements, we conducted the following tests:

#### 1. Connectivity Testing (Before VPN Setup):

- A basic ping test was performed from **PC-A (192.168.1.3)** to **PC-C (192.168.3.3)**.
- This confirmed that physical and logical connectivity existed across the network via R2, but **no security was applied yet**.

## 2. VPN Tunnel Activation via Interesting Traffic:

- An **Access Control List (ACL 110)** was created on both R1 and R3 to define the "interesting" traffic (i.e., traffic that should be encrypted between LANs).
- After VPN configuration, another ping from PC-A to PC-C was performed. This traffic successfully triggered the creation of the IPsec tunnel.

## 3. VPN Tunnel Verification:

- The command `show crypto ipsec` was issued before and after the ping to check:
  - **Packet encryption/decryption counters.**
  - **Tunnel status and security associations.**
- After initiating the ping, we observed that **packet counters increased**, confirming that data was encrypted, tunneled, and successfully decrypted.

## 4. Testing for Uninteresting Traffic:

- A ping from **PC-A to PC-B (192.168.2.3)** was performed to ensure this traffic was **not encrypted** by the tunnel.
- The tunnel counters remained unchanged, confirming the **ACL effectively filtered traffic** and VPN applied only to defined subnets.

## System Analysis and Evaluation

To evaluate the system, we focused on the following attributes:

| Attribute   | Evaluation Method  | Result  |
|-------------|--|---|
| Performance | Measured responsiveness and success of ping tests through the tunnel | Low latency observed, indicating efficient packet handling                    |
| Security    | Verified encryption using show crypto isakmp and show crypto ipsec   | AES-256 and SHA-1 confirmed as active, ensuring confidentiality and integrity |
| Reliability | Repeated ping tests over time  | Tunnel consistently rebuilt when triggered by interesting traffic             |
| Efficiency  | Analyzed CPU and memory usage during operation (in Packet Tracer)    | Minimal resource impact, confirming lightweight implementation                |

*Table 4-System Analysis and Evaluation*

## 8. Issues

### Engineering Tools and Standards

**Issue:** The project faced challenges in selecting appropriate engineering tools and ensuring compliance with relevant standards for implementing the IPsec solution.

#### Attempted Resolutions:

1. **Tool Evaluation:** The team initially evaluated several tools for VPN setup, including both commercial and open-source software. This process was time-consuming and led to confusion regarding the best options for our specific requirements.

2. **Standard Compliance:** Ensuring that the chosen tools complied with industry standards (e.g., AES for encryption, IKEv2 for key exchange) was a significant hurdle, as not all tools met these standards seamlessly.

#### **Final Resolution:**

- **Phase 1 (ISAKMP/IKE Policy Setup):**  
Created a secure authenticated channel using **AES-256 encryption**, **SHA-1 hashing**, **Diffie-Hellman Group 5** for key exchange, and **pre-shared keys**.
- **Phase 2 (IPsec Policy Setup):**  
Configured a **transform set** combining **ESP-AES** (encryption) and **ESP-SHA-HMAC** (authentication) for protecting the data payload.
- **ACL Configuration:**  
Defined **interesting traffic** (between 192.168.1.0/24 and 192.168.3.0/24) to trigger VPN tunnel establishment only when necessary, optimizing performance and security.
- **Crypto Map Application:**  
Bound the VPN policies to the routers' serial interfaces, ensuring that all relevant traffic was encrypted automatically.
- **Testing and Verification:**  
Conducted controlled tests (ping, traceroute, show crypto ipsec sa) to verify that the tunnel was:  
  
Properly **initiated** by interesting traffic.
- **Encrypting and decrypting** packets correctly.  
Not affecting unrelated (uninteresting) traffic.

## 9. Engineering Tools and Standards

Engineering Tools refer to the software and hardware applications used in the design, implementation, and maintenance of engineering projects. In the context of implementing an IPsec solution, these tools are essential for ensuring secure communication and effective network management. Key categories include:

1. **Network Management Tools:** Software that monitors network performance, traffic, and security. Tools like Wireshark can be used for packet analysis to troubleshoot issues.
2. **Testing Tools:** Applications like Packet Tracer allow for the simulation of network conditions and the testing of VPN performance, enabling users to visualize and analyze network configurations.

Standards are established guidelines and protocols that ensure consistency, security, and interoperability among different systems and tools. In the context of IPsec implementation, important standards include:

1. **Encryption Standards:** Protocols like AES (Advanced Encryption Standard) define how data should be encrypted to protect it from unauthorized access.
2. **Authentication Standards:** Protocols such as IKEv2 (Internet Key Exchange version 2) specify how secure keys are exchanged between parties to establish a secure connection.

3. **Network Protocol Standards:** Standards such as IPsec itself dictate how data packets are secured during transmission, ensuring confidentiality and integrity.
4. **Compliance Standards:** Regulations like GDPR or HIPAA may dictate specific security measures that must be implemented to protect sensitive data.

By utilizing the right engineering tools and adhering to established standards, organizations can effectively implement secure IPsec solutions that safeguard their **communications against cyber threats. This approach not only enhances security but also promotes trust and reliability in network operations.**

## 10. Teamwork

| Week1 |                     |       |   |         |
|-------|---------------------|-------|---|---------|
| No    | Member              | Tasks | Status<br>(finished, late, not started) | Remarks |
| 1     | Yazan Fahad         | -     | not started                             | -       |
| 2     | Mohammed Alharbi    | -     | not started                             | -       |
| 3     | Bandar Almutairi    | -     | not started                             | -       |
| 4     | Meshal Mohammed     | -     | not started                             | -       |
| 5     | Hatem Alhamar       | -     | not started                             | -       |
| 6     | Abdulaziz aldughaim | -     | not started                             | -       |



*Table 5-Teamwork(Week1)*

| Week2 |                     |   |   |  |
|-------|---------------------|---|---|--|
| No    | Member              | Tasks   | Status<br>(finished, late, not started) | Remarks  |
| 1     | Yazan Fahad         | Take attention to all the tools and provide us with a report on them. | finished                                | Finding the necessary equipment to begin the endeavor was first challenging. |
| 2     | Mohammed Alharbi    | How packet tracers can be used  | finished                                | -  |
| 3     | Bandar Almutairi    | Learn about the Isakmp policies.                                      | finished                                | -  |
| 4     | Meshal Mohammed     | Learn about protocols such as AES-256.                                | finished                                | -  |
| 5     | Hatem Alhamar       | Utilizing Packet-Tracker  | finished                                | -  |
| 6     | Abdulaziz aldughaim | Additional research on the Ipsec                                      | finished                                | -  |

*Table 6-Teamwork(Week2)*

| Week3 |                     |  |   |         |
|-------|---------------------|--|---|---------|
| No    | Member              | Tasks  | Status<br>(finished, late, not started) | Remarks |
| 1     | Yazan Fahad         | Research and select IPSec protocols and algorithms.  | finished                                | -       |
| 2     | Mohammed Alharbi    | Design logging and monitoring modules.               | finished                                | -       |
| 3     | Bandar Almutairi    | Conduct testing for end- to-end secure communication | finished                                | -       |
| 4     | Meshal Mohammed     | Implement encryption and authentication algorithms.  | finished                                | -       |
| 5     | Hatem Alhamar       | Set up and configure the VPN server .                | finished                                | -       |
| 6     | Abdulaziz aldughaim | Develop VPN client software for secure connections   | finished                                | -       |

*Table 7-Teamwork(Week3)*

| Week4 |                     |  |   |         |
|-------|---------------------|--|---|---------|
| No    | Member              | Tasks  | Status<br>(finished, late, not started) | Remarks |
| 1     | Yazan Fahad         | Design and implement a connection status dashboard for the VPN | finished                                | -       |
| 2     | Mohammed Alharbi    | Develop interface for secure admin access and settings control | finished                                | -       |
| 3     | Bandar Almutairi    | Configure and test firewall rules for VPN traffic filtering    | finished                                | -       |
| 4     | Meshal Mohammed     | Implement and verify logging API endpoints                     | finished                                | -       |
| 5     | Hatem Alhamar       | Create automated scripts for VPN setup and deployment          | finished                                | -       |
| 6     | Abdulaziz aldughaim | Perform initial functional testing of encryption and tunneling | finished                                | -       |

*Table 8-Teamwork(Week4)*

| Week5 |                     |  |   |         |
|-------|---------------------|--|---|---------|
| No    | Member              | Tasks  | Status<br>(finished, late, not started) | Remarks |
| 1     | Yazan Fahad         | Simulate Man-in-the-Middle in Packet tracer        | finished                                | -       |
| 2     | Mohammed Alharbi    | Integrate VPN with Dynamic Routing Protocols       | finished                                | -       |
| 3     | Bandar Almutairi    | Generate and Analyze VPN Usage Reports             | finished                                | -       |
| 4     | Meshal Mohammed     | Create Visual Network Diagrams with VPN Paths      | finished                                | -       |
| 5     | Hatem Alhamar       | Document Configuration Changes and Version Control | finished                                | -       |
| 6     | Abdulaziz aldughaim | Develop VPN Usage Policy for Organization          | finished                                | -       |

*Table 9-Teamwork(Week5)*

| Week6 |                     |       |   |         |
|-------|---------------------|-------|---|---------|
| No    | Member              | Tasks | Status<br>(finished, late, not started) | Remarks |
| 1     | Yazan Fahad         | -     | Take off                                | -       |
| 2     | Mohammed Alharbi    | -     | Take off                                | -       |
| 3     | Bandar Almutairi    | -     | Take off                                | -       |
| 4     | Meshal Mohammed     | -     | Take off                                | -       |
| 5     | Hatem Alhamar       | -     | Take off                                | -       |
| 6     | Abdulaziz aldughaim | -     | Take off                                | -       |

*Table 10-Teamwork(Week6)*

| Week7 |                     |       |   |         |
|-------|---------------------|-------|---|---------|
| No    | Member              | Tasks | Status<br>(finished, late, not started) | Remarks |
| 1     | Yazan Fahad         | -     | Take off                                | -       |
| 2     | Mohammed Alharbi    | -     | Take off                                | -       |
| 3     | Bandar Almutairi    | -     | Take off                                | -       |
| 4     | Meshal Mohammed     | -     | Take off                                | -       |
| 5     | Hatem Alhamar       | -     | Take off                                | -       |
| 6     | Abdulaziz aldughaim | -     | Take off                                | -       |

*Table 11-Teamwork(Week7)*

| Week8 |                     |   |   |         |
|-------|---------------------|---|---|---------|
| No    | Member              | Tasks   | Status<br>(finished, late, not started) | Remarks |
| 1     | Yazan Fahad         | Conduct penetration testing on the VPN tunnel (try to exploit weak points). | finished                                | -       |
| 2     | Mohammed Alharbi    | Configure VPN redundancy and backup tunnels.                                | finished                                | -       |
| 3     | Bandar Almutairi    | Configure VPN redundancy and backup tunnels.                                | finished                                | -       |
| 4     | Meshal Mohammed     | Audit and improve encryption protocols.                                     | finished                                | -       |
| 5     | Hatem Alhamar       | Implement access control lists (ACLs) to restrict VPN traffic.              | finished                                | -       |
| 6     | Abdulaziz aldughaim | Implement access control lists (ACLs) to restrict VPN traffic.              | finished                                | -       |

*Table 12-Teamwork(Week8)*

| Week9 |                     |   |   |         |
|-------|---------------------|---|---|---------|
| No    | Member              | Tasks   | Status<br>(finished, late, not started) | Remarks |
| 1     | Yazan Fahad         | Test the IPsec by use packet tracer   | finished                                | -       |
| 2     | Mohammed Alharbi    | Finalize a performance report (latency, uptime, throughput).                  | finished                                | -       |
| 3     | Bandar Almutairi    | Prepare a project demo (live or recorded walkthrough using Packet Tracer).    | finished                                | -       |
| 4     | Meshal Mohammed     | Create a professional final network diagram with VPN and IPsec layers shown.. | finished                                | -       |
| 5     | Hatem Alhamar       | Implement access control lists (ACLs) to restrict VPN traffic.                | finished                                | -       |
| 6     | Abdulaziz aldughaim | Finalize a performance report (latency, uptime, throughput).                  | finished                                | -       |

Table 13-Teamwork(Week9)



| Week10 |                     |                           |   |         |
|--------|---------------------|---------------------------|---|---------|
| No     | Member              | Tasks                     | Status<br>(finished, late, not started) | Remarks |
| 1      | Yazan Fahad         | Prepare a project Report  | finished                                | -       |
| 2      | Mohammed Alharbi    | Prepare a project Report  | finished                                | -       |
| 3      | Bandar Almutairi    | Prepare a project Report. | finished                                | -       |
| 4      | Meshal Mohammed     | Prepare a project Report  | finished                                | -       |
| 5      | Hatem Alhamar       | Prepare a project Report  | finished                                | -       |
| 6      | Abdulaziz aldughaim | Prepare a project Report  | finished                                | -       |

Table 14-Teamwork(Week10)

| Week11 |                     |   |   |         |
|--------|---------------------|---|---|---------|
| No     | Member              | Tasks   | Status<br>(finished, late, not started) | Remarks |
| 1      | Yazan Fahad         | Prepare a PowerPoint presentation summarizing the project from start to finish. | finished                                | -       |
| 2      | Mohammed Alharbi    | Prepare a PowerPoint presentation summarizing the project from start to finish. | finished                                | -       |
| 3      | Bandar Almutairi    | Prepare a PowerPoint presentation summarizing the project from start to finish. | finished                                | -       |
| 4      | Meshal Mohammed     | Prepare a PowerPoint presentation summarizing the project from start to finish. | finished                                | -       |
| 5      | Hatem Alhamar       | Prepare a PowerPoint presentation summarizing the project from start to finish. | finished                                | -       |
| 6      | Abdulaziz aldughaim | Prepare a PowerPoint presentation summarizing the project from start to finish. | finished                                | -       |

Table 15-Teamwork(Week11)

## **11. Conclusions**

We gained a comprehensive understanding of how IPsec VPNs function to provide secure communication over untrusted networks like the internet. We learned how to:

- Configure a secure tunnel using Cisco CLI.
- Set up both Phase 1 (ISAKMP) and Phase 2 (IPsec) policies.
- Identify and encrypt only “interesting traffic” using access control lists.
- Troubleshoot and verify tunnel status using various show commands.

What would you do differently in a similar project?

If given the chance to redo or extend this project, we would:

- Add real-time monitoring tools to track tunnel performance and security in real-time.
- Simulate external threats or attacks to test the robustness of the VPN tunnel.

### **Personal result**

This project provided valuable real-world insight into secure network design. It highlighted how crucial encryption, authentication, and policy enforcement are in maintaining data integrity and privacy. We also realized the importance of proper planning, documentation, and testing in deploying network security solutions. Overall, it reinforced the need for strong cybersecurity practices and gave us confidence in handling similar challenges in professional environments.