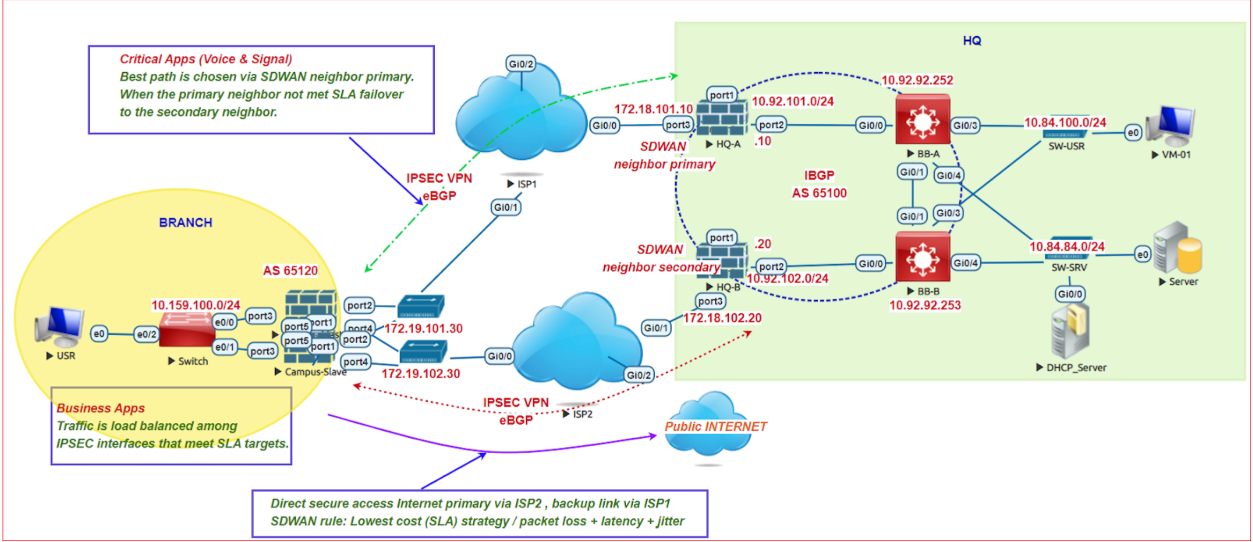
Description

- This Lab describes how to use SD-WAN on FortiGate Firewall control traffic VPN IPSEC and secure INTERNET access.
- A Branch FortiGate has two ISP links for redundancy Internet access.
- At the remote site, two gateways reside in different locations in the Data Center. Two Firewall Gateways connect to Router Backbone using the dynamic routing IBGP.
- Between Branch Firewall and two remote Firewalls at Data Center setup two VPN IPSEC tunnel links for transferring Critical Traffic and Business Traffic.
- Using eBGP routing protocol to exchange the prefixes via VPN IPSEC Tunnel Links.
- DHCP, DNS, RADIUS Servers at Data Center assign IP addresses and manage clients at the Branch site.

Topology



Critical Apps (Voice & Signal)
Best path is chosen via SDWAN neighbor primary. When the primary neighbor not met SLA failover to the secondary neighbor.

Business Apps
Traffic is load balanced among IPSEC interfaces that meet SLA targets.

Direct secure access Internet primary via ISP2 , backup link via ISP1
SDWAN rule: Lowest cost (SLA) strategy / packet loss + latency + jitter

Type of Traffic

No	Type of Traffic	Purpose
1	Critical Apps	- VoIP Signalling SCTP - The traffic for management PC Client as DHCP, DNS, SMTP, RADIUS - Control and Provisioning of Wireless Access Points (CAPWAP)
2	Business Apps	- The rest traffic exchange between Branch and Data Center
3	Secure Internet	- The traffic goes out Public Internet: HTTP, HTTPS, ICMP

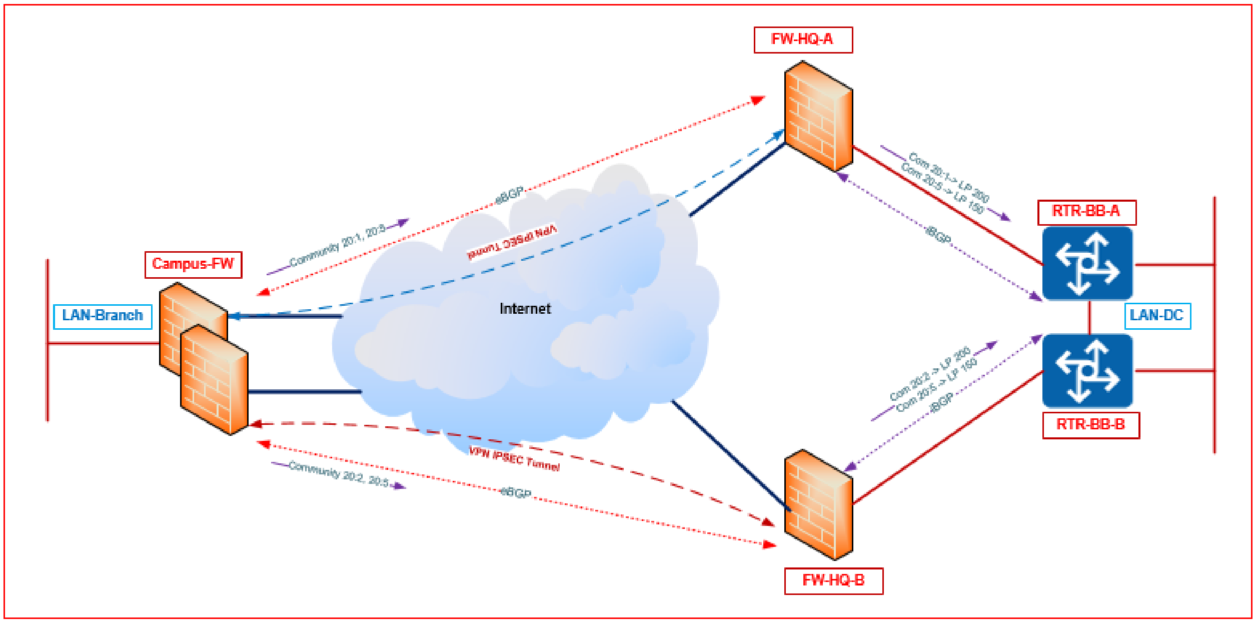
Requirement

1. Critical Apps Traffic are VoIP traffic, signaling traffic as SCTP, CAPWAP, DHCP, DNS, Radius shall transfer via primary IPSEC Tunnel to SD-WAN primary neighbor if it's SLA meets the threshold. And the backup link via secondary IPSEC Tunnel to SD-WAN secondary neighbor. The SLA threshold use three items include packet loss ratio, latency, and jitter.
2. Business Apps Traffic is the rest of Traffic exchange between Branch site and Data Center Site will be load balancer via two links IPSEC Tunnel when they meet the SLA threshold.
3. Secure Internet Traffic uses the primary link via ISP2 and the backup link via ISP1.
4. Marking DSCP 46 (EF) for Critical Traffic and DSCP 34 (AF41) for Business Traffic, other traffic shall be marked to DSCP 0 (BE).
5. A traffic shaping policy applied to the outgoing WAN interface to indicate the priority of Critical_Apps, Business_Apps, and Others.

Solution:

1. Configure BGP routing between the Branch Firewall with two Firewalls at the Data Center site. Use Performance SLA to health check the status of SD-WAN neighbors.

Case	Status	SD-WAN neighbor status	BGP community advertised
Health Check VPN1 link	OK	Primary	To primary: 20:1 To secondary: 20:5
Health Check VPN2 link	OK		
Health Check VPN1 link	OK	Primary	To primary: 20:1 To secondary: 20:5
Health Check VPN2 link	NOK		
Health Check VPN1 link	NOK	Secondary	To primary: 20:5 To secondary: 20:2
Health Check VPN2 link	OK		
Health Check VPN1 link	NOK	Standalone	To primary: 20:5 To secondary: 20:5
Health Check VPN2 link	NOK		



2. Create SD-WAN Rules for Critical Traffic to SD-WAN primary neighbor, backup link to SD-WAN secondary neighbor.
3. Create An SD-WAN Rule for load balancing Business Traffic.
4. Create An SD-WAN Rule for Secure Internet with the primary link via ISP2, the backup link via ISP1.
5. Marking DSCP for the outgoing traffic on SD-WAN Rule follows the table:

Type of Traffic	**DSCP marking**
Critical_Apps	46
Business_Apps	34
Other	0

6. Apply The Traffic Policy Profile to the outgoing WAN Interfaces

Class of Traffic	**Guaranteed Bandwidth**	**Maximum Bandwidth**	**Priority**
Critical_Apps	90%	100%	critical
Business_Apps	8%	100%	high
Others	2%	100%	low

Configuration Roadmap

1. **Basic configuration on Three Firewalls: HA, Interface, management:**

At The Data Center

a. **Create interfaces**

```
HQ-A # config system interface
    edit "port2"
        set vdom "root"
        set ip 10.92.101.10 255.255.255.0
        set type physical
        set alias "Inside"
        set role lan
    next
    edit "port3"
        set vdom "root"
        set ip 172.18.101.10 255.255.255.0
        set type physical
        set alias "WAN"
        set estimated-upstream-bandwidth 2000
        set estimated-downstream-bandwidth 2000
        set role wan
    next
end
```

```
HQ-B # config system interface
    edit "port2"
        set vdom "root"
        set ip 10.92.102.20 255.255.255.0
        set type physical
        set alias "Internal"
        set role lan
    next
    edit "port3"
        set vdom "root"
        set ip 172.18.102.20 255.255.255.0
        set type physical
        set alias "WAN"
        set estimated-upstream-bandwidth 2000
        set estimated-downstream-bandwidth 2000
        set role wan
    next
end
```

b. Create all subnets in Data Center and Branch Sites

```
HQ-A # config firewall address
    edit "LAN-BR"
        set subnet 10.159.100.0 255.255.255.0
    next
    edit "LAN-SRV"
        set subnet 10.84.84.0 255.255.255.0
    next
    edit "LAN-USR"
        set subnet 10.84.100.0 255.255.255.0
    next
    edit "INTERNAL_HQ_A"
        set subnet 10.92.101.0 255.255.255.0
    next
    edit "TUNNEL_ADD"
        set subnet 10.1.1.0 255.255.255.252
    next
end
HQ-A # config firewall addrgrp
    edit "LAN-HQ"
        set member "LAN-SRV" "LAN-USR" "INTERNAL_HQ_A"
    next
    edit "VPN_via_BGP"
        set member "INTERNAL_HQ_A" "LAN-BR" "LAN-SRV" "LAN-USR" "TUNNEL_ADD"
    next
end
```

```
HQ-B # config firewall address
    edit "LAN-BR"
        set subnet 10.159.100.0 255.255.255.0
    next
    edit "LAN-SRV"
        set subnet 10.84.84.0 255.255.255.0
    next
    edit "LAN-USR"
        set subnet 10.84.100.0 255.255.255.0
    next
    edit "INTERNAL_HQ_B"
        set subnet 10.92.102.0 255.255.255.0
    next
    edit "TUNNEL_ADD"
        set subnet 10.1.1.4 255.255.255.252
    next
end
HQ-B # config firewall addrgrp
    edit "LAN-HQ"
        set member "LAN-SRV" "LAN-USR" "INTERNAL_HQ_B"
    next
    edit "VPN_via_BGP"
        set member "INTERNAL_HQ_B" "LAN-BR" "LAN-SRV" "LAN-USR" "TUNNEL_ADD"
    next
end
```

c. Configure the iBGP routing between two firewalls and Router Backbone

```
HQ-A # config router bgp
    set as 65100
    set ebgp-multipath enable
    config neighbor
        edit "10.92.101.252"
            set next-hop-self enable
            set remote-as 65100
        next
    end
    config network
        edit 1
            set prefix 10.92.101.0 255.255.255.0
        next
    end
```

```
HQ-B # config router bgp
    set as 65100
    set ebgp-multipath enable
    config neighbor
        edit "10.92.102.253"
            set next-hop-self enable
            set remote-as 65100
        next
    end
    config network
        edit 1
            set prefix 10.92.102.0 255.255.255.0
        next
    end
```

d. Advertise the default static route on Firewall HQ-A (primary) with the local-preference value higher than HQ-B

```
HQ-A # config router route-map
    edit "LP"
```

```
        config rule
            edit 1
                set set-local-preference 120
            next
        end
HQ-A (bgp) #config redistribute "static"
    set status enable
    set route-map "LP"
end
```

At Branch

a. Create interfaces

```
Campus-Master # config system interface
    edit "port2"
        set vdom "root"
        set ip 172.19.101.30 255.255.255.0
        set type physical
        set alias "WAN1"
        set estimated-upstream-bandwidth 2000
        set estimated-downstream-bandwidth 2000
        set monitor-bandwidth enable
        set role wan
    next
    edit "port3"
        set vdom "root"
        set dhcp-relay-service enable
        set ip 10.159.100.254 255.255.255.0
        set type physical
        set alias "Internal"
        set role lan
        set dhcp-relay-ip "10.84.84.100"
    next
    edit "port4"
        set vdom "root"
        set ip 172.19.102.30 255.255.255.0
        set type physical
        set alias "WAN2"
        set estimated-upstream-bandwidth 2000
        set estimated-downstream-bandwidth 2000
        set monitor-bandwidth enable
        set role wan
    next
```

```
end
```

b. Create all Subnets in Data Center and Branch Sites

```
Campus-Master # config firewall address
   edit "LAN-BR"
      set subnet 10.159.100.0 255.255.255.0
   next
   edit "LAN-USR"
      set subnet 10.84.100.0 255.255.255.0
   next
   edit "LAN-SRV"
      set subnet 10.84.84.0 255.255.255.0
   next
   edit "INTERNAL_HQ_A"
      set subnet 10.92.101.0 255.255.255.0
   next
   edit "INTERNAL_HQ_B"
      set subnet 10.92.102.0 255.255.255.0
   next
   edit "TUNNEL_ADD"
      set subnet 10.1.1.0 255.255.255.248
   next
end
Campus-Master # config firewall addrgrp
   edit "LAN-HQ"
      set member "LAN-SRV" "LAN-USR" "INTERNAL_HQ_A" "INTERNAL_HQ_B"
   next
   edit "VPN_via_BGP"
      set member "INTERNAL_HQ_A" "INTERNAL_HQ_B" "LAN-BR" "LAN-SRV" "LAN-USR"
"TUNNEL_ADD"
   next
end
```

2. Configure Internet access via SD-WAN

At The Data Center

a. Create New SD-WAN Zone name INTERNET

```
HQ-A # config system sdwan
   set status enable
   config zone
      edit "INTERNET"
```

```
        next
    end
```

```
HQ-B # config system sdwan
    set status enable
    config zone
        edit "INTERNET"
        next
    end
```

b. Add WAN interface member into INTERNET Zone

```
HQ-A (sdwan) # config members
    edit 1
        set interface "port3"
        set zone "INTERNET"
        set gateway 172.18.101.1
    next
```

```
HQ-B (sdwan) # config members
    edit 1
        set interface "port3"
        set zone "INTERNET"
        set gateway 172.18.102.1
    next
```

c. Add the default static route via SD-WAN interface

```
HQ-A # config router static
    edit 1
        set distance 1
        set sdwan enable
    next
end
```

```
HQ-B # config router static
    edit 1
        set distance 1
        set sdwan enable
    next
end
```

d. Add Firewall Policy for secure access internet: icmp, http, https

```
HQ-A # config firewall policy
    edit 1
        set name "INTERNET"
        set srcintf "port2"
        set dstintf "INTERNET"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL_ICMP" "HTTP" "HTTPS"
        set nat enable
    next
end
```

```
HQ-B # config firewall policy
    edit 1
        set name "INTERNET"
        set srcintf "port2"
        set dstintf "INTERNET"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

e. Configure Performance SLA to health check Google Server

```
HQ-A (sdwan) # config health-check
    edit "CheckINTERNET"
        set server "8.8.8.8"
        set interval 500
        set probe-timeout 500
        set failtime 5
        set recoverytime 5
        set probe-count 30
        set update-cascade-interface enable
        set update-static-route enable
        set members 1
        config sla
            edit 1
                set latency-threshold 50
                set jitter-threshold 50
                set packetloss-threshold 2
            next
        end
    next
end
```

```
HQ-B (sdwan) # config health-check
    edit "CheckINTERNET"
        set server "8.8.8.8"
        set interval 500
        set probe-timeout 500
        set failtime 5
        set recoverytime 5
        set probe-count 30
        set update-cascade-interface enable
        set update-static-route enable
        set members 1
        config sla
            edit 1
                set latency-threshold 50
                set jitter-threshold 50
                set packetloss-threshold 2
            next
        end
    next
end
```

f. Configure SD-WAN rule for access Internet

```
HQ-A (sdwan) # config service
     edit 2
        set name "INTERNET"
        set mode sla
        set dst "all"
        set src "LAN-HQ"
        set dscp-forward enable
        set dscp-reverse enable
        config sla
            edit "CheckINTERNET"
```

```
                set id 1
            next
        end
        set priority-members 1
    next
end
```

```
HQ-B (sdwan) # config service
     edit 2
        set name "INTERNET"
        set mode sla
        set dst "all"
        set src "LAN-HQ"
        set dscp-forward enable
        set dscp-reverse enable
        config sla
            edit "CheckINTERNET"
                set id 1
            next
        end
        set priority-members 1
    next
end
```

At Branch

a. **Create New SD-WAN Zone name INTERNET**

```
Campus-Master (sdwan) # config zone
    edit "INTERNET"
    next
end
```

b. **Add two WAN interface members into INTERNET Zone**

```
Campus-Master (sdwan) # config members
    edit 1
        set interface "port2"
        set zone "INTERNET"
        set gateway 172.19.101.1
        set cost 10
    next
    edit 2
        set interface "port4"
    set zone "INTERNET"
    set gateway 172.19.102.1
    set cost 5
  next
```

c. Add the default static route via SD-WAN interface

```
Campus-Master # config router static
  edit 1
    set distance 1
    set sdwan enable
  next
end
```

d. Add Firewall Policy for secure access internet: icmp, http, https

```
Campus-Master # config firewall policy
  edit 1
    set name "INTERNET"
    set srcintf "port3"
    set dstintf "INTERNET"
    set srcaddr "LAN-BR"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL_ICMP" "HTTP" "HTTPS"
    set nat enable
  next
end
```

e. Configure Performance SLA to health check Google Server

```
Campus-Master (sdwan) # config health-check
  edit "CheckINTERNET"
    set server "8.8.8.8"
    set interval 500
    set probe-timeout 500
    set failtime 5
    set recoverytime 5
    set probe-count 30
    set update-cascade-interface enable
```

```
        set update-static-route enable
        set members 1 2
        config sla
            edit 1
                set latency-threshold 50
                set jitter-threshold 50
                set packetloss-threshold 2
            next
        end
    next
end
```

f. Create An SD-WAN Rule allows the primary link via WAN2 and the backup link via WAN1

```
Campus-Master (sdwan) #  config service
     edit 2
        set name "INTERNET"
        set mode sla
        set dst "all"
        set src "all"
        set dscp-forward enable
        set dscp-reverse enable
        config sla
            edit "CheckINTERNET"
                set id 1
            next
        end
        set priority-members 1 2
    next
end
```

3. Configure VPN IPSEC Tunnel using SD-WAN control traffic

At The Data Center

a. Create VPN IPSEC Tunnel

```
HQ-A #  config vpn ipsec phase1-interface
    edit "VPN_to_BR_port2"
        set interface "port3"
        set peertype any
        set net-device disable
        set proposal des-md5 des-sha1
        set comments "VPN_to_BR_port2"
        set nattraversal disable
        set remote-gw 172.19.101.30
        set psksecret 123456
   next
end
HQ-A #   config vpn ipsec phase2-interface
    edit "VPN_to_BR_port2"
        set phase1name "VPN_to_BR_port2"
        set proposal des-md5 des-sha1
        set src-addr-type name
        set dst-addr-type name
        set src-name "VPN_via_BGP"
        set dst-name "VPN_via_BGP"
    next
end
HQ-A # config system interface
    edit "VPN_to_BR_port2"
        set vdom "root"
        set ip 10.1.1.1 255.255.255.255
        set type tunnel
         set remote-ip 10.1.1.2 255.255.255.252
        set interface "port3"
    next
end
```

```
HQ-B #   config vpn ipsec phase1-interface
    edit "VPN_to_BR"
        set interface "port3"
        set peertype any
        set net-device disable
        set proposal des-md5 des-sha1
        set nattraversal disable
        set remote-gw 172.19.102.30
        set psksecret 123456
    next
end
HQ-B #   config vpn ipsec phase2-interface
    edit "VPN_to_BR"
        set phase1name "VPN_to_BR"
        set proposal des-md5 des-sha1
        set src-addr-type name
        set dst-addr-type name
        set src-name "VPN_via_BGP"
        set dst-name "VPN_via_BGP"
    next
end
HQ-B # config system interface
    edit "VPN_to_BR"
        set vdom "root"
        set ip 10.1.1.5 255.255.255.255
        set type tunnel
        set remote-ip 10.1.1.6 255.255.255.252
        set interface "port3"
    next
end
```

b. Configure eBGP routing with Branch Firewall

```
HQ-A #   config router bgp
    config neighbor
        edit "10.1.1.2"
            set soft-reconfiguration enable
            set remote-as 65120
        next
    end
    config network
        edit 1
            set prefix 10.92.101.0 255.255.255.0
        next
    end
```

```
HQ-B # config router bgp
    config neighbor
        edit "10.1.1.6"
            set soft-reconfiguration enable
            set remote-as 65120
        next
    end
    config network
        edit 1
            set prefix 10.92.102.0 255.255.255.0
        next
    end
```

c. Create new SD-WAN Zone name VPN and assign SD-WAN members into this Zone

```
HQ-A # config system sdwan
  config zone
    edit "VPN"
    next
  end
  config members
    edit 2
      set interface "VPN_to_BR_port2"
      set zone "VPN"
      set source 10.92.101.10
    next
  end
```

```
HQ-B # config system sdwan
  config zone
    edit "VPN"
    next
  end
  config members
    edit 2
      set interface "VPN_to_BR"
      set zone "VPN"
      set source 10.92.102.20
    next
  end
```

d. Create Performance SLA to health check the internal IP address via VPN Link

```
HQ-A # config system sdwan
edit "CheckVPN"
      set server "10.159.100.254"
      set members 2
      config sla
        edit 1
          set latency-threshold 20
          set jitter-threshold 20
        next
      end
    next
  end
```

```
HQ-B # config system sdwan
    edit "CheckVPN"
```

```
      set server "10.159.100.254"
      set members 2
      config sla
        edit 1
          set latency-threshold 20
          set jitter-threshold 20
        next
      end
    next
  end
```

e. Configure Firewall Policies for VPN Traffic and SD-WAN Rules for many types of Traffic via VPN tunnel link

```
HQ-A # config firewall policy
  edit 2
    set name "VPN_IN"
    set srcintf "VPN"
    set dstintf "port2"
    set srcaddr "LAN-BR"
    set dstaddr "LAN-HQ"
    set action accept
    set schedule "always"
    set service "ALL"
    set ssl-ssh-profile "custom-deep-inspection"
  next
  edit 3
    set name "VPN_OUT"
    set srcintf "port2"
    set dstintf "VPN"
    set srcaddr "LAN-HQ"
    set dstaddr "LAN-BR"
    set action accept
    set schedule "always"
    set service "ALL"
    set ssl-ssh-profile "custom-deep-inspection"
  next
end
HQ-A # config system sdwan
  config service
    edit 7
      set name "VPN_SCTP"
      set mode sla
```

```
        set protocol 132
        set dst "LAN-BR"
        set src "LAN-HQ"
        config sla
            edit "CheckVPN"
                set id 1
            next
        end
        set priority-members 2
    next
    edit 3
        set name "VPN_CAPWAP"
        set mode sla
        set protocol 6
        set start-port 5246
        set end-port 5247
        set dst "LAN-BR"
        set src "LAN-HQ"
        config sla
            edit "CheckVPN"
                set id 1
            next
        end
        set priority-members 2
    next
    edit 4
        set name "VPN_DNS"
        set mode sla
        set protocol 6
        set start-port 53
        set end-port 53
        set dst "LAN-BR"
        set src "LAN-HQ"
        config sla
            edit "CheckVPN"
                set id 1
            next
        end
        set priority-members 2
    next
    edit 5
        set name "VPN_DHCP"
        set mode sla
```

```
            set protocol 17
            set start-port 67
            set end-port 67
            set dst "LAN-BR"
            set src "LAN-HQ"
            config sla
                edit "CheckVPN"
                    set id 1
                next
            end
            set priority-members 2
        next
        edit 6
            set name "VPN_RADIUS"
            set mode sla
            set protocol 6
            set start-port 1812
            set end-port 1813
            set dst "LAN-BR"
            set src "LAN-HQ"
            config sla
                edit "CheckVPN"
                    set id 1
                next
            end
            set priority-members 2
        next
        edit 1
            set name "VPN"
            set mode sla
            set dst "LAN-BR"
            set src "LAN-HQ"
            config sla
                edit "CheckVPN"
                    set id 1
                next
            end
            set priority-members 2
        next
end
```

```
HQ-B # config firewall policy
    edit 2
        set name "VPN_IN"
        set srcintf "VPN"
        set dstintf "port2"
        set srcaddr "LAN-BR"
        set dstaddr "LAN-HQ"
        set action accept
        set schedule "always"
        set service "ALL"
        set ssl-ssh-profile "custom-deep-inspection"
    next
    edit 3
        set name "VPN_OUT"
        set srcintf "port2"
        set dstintf "VPN"
        set srcaddr "LAN-HQ"
        set dstaddr "LAN-BR"
        set action accept
        set schedule "always"
        set service "ALL"
        set ssl-ssh-profile "custom-deep-inspection"
    next
end
HQ-B # config system sdwan
 config service
        edit 3
            set name "VPN_SCTP"
            set mode sla
            set protocol 132
            set dst "LAN-BR"
            set src "LAN-HQ"
            config sla
                edit "CheckVPN"
                    set id 1
                next
            end
            set priority-members 2
        next
        edit 4
            set name "VPN_DHCP"
            set mode sla
            set protocol 17
            set start-port 67
            set end-port 67
            set dst "LAN-BR"
            set src "LAN-HQ"
            config sla
                edit "CheckVPN"
                    set id 1
                next
            end
            set priority-members 2
        next
        edit 5
            set name "VPN_DNS"
            set mode sla
            set protocol 17
            set start-port 53
            set end-port 53
            set dst "LAN-BR"
            set src "LAN-HQ"
            config sla
                edit "CheckVPN"
                    set id 1
                next
            end
            set priority-members 2
        next
        edit 6
            set name "VPN_CAPWAP"
            set mode sla
            set protocol 6
            set start-port 5246
            set end-port 5247
            set dst "LAN-BR"
            set src "LAN-HQ"
            config sla
                edit "CheckVPN"
                    set id 1
                next
            end
            set priority-members 2
        next
        edit 7
            set name "VPN_RADIUS"
            set mode sla
            set protocol 6
            set start-port 1812
```

```
            set end-port 1813
            set dst "LAN-BR"
            set src "LAN-HQ"
            config sla
                edit "CheckVPN"
                    set id 1
                next
            end
            set priority-members 2
        next
        edit 1
            set name "VPN"
            set mode sla
            set dst "LAN-BR"
            set src "LAN-HQ"
            config sla
                edit "CheckVPN"
                    set id 1
                next
            end
            set priority-members 2
        next
end
```

f. Configure the route-map under BGP routing to update the local-preference depending on community values received

```
HQ-A # config router route-map
    edit "comm1"
        config rule
            edit 1
                set match-community "20:1"
                set set-local-preference 200
            next
            edit 2
                set match-community "20:5"
                set set-local-preference 150
            next
        end
    next
end
HQ-A #  config router bgp
    config neighbor
```

```
        edit "10.1.1.2"
            set route-map-in "comm1"
        next
    end
```

```
HQ-B # config router route-map
    edit "comm2"
        config rule
            edit 1
                set match-community "20:2"
                set set-local-preference 200
            next
            edit 2
                set match-community "20:5"
                set set-local-preference 150
            next
        end
    next
end

HQ-B # config router bgp
    config neighbor
        edit "10.1.1.6"
            set route-map-in "comm2"
        next
    end
```

At Branch

a. Create VPN IPSEC Tunnels

```
Campus-Master #  config vpn ipsec phase1-interface
    edit "VPN_to_A_ISP1"
        set interface "port2"
        set peertype any
        set net-device disable
        set proposal des-md5 des-sha1
        set comments "VPN_to_A_ISP1"
        set nattraversal disable
        set remote-gw 172.18.101.10
        set psksecret 123456
    next
    edit "VPN_to_B_ISP2"
        set interface "port4"
        set peertype any
        set net-device disable
        set proposal des-md5 des-sha1
        set nattraversal disable
        set remote-gw 172.18.102.20
        set psksecret 123456
    next
end
Campus-Master #  config vpn ipsec phase2-interface
    edit "VPN_to_A_ISP1"
        set phase1name "VPN_to_A_ISP1"
        set proposal des-md5 des-sha1
        set src-addr-type name
        set dst-addr-type name
        set src-name "VPN_via_BGP"
        set dst-name "VPN_via_BGP"
    next
    edit "VPN_to_B_ISP2"
        set phase1name "VPN_to_B_ISP2"
        set proposal des-md5 des-sha1
        set src-addr-type name
        set dst-addr-type name
        set src-name "VPN_via_BGP"
        set dst-name "VPN_via_BGP"
    next
end
Campus-Master # config system interface
edit "VPN_to_A_ISP1"
        set vdom "root"
        set ip 10.1.1.2 255.255.255.255
        set type tunnel
        set remote-ip 10.1.1.1 255.255.255.252
        set interface "port2"
    next
    edit "VPN_to_B_ISP2"
        set vdom "root"
        set ip 10.1.1.6 255.255.255.255
        set type tunnel
        set remote-ip 10.1.1.5 255.255.255.252
        set interface "port4"
    next
```

b. Configure eBGP routing with two Firewall at the Data Center

```
Campus-Master # config router access-list
    edit "net10.159"
        config rule
            edit 1
                set prefix 10.159.100.0 255.255.255.0
            next
        end
    next
end
Campus-Master # config router route-map
    edit "comm1"
        config rule
            edit 1
                set match-ip-address "net10.159"
                set set-community "20:1"
            next
        end
    next
    edit "comm2"
        config rule
            edit 1
                set match-ip-address "net10.159"
                set set-community "20:2"
            next
        end
    next
    edit "comm5"
        config rule
            edit 1
                set match-ip-address "net10.159"
                set set-community "20:5"
            next
        end
    next
end
Campus-Master # config router bgp
    set as 65120
    set ebgp-multipath enable
    config neighbor
        edit "10.1.1.1"
            set soft-reconfiguration enable
            set remote-as 65100
            set route-map-out "comm5"
            set route-map-out-preferable "comm1"
        next
        edit "10.1.1.5"
            set soft-reconfiguration enable
            set remote-as 65100
            set route-map-out "comm5"
            set route-map-out-preferable "comm2"
        next
    end
    config network
        edit 1
            set prefix 10.159.100.0 255.255.255.0
        next
    end
```

c. **Create new SD-WAN Zone name VPN and assign SD-WAN members into this Zone**

```
Campus-Master # config system sdwan
    config zone
        edit "VPN"
        next
    end
    config members
        edit 3
            set interface "VPN_to_A_ISP1"
            set zone "VPN"
            set source 10.159.100.254
            set cost 5
        next
        edit 4
            set interface "VPN_to_B_ISP2"
            set zone "VPN"
            set source 10.159.100.254
            set cost 10
        next
    end
```

d. **Create Performance SLA to health check the internal IP address via VPN Links**

```
Campus-Master # config system sdwan
config health-check
```

```
        edit "CheckVPN_A"
            set server "10.92.101.10"
            set members 3
            config sla
                edit 1
                    set latency-threshold 20
                    set jitter-threshold 20
                next
            end
        next
        edit "CheckVPN_B"
            set server "10.92.102.20"
            set members 4
            config sla
                edit 1
                    set latency-threshold 20
                    set jitter-threshold 20
                next
            end
        next
    end
Campus-Master # config system sdwan
 config neighbor
        edit "10.1.1.1"
            set member 3
            set role primary
            set health-check "CheckVPN_A"
            set sla-id 1
        next
        edit "10.1.1.5"
            set member 4
            set role secondary
            set health-check "CheckVPN_B"
            set sla-id 1
        next
    end
```

e. Configure Firewall Policies for VPN Traffic and SD-WAN Rules for many types of Traffic via VPN tunnel links

```
Campus-Master # config system sdwan
    config service
        edit 11
        set name "VPN_SCTP"
        set mode sla
        set role primary
        set protocol 132
        set dst "LAN-HQ"
        set src "LAN-BR"
        config sla
            edit "CheckVPN_A"
                set id 1
            next
        end
        set priority-members 3
    next
    edit 12
        set name "VPN_SCTP_BK"
        set mode sla
        set role secondary
        set protocol 132
        set dst "LAN-HQ"
        set src "LAN-BR"
        config sla
            edit "CheckVPN_B"
                set id 1
            next
        end
        set priority-members 4
    next
    edit 1
        set name "VPN_CAPWAP"
        set mode sla
        set role primary
        set protocol 6
        set start-port 5246
        set end-port 5247
        set dst "LAN-HQ"
        set src "LAN-BR"
        config sla
            edit "CheckVPN_A"
                set id 1
            next
        end
        set priority-members 3
    next
    edit 4
        set name "VPN_CAPWAP_BK"
        set mode sla
        set role secondary
        set protocol 6
        set start-port 5246
        set end-port 5247
        set dst "LAN-HQ"
        set src "LAN-BR"
        config sla
            edit "CheckVPN_B"
                set id 1
            next
        end
        set priority-members 4
    next
    edit 5
        set name "VPN_DNS"
        set mode sla
        set role primary
        set protocol 6
        set start-port 53
        set end-port 53
        set dst "LAN-HQ"
        set src "LAN-BR"
        config sla
            edit "CheckVPN_A"
                set id 1
            next
        end
        set priority-members 3
    next
    edit 6
        set name "VPN_DNS_BK"
        set mode sla
        set role secondary
        set protocol 6
        set start-port 53
        set end-port 53
        set dst "LAN-HQ"
        set src "LAN-BR"
        config sla
            edit "CheckVPN_B"
            set id 1
        next
    end
    set priority-members 4
next
edit 7
    set name "VPN_RADIUS"
    set mode sla
    set role primary
    set protocol 6
    set start-port 1812
    set end-port 1813
    set dst "LAN-HQ"
    set src "LAN-BR"
    config sla
        edit "CheckVPN_A"
            set id 1
        next
    end
    set priority-members 3
next
edit 8
    set name "VPN_RADIUS_BK"
    set mode sla
    set role secondary
    set dst "LAN-HQ"
    set src "LAN-BR"
    config sla
        edit "CheckVPN_B"
            set id 1
        next
    end
    set priority-members 4
next
edit 9
    set name "VPN_DCHP"
    set mode sla
    set role primary
    set protocol 17
    set start-port 67
    set end-port 67
    set dst "LAN-HQ"
    set src "LAN-BR"
```

```
        config sla
            edit "CheckVPN_A"
                set id 1
            next
        end
        set priority-members 3
    next
    edit 10
        set name "VPN_DHCP_BK"
        set mode sla
        set role secondary
        set protocol 17
        set start-port 67
        set end-port 67
        set dst "LAN-HQ"
        set src "LAN-BR"
        config sla
            edit "CheckVPN_B"
                set id 1
            next
        end
        set priority-members 4
    next
    edit 3
        set name "VPN"
        set mode load-balance
        set dst "LAN-HQ"
        set src "LAN-BR"
        config sla
            edit "CheckVPN_A"
                set id 1
            next
            edit "CheckVPN_B"
                set id 1
            next
        end
        set priority-members 4 3
    next
```

4. Marking DSCP for the outgoing traffic and apply the Traffic Shaping Profile under WAN interfaces

_At The Data Center

a. Marking DSCP for the outgoing traffic

```
HQ-A # config system sdwan
config service
        edit 7
            set name "VPN_SCTP"
            set dscp-forward enable
            set dscp-reverse enable
            set dscp-forward-tag 101110
            set dscp-reverse-tag 101110
        next
        edit 3
            set name "VPN_CAPWAP"
            set dscp-forward enable
            set dscp-reverse enable
            set dscp-forward-tag 101110
            set dscp-reverse-tag 101110
        next
        edit 4
            set name "VPN_DNS"
            set dscp-forward enable
            set dscp-reverse enable
            set dscp-forward-tag 101110
            set dscp-reverse-tag 101110
        next
        edit 5
            set name "VPN_DHCP"
            set dscp-forward enable
            set dscp-reverse enable
            set dscp-forward-tag 101110
            set dscp-reverse-tag 101110
        next
        edit 6
            set name "VPN_RADIUS"
            set dscp-forward enable
            set dscp-reverse enable
            set dscp-forward-tag 101110
            set dscp-reverse-tag 101110
        next
        edit 1
            set name "VPN"
            set dscp-forward enable
            set dscp-reverse enable
            set dscp-forward-tag 100010
            set dscp-reverse-tag 100010
        next
end
```

```
HQ-B # config system sdwan
    config service
        edit 3
            set name "VPN_SCTP"
            set dscp-forward enable
            set dscp-reverse enable
            set dscp-forward-tag 101110
            set dscp-reverse-tag 101110
        next
        edit 4
            set name "VPN_DHCP"
            set dscp-forward enable
            set dscp-reverse enable
            set dscp-forward-tag 101110
            set dscp-reverse-tag 101110
        next
        edit 5
            set name "VPN_DNS"
            set dscp-forward enable
            set dscp-reverse enable
            set dscp-forward-tag 101110
            set dscp-reverse-tag 101110
        next
        edit 6
            set name "VPN_CAPWAP"
            set dscp-forward enable
            set dscp-reverse enable
            set dscp-forward-tag 101110
            set dscp-reverse-tag 101110
        next
        edit 7
            set name "VPN_RADIUS"
            set dscp-forward enable
            set dscp-reverse enable
            set dscp-forward-tag 101110
            set dscp-reverse-tag 101110
        next
        edit 1
            set name "VPN"
            set dscp-forward enable
            set dscp-reverse enable
            set dscp-forward-tag 100010
            set dscp-reverse-tag 100010
        next
```

b. Create the Traffic Shaping Policy and Profile

```
HQ-A #   config firewall shaping-policy
    edit 1
        set name "Critical_Apps"
        set service "ALL_ICMP" "BGP" "DHCP" "DNS" "RADIUS" "SMTP" "CAPWAP" "SCTP"
        set dstintf "VPN"
        set traffic-shaper "high-priority"
        set traffic-shaper-reverse "high-priority"
        set srcaddr "TUNNEL_ADD" "LAN-HQ"
        set dstaddr "LAN-BR" "TUNNEL_ADD"
    next
    edit 2
        set name "Business_Apps"
        set service "ALL"
        set dstintf "VPN"
        set traffic-shaper "medium-priority"
        set traffic-shaper-reverse "medium-priority"
        set srcaddr "LAN-HQ"
        set dstaddr "LAN-BR"
    next
    edit 3
        set name "Secure_Internet"
        set service "ALL"
        set dstintf "INTERNET"
        set traffic-shaper "low-priority"
        set traffic-shaper-reverse "low-priority"
        set srcaddr "all"
        set dstaddr "all"
    next
end
HQ-A #   config firewall shaping-profile
    edit "All_Service"
        set default-class-id 4
        config shaping-entries
            edit 1
                set class-id 4
                set priority low
                set guaranteed-bandwidth-percentage 2
                set maximum-bandwidth-percentage 100
            next
            edit 2
                set class-id 2
                set priority critical
                set guaranteed-bandwidth-percentage 90
                set maximum-bandwidth-percentage 100
            next
            edit 3
                set class-id 3
                set guaranteed-bandwidth-percentage 8
                set maximum-bandwidth-percentage 100
            next
        end
    next
end
```

```
HQ-B #   config firewall shaping-policy
    edit 1
        set name "Critical_Apps"
        set service "ALL_ICMP" "BGP" "DHCP" "DNS" "RADIUS" "SMTP" "CAPWAP" "SCTP"
        set dstintf "VPN"
        set traffic-shaper "high-priority"
        set traffic-shaper-reverse "high-priority"
        set srcaddr "TUNNEL_ADD" "LAN-HQ"
        set dstaddr "LAN-BR" "TUNNEL_ADD"
    next
    edit 2
        set name "Business_Apps"
        set service "ALL"
        set dstintf "VPN"
        set traffic-shaper "medium-priority"
        set traffic-shaper-reverse "medium-priority"
        set srcaddr "LAN-HQ"
        set dstaddr "LAN-BR"
    next
    edit 3
        set name "Secure_Internet"
        set service "ALL"
        set dstintf "INTERNET"
        set traffic-shaper "low-priority"
        set traffic-shaper-reverse "low-priority"
        set srcaddr "all"
        set dstaddr "all"
    next
end
HQ-B # config firewall shaping-profile
    edit "All_Service"
        set default-class-id 4
        config shaping-entries
            edit 1
                set class-id 2
                set priority critical
                set guaranteed-bandwidth-percentage 90
                set maximum-bandwidth-percentage 100
            next
            edit 2
                set class-id 3
                set guaranteed-bandwidth-percentage 8
                set maximum-bandwidth-percentage 100
            next
            edit 3
                set class-id 4
                set priority low
                set guaranteed-bandwidth-percentage 2
                set maximum-bandwidth-percentage 100
            next
        end
    next
end
```

c. Apply the Traffic Shaping Profile under WAN interaces

```
HQ-A # config system interface
    edit "port3"
        set outbandwidth 2000
        set egress-shaping-profile "All_Service"
    next
```

```
HQ-B # config system interface
    edit "port3"
        set outbandwidth 2000
        set egress-shaping-profile "All_Service"
    next
```

At Branch

a. Marking DSCP for the outgoing traffic

```
Campus-Master # config system sdwan
 config service
     edit 11
        set name "VPN_SCTP"
        set dscp-forward enable
        set dscp-reverse enable
        set dscp-forward-tag 101110
        set dscp-reverse-tag 101110
     next
     edit 12
        set name "VPN_SCTP_BK"
        set dscp-forward enable
        set dscp-reverse enable
        set dscp-forward-tag 101110
        set dscp-reverse-tag 101110
     next
     edit 1
        set name "VPN_CAPWAP"
        set dscp-forward enable
        set dscp-reverse enable
        set dscp-forward-tag 101110
        set dscp-reverse-tag 101110
     next
     edit 4
        set name "VPN_CAPWAP_BK"
        set dscp-forward enable
        set dscp-reverse enable
        set dscp-forward-tag 101110
        set dscp-reverse-tag 101110
     next
     edit 5
        set name "VPN_DNS"
        set dscp-forward enable
        set dscp-reverse enable
        set dscp-forward-tag 101110
        set dscp-reverse-tag 101110
     next
     edit 6
        set name "VPN_DNS_BK"
        set dscp-forward enable
        set dscp-reverse enable
        set dscp-forward-tag 101110
```

```
      set dscp-reverse-tag 101110
    next
    edit 7
      set name "VPN_RADIUS"
      set dscp-forward enable
      set dscp-reverse enable
      set dscp-forward-tag 101110
      set dscp-reverse-tag 101110
    next
    edit 8
      set name "VPN_RADIUS_BK"
      set dscp-forward enable
      set dscp-reverse enable
      set dscp-forward-tag 101110
      set dscp-reverse-tag 101110
    next
    edit 9
      set name "VPN_DCHP"
      set dscp-forward enable
      set dscp-reverse enable
      set dscp-forward-tag 101110
      set dscp-reverse-tag 101110
    next
    edit 10
      set name "VPN_DHCP_BK"
      set dscp-forward enable
      set dscp-reverse enable
      set dscp-forward-tag 101110
      set dscp-reverse-tag 101110
    next
    edit 3
      set name "VPN"
      set dscp-forward enable
      set dscp-reverse enable
      set dscp-forward-tag 100010
      set dscp-reverse-tag 100010
    next
```

b. Create the Traffic Shaping Policy and Profile

```
Campus-Master #   config firewall shaping-policy
  edit 1
    set name "Critical_Apps"
```

```
        set service "BGP" "DHCP" "DNS" "RADIUS" "SMTP" "Windows AD" "CAPWAP" "SCTP"
        set dstintf "VPN"
        set class-id 2
        set srcaddr "LAN-BR" "TUNNEL_ADD"
        set dstaddr "TUNNEL_ADD" "LAN-HQ"
    next
    edit 2
        set name "Business_Apps"
        set service "ALL"
        set dstintf "VPN"
        set class-id 3
        set srcaddr "LAN-BR"
        set dstaddr "LAN-HQ"
    next
    edit 3
        set name "Secure_Internet"
        set service "ALL"
        set dstintf "INTERNET"
        set class-id 4
        set srcaddr "all"
        set dstaddr "all"
    next
end
Campus-Master #   config firewall shaping-profile
    edit "All_Service"
        set default-class-id 4
        config shaping-entries
            edit 1
                set class-id 2
                set priority critical
                set guaranteed-bandwidth-percentage 90
                set maximum-bandwidth-percentage 100
            next
            edit 2
                set class-id 3
                set guaranteed-bandwidth-percentage 8
                set maximum-bandwidth-percentage 100
            next
            edit 3
                set class-id 4
                set priority low
                set guaranteed-bandwidth-percentage 2
                set maximum-bandwidth-percentage 100
            next
        end
    next
end
```

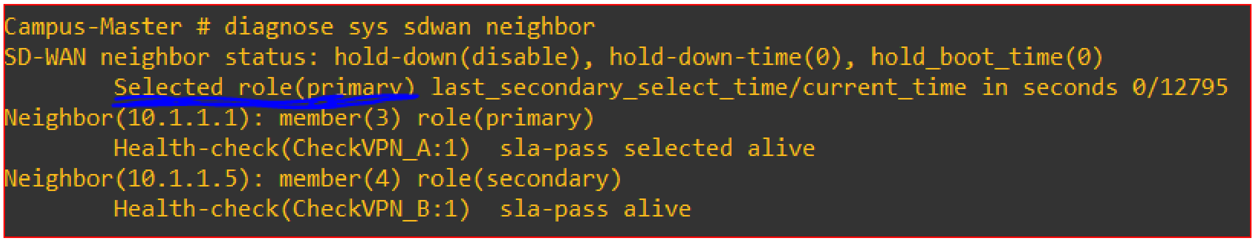
c. Apply the Traffic Shaping Profile under WAN interfaces

```
Campus-Master # config system interface

 edit "port2"
        set outbandwidth 2000
        set egress-shaping-profile "All_Service"
    next
    edit "port4"
        set outbandwidth 2000
        set egress-shaping-profile "All_Service"
    next
```

Verification:

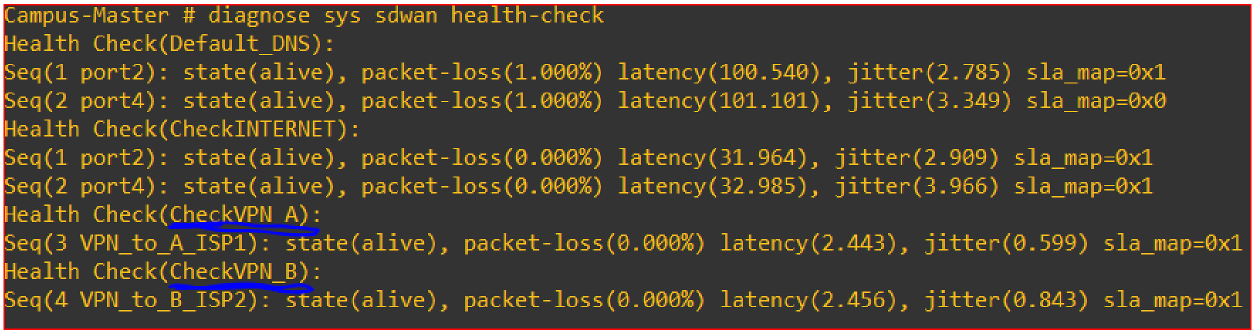
1. **Verification the Critical traffic will be transferred on the primary IPSEC tunnel link when it meets the SLA threshold**

- Check selected neighbor on Branch Firewall



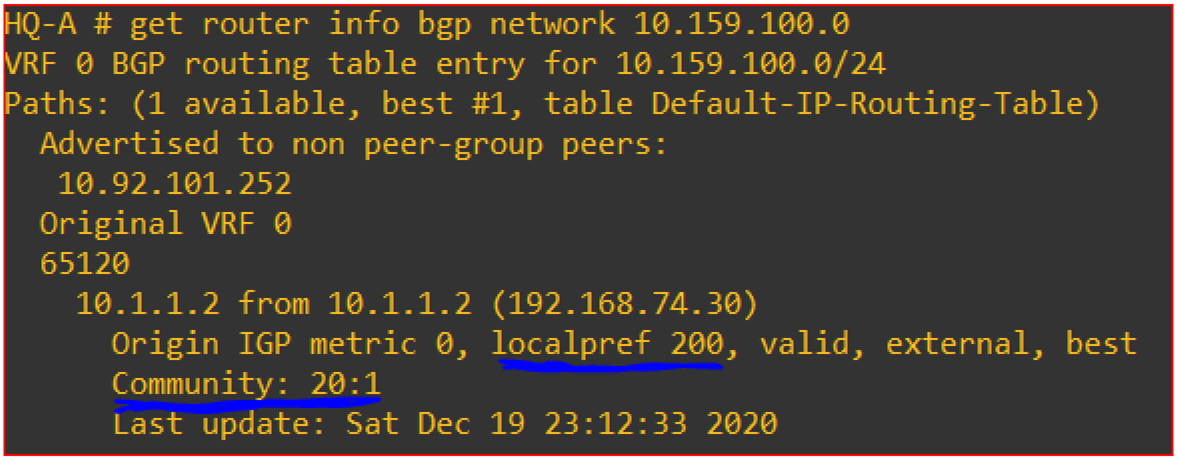
```
Campus-Master # diagnose sys sdwan neighbor
SD-WAN neighbor status: hold-down(disable), hold-down-time(0), hold_boot_time(0)
        Selected role(primary) last_secondary_select_time/current_time in seconds 0/12795
Neighbor(10.1.1.1): member(3) role(primary)
        Health-check(CheckVPN_A:1)  sla-pass selected alive
Neighbor(10.1.1.5): member(4) role(secondary)
        Health-check(CheckVPN_B:1)  sla-pass alive
```

- In the normal state, two VPN IPSEC links all get SLA target

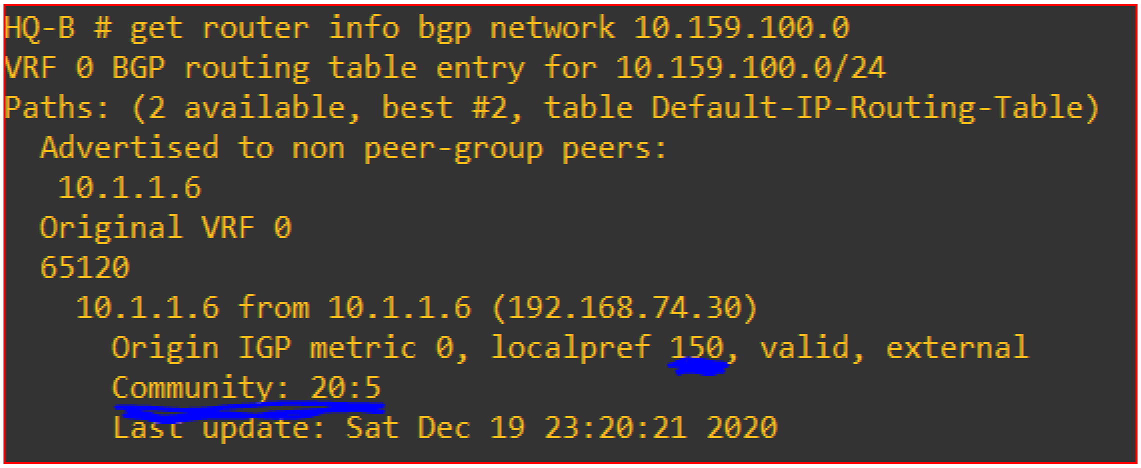


```
Campus-Master # diagnose sys sdwan health-check
Health Check(Default_DNS):
Seq(1 port2): state(alive), packet-loss(1.000%) latency(100.540), jitter(2.785) sla_map=0x1
Seq(2 port4): state(alive), packet-loss(1.000%) latency(101.101), jitter(3.349) sla_map=0x0
Health Check(CheckINTERNET):
Seq(1 port2): state(alive), packet-loss(0.000%) latency(31.964), jitter(2.909) sla_map=0x1
Seq(2 port4): state(alive), packet-loss(0.000%) latency(32.985), jitter(3.966) sla_map=0x1
Health Check(CheckVPN_A):
Seq(3 VPN_to_A_ISP1): state(alive), packet-loss(0.000%) latency(2.443), jitter(0.599) sla_map=0x1
Health Check(CheckVPN_B):
Seq(4 VPN_to_B_ISP2): state(alive), packet-loss(0.000%) latency(2.456), jitter(0.843) sla_map=0x1
```

- Check BGP community that Branch Firewall advertised to two neighbors at the Data Center



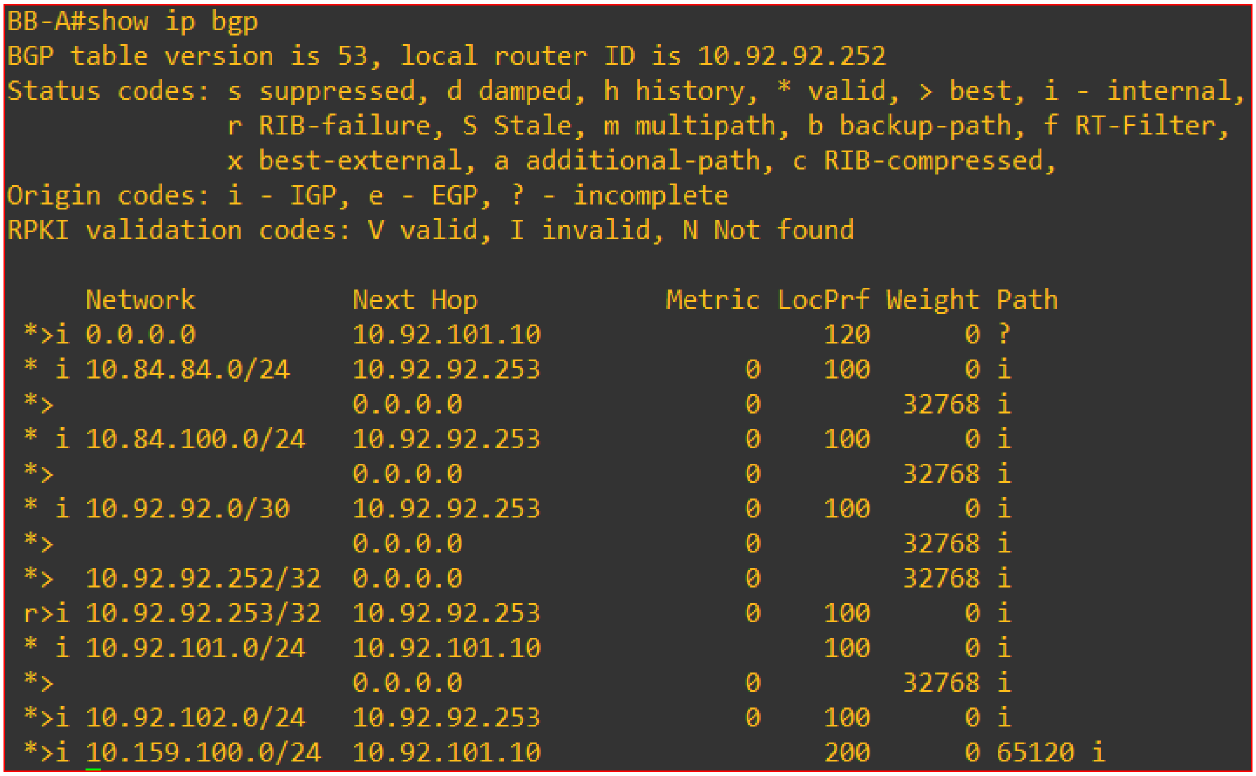
```
HQ-A # get router info bgp network 10.159.100.0
VRF 0 BGP routing table entry for 10.159.100.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
   10.92.101.252
  Original VRF 0
  65120
    10.1.1.2 from 10.1.1.2 (192.168.74.30)
      Origin IGP metric 0, localpref 200, valid, external, best
      Community: 20:1
      Last update: Sat Dec 19 23:12:33 2020
```



```
HQ-B # get router info bgp network 10.159.100.0
VRF 0 BGP routing table entry for 10.159.100.0/24
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
   10.1.1.6
  Original VRF 0
  65120
    10.1.1.6 from 10.1.1.6 (192.168.74.30)
      Origin IGP metric 0, localpref 150, valid, external
      Community: 20:5
      Last update: Sat Dec 19 23:20:21 2020
```

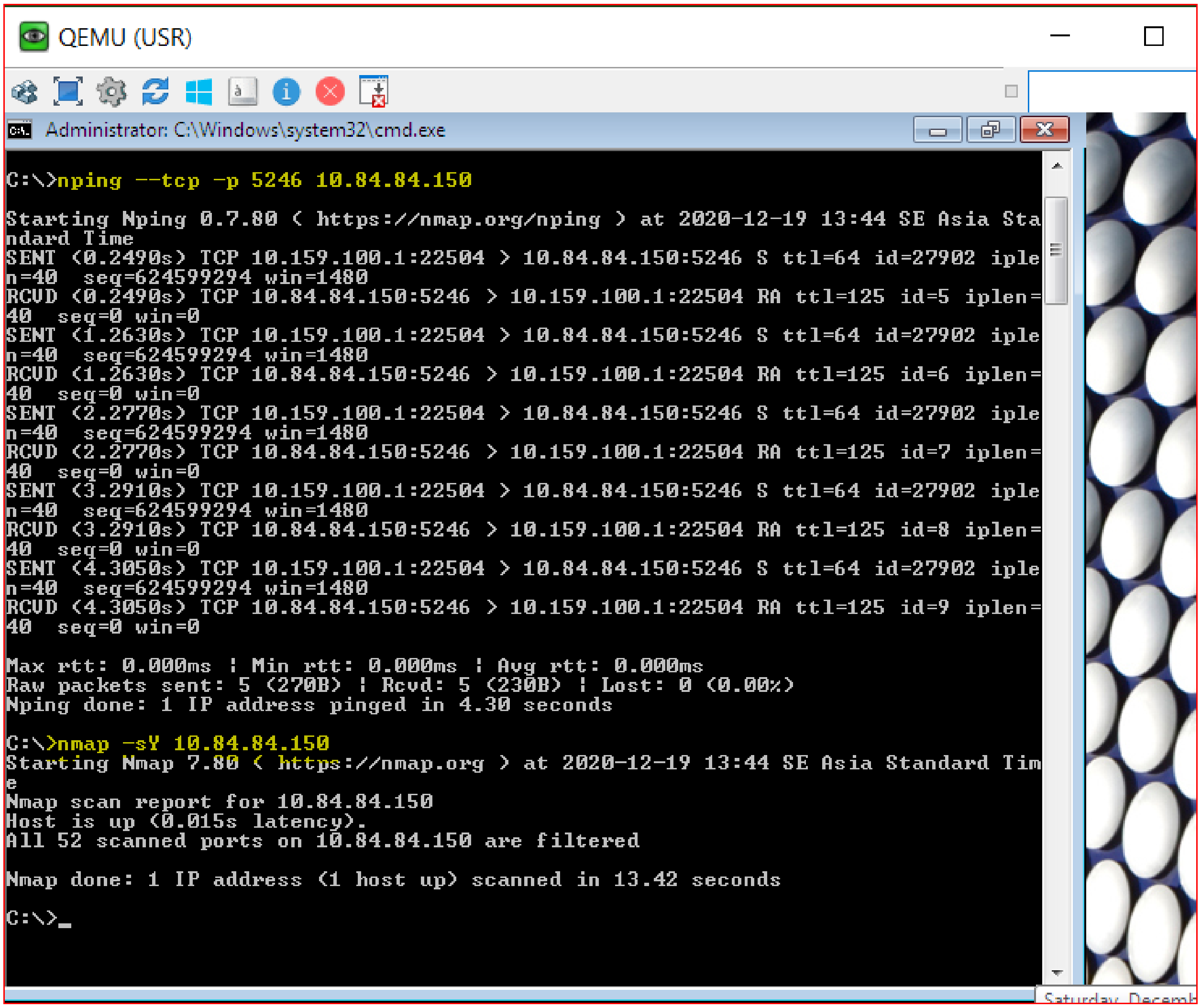
-> On two Firewalls at the Data Center depending on the community that they received from the Branch Firewall will advertise the local-preference to Router Backbone. (200 for community 20:1 and 150 for community 20:5)

- On Router Backbone, the best path to Firewall HQ-A



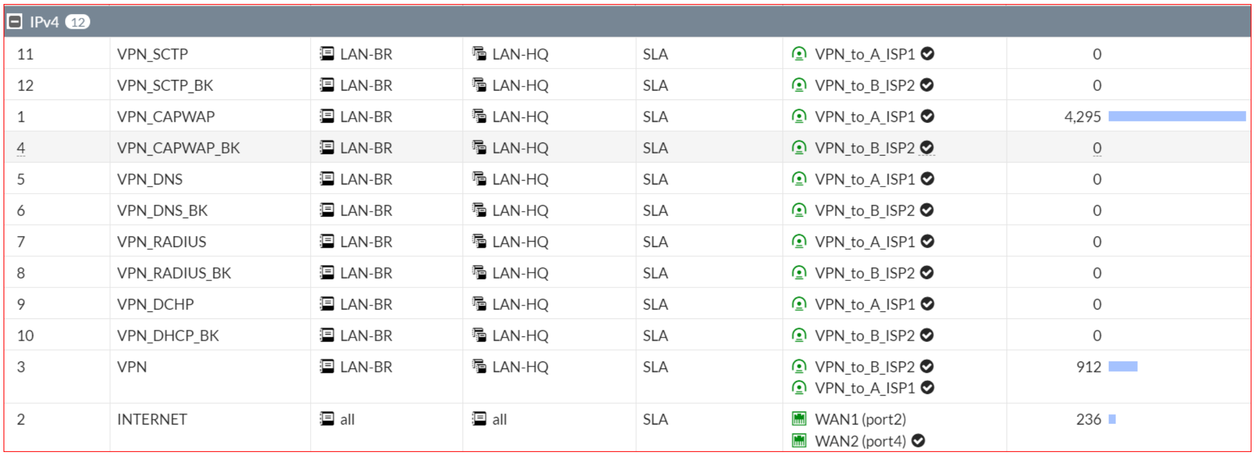
```
BB-A#show ip bgp
BGP table version is 53, local router ID is 10.92.92.252
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>i 0.0.0.0          10.92.101.10                 120      0 ?
 * i 10.84.84.0/24    10.92.92.253             0    100      0 i
 *>                   0.0.0.0                  0         32768 i
 * i 10.84.100.0/24   10.92.92.253             0    100      0 i
 *>                   0.0.0.0                  0         32768 i
 * i 10.92.92.0/30    10.92.92.253             0    100      0 i
 *>                   0.0.0.0                  0         32768 i
 *>  10.92.92.252/32  0.0.0.0                  0         32768 i
 r>i 10.92.92.253/32  10.92.92.253             0    100      0 i
 * i 10.92.101.0/24   10.92.101.10                 100      0 i
 *>                   0.0.0.0                  0         32768 i
 *>i 10.92.102.0/24   10.92.92.253             0    100      0 i
 *>i 10.159.100.0/24  10.92.101.10                 200      0 65120 i
```

- Install nmap on USR PC at Branch and on Server PC at the Data Center.
- Generate the traffic as DHCP, DNS, CAPWAP, RADIUS, SMTP, SCTP to test traffic via SD-WAN rules
    - Nping --udp -p 67 10.84.84.150
    - Nping --udp -p 53 10.84.84.150
    - Nping --tcp -p 5246 10.84.84.150
    - Nping --tcp -p 1812 10.84.84.150
    - Nping --tcp -p 25 10.84.84.150
    - Nmap -sY 10.84.84.150 *//For SCTP INIT*
- On USR PC:



```
C:\>nping --tcp -p 5246 10.84.84.150

Starting Nping 0.7.80 ( https://nmap.org/nping ) at 2020-12-19 13:44 SE Asia Sta
ndard Time
SENT (0.2490s) TCP 10.159.100.1:22504 > 10.84.84.150:5246 S ttl=64 id=27902 iple
n=40  seq=624599294 win=1480
RCVD (0.2490s) TCP 10.84.84.150:5246 > 10.159.100.1:22504 RA ttl=125 id=5 iplen=
40  seq=0 win=0
SENT (1.2630s) TCP 10.159.100.1:22504 > 10.84.84.150:5246 S ttl=64 id=27902 iple
n=40  seq=624599294 win=1480
RCVD (1.2630s) TCP 10.84.84.150:5246 > 10.159.100.1:22504 RA ttl=125 id=6 iplen=
40  seq=0 win=0
SENT (2.2770s) TCP 10.159.100.1:22504 > 10.84.84.150:5246 S ttl=64 id=27902 iple
n=40  seq=624599294 win=1480
RCVD (2.2770s) TCP 10.84.84.150:5246 > 10.159.100.1:22504 RA ttl=125 id=7 iplen=
40  seq=0 win=0
SENT (3.2910s) TCP 10.159.100.1:22504 > 10.84.84.150:5246 S ttl=64 id=27902 iple
n=40  seq=624599294 win=1480
RCVD (3.2910s) TCP 10.84.84.150:5246 > 10.159.100.1:22504 RA ttl=125 id=8 iplen=
40  seq=0 win=0
SENT (4.3050s) TCP 10.159.100.1:22504 > 10.84.84.150:5246 S ttl=64 id=27902 iple
n=40  seq=624599294 win=1480
RCVD (4.3050s) TCP 10.84.84.150:5246 > 10.159.100.1:22504 RA ttl=125 id=9 iplen=
40  seq=0 win=0

Max rtt: 0.000ms | Min rtt: 0.000ms | Avg rtt: 0.000ms
Raw packets sent: 5 (270B) | Rcvd: 5 (230B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 4.30 seconds

C:\>nmap -sY 10.84.84.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-19 13:44 SE Asia Standard Tim
e
Nmap scan report for 10.84.84.150
Host is up (0.015s latency).
All 52 scanned ports on 10.84.84.150 are filtered

Nmap done: 1 IP address (1 host up) scanned in 13.42 seconds

C:\>_
```

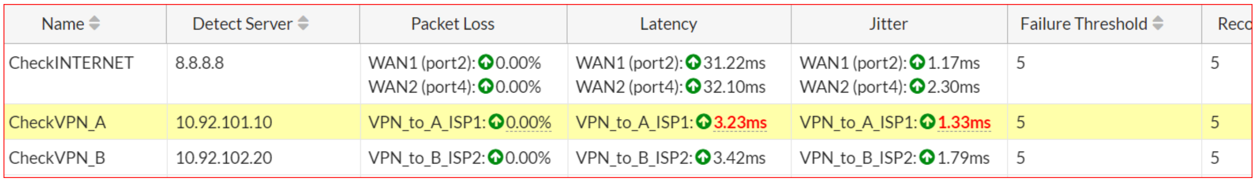
- Check Hit Count on SD-WAN Rules on the Branch Firewall



11	VPN_SCTP	LAN-BR	LAN-HQ	SLA	VPN_to_A_ISP1 ✓	0
12	VPN_SCTP_BK	LAN-BR	LAN-HQ	SLA	VPN_to_B_ISP2 ✓	0
1	VPN_CAPWAP	LAN-BR	LAN-HQ	SLA	VPN_to_A_ISP1 ✓	4,295
4	VPN_CAPWAP_BK	LAN-BR	LAN-HQ	SLA	VPN_to_B_ISP2 ✓	0
5	VPN_DNS	LAN-BR	LAN-HQ	SLA	VPN_to_A_ISP1 ✓	0
6	VPN_DNS_BK	LAN-BR	LAN-HQ	SLA	VPN_to_B_ISP2 ✓	0
7	VPN_RADIUS	LAN-BR	LAN-HQ	SLA	VPN_to_A_ISP1 ✓	0
8	VPN_RADIUS_BK	LAN-BR	LAN-HQ	SLA	VPN_to_B_ISP2 ✓	0
9	VPN_DCHP	LAN-BR	LAN-HQ	SLA	VPN_to_A_ISP1 ✓	0
10	VPN_DHCP_BK	LAN-BR	LAN-HQ	SLA	VPN_to_B_ISP2 ✓	0
3	VPN	LAN-BR	LAN-HQ	SLA	VPN_to_B_ISP2 ✓ VPN_to_A_ISP1 ✓	912
2	INTERNET	all	all	SLA	WAN1 (port2) WAN2 (port4) ✓	236

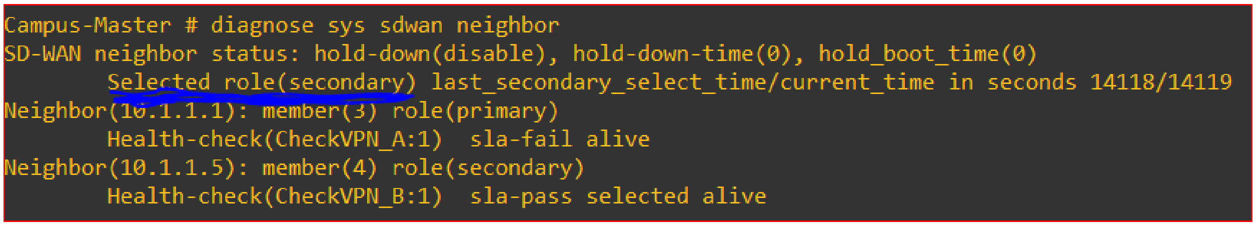
2. Verification failover when the primary Tunnel link does not meet the SLA threshold

- Set the SLA threshold decrease to test



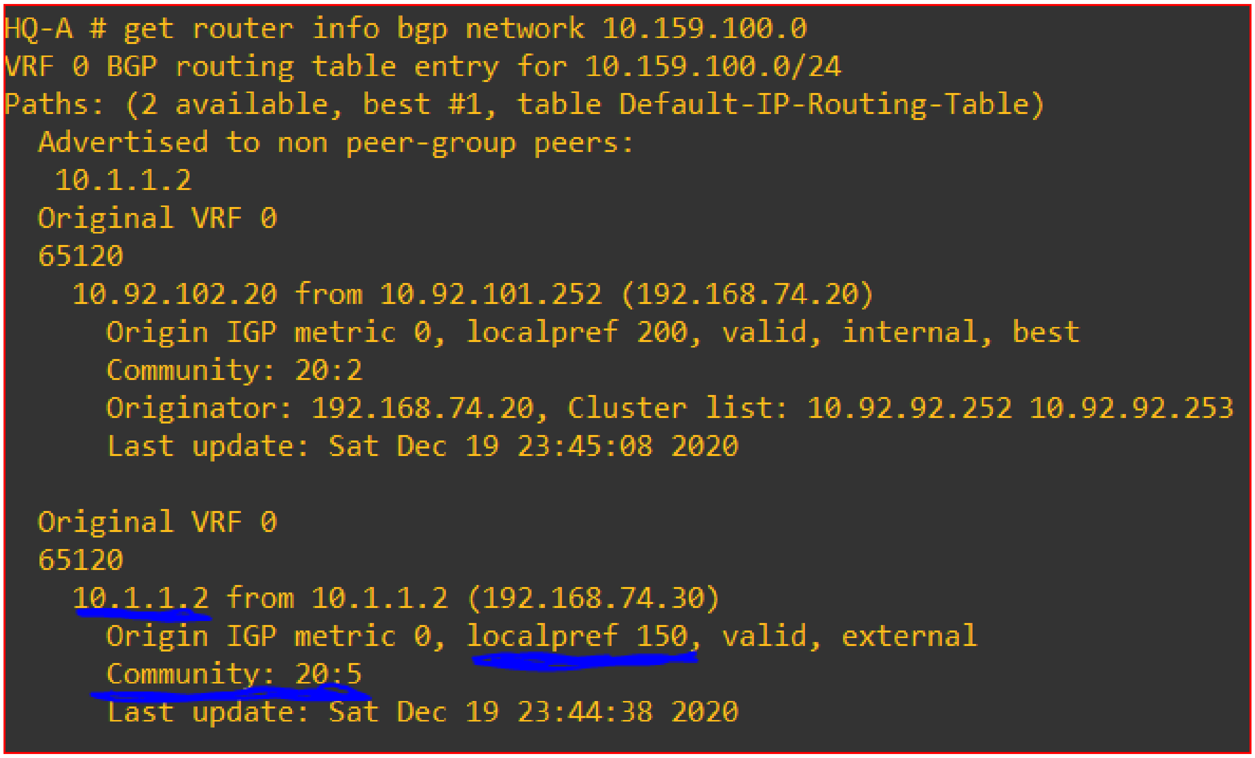
Name ⬍	Detect Server ⬍	Packet Loss	Latency	Jitter	Failure Threshold ⬍	Reco
CheckINTERNET	8.8.8.8	WAN1 (port2): ⬆0.00% WAN2 (port4): ⬆0.00%	WAN1 (port2): ⬆31.22ms WAN2 (port4): ⬆32.10ms	WAN1 (port2): ⬆1.17ms WAN2 (port4): ⬆2.30ms	5	5
CheckVPN_A	10.92.101.10	VPN_to_A_ISP1: ⬆0.00%	VPN_to_A_ISP1: ⬆3.23ms	VPN_to_A_ISP1: ⬆1.33ms	5	5
CheckVPN_B	10.92.102.20	VPN_to_B_ISP2: ⬆0.00%	VPN_to_B_ISP2: ⬆3.42ms	VPN_to_B_ISP2: ⬆1.79ms	5	5

- Check the SD-WAN neighbor status on Branch Firewall



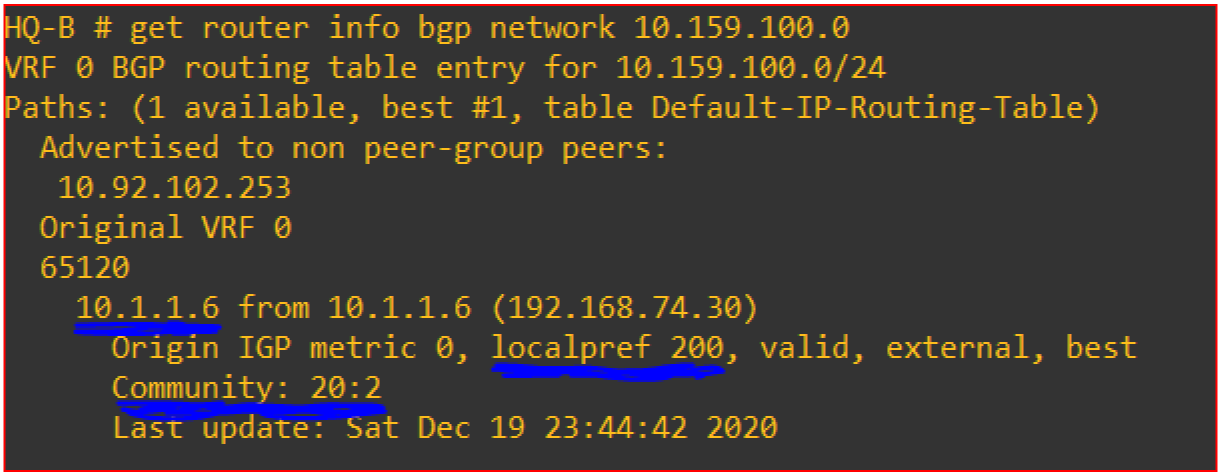
```
Campus-Master # diagnose sys sdwan neighbor
SD-WAN neighbor status: hold-down(disable), hold-down-time(0), hold_boot_time(0)
        Selected role(secondary) last_secondary_select_time/current_time in seconds 14118/14119
Neighbor(10.1.1.1): member(3) role(primary)
        Health-check(CheckVPN_A:1)  sla-fail alive
Neighbor(10.1.1.5): member(4) role(secondary)
        Health-check(CheckVPN_B:1)  sla-pass selected alive
```

- Check the BGP community updated to BGP neighbors at the Data Center.



```
HQ-A # get router info bgp network 10.159.100.0
VRF 0 BGP routing table entry for 10.159.100.0/24
Paths: (2 available, best #1, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
   10.1.1.2
  Original VRF 0
  65120
    10.92.102.20 from 10.92.101.252 (192.168.74.20)
      Origin IGP metric 0, localpref 200, valid, internal, best
      Community: 20:2
      Originator: 192.168.74.20, Cluster list: 10.92.92.252 10.92.92.253
      Last update: Sat Dec 19 23:45:08 2020

  Original VRF 0
  65120
    10.1.1.2 from 10.1.1.2 (192.168.74.30)
      Origin IGP metric 0, localpref 150, valid, external
      Community: 20:5
      Last update: Sat Dec 19 23:44:38 2020
```

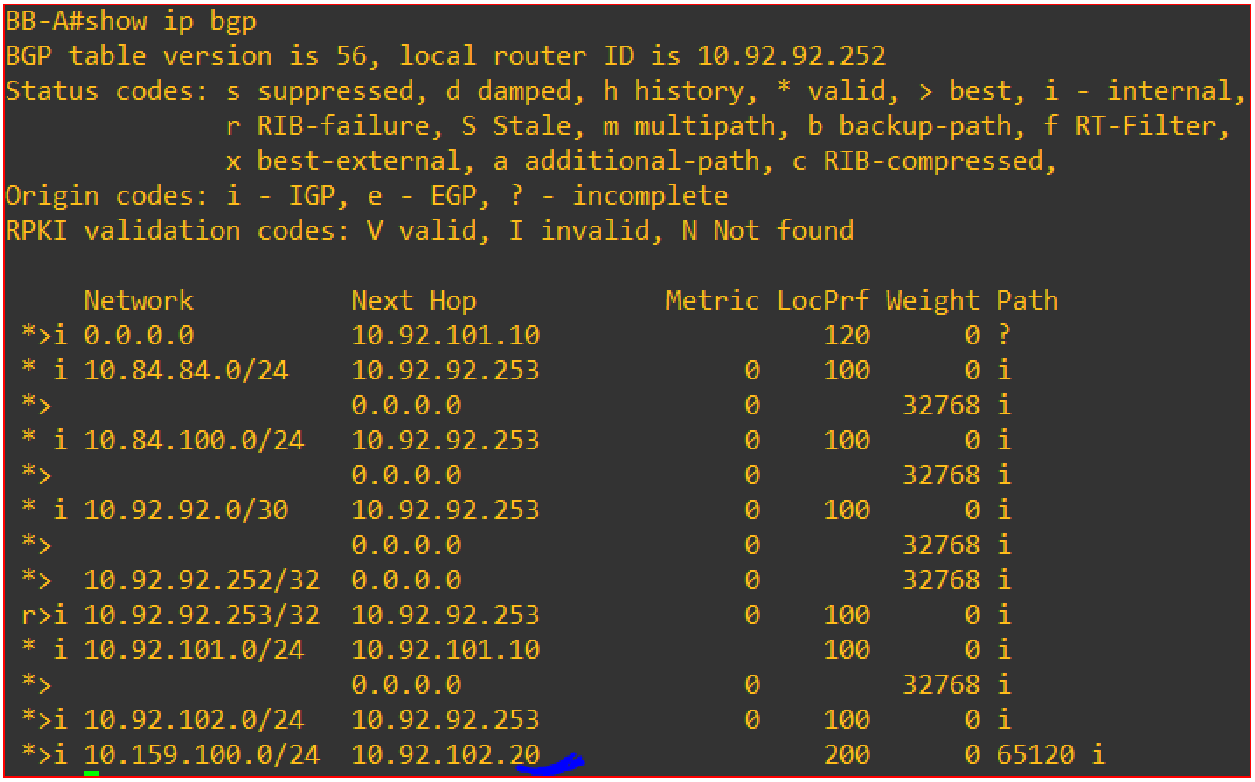
-> On Firewall HQ-A received community 20:5 from the Branch Firewall and it will advertise this prefix with the local-preference 150



```
HQ-B # get router info bgp network 10.159.100.0
VRF 0 BGP routing table entry for 10.159.100.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
   10.92.102.253
  Original VRF 0
  65120
    10.1.1.6 from 10.1.1.6 (192.168.74.30)
      Origin IGP metric 0, localpref 200, valid, external, best
      Community: 20:2
      Last update: Sat Dec 19 23:44:42 2020
```

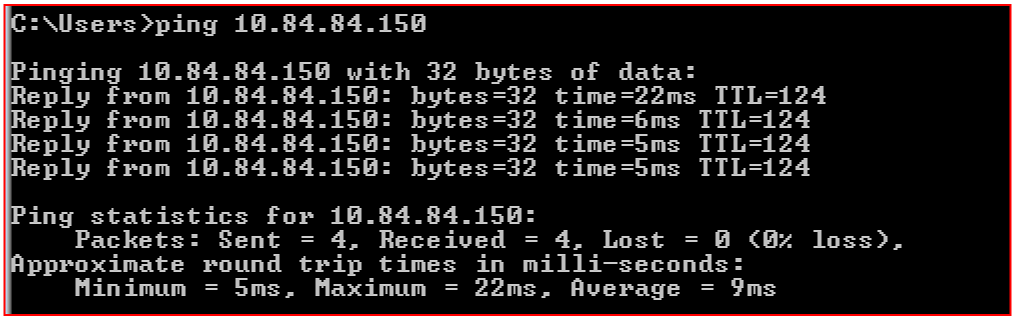
-> On Firewall HQ-B received community 20:2, it will advertise with the local-preference 200 to Router Backbone

- On Router Backbone, the best path to Firewall HQ-B

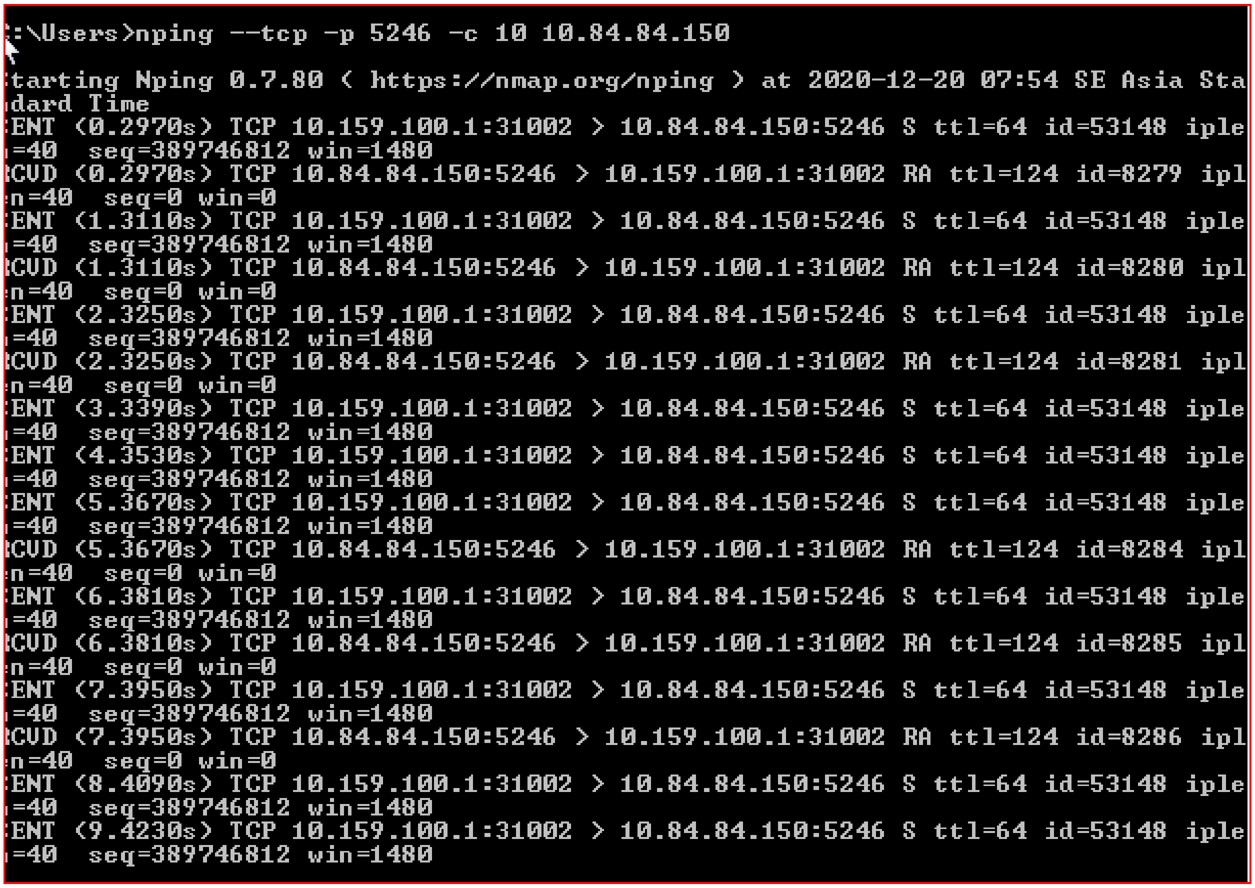


```
BB-A#show ip bgp
BGP table version is 56, local router ID is 10.92.92.252
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>i 0.0.0.0          10.92.101.10                  120      0 ?
 * i 10.84.84.0/24    10.92.92.253             0    100      0 i
 *>                   0.0.0.0                  0         32768 i
 * i 10.84.100.0/24   10.92.92.253             0    100      0 i
 *>                   0.0.0.0                  0         32768 i
 * i 10.92.92.0/30    10.92.92.253             0    100      0 i
 *>                   0.0.0.0                  0         32768 i
 *>  10.92.92.252/32  0.0.0.0                  0         32768 i
 r>i 10.92.92.253/32  10.92.92.253             0    100      0 i
 * i 10.92.101.0/24   10.92.101.10                  100      0 i
 *>                   0.0.0.0                  0         32768 i
 *>i 10.92.102.0/24   10.92.92.253             0    100      0 i
 *>i 10.159.100.0/24  10.92.102.20                  200      0 65120 i
```

- Ping Test and Generate CAPWAP traffic from USR PC to Server PC at the Data Center
- On USR PC

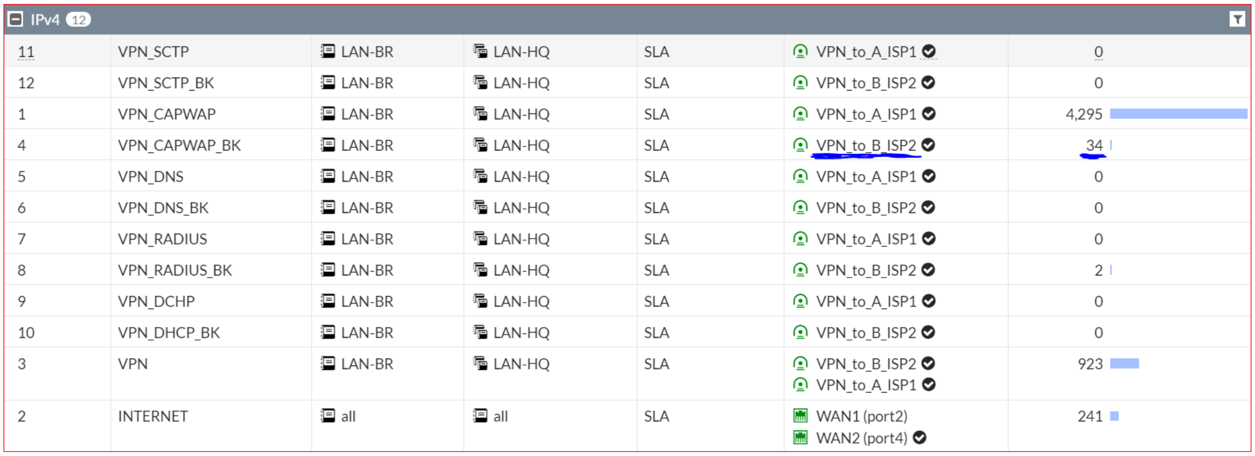


```
C:\Users>ping 10.84.84.150

Pinging 10.84.84.150 with 32 bytes of data:
Reply from 10.84.84.150: bytes=32 time=22ms TTL=124
Reply from 10.84.84.150: bytes=32 time=6ms TTL=124
Reply from 10.84.84.150: bytes=32 time=5ms TTL=124
Reply from 10.84.84.150: bytes=32 time=5ms TTL=124

Ping statistics for 10.84.84.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 22ms, Average = 9ms
```



```
:\Users>nping --tcp -p 5246 -c 10 10.84.84.150

tarting Nping 0.7.80 ( https://nmap.org/nping ) at 2020-12-20 07:54 SE Asia Sta
dard Time
ENT (0.2970s) TCP 10.159.100.1:31002 > 10.84.84.150:5246 S ttl=64 id=53148 iple
=40  seq=389746812 win=1480
CVD (0.2970s) TCP 10.84.84.150:5246 > 10.159.100.1:31002 RA ttl=124 id=8279 ipl
n=40  seq=0 win=0
ENT (1.3110s) TCP 10.159.100.1:31002 > 10.84.84.150:5246 S ttl=64 id=53148 iple
=40  seq=389746812 win=1480
CVD (1.3110s) TCP 10.84.84.150:5246 > 10.159.100.1:31002 RA ttl=124 id=8280 ipl
n=40  seq=0 win=0
ENT (2.3250s) TCP 10.159.100.1:31002 > 10.84.84.150:5246 S ttl=64 id=53148 iple
=40  seq=389746812 win=1480
CVD (2.3250s) TCP 10.84.84.150:5246 > 10.159.100.1:31002 RA ttl=124 id=8281 ipl
n=40  seq=0 win=0
ENT (3.3390s) TCP 10.159.100.1:31002 > 10.84.84.150:5246 S ttl=64 id=53148 iple
=40  seq=389746812 win=1480
ENT (4.3530s) TCP 10.159.100.1:31002 > 10.84.84.150:5246 S ttl=64 id=53148 iple
=40  seq=389746812 win=1480
ENT (5.3670s) TCP 10.159.100.1:31002 > 10.84.84.150:5246 S ttl=64 id=53148 iple
=40  seq=389746812 win=1480
CVD (5.3670s) TCP 10.84.84.150:5246 > 10.159.100.1:31002 RA ttl=124 id=8284 ipl
n=40  seq=0 win=0
ENT (6.3810s) TCP 10.159.100.1:31002 > 10.84.84.150:5246 S ttl=64 id=53148 iple
=40  seq=389746812 win=1480
CVD (6.3810s) TCP 10.84.84.150:5246 > 10.159.100.1:31002 RA ttl=124 id=8285 ipl
n=40  seq=0 win=0
ENT (7.3950s) TCP 10.159.100.1:31002 > 10.84.84.150:5246 S ttl=64 id=53148 iple
=40  seq=389746812 win=1480
CVD (7.3950s) TCP 10.84.84.150:5246 > 10.159.100.1:31002 RA ttl=124 id=8286 ipl
n=40  seq=0 win=0
ENT (8.4090s) TCP 10.159.100.1:31002 > 10.84.84.150:5246 S ttl=64 id=53148 iple
=40  seq=389746812 win=1480
ENT (9.4230s) TCP 10.159.100.1:31002 > 10.84.84.150:5246 S ttl=64 id=53148 iple
=40  seq=389746812 win=1480
```

- Check Hit Count on SD-WAN Rule on the Branch Firewall

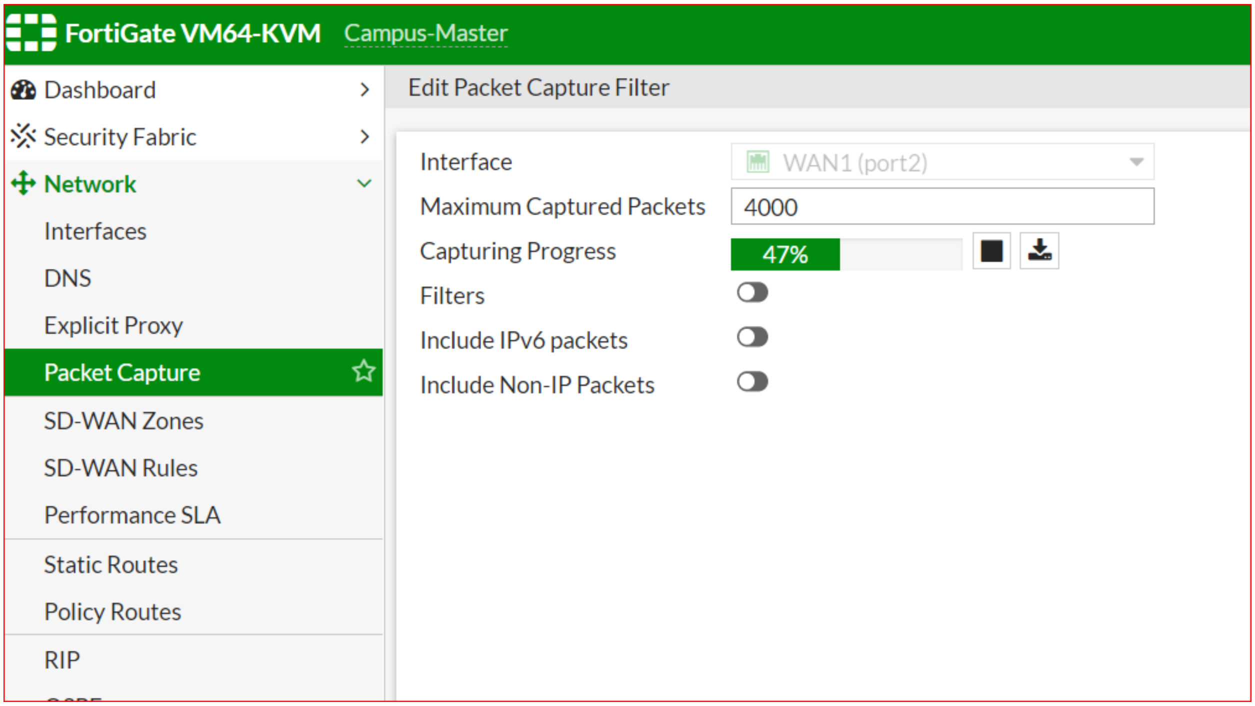


IPv4 12

11	VPN_SCTP	LAN-BR	LAN-HQ	SLA	VPN_to_A_ISP1 ✓	0
12	VPN_SCTP_BK	LAN-BR	LAN-HQ	SLA	VPN_to_B_ISP2 ✓	0
1	VPN_CAPWAP	LAN-BR	LAN-HQ	SLA	VPN_to_A_ISP1 ✓	4,295
4	VPN_CAPWAP_BK	LAN-BR	LAN-HQ	SLA	VPN_to_B_ISP2 ✓	34
5	VPN_DNS	LAN-BR	LAN-HQ	SLA	VPN_to_A_ISP1 ✓	0
6	VPN_DNS_BK	LAN-BR	LAN-HQ	SLA	VPN_to_B_ISP2 ✓	0
7	VPN_RADIUS	LAN-BR	LAN-HQ	SLA	VPN_to_A_ISP1 ✓	0
8	VPN_RADIUS_BK	LAN-BR	LAN-HQ	SLA	VPN_to_B_ISP2 ✓	2
9	VPN_DCHP	LAN-BR	LAN-HQ	SLA	VPN_to_A_ISP1 ✓	0
10	VPN_DHCP_BK	LAN-BR	LAN-HQ	SLA	VPN_to_B_ISP2 ✓	0
3	VPN	LAN-BR	LAN-HQ	SLA	VPN_to_B_ISP2 ✓ VPN_to_A_ISP1 ✓	923
2	INTERNET	all	all	SLA	WAN1 (port2) WAN2 (port4) ✓	241

3. Verification DSCP mapping on ESP packets via ISP network.

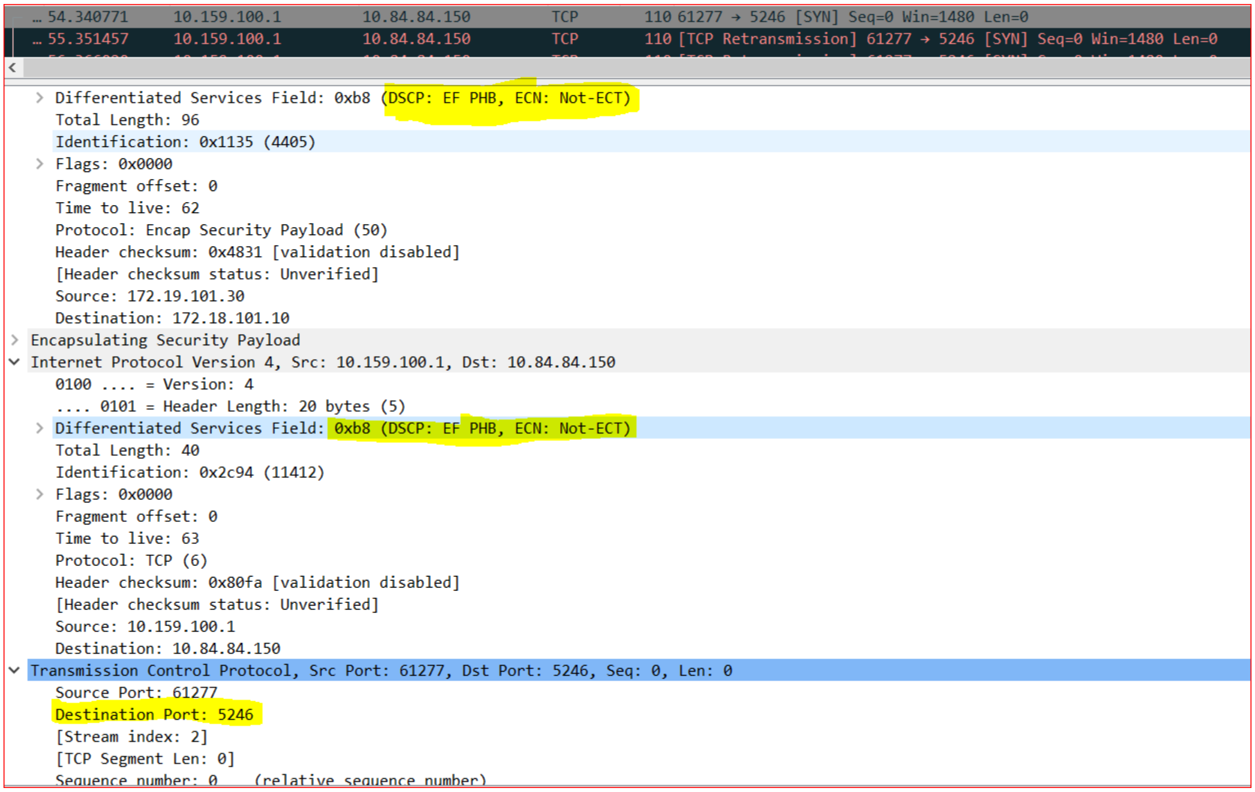
- This link for how to decrypt ESP packets on FortiGate Firewall: *https://kb.fortinet.com/kb/documentLink.do?externalID=FD48280*
- Generate the VPN traffic on USR PC to the Data Center and capture packets with on WAN interface



Edit Packet Capture Filter

Interface: WAN1 (port2)
Maximum Captured Packets: 4000
Capturing Progress: 47%
Filters: ○
Include IPv6 packets: ○
Include Non-IP Packets: ○

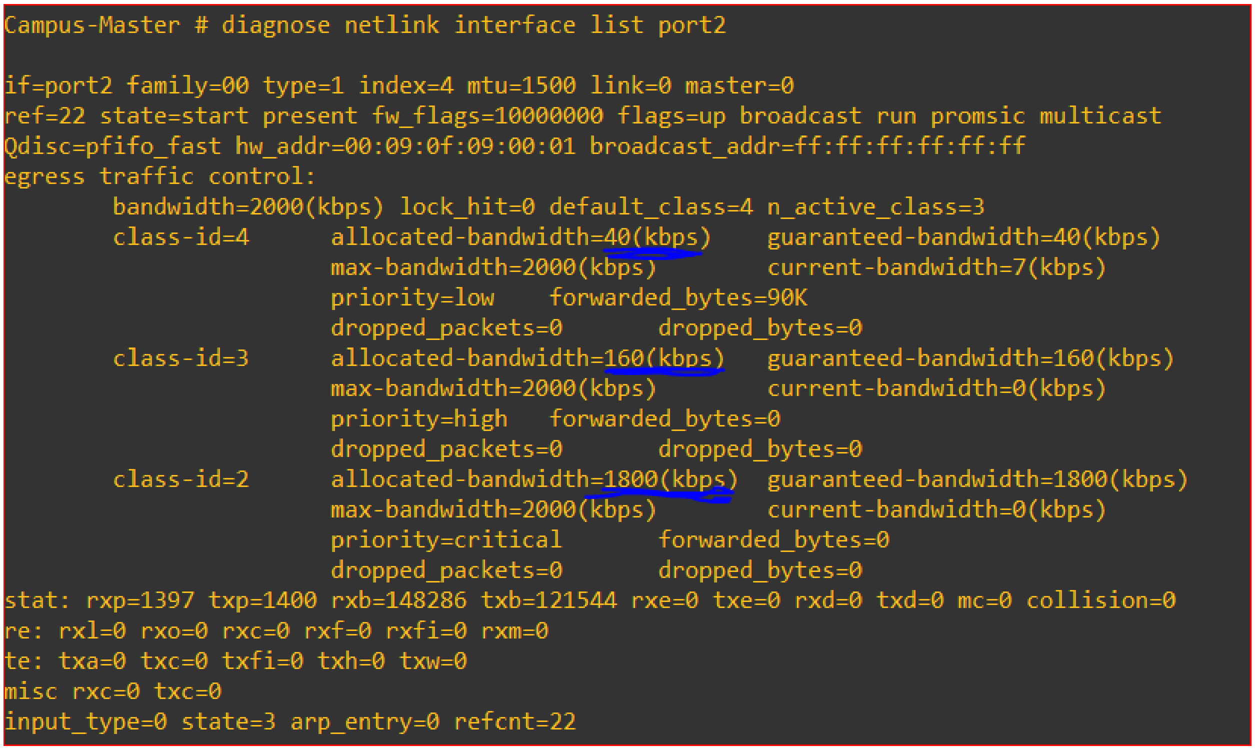
- Use wireshark to decrypt ESP packets



```
… 54.340771    10.159.100.1    10.84.84.150    TCP    110 61277 → 5246 [SYN] Seq=0 Win=1480 Len=0
… 55.351457    10.159.100.1    10.84.84.150    TCP    110 [TCP Retransmission] 61277 → 5246 [SYN] Seq=0 Win=1480 Len=0

  > Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    Total Length: 96
    Identification: 0x1135 (4405)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 62
    Protocol: Encap Security Payload (50)
    Header checksum: 0x4831 [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.19.101.30
    Destination: 172.18.101.10
> Encapsulating Security Payload
v Internet Protocol Version 4, Src: 10.159.100.1, Dst: 10.84.84.150
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0xb8 (DSCP: EF PHB, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x2c94 (11412)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 63
    Protocol: TCP (6)
    Header checksum: 0x80fa [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.159.100.1
    Destination: 10.84.84.150
v Transmission Control Protocol, Src Port: 61277, Dst Port: 5246, Seq: 0, Len: 0
    Source Port: 61277
    Destination Port: 5246
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence number: 0    (relative sequence number)
```

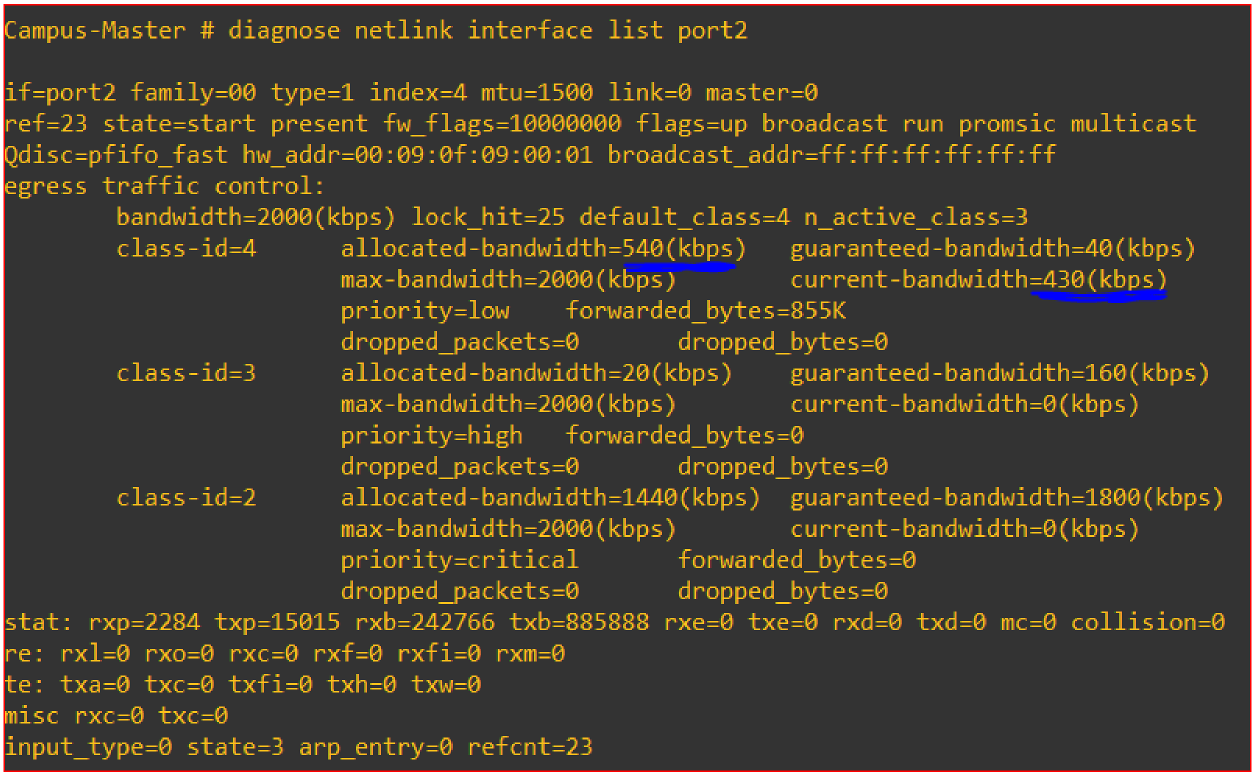
4. Verification Traffic shaping on WAN interface

- Check allocated bandwidth on WAN1 interface (assume the link to ISP2 down -> all traffic via one physical link)



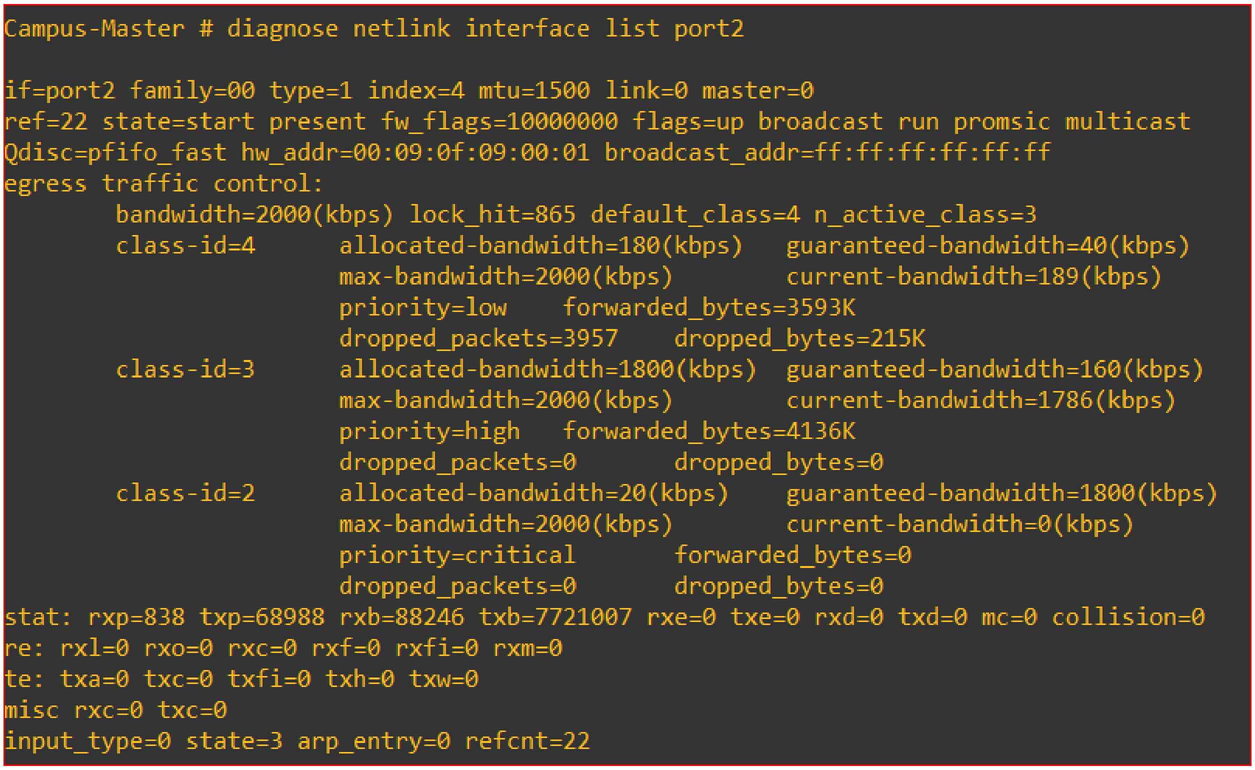
```
Campus-Master # diagnose netlink interface list port2

if=port2 family=00 type=1 index=4 mtu=1500 link=0 master=0
ref=22 state=start present fw_flags=10000000 flags=up broadcast run promsic multicast
Qdisc=pfifo_fast hw_addr=00:09:0f:09:00:01 broadcast_addr=ff:ff:ff:ff:ff:ff
egress traffic control:
        bandwidth=2000(kbps) lock_hit=0 default_class=4 n_active_class=3
        class-id=4      allocated-bandwidth=40(kbps)    guaranteed-bandwidth=40(kbps)
                        max-bandwidth=2000(kbps)        current-bandwidth=7(kbps)
                        priority=low    forwarded_bytes=90K
                        dropped_packets=0       dropped_bytes=0
        class-id=3      allocated-bandwidth=160(kbps)   guaranteed-bandwidth=160(kbps)
                        max-bandwidth=2000(kbps)        current-bandwidth=0(kbps)
                        priority=high   forwarded_bytes=0
                        dropped_packets=0       dropped_bytes=0
        class-id=2      allocated-bandwidth=1800(kbps)  guaranteed-bandwidth=1800(kbps)
                        max-bandwidth=2000(kbps)        current-bandwidth=0(kbps)
                        priority=critical       forwarded_bytes=0
                        dropped_packets=0       dropped_bytes=0
stat: rxp=1397 txp=1400 rxb=148286 txb=121544 rxe=0 txe=0 rxd=0 txd=0 mc=0 collision=0
re: rxl=0 rxo=0 rxc=0 rxf=0 rxfi=0 rxm=0
te: txa=0 txc=0 txfi=0 txh=0 txw=0
misc rxc=0 txc=0
input_type=0 state=3 arp_entry=0 refcnt=22
```

- Now generate the Internet Traffic from PC to check allocated bandwidth in that time



```
Campus-Master # diagnose netlink interface list port2

if=port2 family=00 type=1 index=4 mtu=1500 link=0 master=0
ref=23 state=start present fw_flags=10000000 flags=up broadcast run promsic multicast
Qdisc=pfifo_fast hw_addr=00:09:0f:09:00:01 broadcast_addr=ff:ff:ff:ff:ff:ff
egress traffic control:
        bandwidth=2000(kbps) lock_hit=25 default_class=4 n_active_class=3
        class-id=4      allocated-bandwidth=540(kbps)   guaranteed-bandwidth=40(kbps)
                        max-bandwidth=2000(kbps)        current-bandwidth=430(kbps)
                        priority=low    forwarded_bytes=855K
                        dropped_packets=0       dropped_bytes=0
        class-id=3      allocated-bandwidth=20(kbps)    guaranteed-bandwidth=160(kbps)
                        max-bandwidth=2000(kbps)        current-bandwidth=0(kbps)
                        priority=high   forwarded_bytes=0
                        dropped_packets=0       dropped_bytes=0
        class-id=2      allocated-bandwidth=1440(kbps)  guaranteed-bandwidth=1800(kbps)
                        max-bandwidth=2000(kbps)        current-bandwidth=0(kbps)
                        priority=critical       forwarded_bytes=0
                        dropped_packets=0       dropped_bytes=0
stat: rxp=2284 txp=15015 rxb=242766 txb=885888 rxe=0 txe=0 rxd=0 txd=0 mc=0 collision=0
re: rxl=0 rxo=0 rxc=0 rxf=0 rxfi=0 rxm=0
te: txa=0 txc=0 txfi=0 txh=0 txw=0
misc rxc=0 txc=0
input_type=0 state=3 arp_entry=0 refcnt=23
```

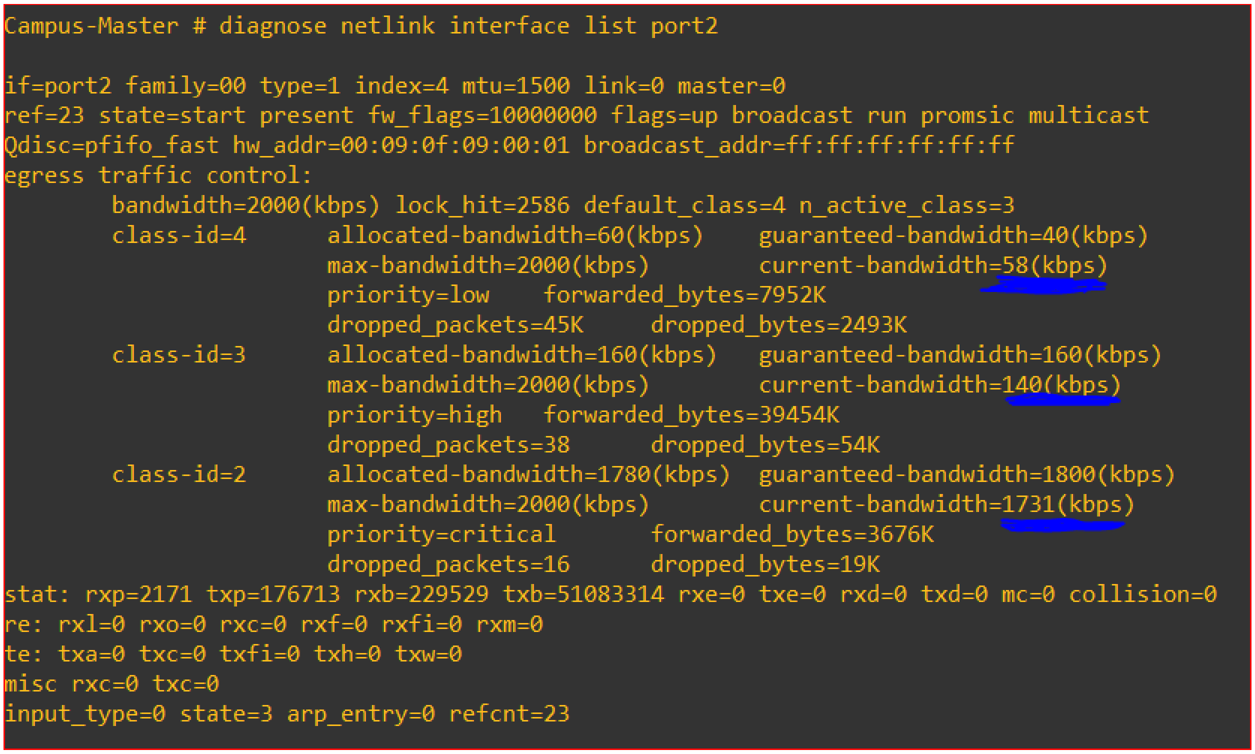
- Generate the VPN traffic between Branch and the Data Center (Business Apps) with bandwidth equal 1.7M



```
Campus-Master # diagnose netlink interface list port2

if=port2 family=00 type=1 index=4 mtu=1500 link=0 master=0
ref=22 state=start present fw_flags=10000000 flags=up broadcast run promsic multicast
Qdisc=pfifo_fast hw_addr=00:09:0f:09:00:01 broadcast_addr=ff:ff:ff:ff:ff:ff
egress traffic control:
        bandwidth=2000(kbps) lock_hit=865 default_class=4 n_active_class=3
        class-id=4      allocated-bandwidth=180(kbps)   guaranteed-bandwidth=40(kbps)
                        max-bandwidth=2000(kbps)        current-bandwidth=189(kbps)
                        priority=low    forwarded_bytes=3593K
                        dropped_packets=3957    dropped_bytes=215K
        class-id=3      allocated-bandwidth=1800(kbps)  guaranteed-bandwidth=160(kbps)
                        max-bandwidth=2000(kbps)        current-bandwidth=1786(kbps)
                        priority=high   forwarded_bytes=4136K
                        dropped_packets=0       dropped_bytes=0
        class-id=2      allocated-bandwidth=20(kbps)    guaranteed-bandwidth=1800(kbps)
                        max-bandwidth=2000(kbps)        current-bandwidth=0(kbps)
                        priority=critical       forwarded_bytes=0
                        dropped_packets=0       dropped_bytes=0
stat: rxp=838 txp=68988 rxb=88246 txb=7721007 rxe=0 txe=0 rxd=0 txd=0 mc=0 collision=0
re: rxl=0 rxo=0 rxc=0 rxf=0 rxfi=0 rxm=0
te: txa=0 txc=0 txfi=0 txh=0 txw=0
misc rxc=0 txc=0
input_type=0 state=3 arp_entry=0 refcnt=22
```

-> *Secure_Internet Class Traffic will be dropped to give bandwidth for Business Class with the priority higher.*

- Continue generate DHCP traffic (UDP 67) from PC to the Data Center (Critical_Apps) with bandwidth equal 1.8M



```
Campus-Master # diagnose netlink interface list port2

if=port2 family=00 type=1 index=4 mtu=1500 link=0 master=0
ref=23 state=start present fw_flags=10000000 flags=up broadcast run promsic multicast
Qdisc=pfifo_fast hw_addr=00:09:0f:09:00:01 broadcast_addr=ff:ff:ff:ff:ff:ff
egress traffic control:
        bandwidth=2000(kbps) lock_hit=2586 default_class=4 n_active_class=3
        class-id=4      allocated-bandwidth=60(kbps)    guaranteed-bandwidth=40(kbps)
                        max-bandwidth=2000(kbps)        current-bandwidth=58(kbps)
                        priority=low    forwarded_bytes=7952K
                        dropped_packets=45K     dropped_bytes=2493K
        class-id=3      allocated-bandwidth=160(kbps)   guaranteed-bandwidth=160(kbps)
                        max-bandwidth=2000(kbps)        current-bandwidth=140(kbps)
                        priority=high   forwarded_bytes=39454K
                        dropped_packets=38      dropped_bytes=54K
        class-id=2      allocated-bandwidth=1780(kbps)  guaranteed-bandwidth=1800(kbps)
                        max-bandwidth=2000(kbps)        current-bandwidth=1731(kbps)
                        priority=critical       forwarded_bytes=3676K
                        dropped_packets=16      dropped_bytes=19K
stat: rxp=2171 txp=176713 rxb=229529 txb=51083314 rxe=0 txe=0 rxd=0 txd=0 mc=0 collision=0
re: rxl=0 rxo=0 rxc=0 rxf=0 rxfi=0 rxm=0
te: txa=0 txc=0 txfi=0 txh=0 txw=0
misc rxc=0 txc=0
input_type=0 state=3 arp_entry=0 refcnt=23
```

-> *Current Bandwidth of Secure Internet and Business Classes have decreased to guaranteed bandwidth.*