PW 7: VPN and IPSec Lab Exercise

Dr. Mohamed Amine Ferrag
Guelma University

17/04/2025

Introduction

Virtual Private Networks (VPNs) provide secure connectivity over public or untrusted networks. IPSec is one of the most widely used protocols to create VPN tunnels. In this lab exercise, you will configure a site-to-site IPSec VPN between two Cisco routers using Packet Tracer. This exercise demonstrates how to:

- Configure ISAKMP (Internet Security Association and Key Management Protocol) policies.
- Set up IPSec transform sets.
- Define a crypto map to apply IPSec to router interfaces.
- Verify the IPSec tunnel and security associations.

Example Scenario: Two remote sites need to exchange data securely over the Internet. Router R1 connects the first site with LAN 192.168.1.0/24, while Router R2 connects the second site with LAN 192.168.2.0/24. A secure IPSec VPN tunnel is established over their WAN interfaces (using public IP addresses) to allow encrypted communication between the two LANs.

Objective

- Establish a site-to-site IPSec VPN tunnel between two Cisco routers (R1 and R2).
- Configure ISAKMP policies, pre-shared keys, and transform sets.
- Apply a crypto map to the WAN interfaces.
- Verify that LAN-to-LAN connectivity is achieved through the secure tunnel.

Lab Requirements

- Cisco Packet Tracer with at least two routers.
- Basic familiarity with Cisco IOS commands.
- Understanding of IPSec and VPN concepts.

Topology Overview and IP Addressing

Configure the topology with the following addressing scheme:

- **Router R1:**
  - LAN interface (G0/0): IP `192.168.1.1/24` (LAN 192.168.1.0/24)
  - WAN interface (Serial0/0): Public IP `10.0.0.1/30`
- **Router R2:**
  - LAN interface (G0/0): IP `192.168.2.1/24` (LAN 192.168.2.0/24)
  - WAN interface (Serial0/0): Public IP `10.0.0.2/30`

Connectivity Verification:

- Verify that you can ping between R1's WAN interface (`10.0.0.1`) and R2's WAN interface (`10.0.0.2`).

Lab Execution Steps

Part 1: Configure IPSec VPN on Router R1

1. **Enter Global Configuration Mode:**

```
Router> enable
! Enter privileged EXEC mode
Router# configure terminal
! Enter global configuration mode
```

Listing 1: Access Global Configuration on R1

2. **Configure ISAKMP Policy:**

```
Router(config)# crypto isakmp policy 10
! Create ISAKMP policy with priority 10
Router(config-isakmp)# encr aes
! Set encryption to AES
Router(config-isakmp)# hash sha256
! Set hash algorithm to SHA-256
Router(config-isakmp)# authentication pre-share
! Use pre-shared keys for authentication
Router(config-isakmp)# group 2
! Set Diffie-Hellman group to 2
Router(config-isakmp)# lifetime 86400
! Set lifetime to 86400 seconds (24 hours)
Router(config-isakmp)# exit
! Exit ISAKMP configuration mode
```

Listing 2: Configure ISAKMP Policy on R1

3. **Set the Pre-shared Key:**

```
Router(config)# crypto isakmp key MySecretKey address 10.0.0.2
! Configure pre-shared key "MySecretKey" for peer with IP 10.0.0.2 (R2 WAN)
```

Listing 3: Set Pre-shared Key on R1

4. **Configure IPSec Transform Set:**

```
Router(config)# crypto ipsec transform-set TRANS1 esp-aes esp-sha-hmac
! Create transform set named TRANS1 using AES encryption and SHA for HMAC
```

Listing 4: Configure IPSec Transform Set on R1

5. **Configure the Crypto Map:**

```
Router(config)# crypto map VPNMAP 10 ipsec-isakmp
! Create crypto map "VPNMAP" with sequence number 10
Router(config-crypto-map)# set peer 10.0.0.2
! Specify the remote peer's IP (R2 WAN) as 10.0.0.2
Router(config-crypto-map)# set transform-set TRANS1
! Apply transform set TRANS1 to the crypto map
Router(config-crypto-map)# match address 100
! Use ACL number 100 to define interesting traffic for the VPN
Router(config-crypto-map)# exit
! Exit crypto map configuration
```

Listing 5: Configure Crypto Map on R1

6. **Create an Access List for Interesting Traffic:**

```
Router(config)# access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
! Permit traffic from LAN 192.168.1.0/24 (R1 LAN) to LAN 192.168.2.0/24 (R2 LAN)
```

Listing 6: Access List for VPN on R1

7. **Apply the Crypto Map to the WAN Interface:**

```
Router(config)# interface Serial0/0
! Enter interface configuration for Serial0/0
Router(config-if)# crypto map VPNMAP
! Apply crypto map "VPNMAP" to interface Serial0/0
Router(config-if)# end
! Exit configuration mode
```

Listing 7: Apply Crypto Map on R1 WAN Interface

Part 2: Configure IPSec VPN on Router R2

Repeat similar steps on R2, adjusting IP addresses accordingly:

1. **Access Global Configuration Mode:**

```
Router> enable
! Enter privileged EXEC mode on R2
Router# configure terminal
! Enter global configuration mode on R2
```

Listing 8: Access Global Configuration on R2

2. **Configure ISAKMP Policy:**

```
Router(config)# crypto isakmp policy 10
! Create ISAKMP policy with priority 10 on R2
Router(config-isakmp)# encr aes
! Set encryption to AES
Router(config-isakmp)# hash sha256
! Set hash algorithm to SHA-256
Router(config-isakmp)# authentication pre-share
! Use pre-shared key for authentication
Router(config-isakmp)# group 2
! Set Diffie-Hellman group to 2
Router(config-isakmp)# lifetime 86400
! Set lifetime to 86400 seconds (24 hours)
Router(config-isakmp)# exit
! Exit ISAKMP configuration mode
```

Listing 9: Configure ISAKMP Policy on R2

3. **Set the Pre-shared Key:**

```
Router(config)# crypto isakmp key MySecretKey address 10.0.0.1
! Configure pre-shared key "MySecretKey" for peer with IP 10.0.0.1 (R1 WAN)
```

Listing 10: Set Pre-shared Key on R2

4. **Configure IPSec Transform Set:**

```
Router(config)# crypto ipsec transform-set TRANS1 esp-aes esp-sha-hmac
! Create transform set TRANS1 (same as R1) on R2 using AES and SHA-HMAC
```

Listing 11: Configure IPSec Transform Set on R2

5. **Configure the Crypto Map:**

```
Router(config)# crypto map VPNMAP 10 ipsec-isakmp
! Create crypto map "VPNMAP" with sequence number 10 on R2
Router(config-crypto-map)# set peer 10.0.0.1
! Set peer to 10.0.0.1 (R1's WAN IP)
Router(config-crypto-map)# set transform-set TRANS1
! Apply transform set TRANS1 on R2
Router(config-crypto-map)# match address 100
! Use ACL 100 to define interesting traffic for the VPN on R2
Router(config-crypto-map)# exit
! Exit crypto map configuration mode
```

Listing 12: Configure Crypto Map on R2

6. **Create an Access List for Interesting Traffic:**

```
Router(config)# access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
! Permit traffic from LAN 192.168.2.0/24 (R2 LAN) to LAN 192.168.1.0/24 (R1 LAN)
```

Listing 13: Access List for VPN on R2

7. **Apply the Crypto Map to the WAN Interface:**

```
Router(config)# interface Serial0/0
! Enter interface Serial0/0 configuration on R2
Router(config-if)# crypto map VPNMAP
! Apply crypto map "VPNMAP" to Serial0/0 interface
Router(config-if)# end
! Exit configuration mode
```

Listing 14: Apply Crypto Map on R2 WAN Interface

Part 3: Verification and Testing

1. **Verify WAN Reachability:** On both routers, confirm reachability of the remote WAN interface.

```
Router# ping 10.0.0.2 ! From R1, ping R2's WAN interface
Router# ping 10.0.0.1 ! From R2, ping R1's WAN interface
```

Listing 15: Ping Remote WAN Interface

2. **Verify Security Associations:** Check the status of ISAKMP and IPSec SAs.

```
Router# show crypto isakmp sa ! Display ISAKMP Security Associations
Router# show crypto ipsec sa ! Display IPSec Security Associations
```

Listing 16: Show ISAKMP and IPSec SAs

3. **Test LAN-to-LAN Connectivity:** From a host in LAN 192.168.1.0/24 (behind R1), ping a host in LAN 192.168.2.0/24 (behind R2) to verify that traffic is passing securely through the IPSec tunnel.

Conclusion

In this lab exercise, you have:

1. Configured a site-to-site IPSec VPN between two Cisco routers using Packet Tracer.
2. Established ISAKMP policies, pre-shared keys, IPSec transform sets, and crypto maps.
3. Applied the crypto map to the WAN interfaces.
4. Verified secure LAN-to-LAN connectivity through the IPSec tunnel.

This exercise provides essential hands-on experience with VPN and IPSec configurations, reinforcing the principles of secure communications over public networks.