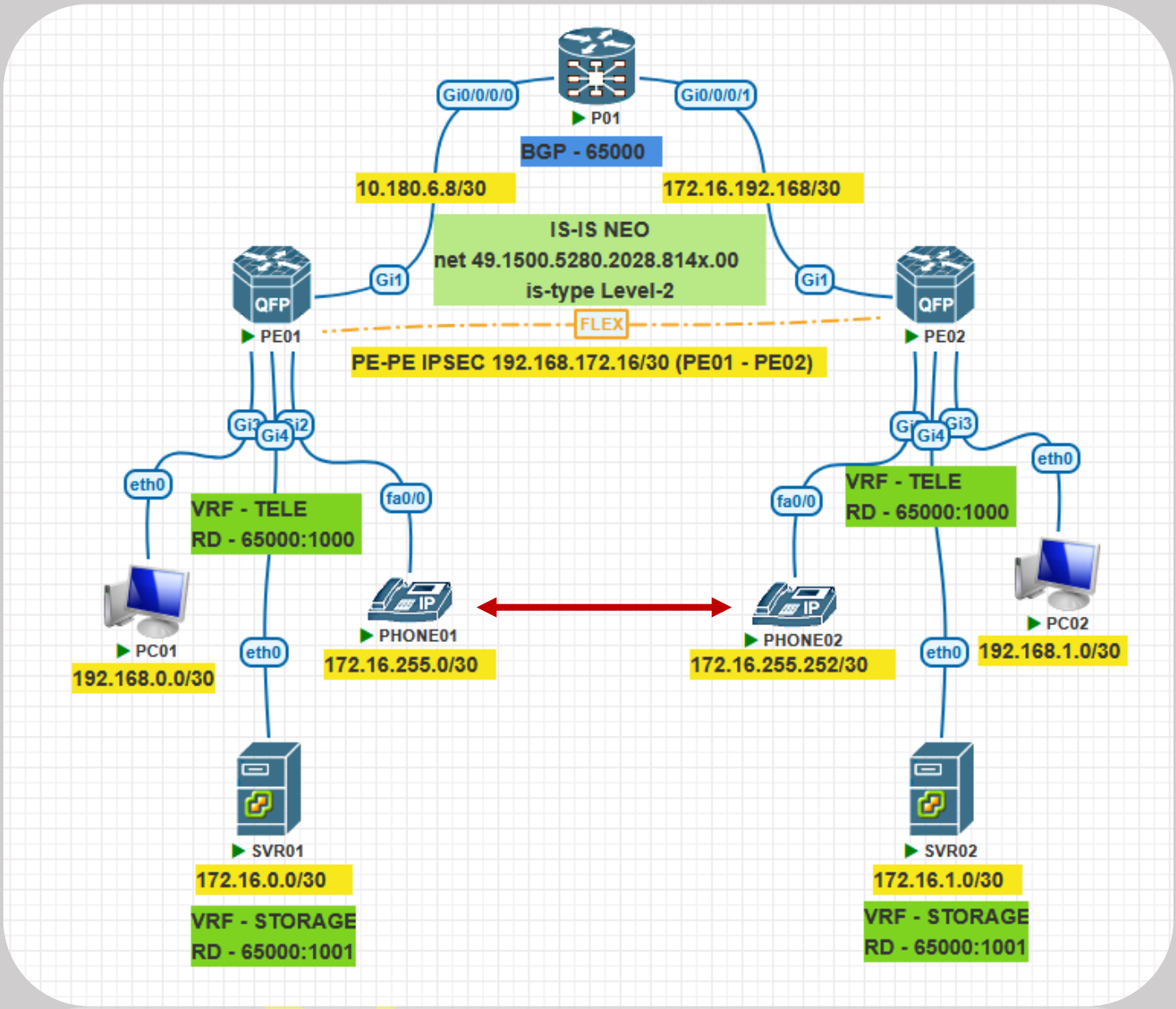
PE–PE IPsec Tunnel using FlexVPN in an MPLS L3VPN Core



Lab Requirements

1. In **VRF–TELE**, forwarding must be differentiated on a per–prefix basis:
   a. Prefixes of **IP–PHONES** must be transported over the **PE–PE IPsec tunnel.**

b. Prefixes of **PCs** must use the native MPLS L3VPN forwarding path (**no IPsec encapsulation**).

2. All traffic in **VRF–STORAGE** must use the native MPLS L3VPN forwarding path.

MPLS CORE NETWORK

IGP Configuration: IS–IS

P01

```
router isis NEO
 is–type level–2–only
 net 49.1500.5280.2028.8143.00
 address–family ipv4 unicast
  metric–style wide
!
interface Loopback0
 address–family ipv4 unicast
!
interface GigabitEthernet0/0/0/0
 point–to–point
 hello–interval 3
 hello–multiplier 4
 address–family ipv4 unicast
!
interface GigabitEthernet0/0/0/1
 point–to–point
```

```
 hello-interval 3
 hello-multiplier 4
 address-family ipv4 unicast
 !
```

PE01

```
router isis NEO
 net 49.1500.5280.2028.8144.00
 is-type level-2-only
 metric-style wide
!
interface GigabitEthernet1
ip router isis NEO
isis network point-to-point
 isis hello-multiplier 4
 isis hello-interval 3
!
```

PE02

```
router isis NEO
 net 49.1500.5280.2028.8145.00
 is-type level-2-only
 metric-style wide
!
interface GigabitEthernet1
ip router isis NEO
```

```
isis network point-to-point
 isis hello-multiplier 4
 isis hello-interval 3
!
```

Configure MPLS in Respective Interfaces

```
!
```

VRF Configuration

PE01

```
ip vrf STORAGE
 rd 65000:1001
 route-target both 65000:1001
!
ip vrf TELE
 rd 65000:1000
 route-target both 65000:1000
 !
interface GigabitEthernet2
 ip vrf forwarding TELE
 ip address 172.16.255.2 255.255.255.252
!
interface GigabitEthernet3
 ip vrf forwarding TELE
 ip address 192.168.0.2 255.255.255.252
!
```

```
interface GigabitEthernet4
 ip vrf forwarding STORAGE
 ip address 172.16.0.2 255.255.255.252
!
```

PE02

```
ip vrf STORAGE
 rd 65000:1001
 route-target both 65000:1001
!
ip vrf TELE
 rd 65000:1000
 route-target both 65000:1000
 !
interface GigabitEthernet2
 ip vrf forwarding TELE
 ip address 172.16.255.254 255.255.255.252
!
interface GigabitEthernet3
 ip vrf forwarding TELE
 ip address 192.168.1.2 255.255.255.252
!
interface GigabitEthernet4
 ip vrf forwarding STORAGE
 ip address 172.16.1.2 255.255.255.252
```

MP-BGP Configuration

P01

```
router bgp 65000
 bgp router-id 10.255.255.1
 address-family ipv4 unicast
 !
 address-family vpnv4 unicast
 !
 neighbor 10.255.255.2
  remote-as 65000
  password kolwin!!!!
  update-source Loopback0
  address-family ipv4 unicast
   route-reflector-client
  !
  address-family vpnv4 unicast
   route-reflector-client
  !
 !
 neighbor 10.255.255.3
  remote-as 65000
  password kolwin!!!!
  update-source Loopback0
  address-family ipv4 unicast
```

```
  route-reflector-client
 !
 address-family vpnv4 unicast
  route-reflector-client
 !
```

PE01

```
router bgp 65000
 bgp router-id 10.255.255.2
 neighbor 10.255.255.1 remote-as 65000
 neighbor 10.255.255.1 password kolwin!!!!
 neighbor 10.255.255.1 update-source Loopback0
 !
 address-family ipv4
  neighbor 10.255.255.1 activate
 exit-address-family
 !
 address-family vpnv4
  neighbor 10.255.255.1 activate
  neighbor 10.255.255.1 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf STORAGE
  network 172.16.0.0 mask 255.255.255.252
 exit-address-family
```

```
 address-family ipv4 vrf TELE
  network 172.16.255.0 mask 255.255.255.252
  network 192.168.0.0 mask 255.255.255.252
 !
```

PE02

```
router bgp 65000
 bgp router-id 10.255.255.3
 bgp log-neighbor-changes
 neighbor 10.255.255.1 remote-as 65000
 neighbor 10.255.255.1 password kolwin!!!!
 neighbor 10.255.255.1 update-source Loopback0
 !
 address-family ipv4
  neighbor 10.255.255.1 activate
 exit-address-family
 !
 address-family vpnv4
  neighbor 10.255.255.1 activate
  neighbor 10.255.255.1 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf STORAGE
  network 172.16.1.0 mask 255.255.255.252
 exit-address-family
```

```
 address-family ipv4 vrf TELE
  network 172.16.255.252 mask 255.255.255.252
  network 192.168.1.0 mask 255.255.255.252
 !
```

IPSEC Configuration

PE01

```
crypto ikev2 proposal PE-PROPOSAL
 encryption aes-cbc-256
 integrity sha512
 group 14
 !
crypto ikev2 policy PE-POLICY
 proposal PE-PROPOSAL
!
crypto ikev2 keyring PE-KEYRING
 peer PE02
  address 172.16.192.169
  pre-shared-key local kolwin!!!!
  pre-shared-key remote kolwin!!!!
 !
 crypto ikev2 profile PE-PROFILE
 match identity remote address 172.16.192.169 255.255.255.252
 authentication local pre-share
 authentication remote pre-share
```

```
 keyring local PE-KEYRING
 !
crypto ipsec transform-set PE-SET esp-aes esp-sha512-hmac
!
crypto ipsec profile PE-IPSEC-PROFILE
 set transform-set PE-SET
 set ikev2-profile PE-PROFILE
 !
 interface Tunnel24
 ip vrf forwarding TELE
 ip address 192.168.172.17 255.255.255.252
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel source 10.180.6.9
 tunnel destination 172.16.192.169
 tunnel protection ipsec profile PE-IPSEC-PROFILE
!
PE02
crypto ikev2 proposal PE-PROPOSAL
 encryption aes-cbc-256
 integrity sha512
 group 14
 !
crypto ikev2 policy PE-POLICY
```

```
 proposal PE-PROPOSAL
 !
crypto ikev2 keyring PE-KEYRING
 peer PE01
  address 10.180.6.9
  pre-shared-key local kolwin!!!!
  pre-shared-key remote kolwin!!!!
!
crypto ikev2 profile PE-PROFILE
 match identity remote address 10.180.6.9 255.255.255.252
 authentication local pre-share
 authentication remote pre-share
 keyring local PE-KEYRING
 !
crypto ipsec transform-set PE-SET esp-aes esp-sha512-hmac
!
crypto ipsec profile PE-IPSEC-PROFILE
 set transform-set PE-SET
 set ikev2-profile PE-PROFILE
!
 interface Tunnel24
 ip vrf forwarding TELE
 ip address 192.168.172.18 255.255.255.252
 ip mtu 1400
```

ip tcp adjust–mss 1360

tunnel source 172.16.192.169

tunnel destination 10.180.6.9

tunnel protection ipsec profile **PE–IPSEC–PROFILE**

!

Selective VRF Traffic Steering over PE–PE IPsec Tunnel

PE01

ip route vrf **TELE** 172.16.255.252 255.255.255.252 Tunnel24

!

PE02

ip route vrf **TELE** 172.16.255.0 255.255.255.252 Tunnel24

!

Verfication

IPSec on PE01

```
PE01#show crypto ipsec sa

interface: Tunnel24
    Crypto map tag: Tunnel24-head-0, local addr 10.180.6.9

   protected vrf: TELE
   local  ident (addr/mask/prot/port): (10.180.6.9/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.192.169/255.255.255.255/47/0)
   current_peer 172.16.192.169 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 361, #pkts encrypt: 361, #pkts digest: 361
    #pkts decaps: 360, #pkts decrypt: 360, #pkts verify: 360
```

```
PE01#sh crypto session
Crypto session current status

Interface: Tunnel24
Profile: PE-PROFILE
Session status: UP-ACTIVE
Peer: 172.16.192.169 port 500
  Session ID: 5
  IKEv2 SA: local 10.180.6.9/500 remote 172.16.192.169/500 Active
  IPSEC FLOW: permit 47 host 10.180.6.9 host 172.16.192.169
        Active SAs: 2, origin: crypto map
```

IPSec on PE02

```
PE02#sh crypto session
Crypto session current status

Interface: Tunnel24
Profile: PE-PROFILE
Session status: UP-ACTIVE
Peer: 10.180.6.9 port 500
  Session ID: 8
  IKEv2 SA: local 172.16.192.169/500 remote 10.180.6.9/500 Active
  IPSEC FLOW: permit 47 host 172.16.192.169 host 10.180.6.9
        Active SAs: 2, origin: crypto map
```

```
PE02#sh crypto ipsec sa

interface: Tunnel24
    Crypto map tag: Tunnel24-head-0, local addr 172.16.192.169

   protected vrf: TELE
   local  ident (addr/mask/prot/port): (172.16.192.169/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.180.6.9/255.255.255.255/47/0)
   current_peer 10.180.6.9 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 360, #pkts encrypt: 360, #pkts digest: 360
    #pkts decaps: 361, #pkts decrypt: 361, #pkts verify: 361
```

User POV: PHONE01

```
PHONE01#ping 172.16.255.253 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 172.16.255.253, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 8/15/32 ms
```

```
PHONE01#traceroute 172.16.255.253
Type escape sequence to abort.
Tracing the route to 172.16.255.253
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.255.2 8 msec 8 msec 12 msec
  2 192.168.172.18 12 msec 8 msec 12 msec
  3 172.16.255.253 12 msec *  12 msec
```

"Use the IPSec Tunnel"

User POV: PC01

```
PC01> ping 192.168.1.1

84 bytes from 192.168.1.1 icmp_seq=1 ttl=61 time=9.812 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=61 time=10.842 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=61 time=9.346 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=61 time=8.818 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=61 time=9.788 ms

PC01> trace 192.168.1.1
trace to 192.168.1.1, 8 hops max, press Ctrl+C to stop
 1   192.168.0.2   4.260 ms  3.049 ms  3.788 ms
 2   10.180.6.10   17.112 ms  8.290 ms  8.311 ms
 3   192.168.1.2   11.802 ms  9.621 ms  9.442 ms
 4   *192.168.1.1   9.322 ms (ICMP type:3, code:3, Destination port unreachable)
```

User POV: SVR01

```
SVR01> ping 172.16.1.1

84 bytes from 172.16.1.1 icmp_seq=1 ttl=61 time=10.883 ms
84 bytes from 172.16.1.1 icmp_seq=2 ttl=61 time=8.349 ms
84 bytes from 172.16.1.1 icmp_seq=3 ttl=61 time=10.702 ms
84 bytes from 172.16.1.1 icmp_seq=4 ttl=61 time=9.806 ms
84 bytes from 172.16.1.1 icmp_seq=5 ttl=61 time=9.272 ms

SVR01> trace 172.16.1.1
trace to 172.16.1.1, 8 hops max, press Ctrl+C to stop
 1   172.16.0.2   4.084 ms  3.411 ms  3.844 ms
 2   10.180.6.10   7.481 ms  7.716 ms  7.646 ms
 3   172.16.1.2   9.895 ms  10.048 ms  9.040 ms
 4   *172.16.1.1   9.637 ms (ICMP type:3, code:3, Destination port unreachable)
```

User POV: PHONE02

```
PHONE02#ping 172.16.255.1 repeat 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 172.16.255.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 20/20/32 ms
```

```
PHONE02#traceroute 172.16.255.1
Type escape sequence to abort.
Tracing the route to 172.16.255.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.255.254 16 msec 8 msec 8 msec
  2 192.168.172.17 12 msec 12 msec 12 msec
  3 172.16.255.1 20 msec *  16 msec
```

"Use the IPSec Tunnel"

User POV: PC02

```
PC02> ping 192.168.0.1

84 bytes from 192.168.0.1 icmp_seq=1 ttl=61 time=15.497 ms
84 bytes from 192.168.0.1 icmp_seq=2 ttl=61 time=10.811 ms
84 bytes from 192.168.0.1 icmp_seq=3 ttl=61 time=10.771 ms
84 bytes from 192.168.0.1 icmp_seq=4 ttl=61 time=10.541 ms
84 bytes from 192.168.0.1 icmp_seq=5 ttl=61 time=10.389 ms

PC02> trace 192.168.0.1
trace to 192.168.0.1, 8 hops max, press Ctrl+C to stop
 1   192.168.1.2   3.925 ms  3.866 ms  3.786 ms
 2   172.16.192.170   9.856 ms  7.593 ms  7.361 ms
 3   192.168.0.2   10.335 ms  8.244 ms  9.400 ms
 4   *192.168.0.1   10.157 ms (ICMP type:3, code:3, Destination port unreachable)
```

User POV: SVR02

```
SVR02> ping 172.16.0.1

84 bytes from 172.16.0.1 icmp_seq=1 ttl=61 time=14.291 ms
84 bytes from 172.16.0.1 icmp_seq=2 ttl=61 time=11.596 ms
84 bytes from 172.16.0.1 icmp_seq=3 ttl=61 time=11.114 ms
84 bytes from 172.16.0.1 icmp_seq=4 ttl=61 time=11.398 ms
84 bytes from 172.16.0.1 icmp_seq=5 ttl=61 time=11.202 ms

SVR02> trace 172.16.0.1
trace to 172.16.0.1, 8 hops max, press Ctrl+C to stop
 1   172.16.1.2   3.863 ms  2.873 ms  3.080 ms
 2   172.16.192.170   8.847 ms  8.299 ms  8.513 ms
 3   172.16.0.2   9.674 ms  10.014 ms  8.487 ms
 4   *172.16.0.1   10.451 ms (ICMP type:3, code:3, Destination port unreachable)
```

Ko Lwin (Network)