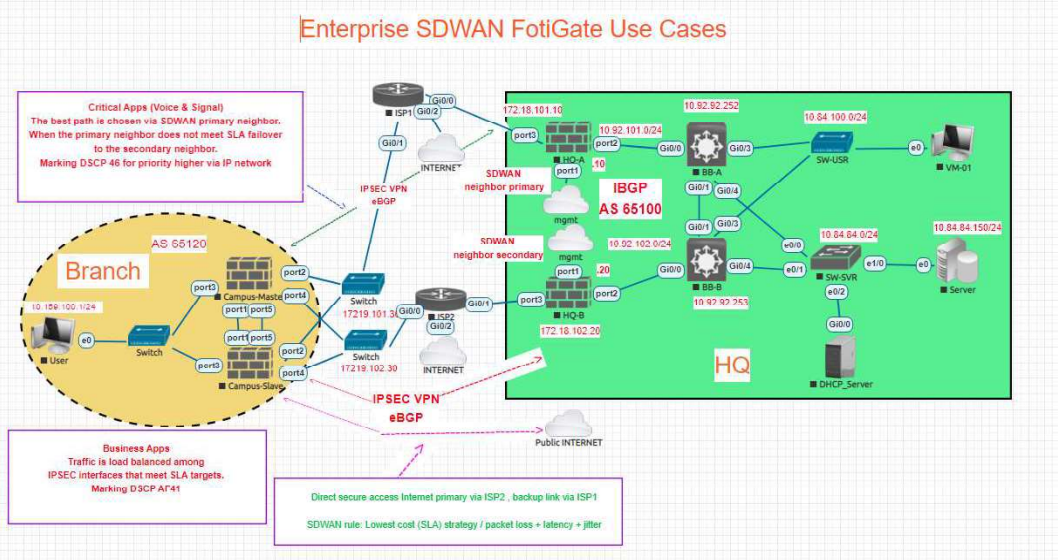
Description

- 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



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

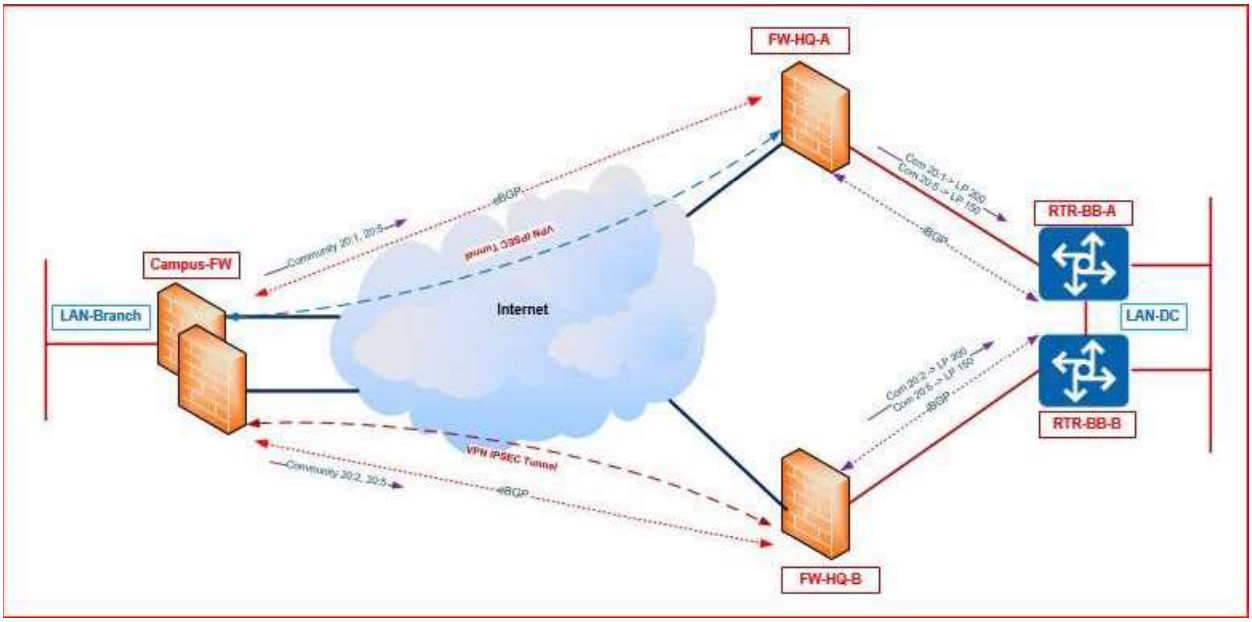
Requirement

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"
```