

**Name Muhammad Shoaib**

**Roll no 279**

**Section 5D**

**Submitted to: Rasikh Ali**

### 

### 

### 

### 

### 

### 

### 

### 

**Site-to-Site VPN Configuration Using Cisco Packet Tracer**

## ****Introduction****

Virtual Private Networks (VPNs) are essential in today's interconnected world for securing data across untrusted networks such as the internet. A Site-to-Site VPN is a type of VPN that enables two remote networks to communicate securely as if they were part of a single network. This project utilizes **Cisco Packet Tracer**, a simulation tool, to demonstrate the practical implementation of Site-to-Site VPNs.

### ****What is a VPN?****

A Virtual Private Network (VPN) is a technology that creates an encrypted connection between two or more devices over a public network. VPNs ensure confidentiality, integrity, and authentication of the data transmitted.

### ****What is a Site-to-Site VPN?****

Unlike remote-access VPNs that connect individual users to a network, Site-to-Site VPNs link entire networks. It is commonly used in enterprises to connect branch offices to the central office over the internet securely.

### ****Importance of the Project****

* Simulating a real-world scenario to enhance security understanding.
* Learning how to configure and troubleshoot a Site-to-Site VPN.
* Understanding cryptographic protocols such as IPsec and IKE.

## ****Objectives****

* To configure a secure VPN tunnel between two remote networks.
* To simulate and verify encrypted data transmission.
* To learn the practical application of VPN protocols and technologies.

## ****Network Diagram****

A well-designed network diagram is critical for understanding the topology and ensuring accuracy during configuration. The topology includes:

1. **Routers**: Two routers acting as VPN gateways.
2. **Switches**: Connecting endpoints within each network.
3. **PCs**: Representing end-users in the two networks.

**Include a detailed diagram of the network topology. Use labeled subnets, interfaces, and devices for clarity.**

## ****Requirements****

### ****Hardware and Software****

* **Cisco Packet Tracer** version 8.0 or later.
* Two routers: Cisco 2911 or similar.
* Two switches: Cisco 2960 or equivalent.
* Four PCs for testing (two per network).

### ****IP Addressing Scheme****

* Network 1: 192.168.1.0/24
* Network 2: 192.168.2.0/24
* WAN Network: 10.0.0.0/30

### ****VPN Protocols****

* **IPsec (Internet Protocol Security)**: Ensures data integrity and confidentiality.
* **IKE (Internet Key Exchange)**: Handles authentication and key exchange.

## ****Theoretical Background****

### ****Overview of IPsec****

IPsec is a suite of protocols designed to secure IP communications. It operates in two modes:

1. **Transport Mode**: Encrypts only the payload of the packet.
2. **Tunnel Mode**: Encrypts the entire packet, commonly used in Site-to-Site VPNs.

### ****How IPsec Works****

1. **Phase 1 (IKE Phase 1)**: Establishes a secure channel between VPN endpoints.
2. **Phase 2 (IKE Phase 2)**: Negotiates IPsec parameters and establishes the tunnel.

## ****Step-by-Step Configuration****

### ****Basic Network Setup****

1. Assign IP addresses to router interfaces.
2. Configure static routes to enable connectivity between subnets.

#### ****Router Configuration Example****

Configure IP addresses:

interface gigabitethernet0/0

ip address 192.168.1.1 255.255.255.0

no shutdown

**Set up static routes:**

**ip route 192.168.2.0 255.255.255.0 10.0.0.2**

### ****Enabling ISAKMP****

Create an ISAKMP policy:

crypto isakmp policy 10

encr aes

hash sha256

authentication pre-share

group 2

lifetime 86400

**Configure a re-shared key:**

**crypto isakmp key MY\_SECRET\_KEY address 10.0.0.2**

**Configuring IPsec**

crypto ipsec transform-set MY\_TRANSFORM\_SET esp-aes esp-sha-hmac

**Create an access control list (ACL**

**access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255**

**Configure a crypto map:**

crypto map MY\_CRYPTO\_MAP 10 ipsec-isakmp

set peer 10.0.0.2

set transform-set MY\_TRANSFORM\_SET

match address 100

**Apply the crypto map to the WAN interface:**

interface gigabitethernet0/1

crypto map MY\_CRYPTO\_MAP

## ****Testing and Verification****

 Use **ping** to test connectivity between end devices.

 Verify VPN tunnel establishment

**Use the command:**

show crypto isakmp sa

**Check IPsec statistics**

Check IPsec statistics

**Observe encrypted traffic in Packet Tracer.**

## ****Troubleshooting and Best Practices****

### ****Common Issues****

1. **VPN Tunnel Not Established**: Verify ISAKMP and IPsec configurations.
2. **Traffic Not Encrypted**: Check ACL definitions.
3. **Ping Fails**: Ensure routing tables are correctly configured.

### ****Debugging Commands****

* debug crypto isakmp
* debug crypto ipsec

## ****Security Considerations****

* Use strong pre-shared keys.
* Regularly update device firmware.
* Monitor VPN connections for unusual activity.

## ****Conclusion****

This project demonstrates the implementation of a secure Site-to-Site VPN using Cisco Packet Tracer. The practical application of IPsec protocols ensures data confidentiality and integrity, emphasizing the importance of VPNs in modern networks.