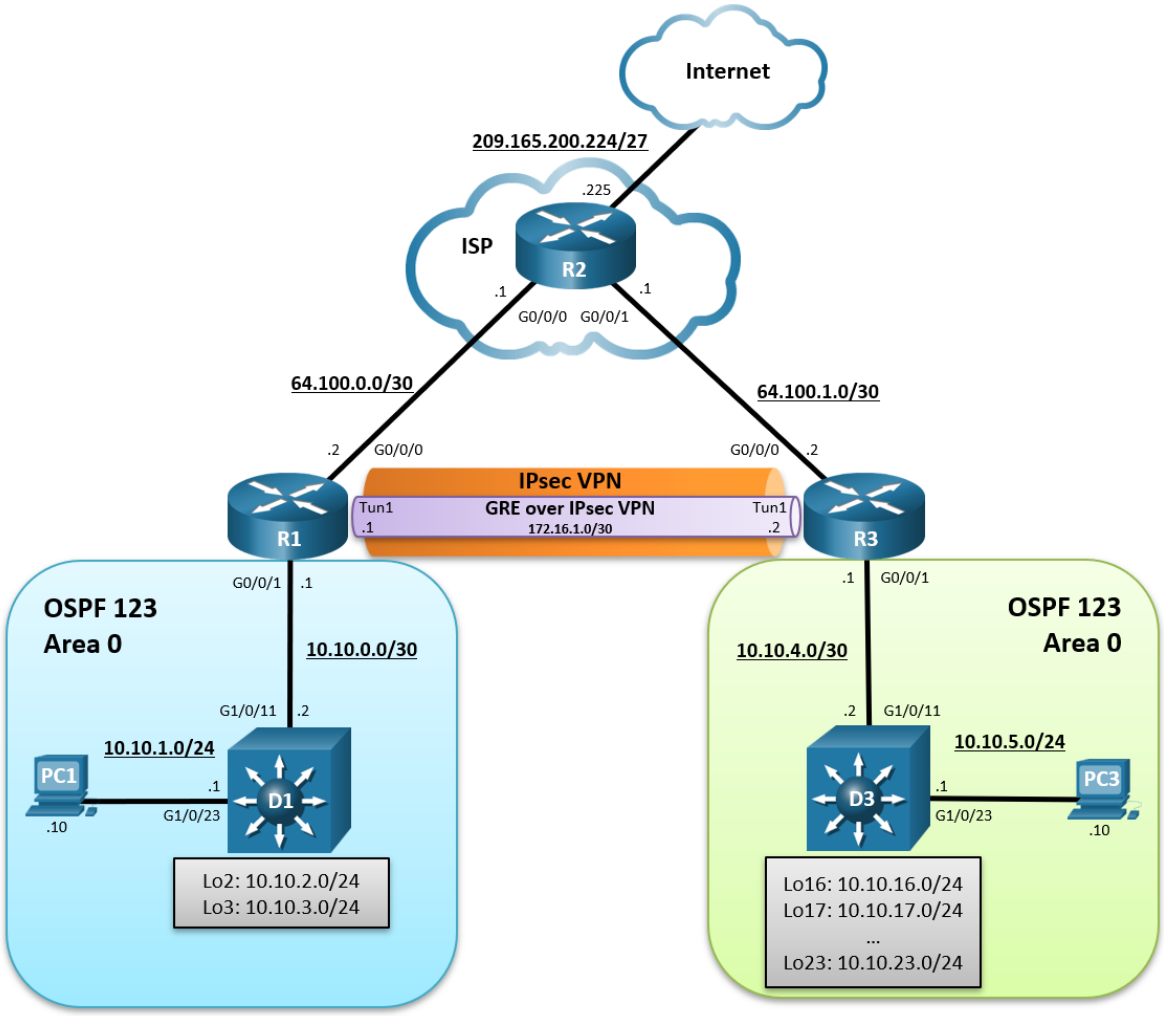
# Lab – Cấu hình GRE Over IPsec site-to-site VPN

**Sơ đồ:**




**Mô tả:**

- Sơ đồ bài Lab gồm 3 Router 2911 và 2 Switch Layer 3 3560 được kết nối với nhau như hình. Bài Lab này có thể dựng trên lab ảo hoá sử dụng các IOL Router L3-ADVENTERPRISEK9-M-15.4-2T, IOL Switch i86bi_linux_l2-advipservicesk9.
- Trong bài Lab này học viên thực hiện Site to Site VPN thông qua GRE tunnel, kết hợp IPsec bằng phương pháp Crypto Map và IPsec Profile

**Bảng quy hoạch IP:**

| Device | Interface | IPv4 Address | Default Gateway |
|---|---|---|---|
| R1 | G0/0/0 | 64.100.0.2/30 | N/A |
| | G0/0/1 | 10.10.0.1/30 | |
| | Tunnel 1 | 172.16.1.1/30 | |
| R2 | G0/0/0 | 64.100.0.1/30 | N/A |
| | G0/0/1 | 64.100.1.1/30 | |
| | Lo0 | 209.165.200.225/27 | |
| R3 | G0/0/0 | 64.100.1.2/30 | N/A |
| | G0/0/1 | 10.10.4.1/30 | |
| | Tunnel 1 | 172.16.1.2/30 | |
| D1 | G1/0/11 | 10.10.0.2/30 | N/A |
| | G1/0/23 | 10.10.1.1/24 | |
| | Lo2 | 10.10.2.1/24 | |
| | Lo3 | 10.10.3.1/24 | |
| D3 | G1/0/11 | 10.10.0.3/30 | N/A |
| | G1/0/23 | 10.10.5.1/24 | |
| | Lo16 | 10.10.16.1/24 | |
| | Lo17 | 10.10.17.1/24 | |
| | Lo18 | 10.10.18.1/24 | |
| | Lo19 | 10.10.19.1/24 | |
| | Lo20 | 10.10.20.1/24 | |
| | Lo21 | 10.10.21.1/24 | |
| | Lo22 | 10.10.22.1/24 | |
| | Lo23 | 10.10.23.1/24 | |
| PC1 | NIC | 10.10.1.10/24 | 10.10.1.1 |
| PC3 | NIC | 10.10.5.10/24 | 10.10.5.1 |

*Bảng 1 – Quy hoạch IP cho sơ đồ Lab*

**Yêu cầu:**

1. Xây dựng mạng, cấu hình cài đặt thiết bị cơ bản và định tuyến
2. Cấu hình GRE qua IPsec bằng Crypto Maps trên R1
3. Cấu hình GRE qua IPsec bằng IPsec Profile trên R3
4. Kiểm tra GRE tunnel IPsec trên R1 và R3

**Thực hiện:**

**Phần 1: Xây dựng mạng, cấu hình cài đặt thiết bị cơ bản và định tuyến**

**Bước 1: Cấu hình cơ bản cho các Router.**

Học viên tiến hành cấu hình cơ bản các thiết bị Router như bên dưới

**Router R1**

```
hostname R1
interface g0/0/0
 description Connection to R2
 ip add 64.100.0.2 255.255.255.252
 no shut
 exit
interface GigabitEthernet0/0/1
 description Connection to D1
 ip address 10.10.0.1 255.255.255.252
 no shut
 exit
router ospf 123
 router-id 1.1.1.1
 auto-cost reference-bandwidth 1000
 network 10.10.0.0 0.0.0.3 area 0
 default-information originate
exit
ip route 0.0.0.0 0.0.0.0 64.100.0.1
```

**Router R2**

```
hostname R2
interface g0/0/0
 description Connection to R1
 ip add 64.100.0.1 255.255.255.252
 no shut
 exit
interface GigabitEthernet0/0/1
 description Connection to R3
 ip address 64.100.1.1 255.255.255.252
 no shut
 exit
int lo0
```

```
 description Internet simulated address
 ip add 209.165.200.225 255.255.255.224
 exit
ip route 0.0.0.0 0.0.0.0 Loopback0
ip route 10.10.0.0 255.255.252.0 64.100.0.2
ip route 10.10.4.0 255.255.252.0 64.100.1.2
ip route 10.10.16.0 255.255.248.0 64.100.1.2
```

**Router R3**

```
hostname R3
interface g0/0/0
 description Connection to R2
 ip add 64.100.1.2 255.255.255.252
 no shut
 exit
interface GigabitEthernet0/0/1
 description Connection to D3
 ip address 10.10.4.1 255.255.255.252
 no shut
 exit
ip route 0.0.0.0 0.0.0.0 64.100.1.1
router ospf 123
 router-id 3.3.3.1
network 10.10.4.0 0.0.0.3 area 0
 default-information originate
exit
```

**Switch D1**

```
hostname D1
interface G1/0/11
 description Connection to R1
 no switchport
 ip address 10.10.0.2 255.255.255.252
 no shut
 exit
interface G1/0/23
 description Connection to PC1
 no switchport
 ip address 10.10.1.1 255.255.255.0
 no shut
 exit
int Lo2
 description Loopback to simulate an OSPF network
 ip add 10.10.2.1 255.255.255.0
 ip ospf network point-to-point
exit
int Lo3
 description Loopback to simulate an OSPF network
 ip add 10.10.3.1 255.255.255.0
```

```
 ip ospf network point-to-point
exit
ip routing
router ospf 123
 router-id 1.1.1.2
  network 10.10.0.0 0.0.3.255 area 0
exit
```

**Switch D3**

```
hostname D3
interface G1/0/11
 description Connection to R3
 no switchport
 ip address 10.10.4.2 255.255.255.252
 no shut
 exit
interface G1/0/23
 description Connection to PC3
 no switchport
 ip address 10.10.5.1 255.255.255.0
 no shut
 exit
int Lo16
 description Loopback to simulate an OSPF network
 ip add 10.10.16.1 255.255.255.0
 ip ospf network point-to-point
exit
int Lo17
 description Loopback to simulate an OSPF network
 ip add 10.10.17.1 255.255.255.0
 ip ospf network point-to-point
 exit
int Lo18
 description Loopback to simulate an OSPF network
 ip add 10.10.18.1 255.255.255.0
 ip ospf network point-to-point
 exit
int Lo19
 description Loopback to simulate an OSPF network
 ip add 10.10.19.1 255.255.255.0
 ip ospf network point-to-point
 exit
int Lo20
 description Loopback to simulate an OSPF network
 ip add 10.10.20.1 255.255.255.0
 ip ospf network point-to-point
 exit
int Lo21
 description Loopback to simulate an OSPF network
```

```
 ip add 10.10.21.1 255.255.255.0
 ip ospf network point-to-point
 exit
int Lo22
 description Loopback to simulate an OSPF network
 ip add 10.10.22.1 255.255.255.0
 ip ospf network point-to-point
 exit
int Lo23
 description Loopback to simulate an OSPF network
 ip add 10.10.23.1 255.255.255.0
 ip ospf network point-to-point
 exit
ip routing
router ospf 123
 router-id 3.3.3.2
 network 10.10.4.0 0.0.1.255 area 0
 network 10.10.16.0 0.0.7.255 area 0
 exit
```

**Bước 2: Kiểm tra bảng định tuyến của R1 và R3.**

Kiểm tra bảng định tuyến trên Router R1.

```
R1# show ip route ospf | begin Gateway
Gateway of last resort is 64.100.0.1 to network 0.0.0.0

   10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
O     10.10.1.0/24 [110/11] via 10.10.0.2, 00:02:45, GigabitEthernet0/0/1
O     10.10.2.0/24 [110/2] via 10.10.0.2, 00:02:45, GigabitEthernet0/0/1
O     10.10.3.0/24 [110/2] via 10.10.0.2, 00:02:45, GigabitEthernet0/0/1
```

Bảng định tuyến của R1 chỉ chứa các route OSPF cục bộ. Bảng định tuyến xác nhận rằng R1 có các mạng được kết nối với D1. Tuy nhiên, lưu ý rằng R1 không có các tuyến đường kết nối với miền OSPF phía R3 nhưng PC1 vẫn có thể đi đến 10.10.5.0 của PC3 là vì R1 có một default route đến R2. R1 chuyển tiếp lưu lượng đến R2, R2 có một static route đến mạng 10.10.5.0 này nó chuyển tiếp đến R3.

Kiểm tra bảng định tuyến trên Router R3.

```
R3# show ip route ospf | begin Gateway
Gateway of last resort is 64.100.1.1 to network 0.0.0.0

   10.0.0.0/8 is variably subnetted, 11 subnets, 3 masks
O     10.10.5.0/24 [110/11] via 10.10.4.2, 00:00:41, GigabitEthernet0/0/1
O     10.10.16.0/24 [110/2] via 10.10.4.2, 00:00:41, GigabitEthernet0/0/1
O     10.10.17.0/24 [110/2] via 10.10.4.2, 00:00:41, GigabitEthernet0/0/1
O     10.10.18.0/24 [110/2] via 10.10.4.2, 00:00:41, GigabitEthernet0/0/1
O     10.10.19.0/24 [110/2] via 10.10.4.2, 00:00:41, GigabitEthernet0/0/1
O     10.10.20.0/24 [110/2] via 10.10.4.2, 00:00:41, GigabitEthernet0/0/1
O     10.10.21.0/24 [110/2] via 10.10.4.2, 00:00:41, GigabitEthernet0/0/1
O     10.10.22.0/24 [110/2] via 10.10.4.2, 00:00:41, GigabitEthernet0/0/1
```

```
O    10.10.23.0/24 [110/2] via 10.10.4.2, 00:00:41, GigabitEthernet0/0/1
```

Giống như R1, bảng định tuyến của R3 chỉ chứa các route cục bộ của nó.

**Bước 3: Cấu hình đặt địa chỉ IP cho PC1 và PC3 và kiểm tra kết nối.**

Đặt ip cho PC1 và PC3 theo bảng quy hoạch IP đồng thời đặt gateway cho hai thiết bị.

Ping kiểm tra 2 PC với nhau

**Phần 2: Cấu hình GRE over IPsec sử dụng Crypto Map trên R1**

**Bước 1: Trên R1, cấu hình ISAKMP policy và pre-shared key.**

Như các VPN site-to-site sử dụng crypto maps, GRE over IPsec cũng yêu cầu một cấu hình ISAKMP policy và pre-shared key.

Trong bài lab này, chúng ta sẽ sử dụng ISAKMP policy 10 trên R1 với các thông số:

Encryption: **aes 256**

Hash: **sha256**

Authentication method: **pre-share key**

Diffie-Hellman group: **14**

Lifetime: **3600** seconds (60 minutes / 1 hour)

Cấu hình ISAKMP policy 10 trên R1:

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#hash sha256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 14
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#exit
```

Cấu hình pre-shared key là **cisco123** trên R1. Câu lệnh này trỏ đến địa chỉ ip của R3 G0/0/0

```
R1(config)# crypto isakmp key cisco123 address 64.100.1.2
```

**Bước 2: Trên R1, cấu hình transform set và VPN ACL.**

Tạo một transform set có tên GRE-VPN bằng cách sử dụng mật mã AES 256 với ESP và hàm băm SHA 256.

Không giống như VPN IPsec site-to-site, transform sẽ phải sử dụng mode transport. Lệnh mode được sử dụng để xác định loại đường hầm sẽ được thiết lập. Mặc định là mode tunnel. Tuy nhiên, GRE qua IPsec nên sử dụng mode transport.

```
R1(config)#crypto ipsec transform-set GRE-VPN esp-aes 256 esp-sha256-hmac
R1(cfg-crypto-trans)#mode transport
R1(cfg-crypto-trans)#exit
```

Tiếp theo, tạo ACL extended đặt tên là GRE-VPN-ACL để khớp với lưu lượng GRE từ IP source tới IP destination của đường tunnel, Source của tunnel là IP public bên R1, destination của tunnel là IP public bên R3, ACL này sẽ sử dụng lại trong Crypto map bên dưới.

```
R1(config)#ip access-list extended GRE-VPN-ACL
R1(config-ext-nacl)#permit gre host 64.100.0.2 host 64.100.1.2
R1(config-ext-nacl)#exit
```

**Bước 3: Trên R1, Cấu hình crypto map và gán vào interface.**

Tạo bộ crypto map tên là **GRE-CMAP** sẽ gọi lại GRE-VPN-ACL, transform set và peer tới IP destination bên kia.

```
R1(config)#crypto map GRE-CMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#match address GRE-VPN-ACL
R1(config-crypto-map)#set transform-set GRE-VPN
R1(config-crypto-map)#set peer 64.100.1.2
R1(config-crypto-map)#exit
```

Cuối cùng, áp crypto map vừa tạo lên interface G0/0/0.

```
R1(config)#interface g0/0/0
R1(config-if)#crypto map GRE-CMAP
```

Vậy lưu lượng đi ra cổng g0/0/0 sẽ được áp crypto map **GRE-CMAP**, GRE-CMAP so sánh thấy khớp lưu lượng **GRE** từ **64.100.0.2** tới **64.100.1.2** được khai báo trong ACL **GRE-VPN-ACL** thì sẽ set transform set **GRE-VPN,** GRE-VPN sẽ áp các cấu hình ipsec được khai báo trong transform set.

**Bước 4: Trên R1, Cấu hình GRE tunnel interface.**

```
R1(config)#interface Tunnel1
R1(config-if)#bandwidth 4000
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ip mtu 1400
R1(config-if)#tunnel source 64.100.0.2
R1(config-if)#tunnel destination 64.100.1.2
R1(config-if)#end
*Feb 19 17:54:21.381: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Tunnel1, changed state to down
*Feb 19 17:54:23.689: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Tunnel1, changed state to up
```

**Phần 3: Cấu hình GRE over IPsec sử dụng một IPsec Profile trên R3**

**Bước 1: Trên R3, Cấu hình ISAKMP policy, pre-shared key, và transform set.**

Cấu hình ISAKMP policy 10 trên R3:

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

```
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#hash sha256
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 14
R3(config-isakmp)#lifetime 3600
R3(config-isakmp)#exit
```

Cấu hình pre-shared key với **cisco123** giống với trên R1. Key này sẽ trỏ đến địa chỉ ip trên cổng G0/0/0 của remote peer R3.

```
R3(config)#crypto isakmp key cisco123 address 64.100.0.2
```

Tạo một transform set mới gọi là GRE-VPN sử dụng cùng các thông số bảo mật và transport mode đã cấu hình trên R1.

```
R3(config)#crypto ipsec transform-set GRE-VPN esp-aes 256 esp-sha256-hmac
R3(cfg-crypto-trans)#mode transport
R3(cfg-crypto-trans)#exit
```

**Bước 2: Trên R3, cấu hình IPsec profile.**

Thay vì một crypto map, chúng ta sẽ cấu hình một IPsec profile gọi là GRE-PROFILE gọi tới transfom set GRE-VPN vừa tạo ở trên.

```
R3(config)#crypto ipsec profile GRE-PROFILE
R3(ipsec-profile)#set transform-set GRE-VPN
R3(ipsec-profile)#exit
```

**Bước 3: Cấu hình tunnel interface.**

Trên R3, Cấu hình GRE tunnel interface.

```
R3(config)#interface Tunnel1
R3(config-if)#bandwidth 4000
R3(config-if)#ip address 172.16.1.2 255.255.255.252
R3(config-if)#ip mtu 1400
R3(config-if)#tunnel source 64.100.1.2
R3(config-if)#tunnel destination 64.100.0.2
*Feb 19 17:57:10.415: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Tunnel1, changed state to down
*Feb 19 17:57:12.660: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Tunnel1, changed state to up
```

Gán IPsec profile GRE-PROFILE vào cổng Tunnel 1

```
R3(config-if)#tunnel protection ipsec profile GRE-PROFILE
*Feb 19 17:58:09.299: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)# end
```

Vậy lưu lượng đi qua cổng tunnel sẽ được áp IPsec profile **GRE-PROFILE**, GRE-PROFILE này gọi tới transform set **GRE-VPN,** GRE-VPN sẽ áp các cấu hình ipsec được khai báo trong transform set.

**Bước 4: Trên R1 và R3, bật tính năng OSPF routing trên cổng tunnel.**

Trên R1, kiểm tra ping đến địa chỉ 10.10.16.1 của R3.

```
R1# ping 10.10.16.1 source 10.10.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.16.1, timeout is 2 seconds:
Packet sent with a source address of 10.10.0.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
```

Ping thành công. Trên R1, xác minh số liệu thống kê được mã hóa và giải mã IPsec SA.

```
R1#show crypto ipsec sa | include encrypt|decrypt
     #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
     #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
```

Không có gói nào được mã hóa.

Từ D1, theo dõi đường dẫn đến R3  có địa chỉ 10.10.16.1.

```
D1#trace 10.10.16.1
Type escape sequence to abort.
Tracing the route to 10.10.16.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.10.0.1 0 msec 9 msec 0 msec
  2 64.100.0.1 0 msec 8 msec 0 msec
  3 64.100.1.2 0 msec 0 msec 9 msec
  4 10.10.4.2 0 msec *  0 msec
```

Trên R1, Cấu hình OSPF để quảng bá các cổng tunnel.

```
R1(config)#router ospf 123
R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
```

Trên R3, Cấu hình OSPF để quảng bá các cổng tunnel.

```
R3(config)# router ospf 123
R3(config-router)# network 172.16.1.0 0.0.0.3 area 0
R3(config-router)#
*Feb 19 18:01:18.613: %OSPF-5-ADJCHG: Process 123, Nbr 1.1.1.1 on Tunnel1
from LOADING to FULL, Loading Done
```

**Phần 4: kiểm tra GRE qua IPsec Tunnel trên R1 và R3**

**Bước 1: trên R1 và R3, kiểm tra các cổng tunnel.**

Sử dụng câu lệnh **show interfaces tunnel 1** để kiểm tra tunnel.

```
R1#show interfaces tunnel 1
```

```
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 172.16.1.1/30
  MTU 9976 bytes, BW 4000 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 64.100.0.2, destination 64.100.1.2
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input 00:00:01, output 00:00:04, output hang never
  Last clearing of "show interface" counters 00:02:01
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
```

Trên R3, sử dụng câu lệnh **show interfaces tunnel 1** để kiểm tra tunnel.

```
R3#show inter tunnel 1 | include is up|Internet address|Enc|Tunnel protocol
Tunnel1 is up, line protocol is up
  Internet address is 172.16.1.2/30
  Encapsulation TUNNEL, loopback not set
  Tunnel protocol/transport GRE/IP
```

**Bước 2: Trên R1 và R3, kiểm tra các cài đặt crypto.**

Trên R1, sử dụng câu lệnh **show crypto session** để kiểm tra hoạt động VPN tunnel.

```
R1#show crypto session
Crypto session current status

Interface: GigabitEthernet0/0/0
Session status: UP-ACTIVE
Peer: 64.100.1.2 port 500
  Session ID: 0
  IKEv1 SA: local 64.100.0.2/500 remote 64.100.1.2/500 Active
  IPSEC FLOW: permit 47 host 64.100.0.2 host 64.100.1.2
        Active SAs: 4, origin: crypto map
```

Trên R3, sử dụng câu lệnh **show crypto session** để kiểm tra hoạt động VPN tunnel.

```
R3#show crypto session
Crypto session current status

Interface: Tunnel1
Session status: UP-ACTIVE
```

```
Peer: 64.100.0.2 port 500
  Session ID: 0
  IKEv1 SA: local 64.100.1.2/500 remote 64.100.0.2/500 Active
  IPSEC FLOW: permit 47 host 64.100.1.2 host 64.100.0.2
        Active SAs: 4, origin: crypto map
```

**Bước 3: Trên R1 và R3, kiểm tra định tuyến OSPF.**

Trên R1 and R3, kiểm tra cổng nào được cấu hình cho OSPF bằng cách sử dụng câu lệnh **show ip ospf interface brief**.

```
R1#show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Tu1          123   0               172.16.1.1/30      250   P2P   1/1
Gi0/0/1      123   0               10.10.0.1/30       1     BDR   1/1

R3#show ip ospf interface brief
Interface    PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Tu1          123   0               172.16.1.2/30      250   P2P   1/1
Gi0/0/1      123   0               10.10.4.1/30       1     BDR   1/1
```

Trên R1 và R3, kiểm tra OSPF láng giềng sử dụng câu lệnh **show ip ospf interface brief**.

```
R1#show ip ospf neighbor
Neighbor ID  Pri   State      Dead Time   Address         Interface
3.3.3.1      0   FULL/  -     00:00:32    172.16.1.2      Tunnel1
1.1.1.2      1   FULL/DR      00:00:35    10.10.0.2  GigabitEthernet0/0/1

R3#show ip ospf neighbor

Neighbor ID  Pri   State      Dead Time   Address         Interface
1.1.1.1       0   FULL/  -     00:00:36    172.16.1.1      Tunnel1
3.3.3.2       1   FULL/DR      00:00:36    10.10.4.2  GigabitEthernet0/0/1
```

Kiểm tra bảng định tuyến R1 cho các tuyến OSPF.

```
R1#show ip route ospf | begin Gateway
Gateway of last resort is 64.100.0.1 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 15 subnets, 3 masks
O     10.10.1.0/24 [110/11] via 10.10.0.2, 00:25:20, GigabitEthernet0/0/1
O     10.10.2.0/24 [110/2] via 10.10.0.2, 00:25:20, GigabitEthernet0/0/1
O     10.10.3.0/24 [110/2] via 10.10.0.2, 00:25:20, GigabitEthernet0/0/1
O     10.10.4.0/30 [110/251] via 172.16.1.2, 00:05:22, Tunnel1
O     10.10.5.0/24 [110/261] via 172.16.1.2, 00:05:22, Tunnel1
O     10.10.16.0/24 [110/252] via 172.16.1.2, 00:05:22, Tunnel1
O     10.10.17.0/24 [110/252] via 172.16.1.2, 00:05:22, Tunnel1
O     10.10.18.0/24 [110/252] via 172.16.1.2, 00:05:22, Tunnel1
O     10.10.19.0/24 [110/252] via 172.16.1.2, 00:05:22, Tunnel1
(……)
```

Kiểm tra bảng định tuyến R3 cho các tuyến OSPF.

```
R3#show ip route ospf | begin Gateway
Gateway of last resort is 64.100.1.1 to network 0.0.0.0

   10.0.0.0/8 is variably subnetted, 15 subnets, 3 masks
O      10.10.0.0/30 [110/251] via 172.16.1.1, 00:40:45, Tunnel1
O      10.10.1.0/24 [110/261] via 172.16.1.1, 00:40:45, Tunnel1
O      10.10.2.0/24 [110/252] via 172.16.1.1, 00:40:45, Tunnel1
O      10.10.3.0/24 [110/252] via 172.16.1.1, 00:40:45, Tunnel1
O      10.10.5.0/24 [110/11] via 10.10.4.2, 01:00:49, GigabitEthernet0/0/1
O      10.10.16.0/24 [110/2] via 10.10.4.2, 01:00:49, GigabitEthernet0/0/1
O      10.10.17.0/24 [110/2] via 10.10.4.2, 01:00:49, GigabitEthernet0/0/1
(……)
```

Kiểm tra rằng có một liên kết điểm-điểm hoạt động giữa R1 và R3 bằng cách sử dụng cổng đường hầm GRE.

```
R1#show ip route 172.16.0.0
Routing entry for 172.16.0.0/16, 2 known subnets
  Attached (2 connections)
  Variably subnetted with 2 masks
C        172.16.1.0/30 is directly connected, Tunnel1
L        172.16.1.1/32 is directly connected, Tunnel1

R3#show ip route 172.16.0.0
Routing entry for 172.16.0.0/16, 2 known subnets
  Attached (2 connections)
  Variably subnetted with 2 masks
C        172.16.1.0/30 is directly connected, Tunnel1
L        172.16.1.2/32 is directly connected, Tunnel1
```

**Bước 4: Kiểm tra GRE qua IPsec VPN tunnel.**

Trên D1, kiểm tra đường đi đến cổng của R3 với địa chỉ 10.10.16.1.

```
D1#trace 10.10.16.1

Type escape sequence to abort.

Tracing the route to 10.10.16.1

VRF info: (vrf in name/id, vrf out name/id)

  1 10.10.0.1 2 msec 2 msec 2 msec

  2 172.16.1.2 3 msec 2 msec 2 msec

  3 10.10.4.2 4 msec *  3 msec
```

Trên R1, kiểm tra thống kê các gói tin được mã hoá và giải mã.

```
R1#show crypto ipsec sa | include encrypt|decrypt

    #pkts encaps: 296, #pkts encrypt: 296, #pkts digest: 296

    #pkts decaps: 295, #pkts decrypt: 295, #pkts verify: 295
```