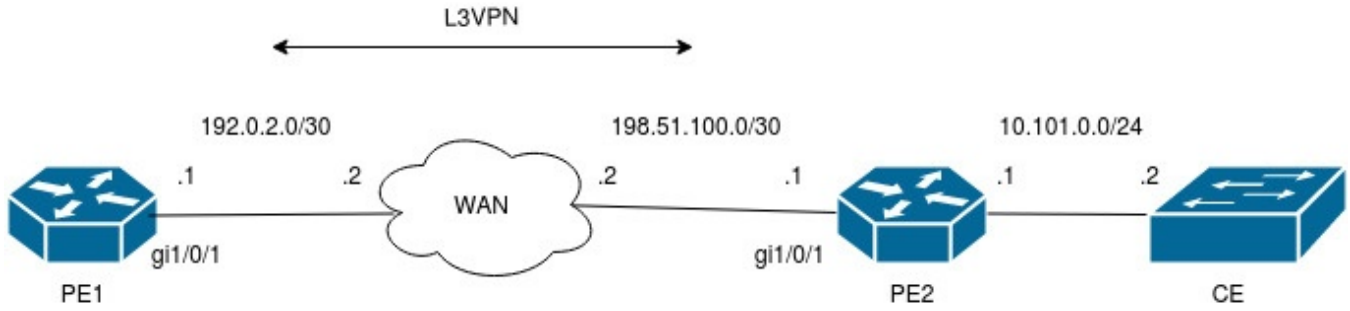
ssh/telnet Firewall



:

1.20.4 Firewall MPLS (`ip firewall disable` , MPLS). CE ssh/telnet PE1(ESR) L3VPN.

:

ssh/telnet `ip ssh access-addresses vrf VRF <object-group name>/ip telnet access-addresses vrf VRF <object-group name>`. L3VPN over GRE Firewall (`ip firewall disable`) tunnel gre.

PE1:

```
PE1# sh ru
hostname PE1

object-group network ssh_access
  ip prefix 192.168.30.0/24
exit
object-group network telnet_access
  ip prefix 10.101.0.0/24
  ip prefix 192.168.30.0/24
exit

ip vrf VRF
  ip protocols bgp max-routes 10
  rd 1:1
  route-target export 1:1
  route-target import 1:1
exit

syslog file tmpsys:syslog/debug
  severity debug
exit

security zone untrusted
exit

router bgp 1
  neighbor 172.16.1.2
    remote-as 1
    update-source gre 1
    address-family ipv4 unicast
      send-label
      enable
    exit
    enable
  exit
  neighbor 192.168.1.2
    remote-as 1
    update-source loopback 1
    address-family vpnv4 unicast
      send-community extended
      enable
    exit
```

```
    enable
  exit
  address-family ipv4 unicast
    network 192.168.1.1/32
  exit
  enable
  vrf VRF
    address-family ipv4 unicast
      redistribute connected
    exit
  exit
exit


interface gigabitethernet 1/0/1
  description "WAN"
  security-zone untrusted
  ip address 192.0.2.1/30
exit
interface loopback 1
  ip address 192.168.1.1/32
exit
interface loopback 2
  ip vrf forwarding VRF
  description "Management_ip"
  ip address 192.168.20.1/32
exit
tunnel gre 1
  description "to_PE2"
  mtu 1472
  ip firewall disable
  local address 192.0.2.1
  remote address 198.51.100.1
  ip address 172.16.1.1/30
  enable
exit

mpls
  forwarding interface gre 1
exit
security zone-pair untrusted self
  rule 1
    action permit
    match protocol gre
    enable
  exit
exit

ip route 198.51.100.0/30 192.0.2.2

ip telnet server vrf VRF
ip telnet access-addresses vrf VRF telnet_access
ip ssh server vrf VRF
ip ssh access-addresses vrf VRF ssh_access

PE1# sh bgp neighbors
BGP neighbor is 172.16.1.2
    BGP state:                      Established
    Type:                           Static neighbor
    Neighbor address:               172.16.1.2
    Neighbor AS:                    1
    Neighbor ID:                    192.168.1.2
    Neighbor caps:                  refresh enhanced-refresh restart-aware AS4
    Session:                        internal multihop AS4
    Source address:                 172.16.1.1
    Weight:                         0
    Hold timer:                     103/180
    Keepalive timer:                19/60
    Address family ipv4 unicast:
      Send-label:                   Yes
      Default originate:            No
```

```
      Default information originate: No
    Uptime:                          178 s
BGP neighbor is 192.168.1.2
    BGP state:                       Established
    Type:                            Static neighbor
    Neighbor address:                192.168.1.2
    Neighbor AS:                     1
    Neighbor ID:                     192.168.1.2
    Neighbor caps:                   refresh enhanced-refresh restart-aware AS4
    Session:                         internal multihop AS4
    Source address:                  192.168.1.1
    Weight:                          0
    Hold timer:                      137/180
    Keepalive timer:                 29/60
    Address family vpnv4 unicast:
    Uptime:                          131 s
PE1#
PE1# sh bgp vpnv4 unicast all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   IP Prefix          Next hop        Metric     Label   LocPrf     Weight
Path
----- --------------------- ------------------ --------------- ---------- ------- ---------- ------
----------------
*>i   1:1                   192.168.40.0/24    192.168.1.2     --         16      100        0      ?
*>i   1:1                   192.168.30.0/24    192.168.1.2     --         16      100        0      ?
*>    1:1                   192.168.20.1/32    --              --         16      --         --     ?
```

PE2:

```
PE2# sh ru
hostname PE2

ip vrf VRF
  ip protocols bgp max-routes 10
  rd 1:1
  route-target export 1:1
  route-target import 1:1
exit

security zone untrusted
exit

router bgp 1
  neighbor 172.16.1.1
    remote-as 1
    update-source gre 1
    address-family ipv4 unicast
      send-label
      enable
    exit
    enable
  exit
  neighbor 192.168.1.1
    remote-as 1
    update-source loopback 1
    address-family vpnv4 unicast
      send-community extended
      enable
    exit
    enable
  exit
  address-family ipv4 unicast
    network 192.168.1.2/32
  exit
  enable
  vrf VRF
    address-family ipv4 unicast
```

```
      redistribute connected
    exit
  exit
exit

interface gigabitethernet 1/0/1
  description "WAN"
  security-zone untrusted
  ip address 198.51.100.1/30
exit
interface gigabitethernet 1/0/2
  ip vrf forwarding VRF
  ip firewall disable
  ip address 192.168.30.1/24
  ip address 192.168.40.1/24
exit
interface loopback 1
  ip address 192.168.1.2/32
exit

tunnel gre 1
  mtu 1472
  ip firewall disable
  local address 198.51.100.1
  remote address 192.0.2.1
  ip address 172.16.1.2/30
  enable
exit

mpls
  forwarding interface gre 1
exit

security zone-pair untrusted self
  rule 1
    action permit
    match protocol gre
    enable
  exit
exit

ip route 192.0.2.0/30 198.51.100.2

PE2# sh bgp neighbors
BGP neighbor is 172.16.1.1
    BGP state:                        Established
    Type:                             Static neighbor
    Neighbor address:                 172.16.1.1
    Neighbor AS:                      1
    Neighbor ID:                      192.168.1.1
    Neighbor caps:                    refresh enhanced-refresh restart-aware AS4
    Session:                          internal multihop AS4
    Source address:                   172.16.1.2
    Weight:                           0
    Hold timer:                       132/180
    Keepalive timer:                  29/60
    Address family ipv4 unicast:
      Send-label:                     Yes
      Default originate:              No
      Default information originate: No
    Uptime:                           270 s
BGP neighbor is 192.168.1.1
    BGP state:                        Established
    Type:                             Static neighbor
    Neighbor address:                 192.168.1.1
    Neighbor AS:                      1
    Neighbor ID:                      192.168.1.1
    Neighbor caps:                    refresh enhanced-refresh restart-aware AS4
    Session:                          internal multihop AS4
    Source address:                   192.168.1.2
    Weight:                           0
```

```
    Hold timer:                     161/180
    Keepalive timer:                50/60
    Address family vpnv4 unicast:
    Uptime:                         223 s
PE2#
PE2#
PE2# sh bgp vpnv4 unicast all
Status codes: * - valid, > - best, i - internal, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Codes Route Distinguisher   IP Prefix          Next hop        Metric     Label   LocPrf     Weight
Path
----- --------------------- ------------------ --------------- ---------- ------- ---------- ------
----------------
*>    1:1                   192.168.40.0/24    --              --         16      --         --     ?
*>    1:1                   192.168.30.0/24    --              --         16      --         --     ?
*>i   1:1                   192.168.20.1/32    192.168.1.1     --         16      100        0      ?
```

ssh CE 192.168.30.0/24 PE1:

```
PE1# sh users
SID    User name              Logged in at        Host                  Timers Login/Priv   level
----   --------------------   -----------------   -------------------   -----------------   -----
1      admin                  16/01/24 04:38:10   192.168.30.2          00:29:54/00:00:00   15

PE1# monitor gre 1
04:39:40.136173  In ethertype MPLS unicast (0x8847), length 136: MPLS (label 16, exp 0, [S], ttl 63)
        (tos 0x10, ttl 63, id 25340, offset 0, flags [DF], proto TCP (6), length 116)
    192.168.30.2.34068 > 192.168.20.1.22: Flags [P.], cksum 0x4eb1 (correct), seq 421000999:421001063, ack
1498711829, win 276, options [nop,nop,TS val 336768366 ecr 34812582], length 64
04:39:40.137460 Out ethertype MPLS unicast (0x8847), length 72: MPLS (label 16, exp 0, [S], ttl 64)
        (tos 0x80, ttl 64, id 25785, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.20.1.22 > 192.168.30.2.34068: Flags [.], cksum 0x518d (correct), ack 64, win 432, options [nop,nop,
TS val 34813573 ecr 336768366], length 0
```

telnet CE 192.168.30.0/24 PE1:

```
PE1# sh users
SID    User name              Logged in at        Host                  Timers Login/Priv   level
----   --------------------   -----------------   -------------------   -----------------   -----
1      admin                  16/01/24 04:43:39   192.168.30.2          00:29:53/00:00:00   15

PE1# monitor gre 1
04:44:01.778469  In ethertype MPLS unicast (0x8847), length 74: MPLS (label 16, exp 0, [S], ttl 63)
        (tos 0x0, ttl 63, id 19073, offset 0, flags [DF], proto TCP (6), length 54)
    192.168.30.2.53088 > 192.168.20.1.23: Flags [P.], cksum 0x47a4 (correct), seq 1:3, ack 1, win 206, options
[nop,nop,TS val 336794529 ecr 34837663], length 2
04:44:01.795869 Out ethertype MPLS unicast (0x8847), length 74: MPLS (label 16, exp 0, [S], ttl 64)
        (tos 0x80, ttl 64, id 17980, offset 0, flags [DF], proto TCP (6), length 54)
    192.168.20.1.23 > 192.168.30.2.53088: Flags [P.], cksum 0x3f74 (correct), seq 1:3, ack 3, win 224, options
[nop,nop,TS val 34839739 ecr 336794529], length 2
```

ssh/telnet CE 192.168.40.0/24 PE1:

```
#ssh connect
PE1# monitor gre 1
04:47:32.403406  In ethertype MPLS unicast (0x8847), length 80: MPLS (label 16, exp 0, [S], ttl 63)
        (tos 0x0, ttl 63, id 26830, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.40.2.34014 > 192.168.20.1.22: Flags [S], cksum 0x12a4 (correct), seq 172625192, win 25200, options
[mss 1260,sackOK,TS val 336815590 ecr 0,nop,wscale 7], length 0
04:47:33.396775  In ethertype MPLS unicast (0x8847), length 80: MPLS (label 16, exp 0, [S], ttl 63)
        (tos 0x0, ttl 63, id 26831, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.40.2.34014 > 192.168.20.1.22: Flags [S], cksum 0x1240 (correct), seq 172625192, win 25200, options
[mss 1260,sackOK,TS val 336815690 ecr 0,nop,wscale 7], length 0
04:47:35.396939  In ethertype MPLS unicast (0x8847), length 80: MPLS (label 16, exp 0, [S], ttl 63)
        (tos 0x0, ttl 63, id 26832, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.40.2.34014 > 192.168.20.1.22: Flags [S], cksum 0x1178 (correct), seq 172625192, win 25200, options
[mss 1260,sackOK,TS val 336815890 ecr 0,nop,wscale 7], length 0

#telnet connect
PE1# monitor gre 1
04:48:37.596065  In ethertype MPLS unicast (0x8847), length 80: MPLS (label 16, exp 0, [S], ttl 63)
        (tos 0x0, ttl 63, id 28160, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.40.2.42313 > 192.168.20.1.23: Flags [S], cksum 0x9d16 (correct), seq 1103040861, win 25200, options
[mss 1260,sackOK,TS val 336822109 ecr 0,nop,wscale 7], length 0
04:48:38.589994  In ethertype MPLS unicast (0x8847), length 80: MPLS (label 16, exp 0, [S], ttl 63)
        (tos 0x0, ttl 63, id 28161, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.40.2.42313 > 192.168.20.1.23: Flags [S], cksum 0x9cb2 (correct), seq 1103040861, win 25200, options
[mss 1260,sackOK,TS val 336822209 ecr 0,nop,wscale 7], length 0
04:48:40.590125  In ethertype MPLS unicast (0x8847), length 80: MPLS (label 16, exp 0, [S], ttl 63)
        (tos 0x0, ttl 63, id 28162, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.40.2.42313 > 192.168.20.1.23: Flags [S], cksum 0x9bea (correct), seq 1103040861, win 25200, options
[mss 1260,sackOK,TS val 336822409 ecr 0,nop,wscale 7], length 0
```