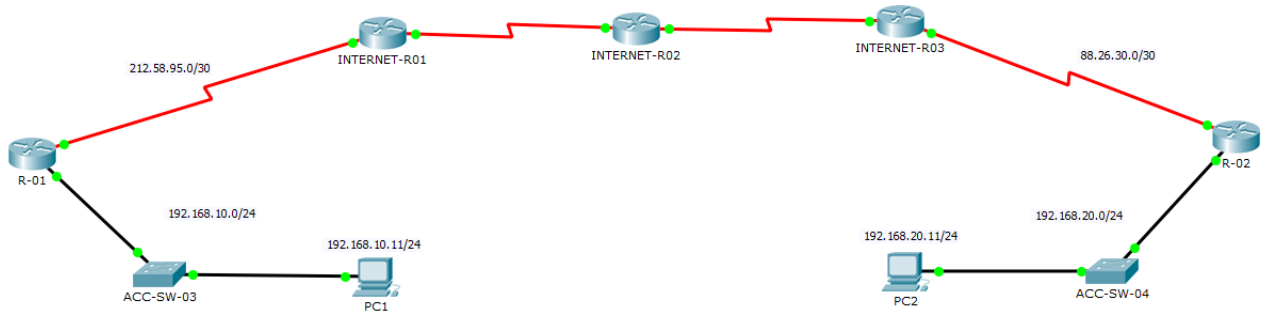
LAB-242



Hedef

Internet üzerinden birbirleri ile haberleşebilen iki Router arasında GRE VPN tünel kurulması. Ve tünel üzerinden OSPF konfigurasyonu yaparak uzak lokasyonların haberleşmesini sağlamak

PC'lerin IP konfigurasyonları

PC1	VLAN 10	192.168.10.11/24	Default GateWay 192.168.10.1
PC2	VLAN 20	192.168.20.11/24	Default GateWay 192.168.20.1

Çalışma-01

Şekilde de görüldüğü gibi R-01 ve R-02 Internet üzerinden birbirleri ile iletişime geçebilirken, arkalarındaki 192.168.10.0/24 ve 192.168.20.0/24 networkleri birbirleri ile haberleşememektedir. Zaten Private blok olan bu IP adreslerinin Internet üzerinden yönlendirilmesi mümkün değildir. Bu ihtiyacı gidermek için R-01 ve R-02 arasında Internet erişimi üzerinden **Generic Routing Encapsulation (GRE)** tünel yapılandırması kuracağız. Bu sayede aralarında **VPN** tesis edilecek olan bu iki router adeta Directly Connected gibi haberleşecekler.

Konfigurasyona geçmeden önce R-01 ve R-02 nin Internet üzerinden erişimlerini test ediyoruz.

```
R-01#ping 88.26.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 88.26.30.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/9/15 ms

R-01#
```

VPN yapılanması için öncelikle router'larda birer adet sanal interface olan **Tunnel Interface** oluşturuyoruz. Bu ınterface'e IP adresi verdikten sonra Tünelimizin ihtiyaç duyduğu konfigurasyonu yapıyoruz.

```
R-01#configure terminal
R-01(config)#
R-01(config)#interface tunnel 1
R-01(config-if)#
%LINK-5-CHANGED: Interface Tunnel1, changed state to up
R-01(config-if)#tunnel mode gre ip
R-01(config-if)#
R-01(config-if)#ip address 172.16.12.1 255.255.255.0
R-01(config-if)#
R-01(config-if)#tunnel source serial 0/0/0
R-01(config-if)#
R-01(config-if)#tunnel destination 88.26.30.1
R-01(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
R-01(config-if)#end
R-01#

R-02#configure terminal
R-02(config)#
R-02(config)#interface tunnel 1
R-02(config-if)#
%LINK-5-CHANGED: Interface Tunnel1, changed state to up
R-02(config-if)#tunnel mode gre ip
R-02(config-if)#
R-02(config-if)#ip address 172.16.12.2 255.255.255.0
R-02(config-if)#
R-02(config-if)#tunnel source Serial0/0/0
R-02(config-if)#
R-02(config-if)#tunnel destination 212.58.95.1
R-02(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
R-02(config-if)#end
R-02#
```

```
R-01#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.10.1    YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Serial0/0/0            212.58.95.1     YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
Tunnel1                172.16.12.1     YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
R-01#
```

```
R-02#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.20.1    YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Serial0/0/0            88.26.30.1      YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
Tunnel1                172.16.12.2     YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
R-02#
```

```
R-01#show interfaces tunnel 1

Tunnel1 is up, line protocol is up (connected)
  Hardware is Tunnel
  Internet address is 172.16.12.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 212.58.95.1 (Serial0/0/0), destination 88.26.30.1
  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 never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
      0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out

R-01#

R-01#ping 172.16.12.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/8/12 ms

R-01#
```

```
R-01#traceroute 172.16.12.2

Type escape sequence to abort.
Tracing the route to 172.16.12.2

  1   172.16.12.2     17 msec   4 msec    4 msec

R-01#
```

Özellikle bu trace çıktısını yorumlamamız çok önemlidir. Girmiş olduğumuz VPN yapılanması sayesinde R-01 ve R-02 adeta birbirlerine direk bağlı gibi olmuşlardır. R-01'in tunnel 1 interface'i ile R-02'nin tunnel 1 interface'leri sanki directly connected gibidirler.

Şimdi bu interface'ler üzerinden OSPF protokolü koşuşturarak R-01 ve R-02'nin arkalarındaki networkleri birbirlerine öğretmelerini sağlayacağız.

```
R-01#configure terminal
R-01(config)#
R-01(config)#router ospf 1
R-01(config-router)#
R-01(config-router)#router-id 1.1.1.1
R-01(config-router)#
R-01(config-router)#passive-interface gigabitEthernet 0/0
R-02(config-router)#
R-02(config-router)#network 192.168.10.1 0.0.0.0 area 0
R-02(config-router)#
R-01(config-router)#network 172.16.12.1 0.0.0.0 area 0
R-01(config-router)#
R-01(config-router)#end
R-01#

R-02#configure terminal
R-02(config)#
R-02(config)#router ospf 1
R-02(config-router)#
R-02(config-router)#router-id 2.2.2.2
R-02(config-router)#
R-02(config-router)#passive-interface gigabitEthernet 0/0
R-02(config-router)#
R-02(config-router)#network 192.168.20.1 0.0.0.0 area 0
R-02(config-router)#
R-02(config-router)#network 172.16.12.2 0.0.0.0 area 0
R-02(config-router)#
R-02(config-router)#end
R-02#
```

```
R-01#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           0   FULL/  -        00:00:35    172.16.12.2     Tunnel1

R-01#

R-01#show ip ospf interface

Tunnel1 is up, line protocol is up
  Internet address is 172.16.12.1/24, Area 0
  Process ID 1, Router ID 1.1.1.1, Network Type POINT-TO-POINT, Cost: 1000
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:04
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)

R-01#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.12.1 0.0.0.0 area 0
    192.168.10.1 0.0.0.0 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:10:35
    2.2.2.2              110      00:11:53
  Distance: (default is 110)

R-01#
```

Router'ların IP routing tablolarına bakacak olursak:

```
R-01#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.12.0/24 is directly connected, Tunnel1
L       172.16.12.1/32 is directly connected, Tunnel1
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
O    192.168.20.0/24 [110/1001] via 172.16.12.2, 00:01:48, Tunnel1
     212.58.95.0/24 is variably subnetted, 2 subnets, 2 masks
C       212.58.95.0/30 is directly connected, Serial0/0/0
L       212.58.95.1/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 is directly connected, Serial0/0/0

R-01#
```

```
R-02#sh ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     88.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       88.26.30.0/30 is directly connected, Serial0/0/0
L       88.26.30.1/32 is directly connected, Serial0/0/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.12.0/24 is directly connected, Tunnel1
L       172.16.12.2/32 is directly connected, Tunnel1
O    192.168.10.0/24 [110/1001] via 172.16.12.1, 00:01:24, Tunnel1
     192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, GigabitEthernet0/0
L       192.168.20.1/32 is directly connected, GigabitEthernet0/0
S*   0.0.0.0/0 is directly connected, Serial0/0/0

R-02#
```

Artık PC'lerin birbirlerine erişimine bakabiliriz. PC1 den PC2 ye ping testi yapıyoruz:

```
PC>ping 192.168.20.11

Pinging 192.168.20.11 with 32 bytes of data:

Reply from 192.168.20.11: bytes=32 time=8ms TTL=126
Reply from 192.168.20.11: bytes=32 time=11ms TTL=126
Reply from 192.168.20.11: bytes=32 time=10ms TTL=126
Reply from 192.168.20.11: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.20.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 12ms, Average = 10ms

PC>
```

Dikkat ederseniz şu an Internet üzerinden iki farklı Private IP bloğunun haberleşmesini sağladık. Aradaki Internet cihazları, bu uç/private networklerden haberdar olmamakla birlikte, açtığımız tünel içinden ilgili paketleri taşınmaktadırlar.

Peki bu derece değerli verilerilerimizin Internet gibi bir ortamdan geçip gitmesi ne kadar güvenli? Tabiki hiç güvenli değil. Bu şekilde bir **VPN** kurmak adeta kapıyı açık bırakıp yaz tatiline gitmek gibi olacaktır. Çözüm ise adına **IPsec** dediğimiz ve uçtan uca hem kriptografi hemde şifreleme ve parola mevzularına çözüm olarak geliştirilen uygulamadır.

Müfredatımız içerisinde Ipsec olmasa da bir örneğine bakmanız ve fikir sahibi olmanız açısından şu adresden okuma yapılabilirsiniz https://goo.gl/SnTMWX

Router'ların son config`leri

```
R-01#show running-config
Building configuration...

Current configuration : 1366 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R-01
!
no ip cef
no ipv6 cef
!
license udi pid CISCO2911/K9 sn FTX15247DH9
!
no ip domain-lookup
!
spanning-tree mode pvst
!
interface Tunnel1
 ip address 172.16.12.1 255.255.255.0
 mtu 1476
 tunnel source Serial0/0/0
 tunnel destination 88.26.30.1
!
interface GigabitEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
```

```
!
interface Serial0/0/0
 ip address 212.58.95.1 255.255.255.252
 ip nat outside
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 passive-interface GigabitEthernet0/0
 network 172.16.12.1 0.0.0.0 area 0
 network 192.168.10.1 0.0.0.0 area 0
!
ip nat inside source list 10 interface Serial0/0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
ip flow-export version 9
!
access-list 10 permit 192.168.10.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
line aux 0
!
line vty 0 4
 login
!
end
```

```
R-02#show running-config
Building configuration...

Current configuration : 1366 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R-02
!
no ip cef
no ipv6 cef
!
license udi pid CISCO2911/K9 sn FTX152498HF
!
no ip domain-lookup
!
spanning-tree mode pvst
!
interface Tunnel1
 ip address 172.16.12.2 255.255.255.0
 mtu 1476
 tunnel source Serial0/0/0
 tunnel destination 212.58.95.1
!
interface GigabitEthernet0/0
 ip address 192.168.20.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
```

```
!
interface Serial0/0/0
 ip address 88.26.30.1 255.255.255.252
 ip nat outside
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 passive-interface GigabitEthernet0/0
 network 172.16.12.2 0.0.0.0 area 0
 network 192.168.20.1 0.0.0.0 area 0
!
ip nat inside source list 10 interface Serial0/0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
ip flow-export version 9
!
access-list 10 permit 192.168.20.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
 logging synchronous
!
line aux 0
!
line vty 0 4
 login
!
end
```

https://goo.gl/vT9PhB

Umarım faydalı bir LAB çalışması olmuştur.
Soru ve yorumlarınız için,
aliaydemir80@gmail.com