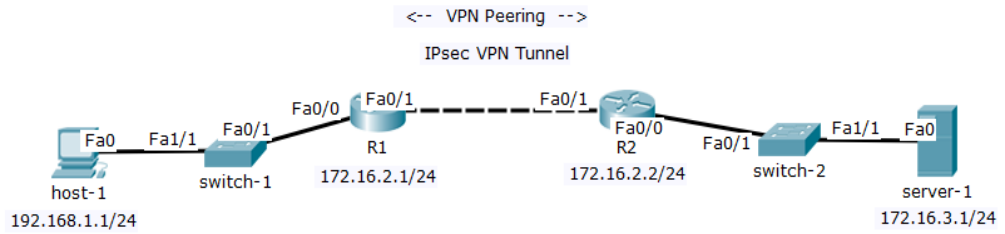
IPsec VPN

Lab Summary

Enable IPsec VPN tunnel between R1 router and R2 router.

Figure 1 Lab Topology



Lab Configuration

Start Packet Tracer File: **IPsec VPN**

R1

Click on the *R1* icon and select the *CLI* folder. Hit the <enter> key for user mode prompt (>).

Step 1: Enter global configuration mode

R1> **enable**
Password: **cisconet**
R1# **configure terminal**

Configure ISAKMP

Step 2: Configure an ISAKMP phase 1 policy

R1(config)# **crypto isakmp policy 1**
R1(config-isakmp)# **encr 3des**
R1(config-isakmp)# **hash md5**
R1(config-isakmp)# **authentication pre-share**
R1(config-isakmp)# **group 2**
R1(config-isakmp)# **lifetime 86400**
R1(config-isakmp)# **exit**

Step 3: Define a pre-shared key for authentication with R2.

R1(config)# **crypto isakmp key cisconet address 172.16.2.2**

Configure IPsec

Step 4: Create extended ACL named **vpn-tunnel** to define interesting traffic permitted across VPN tunnel.

```
R1(config)# ip access-list extended vpn-tunnel
R1(config-ext-nacl)# permit ip 192.168.1.0 0.0.0.255 172.16.3.0 0.0.0.255
R1(config-ext-nacl)# exit
```

Create IPSec Transform (ISAKMP Phase 2)

Step 5: Create IPsec transform set named **ccna** with security parameters.

```
R1(config)# crypto ipsec transform-set ccna esp-3des esp-md5-hmac
```

Step 6: Create crypto map **cisconet** to bind ISAKMP and IPSec policies.

```
R1(config)# crypto map cisconet 10 ipsec-isakmp
R1(config-crypto-map)# set peer 172.16.2.2
R1(config-crypto-map)# set transform-set ccna
R1(config-crypto-map)# match address vpn-tunnel
R1(config-crypto-map)# exit
```

Step 7: Apply crypto map **cisconet** to the public interface Fastethernet 0/1 on R1.

```
R1(config)# interface FastEthernet0/1
R1(config-if)# crypto map cisconet
R1(config-if)# end
R1# copy running-config startup-config
```

Step 8: Disable Network Address Translation across IPsec VPN tunnel.

```
R1(config)# ip nat inside source list 100 interface fa0/1 overload
R1(config)# access-list 100 deny ip 192.168.1.0 0.0.0.255 172.16.3.0
             0.0.0.255
R1(config)# access-list 100 permit ip 192.168.1.0 0.0.0.255 any
```

R2

Click on *R2* icon and select *CLI* folder. Hit <enter> key for user mode prompt (>).

Step 9: Enter global configuration mode

```
R2> enable
Password: cisconet
R2# configure terminal
```

Configure ISAKMP

Step 10: Configure an ISAKMP phase 1 policy

```
R2(config)# crypto isakmp policy 1
R2(config-isakmp)# encr 3des
R2(config-isakmp)# hash md5
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# group 2
R2(config-isakmp)# lifetime 86400
R2(config-isamkp)# exit
```

Step 11: Define a pre-shared key for authentication with R1.

```
R2(config)# crypto isakmp key cisconet address 172.16.2.1
```

Configure IPsec

Step 12: Create extended ACL named **vpn-tunnel** to define interesting traffic permitted across VPN tunnel.

```
R2(config)# ip access-list extended vpn-tunnel
R2(config-nacl)# permit ip 172.16.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R2(config-nacl)# exit
```

Create IPSec Transform (ISAKMP Phase 2)

Step 13: Create IPsec transform set named **ccna** with security parameters.

```
R2(config)# crypto ipsec transform-set ccna esp-3des esp-md5-hmac
```

Step 14: Create crypto map **cisconet** to bind ISAKMP and IPSec policies.

```
R2(config)# crypto map cisconet 10 ipsec-isakmp
R2(config-crypto-map)# set peer 172.16.2.1
R2(config-crypto-map)# set transform-set ccna
R2(config-crypto-map)# match address vpn-tunnel
R2(config-crypto-map)# exit
```

Step 15: Apply crypto map **cisconet** to the public interface Fastethernet 0/1 on R2.

```
R2(config)# interface FastEthernet0/1
R2(config-if)# crypto map cisconet
R2(config-if)# end
R2# copy running-config startup-config
```

Verify Lab:

Ping from host-1 to server-1 and activate VPN tunnel to verify network connectivity.

host-1: c:\> **ping 172.16.3.1**

Pinging 172.16.3.1 with 32 bytes of data:

Reply from 172.16.3.1: bytes=32 time=12ms TTL=126
Reply from 172.16.3.1: bytes=32 time=56ms TTL=126
Reply from 172.16.3.1: bytes=32 time=45ms TTL=126
Reply from 172.16.3.1: bytes=32 time=35ms TTL=126

Ping statistics for 172.16.3.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 12ms, Maximum = 56ms, Average = 37ms

Verify that ISAKMP phase 1 negotiation for the VPN tunnel is working correctly between R1 and R2 peers.

R1# **show crypto isakmp sa**

IPv4 Crypto ISAKMP SA

dst	src	state	conn-id	slot	status
172.16.2.2	172.16.2.1	QM_IDLE	1029	0	**ACTIVE**

IPv6 Crypto ISAKMP SA

Verify that IPsec is working correctly and packets are getting encrypted across the VPN tunnel.

R1# **show crypto ipsec sa**

interface: FastEthernet0/1
Crypto map tag: **cisconet**, local addr 172.16.2.1

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): (**172.16.3.0**/255.255.255.0/0/0)
current_peer **172.16.2.2** port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 0
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 0

#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.: **172.16.2.1**, remote crypto endpt.:**172.16.2.2**
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
current outbound spi: 0x251972B9(622424761)

inbound esp sas:
spi: 0x02776CA1(41381025)
transform: **esp-3des esp-md5-hmac**
in use settings = {**Tunnel**, }
conn id: 2001, flow_id: FPGA:1, **crypto map: cisconet**
sa timing: remaining key lifetime (k/sec): (4525504/3342)
IV size: 16 bytes
replay detection support: N
Status: **ACTIVE**

inbound ah sas:
inbound pcp sas:

outbound esp sas:
spi: 0x251972B9(622424761)
transform: **esp-3des esp-md5-hmac**
in use settings ={**Tunnel**, }
conn id: 2002, flow_id: FPGA:1, **crypto map: cisconet**
sa timing: remaining key lifetime (k/sec): (4525504/3342)
IV size: 16 bytes
replay detection support: N
Status: **ACTIVE**
outbound ah sas:
outbound pcp sas:

Lab Notes:

3DES - encryption method to be used for Phase 1

MD5 - hashing algorithm

Pre-share - Pre-shared key as the authentication method

Group 2 - Diffie-Hellman group to be used

86400 – Session key lifetime