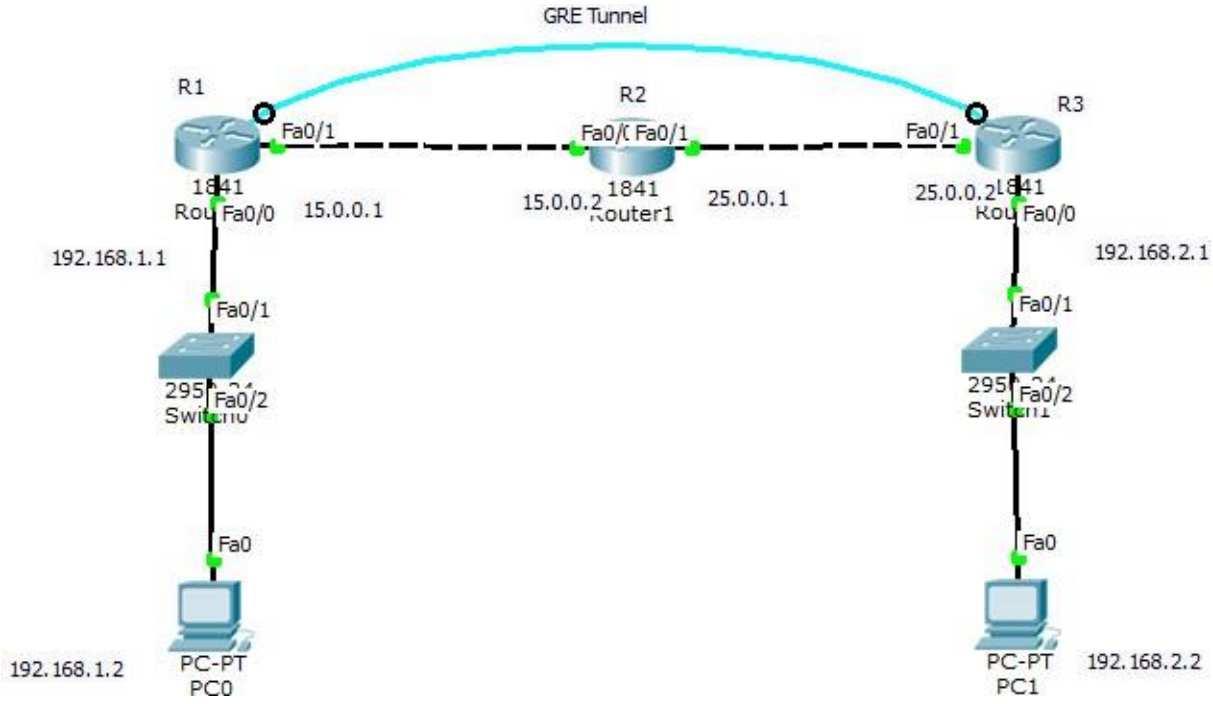
Lab 37

Point-to-Point GRE Tunnels Configuration

Objective:

The main goal of this lab is to configure GRE tunnel between two distant sites, and to allow traffic to pass over it normally

Diagram:



Task 1:

Connect the above diagram, and configure the IP addresses as explained in the figure, and configure a default route on R1 pointed to R2, and in R3 pointed to R2.

!R1

ip route 0.0.0.0 0.0.0.0 fa0/1
!R3

ip route 0.0.0.0 0.0.0.0 fa0/1

Veritifcation:

!R1

show ip route

C 15.0.0.0/8 is directly connected, FastEthernet0/1

C 192.168.1.0/24 is directly connected, FastEthernet0/0

S* 0.0.0.0/0 is directly connected, FastEthernet0/1

Task 2:

Configure R1 & R3 with GRE Tunnel having Interface IP address of 30.0.0.1 and 30.0.0.2.

!R1

```
interface Tunnel0
ip address 30.0.0.1 255.0.0.0
tunnel source FastEthernet0/1
tunnel destination 25.0.0.2
tunnel mode gre ip
!
```

!R3

```
interface Tunnel0
ip address 30.0.0.2 255.0.0.0
tunnel source FastEthernet0/1
tunnel destination 15.0.0.1
tunnel mode gre ip
```

Verification:

!R1

show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.1.1	YES	manual	up	up
FastEthernet0/1	15.0.0.1	YES	manual	up	up
Tunnel0	30.0.0.1	YES	manual	up	up

Task 3:
enable RIP on R1 & R3, and advertise only the LAN networks for every router, and the GRE tunnel network, and ensure the PCs can ping each other normally.
!R1
router rip
version 2
network 192.168.1.0
network 30.0.0.0

!R3
router rip
version 2
network 192.168.2.0
network 30.0.0.0

Verification:
!R1
show ip route
C 15.0.0.0/8 is directly connected, FastEthernet0/1
C 30.0.0.0/8 is directly connected, Tunnel0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
R 192.168.2.0/24 [120/1] via 30.0.0.2, 00:00:03, Tunnel0
S* 0.0.0.0/0 is directly connected, FastEthernet0/1

Ping Between the PCs should be working normally....

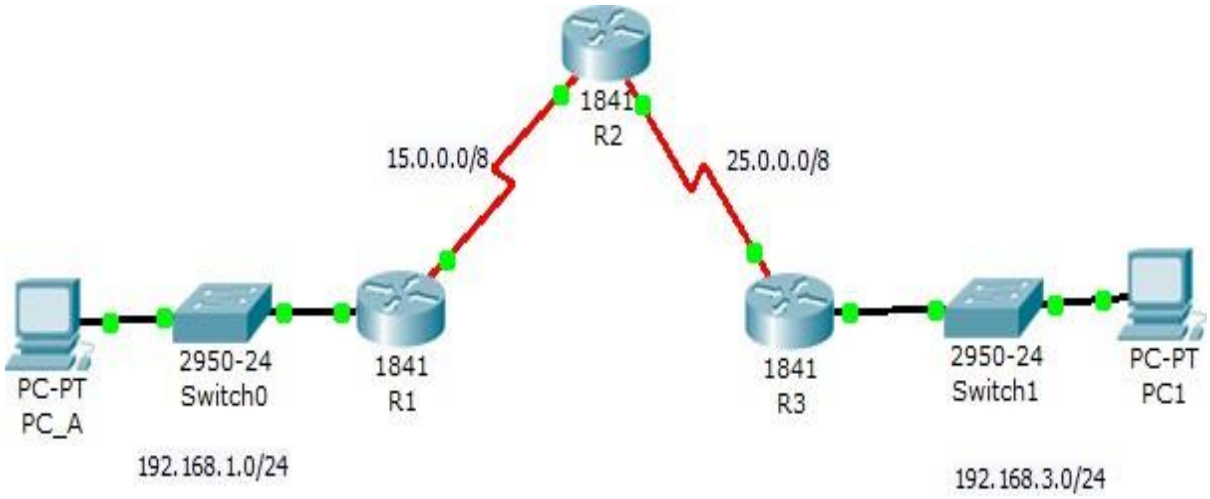
Lab 38

IPSEC SITE-to-SITE VPN Configuration

Objective:

The main goal of this lab is to configure IPSEC tunnel between two distant sites, and to allow traffic to pass over it normally

Diagram:



Task 1:

Connect the network as shown in the above diagram, configure the IP addresses for all routers, and configure a default route on R1 pointed to R2, and in R3 pointed to R2.

!R1

ip route 0.0.0.0 0.0.0.0 S0/1/0

!R3

ip route 0.0.0.0 0.0.0.0 s0/1/0

Task 2

Configure Interesting VPN traffic on R1 & R3, and Then Configure the ISAKMP Parameters and IPSEC Tunnels

!R1

access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

crypto isakmp policy 2

hash md5

authentication pre-share

group 2

life 600

encryption aes 128

exit

crypto isakmp key cisco123 address 25.0.0.3

crypto ipsec transform-set MY-SET esp-aes 256 esp-sha-hmac

crypto map MY-MAP 1 ipsec-isakmp

match address 100

set transform-set MY-SET

set peer 25.0.0.3

int s0/1/0

crypto map MY-MAP

!R3

access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

crypto isakmp policy 2

hash md5

authentication pre-share

group 2

life 600

encryption aes 128

exit

crypto isakmp key cisco123 address 15.0.0.1

crypto ipsec transform-set MY-SET esp-aes 256 esp-sha-hmac

crypto map MY-MAP 1 ipsec-isakmp

match address 100

set transform-set MY-SET

set peer 15.0.0.1

int s0/1/0

crypto map MY-MAP

Verification:

sh crypto ipsec sa

interface: Serial0/1/0

Crypto map tag: MY-MAP, local addr 15.0.0.1

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): (192.168.3.0/255.255.255.0/0/0)

current_peer 25.0.0.3 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0

#pkts decaps: 0, #pkts decrypt: 0, #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 0, #recv errors 0

local crypto endpt.: 15.0.0.1, remote crypto endpt.:25.0.0.3

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0

current outbound spi: 0x0(0)

inbound esp sas:

--More–

Ping between PCs should be working normally.....

Verify the IPSEC tunnel

R1#sh crypto ipsec sa

interface: Serial0/1/0

Crypto map tag: MY-MAP, local addr 15.0.0.1

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): (192.168.3.0/255.255.255.0/0/0)

current_peer 25.0.0.3 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0

#pkts decaps: 6, #pkts decrypt: 6, #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.: 15.0.0.1, remote crypto endpt.:25.0.0.3

path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0

current outbound spi: 0x14E32B46(350432070)

inbound esp sas:

spi: 0x5FED374C(1609381708)

--More–

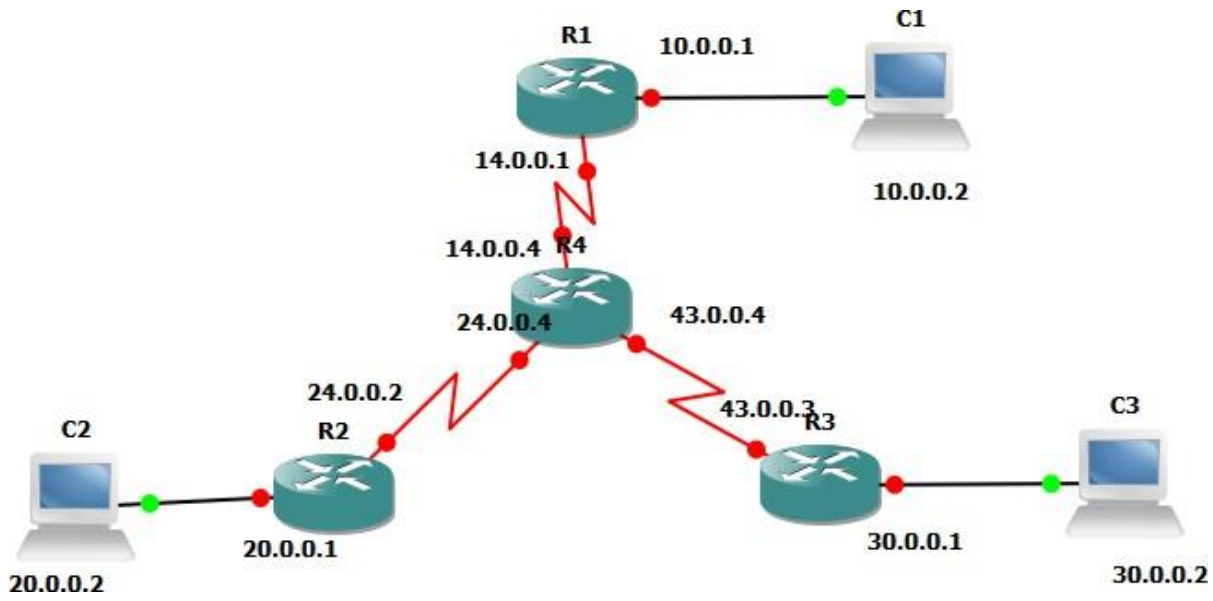
Lab 39

Dynamic Multipoint VPN Configuration

Objective:

The main goal of this lab is to configure DMVPN tunnel between Three distant sites in a HUB and SPOKE topology, and to allow traffic to pass over it normally

Diagram:



Task 1:

Connect the network as shown in the diagram, assign IP addresses as depicted in the figure and configure a default route on R1 (HUB), R2 & R3 (Spokes) pointed to R4 (DMVPN Cloud).

Verification:

Ensure the ping is working normally between the routers....

Task 2

Configure an MGRE Tunnel on every router, setting up R1 as the HUB of the MGRE Tunnel, and NHRP Server (NHS) for the Spokes. Configure the NHRP network id to be 99,NHRP authentication key should be cisco123 and the GRE tunnel key to be 123. Don't Forget to allow multicast traffic to be passed throughout the GRE Tunnel. Tunnel interface IP addresses for R1, R2 & R3 should 123.0.0.1, 123.0.0.2 & 123.0.0.3 respectively.

```
!R1 (HUB)
interface Tunnel0
 ip address 123.0.0.1 255.0.0.0
ip mtu 1412
 ip nhrp authentication cisco123
 ip nhrp map multicast dynamic
 ip nhrp network-id 99
 tunnel source Serial1/0
 tunnel mode gre multipoint
 tunnel key 123
!


!R2 (SPOKE)
interface Tunnel0
 ip address 123.0.0.2 255.0.0.0
ip mtu 1412
```

```
 ip nhrp authentication cisco123
ip nhrp map 123.0.0.1 14.0.0.1
ip nhrp map multicast 14.0.0.1
ip nhrp network-id 99
ip nhrp nhs 123.0.0.1
 tunnel source Serial1/0
 tunnel mode gre multipoint
 tunnel key 123
!

!R3 (SPOKE)
interface Tunnel0
 ip address 123.0.0.3 255.0.0.0
ip mtu 1412
 ip nhrp authentication cisco123
ip nhrp map 123.0.0.1 14.0.0.1
ip nhrp map multicast 14.0.0.1
ip nhrp network-id 99
ip nhrp nhs 123.0.0.1
 tunnel source Serial1/0
 tunnel mode gre multipoint
 tunnel key 123
```

Verification:

!R1

show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	10.0.0.1	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	down
Serial1/0	14.0.0.1	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
SSLVPN-VIF0	unassigned	NO	unset	up	up
Tunnel0	123.0.0.1	YES	manual	up	up

Ping between the tunnel interfaces should be working normally.....

Task 3:

Enable Eigrp 100 on the three routers R1, R2 & R3 and only advertise the Tunnel network and the LAN network for every router. Don't forget to disable the split horizon on the eigrp in tunnel interface.

!R1

router eigrp 100

network 123.0.0.0

```
network 10.0.0.0
!
interface tunnel 0
no ip split-horizon eigrp 100

!R2
router eigrp 100
network 123.0.0.0
network 20.0.0.0
!
interface tunnel 0
no ip split-horizon

!R3
router eigrp 100
network 123.0.0.0
network 30.0.0.0
!
interface tunnel 0
no ip split-horizon
```

Verification:

!R1

show ip route

C 20.0.0.0/8 [90/26882560] via 123.0.0.2, 00:00:40, Tunnel0

C 10.0.0.0/8 is directly connected, FastEthernet0/0

C 123.0.0.0/8 is directly connected, Tunnel0

C 14.0.0.0/8 is directly connected, Serial1/0

D 30.0.0.0/8 [90/26882560] via 123.0.0.3, 00:00:22, Tunnel0

S* 0.0.0.0/0 is directly connected, Serial1/0

ping between the PCs should be working normally.....

Task 4:

Now It is time to protect the tunnel by applying IPSEC on it. Use the suitable hashing, encryption algorithms for both ISAKMP and IPSEC tunnels. Then apply the new profile on the tunnel interface.

!R1/R2/R3

crypto isakmp policy 20

encryption des

hash md5

authentication pre-share

group 2

exit

!

crypto isakmp key hello address 0.0.0.0 0.0.0.0

!

crypto ipsec transform-set MY-SET esp-aes 256 esp-sha-hmac

exit

!

crypto ipsec profile DMVPN

set transform-set MY-SET

!

interface tunnel 0

tunnel protection ipsec profile DMVPN

Verification:

The ping should still be working fine between the PCs.....

However, the tunnel should be protected.

!R1

R1#show crypto ipsec sa

interface: Tunnel0

Crypto map tag: Tunnel0-head-0, local addr 14.0.0.1

protected vrf: (none)

local ident (addr/mask/prot/port): (14.0.0.1/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (24.0.0.2/255.255.255.255/47/0)

current_peer 24.0.0.2 port 500

PERMIT, flags={origin_is_acl,}

#pkts encaps: 38, #pkts encrypt: 38, #pkts digest: 38

#pkts decaps: 38, #pkts decrypt: 38, #pkts verify: 38

#pkts compressed: 0, #pkts decompressed:

0 #pkts not compressed: 0, #pkts compr.

failed: 0

#pkts not decompressed: 0, #pkts decompress

failed: 0 #send errors 6, #recv errors 0

local crypto endpt.: 14.0.0.1, remote crypto endpt.:

24.0.0.2 path mtu 1500, ip mtu 1500, ip mtu idb

Serial1/0

current outbound spi: 0xF7137341(4145247041)

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x4971E78C(1232201612)