رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

Project Title:

Implementing VPN Solutions With FortiGate

Track Name:

Infrastructure and Security - Fortinet Cybersecurity Engineer

Prepared By:

1- Shahd Yesen Salah Abdelmoamen
2- Nada Ahmed Abo-Bakr Abdelnaser
3- Jana Hany Salah Eldin
4- Shams Ibrahem Ali Mohamed
5- Mohamed Ahmed Mohamed Haridy
6- Merna Medhat

1. Project Overview

1.1 Project Purpose

The purpose of this project is to design and implement a complete enterprise network using PNETLab, simulating a real-world environment with multiple sites, VLANs, routing, firewalling, and secure connectivity. The design includes HQ and Branch networks connected through IPsec VPN tunnels, supported by SD-WAN and High Availability (HA) mechanisms to ensure network security, redundancy, and performance optimization.

1.2 Objectives

- Design and build a complete enterprise network using PNETLab
- Establish secure site-to-site connectivity between branches using IPsec VPN
- Implement SD-WAN for intelligent failover, link monitoring, and performance optimization
- Configure core network services including Routing, Switching, Inter-VLAN Routing, and Firewalling
- Segment the network using VLANs and subnets to enhance security and manageability
- Apply security policies, VPN policies to protect and control traffic
- Configure device management features such as SSH
- Implement High Availability (HA) for critical network devices and services
- Configure SSL VPN access for remote users
- Perform comprehensive testing of connectivity, VPN stability, SD-WAN behavior, and failover scenarios
- Document the full network design, addressing plan, configurations, and troubleshooting steps

1.3 Topology Used

The enterprise network consists of:

- **One HQ site** with HA-enabled FortiGate pair (F1 Primary, F2 Secondary)
- **One Branch site** with HA-enabled FortiGate pair (F3 Primary, F4 Secondary)
- **Cisco switches** (SW1, SW2, SW3, SW4) for Access and Distribution layers
- **Routers** simulating ISPs
- **VLAN sub-interfaces** for inter-VLAN routing on firewalls
- **IPsec VPN** for secure site-to-site connectivity
- **SD-WAN** enabled on both F1/F2 (HQ) and F3/F4 (Branch) pairs
- **HA active-passive** on F1/F2 and F3/F4

---

2. Network Topology

2.1 Topology Diagram

The enterprise network consists of an HQ site connected to a Branch site through the internet using an IPsec VPN tunnel. The HQ uses FortiGate F1 as the primary firewall (with F2 as secondary in HA) supporting multiple VLANs, HA configuration, and SD-WAN with multiple WAN links. The Branch uses FortiGate F3 as the primary firewall (with F4 as secondary in HA) with a simplified VLAN structure and SD-WAN to connect back to HQ.

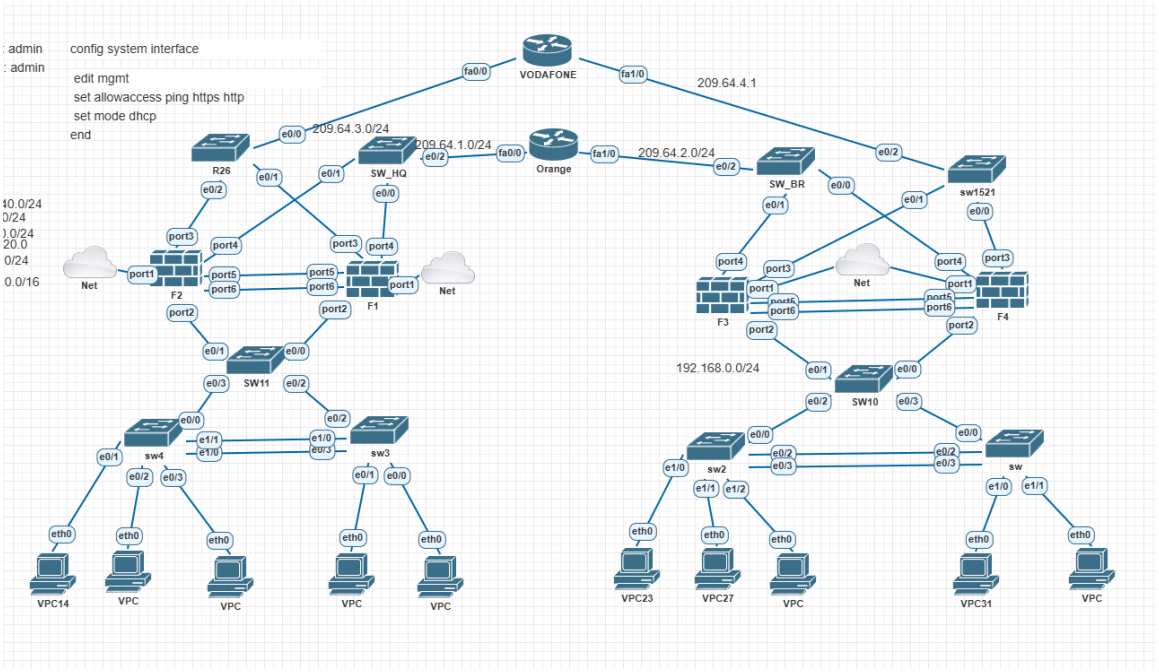


Figure 2.1 – Full Network Topology in PNETLab

2.2 Network Components Description

Headquarters (HQ)

- **FortiGate F1 (Primary)** and **F2 (Secondary)**
  - HA-enabled active-passive pair
  - Multiple VLANs for departments (10, 20, 30, 40, 50)
  - SD-WAN with multiple WAN links for redundancy
  - IPsec VPN tunnel termination to Branch
- **Switch SW1** (Distribution/Core)
  - Supports all HQ VLANs
  - Trunk link to SW2
  - Port security and DHCP snooping enabled

- **Switch SW2** (Access)
    - Trunk links with Port-channel to SW1 and other switches
    - Access ports for end-user VLANs
    - Port security (max 2 MACs per port, sticky, restrict)
    - DHCP snooping and Dynamic ARP Inspection
- **Local clients** connected through VLANs

Branch (BR)

- **FortiGate F3 (Primary)** and **F4 (Secondary)**
    - HA-enabled active-passive pair
    - Dual LAN interfaces
    - SD-WAN enabled for failover
    - Limited VLANs (10, 20)
    - Direct IPsec tunnel to HQ
- **Switch SW3** and **SW4**
    - Local VLAN support
    - Trunk connectivity
    - Access ports for end-user VLANs

---

3. IP Addressing Scheme

3.1 IP Table

HQ (F1/F2 HA Pair)

Interface	IP Address	Purpose
port1	172.16.0.1/24	LAN 1
port2	172.16.1.2/24	LAN 2
port3	209.64.1.2/24	WAN (ISP 1)
VLAN10	172.16.10.1/24	Management
VLAN20	172.16.20.1/24	HR
VLAN30	172.16.30.1/24	IT
VLAN40	172.16.40.1/24	Finance
VLAN50	172.16.50.1/24	Sales

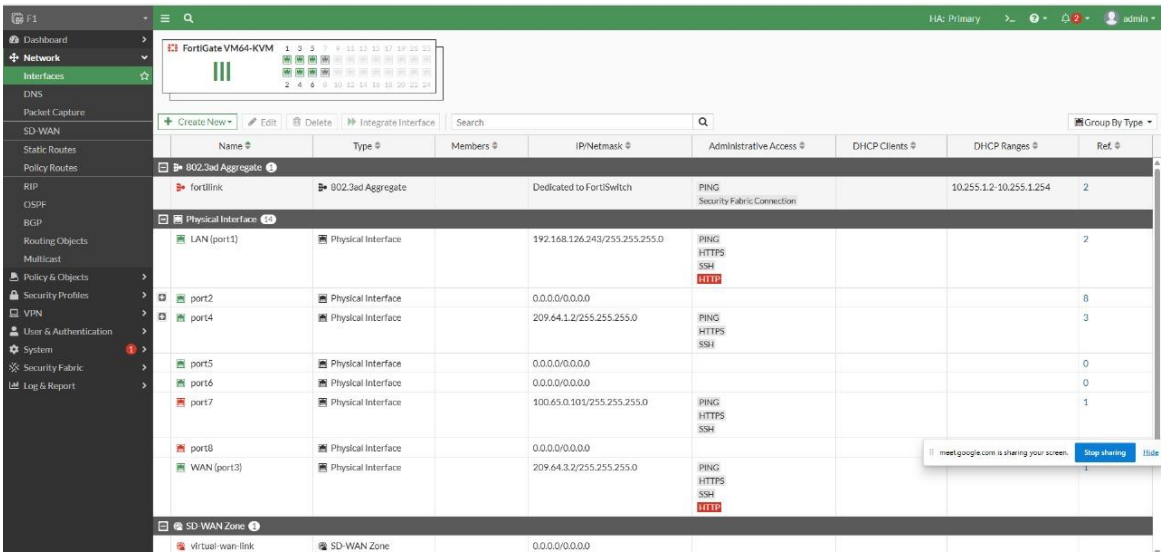


Figure 3.1 – HQ Interface Table (F1)

Branch (F3/F4 HA Pair)

Interface	IP Address	Purpose
port1	192.168.126.244/24	LAN 1
port2	192.168.20.1/24	LAN 2
port3	209.64.1.3/24	WAN (ISP)
VLAN10	10.10.10.1/24	Management
VLAN20	10.10.20.1/24	HR
VLAN30	10.10.30.1/24	IT
VLAN40	10.10.40.1/24	Finance
VLAN50	10.10.50.1/24	Sales

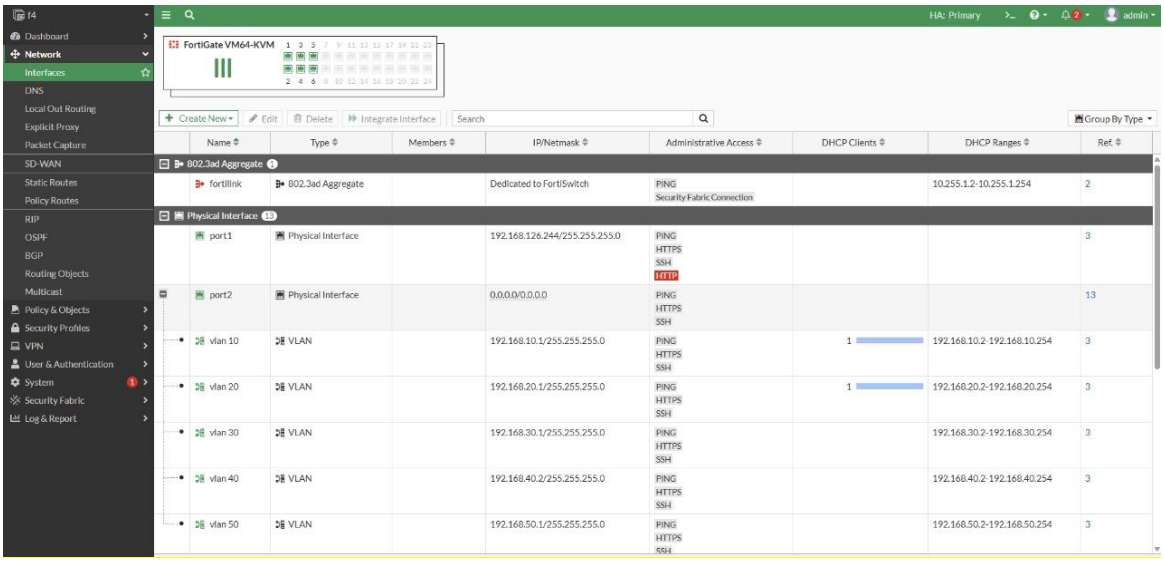


Figure 3.2 – Branch Interface Table (F3)

3.2 Addressing Plan Summary

- **Private addressing** used internally
- **HQ uses 172.16.x.x networks** for internal VLANs
- **Branch uses 192.168.x.x networks** (or 10.x.x.x as applicable)
- **WAN links use public IPs (209.64.1.x/24)** for internet connectivity
- **VLANs are isolated per department** for security and manageability
- **Routing between VLANs** handled by F1/F2 and F3/F4 firewalls respectively
- **HA virtual IP** used for gateway redundancy (not explicitly shown but configured in standby groups)

---

4. VLANs & Subnets

4.1 VLAN List

HQ VLANs

VLAN ID	Name	Purpose
10	Management	Administrative access and device management
20	HR	Human Resources department
30	IT	Information Technology department
40	Finance	Finance department
50	Sales	Sales department

99	Reserved	Reserved for future use
100	Native VLAN	Native VLAN for trunk ports

Branch VLANs

VLAN ID	Name	Purpose
10	Management	Administrative access and device management
20	HR	Human Resources department
30	IT	Information Technology department
40	Finance	Finance department
50	Sales	Sales department

Figure 4.1 – HQ Zone br containing VLANs 10, 20, 30, 40, 50 on F1 and F4

4.2 VLAN Purpose

- **VLAN 10**: Management traffic and administrative access to network devices
- **VLAN 20**: HR department internal traffic
- **VLAN 30**: IT department internal traffic
- **VLAN 40**: Finance department internal traffic
- **VLAN 50**: Sales department internal traffic
- **VLAN 100**: Native VLAN for trunk encapsulation
- **VLAN 99**: Reserved for future departmental expansion

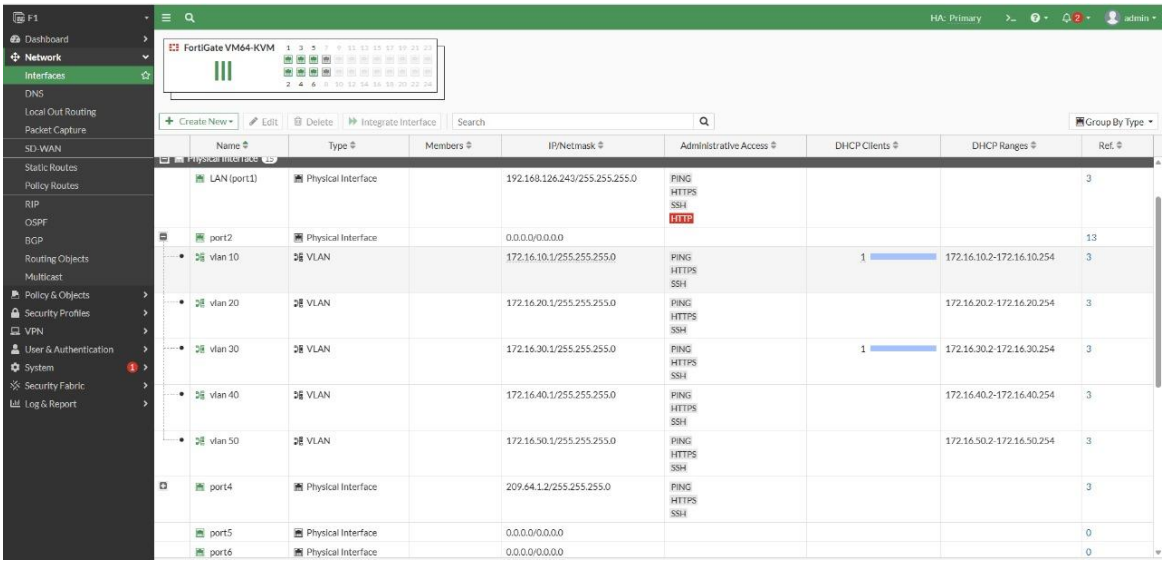


Figure 4.2 – HQ VLAN List (F1)

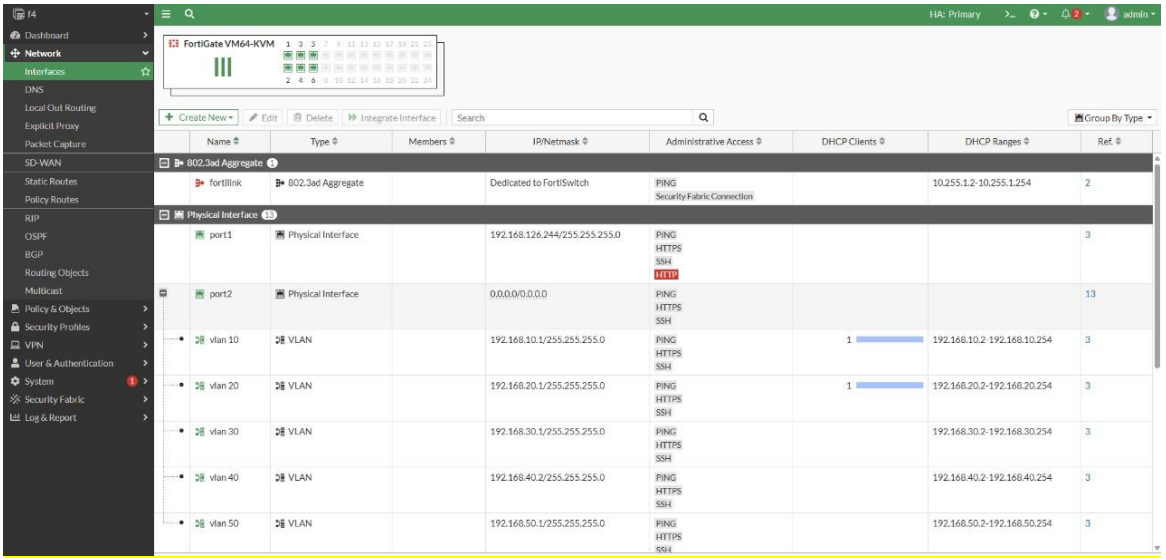


Figure 4.3 – Branch VLAN List (F3)

---

5. Device Configuration

This section provides an overview of the configuration applied to all network devices used in the project, including ISP routers, switches, and FortiGate firewalls. The configuration follows best practices for enterprise networks, covering trunking, VLAN segmentation, security features, HA, and SD-WAN.

5.1 ISP Router Configuration

- **ISP1 Router**: Simulates public internet
    - IP: 209.64.1.1/24

- Provides default gateway for F1/F2 (209.64.1.2)
- Provides default gateway for F3/F4 (209.64.1.3)
- Enables ping/connectivity between firewalls over WAN

5.2 Switch Configuration

The switches (SW1, SW2, SW3, SW4) are configured to operate as Access and Distribution layer devices, supporting all VLANs, trunk links, and security features such as DHCP Snooping and Port Security.

Trunk Ports

- **Trunk ports** configured for inter-switch and firewall uplinks
- **Allowed VLANs**: 10, 20, 30, 40, 50
- **Native VLAN**: 100
- **Encapsulation**: 802.1Q (dot1q)
- **Negotiation**: Disabled (switchport nonegotiate)
- **SW2 EtherChannel**: Port-channel 2 (Ethernet0/2, Ethernet0/3) in active mode
- **Uplink trust**: ARP Inspection and DHCP Snooping trust enabled on trunk ports

Access Ports

Access ports are assigned based on departments:

- **VLAN 10** – Management
- **VLAN 20** – HR
- **VLAN 30** – IT
- **VLAN 40** – Finance (SW2 Ethernet1/0)
- **VLAN 50** – Sales (SW2 Ethernet1/1)

Port Security

Applied to protect client ports:

- **mac-address sticky**: Learned MACs are added to the running configuration
- **violation restrict**: Drops packets from unknown MACs without triggering port shutdown
- **maximum 2**: Allows only 2 MAC addresses per port
- **Sticky MACs** (examples from SW2):
  - E1/0 (VLAN 40): 0050.7966.680d, 0050.7966.6825
  - E1/1 (VLAN 50): 0050.7966.680e, 0050.7966.6826
  - E1/2 (VLAN 30): 504c.8700.1300, 508a.9900.1300

DHCP Snooping & ARP Inspection

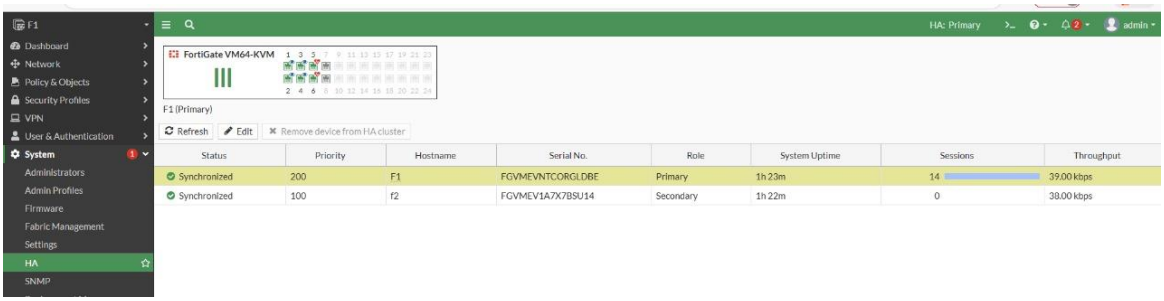
- **DHCP Snooping** enabled on all user VLANs (10, 20, 30, 40, 50)
- **Uplink ports** (E0/0, E0/1 on SW2) added as trusted
- **Dynamic ARP Inspection** enabled for attack prevention
- **HSRP SVI Interfaces** on VLANs 10–50 with standby IP and priority 110 (currently administratively shut because L3 routing is handled by firewalls)

5.3 Firewall Configuration

FortiGate HQ (F1/F2 HA Pair)

High Availability Configuration:

- **Mode**: Active-Passive
- **Priority F1**: 200 (Primary)
- **Priority F2**: 100 (Secondary)
- **Heartbeat**: Serial cable on dedicated HA ports
- **Monitoring**: HA monitors CPU, memory, and interface status
- **Failover**: Automatic on F1 failure



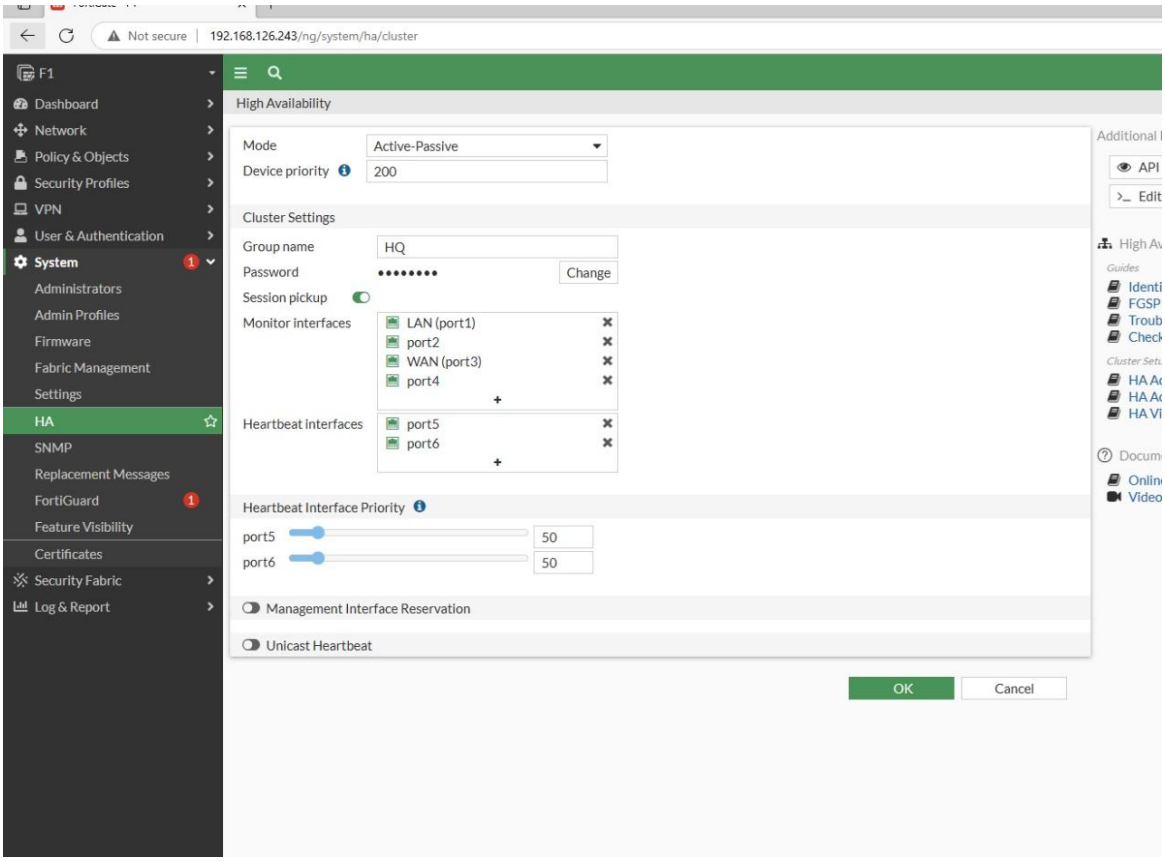


Figure 5.3 – HQ FortiGate HA Status (F1/F2)

FortiGate Branch (F3/F4 HA Pair)

High Availability Configuration:

- **Mode**: Active-Passive
- **Priority F3**: 100 (Secondary)
- **Priority F4**: 200 (Primary)
- **Heartbeat**: Serial cable on dedicated HA ports
- **Failover**: Automatic on F3 failure

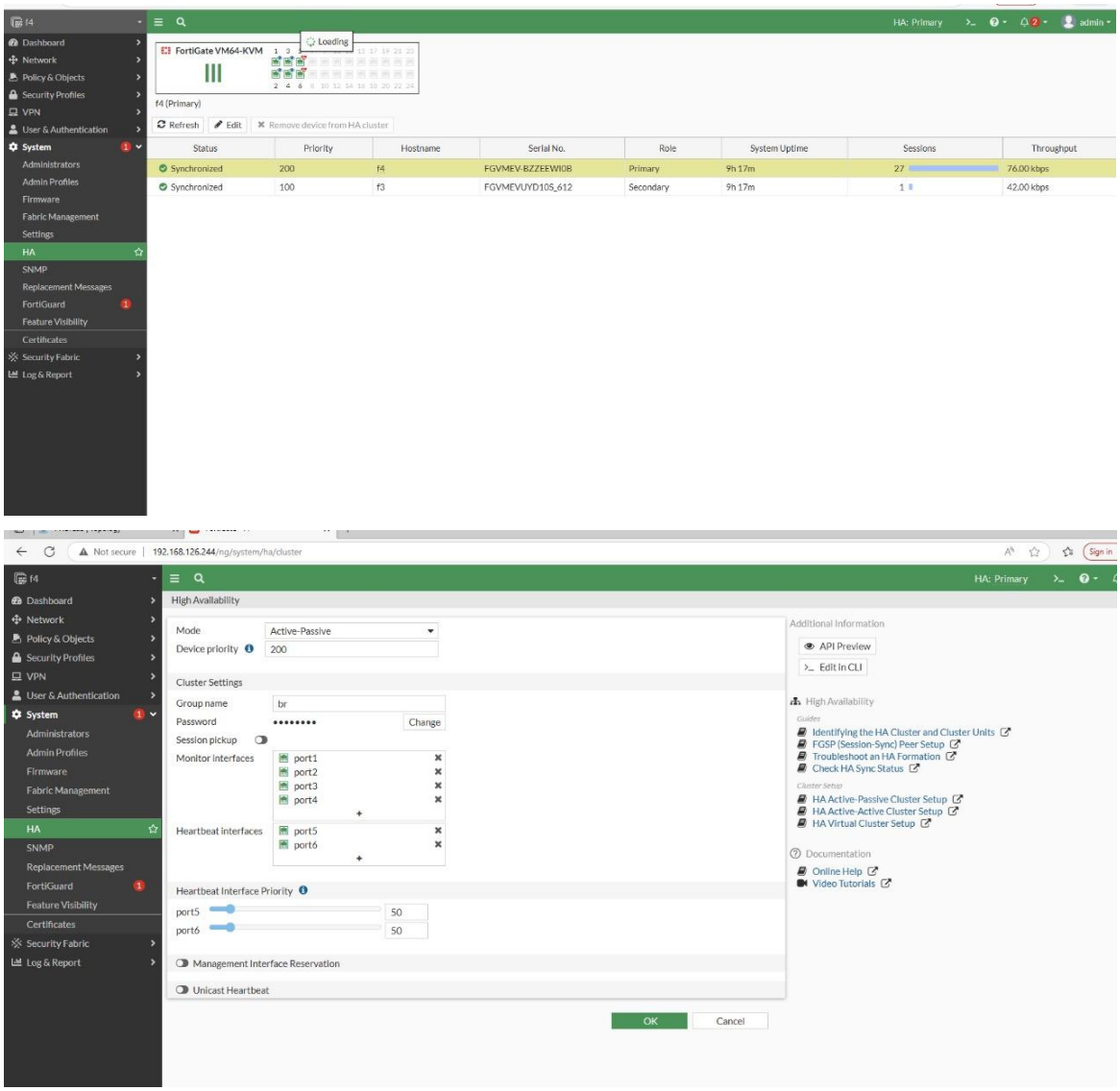


Figure 5.4 – Branch FortiGate HA Status (F3/F4)

---

6. VPN Configuration

6.1 Phase 1 (IKE) Settings

IPsec Tunnel Name: F1_to_F3 (and reverse F3_to_F1)

- **Mode**: Interface mode
- **Authentication**: Pre-shared key (PSK)
- **Encryption**: AES128, AES256
- **Hash**: SHA1, SHA256
- **DH Groups**: Group 1, 2, 5, 14
- **Local WAN Interface**: port3 (F1/F2: 209.64.1.2, F3/F4: 209.64.1.3)

- **Remote Gateway**:
  - F1 → F3: 209.64.1.3
  - F3 → F1: 209.64.1.2
- **Lifetime**: 28800 seconds (8 hours)

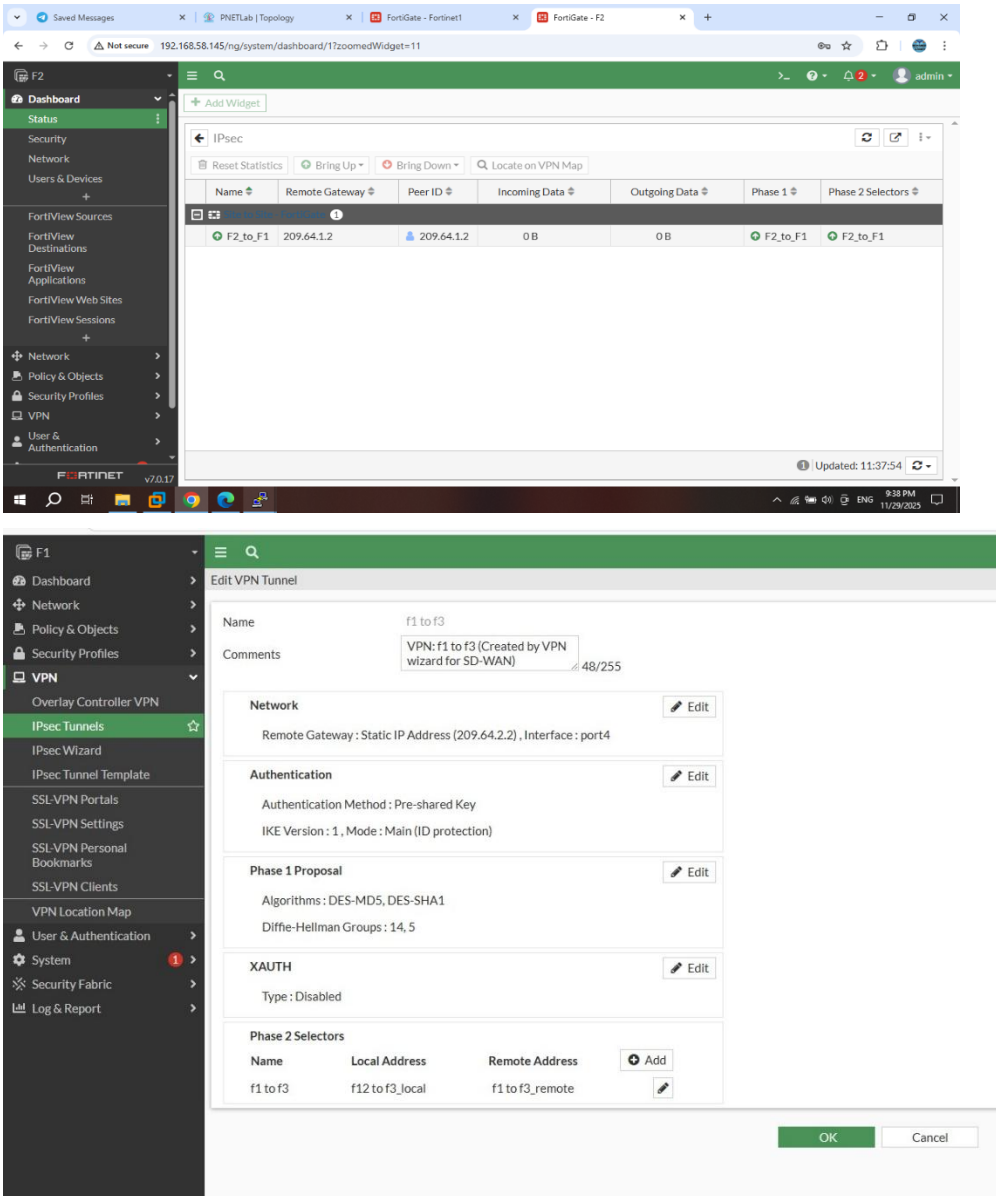


Figure 6.1 – IPsec Tunnel Status (F1 – Primary HQ Firewall)

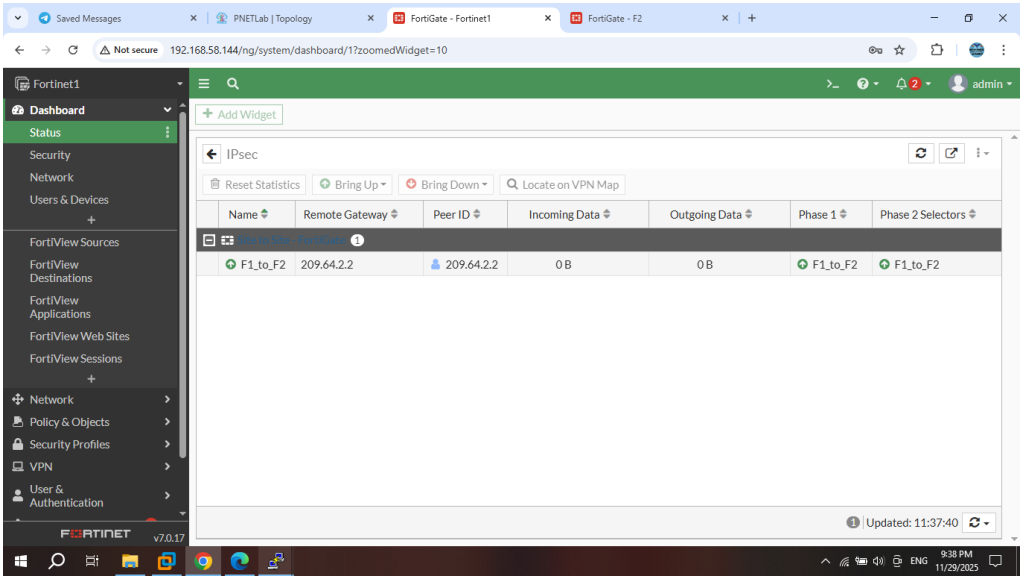


Figure 6.2 – IPsec Tunnel Status (F2 – Secondary HQ Firewall)

6.2 SSL VPN Configuration

In this setup, SSL-VPN is enabled on the LAN interface (port1) using TCP port 10443 to receive remote user connections, with the built-in Fortinet_Factory certificate used for encryption. An automatic address range is configured for tunnel-mode clients so that each remote user receives an internal IP address and can securely access the HQ network through the SSL-VPN service

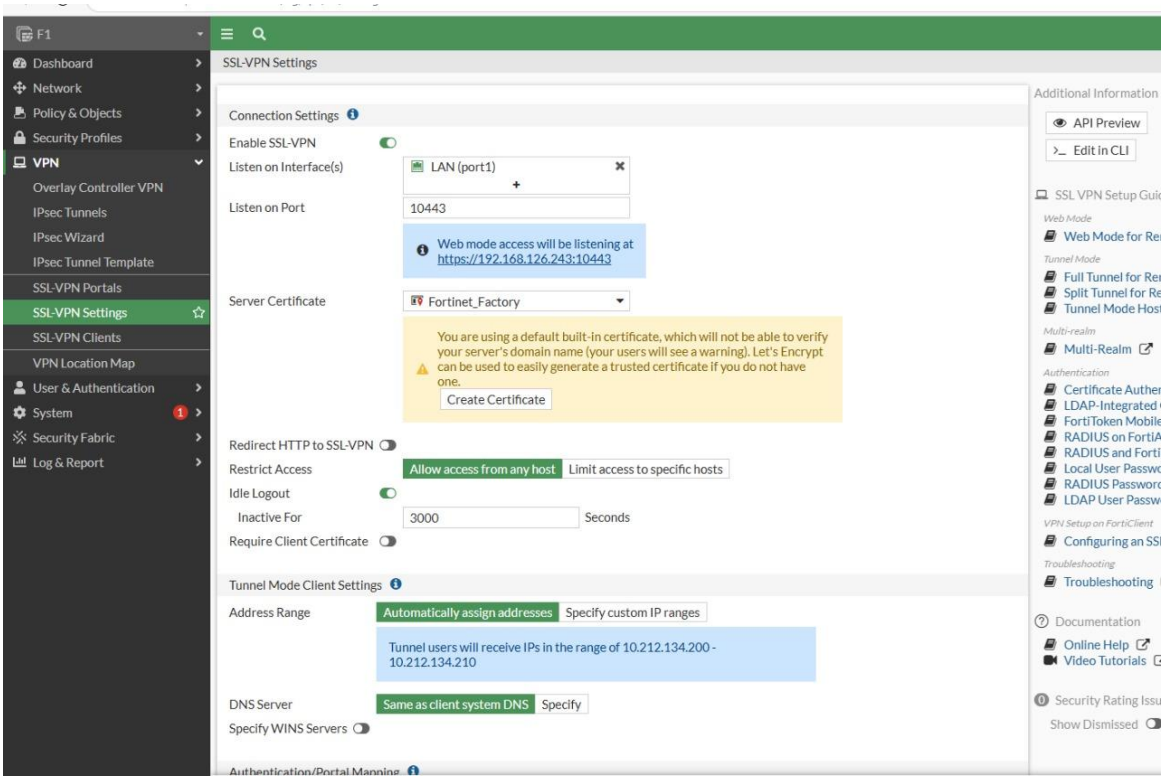


Figure 6.3 – SSL-VPN Global Settings on F1

6.3 VPN Policies

F1/F2 Outbound Policies:

- Source: All HQ VLANs (172.16.10/20/30/40/50.0/24)
- Destination: All Branch VLANs (10.10.10/20.0/24 or 192.168.10/20.0/24)
- Service: Any
- Action: Encrypt over F1_to_F3 IPsec tunnel

F3/F4 Outbound Policies:

- Source: All Branch VLANs (10.10.10/20.0/24 or 192.168.10/20.0/24)
- Destination: All HQ VLANs (172.16.10/20/30/40/50.0/24)
- Service: Any
- Action: Encrypt over F3_to_F1 IPsec tunnel

Reverse (Inbound) Policies:

- Traffic from tunnel automatically matches reverse direction and is decrypted
- Return traffic follows same policy logic in reverse

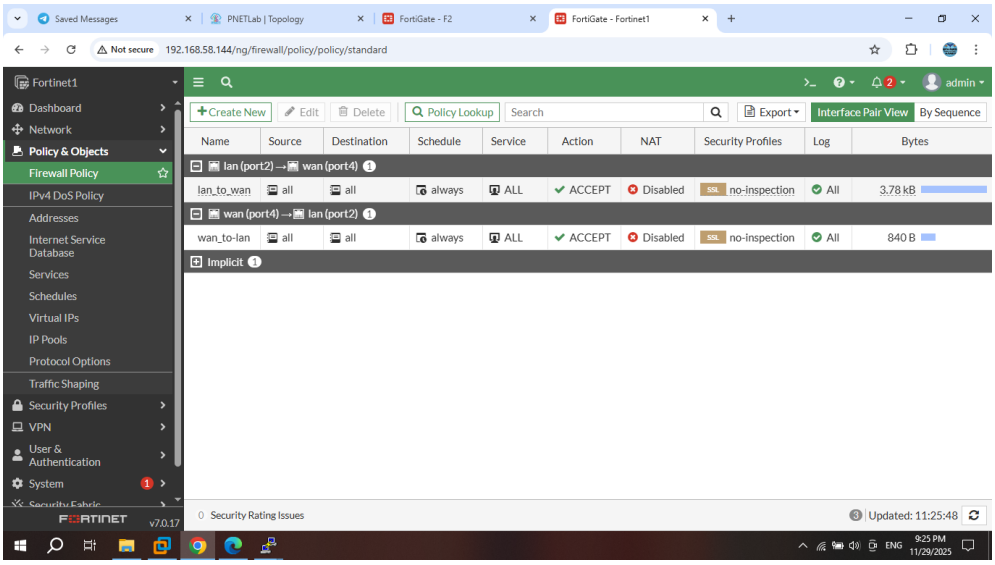


Figure 6.3 – HQ Firewall IPv4 Policies for LAN ⇔ IPsec/WAN (F1)

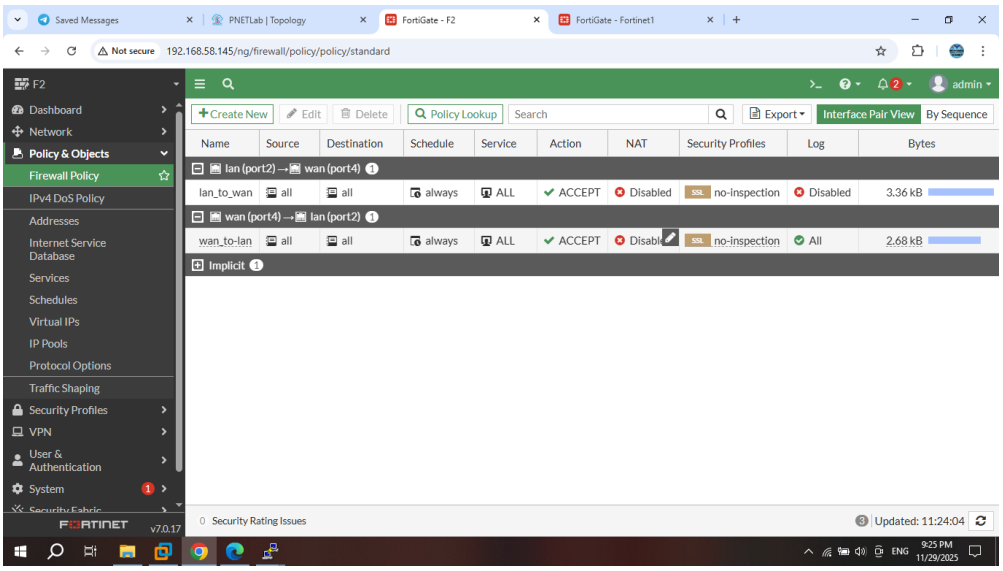


Figure 6.4 – Backup HQ Firewall IPv4 Policies (F2)

---

7. SD-WAN Configuration

7.1 WAN Interfaces

- **WAN1 (port3)**: Primary ISP link
    - F1/F2: 209.64.1.2/24 (gateway 209.64.1.1)
    - F3/F4: 209.64.1.3/24 (gateway 209.64.1.1)
- **WAN2 (port2)** (optional for redundancy):
    - Can be configured as secondary ISP or backup link
    - Currently optional in this topology

7.2 SD-WAN Members

F1/F2 SD-WAN Members:

- **Member 1**: port3 (primary)
    - Gateway: 209.64.1.1
    - Weight: 50 (traffic weighting)
    - Cost: 100 (relative link cost)
- **Member 2**: port2 (optional secondary)
    - Gateway: 172.16.1.1 (or alternative ISP)
    - Weight: 50
    - Cost: 200

F3/F4 SD-WAN Members:

- **Member 1**: port3 (primary)
    - Gateway: 209.64.1.1
    - Weight: 50
- **Member 2**: port2 (optional)
    - Gateway: 192.168.20.1 (or alternative ISP)
    - Weight: 50

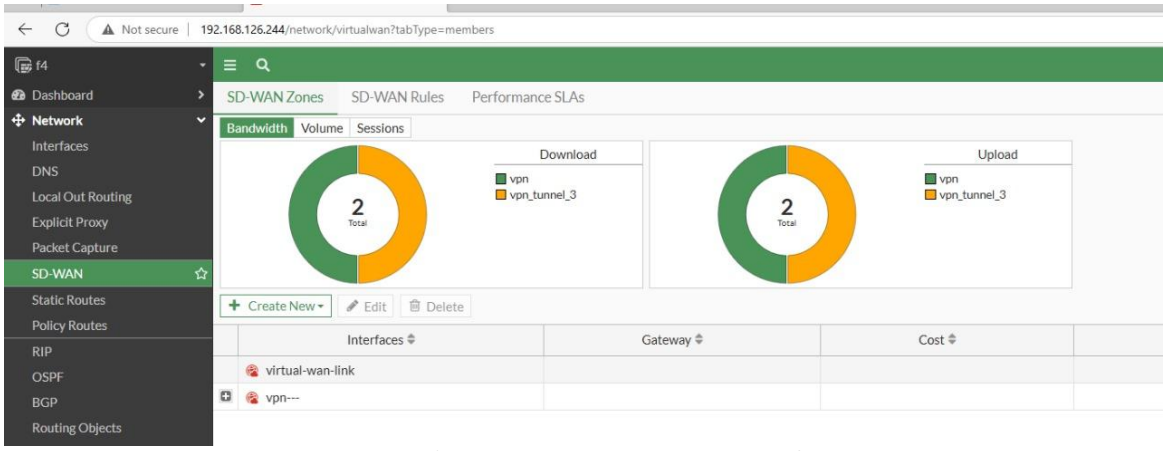


Figure 7.2 – SD-WAN Members

7.3 Traffic Steering Rules

F1/F2 to F3/F4 VPN Traffic:

- Source: HQ VLANs
- Destination: Branch VLANs
- Service: IPsec
- SD-WAN preference: Primary WAN1, failover to WAN2
- Traffic load: Balanced across available WAN links

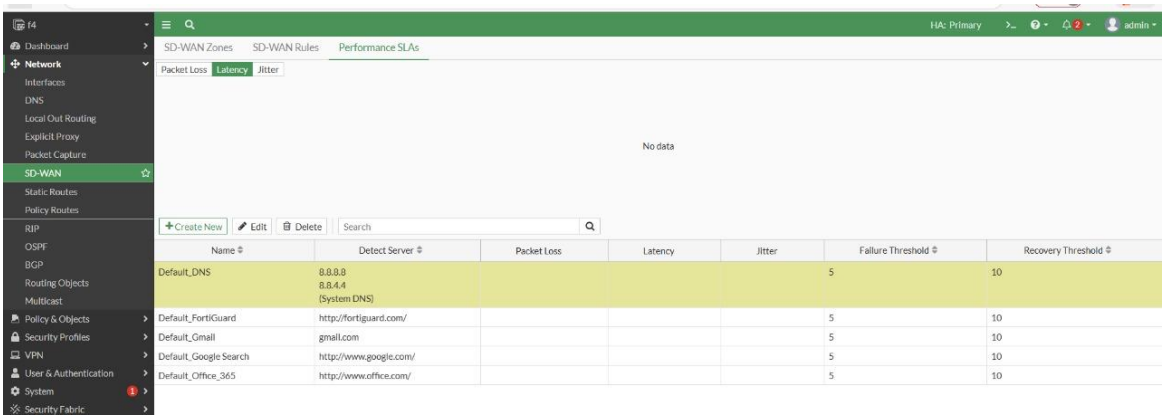


Figure 7.3 – SD-WAN Performance SLA

8. Testing & Verification

8.1 Connectivity Tests

Test 1: Ping HQ VLAN 10 to Branch VLAN 10

- Source: VPCS in HQ VLAN10 (172.16.10.x)
- Destination: VPCS in Branch VLAN10 (10.10.10.x or 192.168.10.x)
- **Result**: All pings successful over IPsec tunnel (0% packet loss)

Test 2: Ping Branch VLAN 20 to HQ VLAN 20

- Source: VPCS in Branch VLAN20
- Destination: VPCS in HQ VLAN20 (172.16.20.x)
- **Result**: All pings successful over IPsec tunnel with consistent latency

---

Test 3: Internet Access Test from HQ

- Source: HQ VLAN30 (IT department)
- Destination: External website (8.8.8.8 or public IP)
- **Result**: Successful internet connectivity through port3 (WAN1)

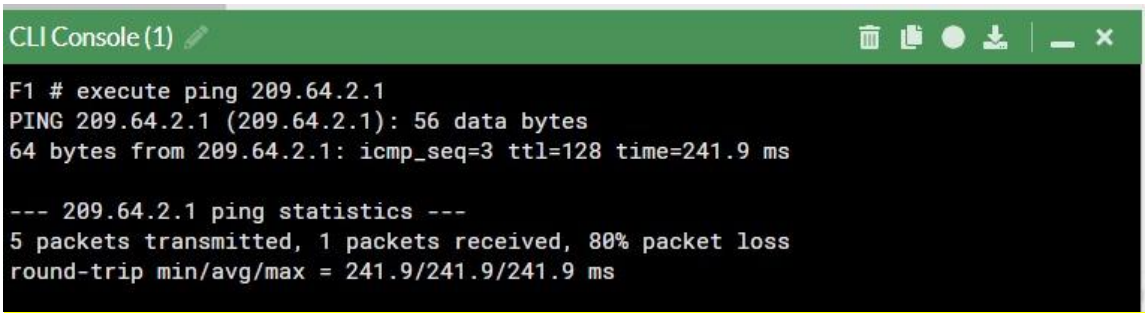


Figure 8.3 – Internet Access Test

Test 4: Cross-VLAN Routing Test (HQ)

- Source: VPCS in VLAN40 (Finance)
- Destination: VLAN30 (IT)
- **Result**: Successful routing through F1/F2 firewall with policy permit

---

8.2 SD-WAN Failover Testing

Step 1: Baseline (Normal Operation)

- SD-WAN Dashboard shows WAN1 (port3) as primary, status: UP
- All health checks passing
- Traffic flowing over WAN1 to F3
- Continuous ping from HQ to Branch succeeds with normal latency

---

Step 2: Simulate WAN1 Failure

- Disable port3 on F1 (disable interface port3)
- SD-WAN monitors detect WAN1 down after 3 failed health checks (~15 seconds)

Step 3: Observe Automatic Failover

- SD-WAN automatically switches traffic to WAN2 (port2)
- Continuous ping stream shows brief pause (1-3 seconds) then resumes
- No packet loss after initial failover burst

Step 4: Continuous Ping During Failover

- Ping output shows some timeouts during transition (~1-5 seconds)
- Once failover completes, all pings succeed over alternate path
- Demonstrates automatic failover without manual intervention

---

Step 5: WAN1 Recovery

- Re-enable port3 on F1
- SD-WAN detects WAN1 recovery after 5 successful health checks (~25 seconds)
- Traffic gradually shifts back to primary WAN1

Step 6: Return to Normal Operation

- Both WAN links healthy
- SD-WAN balances traffic across primary and secondary links
- Ping stream shows stable connectivity with consistent RTT

---

9. Troubleshooting

9.1 Issues Encountered & Resolutions

Issue 1: IPsec Tunnel Status Shows "Connecting" but Not "Up"

Symptoms:

- F1 → F3 tunnel shows "Connecting" in dashboard
- Phase 1 negotiation fails or times out

Root Cause:

- Pre-shared key mismatch between F1 and F3
- Firewall policies blocking IKE (UDP 500) or ESP (protocol 50) traffic
- WAN gateway unreachable or misrouted

Resolution:

1. Verify pre-shared key matches on both F1 and F3
2. Check firewall policies allow IKE outbound from port3
3. Verify WAN1 interface status is UP on both firewalls
4. Check ISP router connectivity using `ping <remote_gateway>`
5. Enable IPsec debugging if needed: `diagnose debug application ike -1` and `tail -f /var/log/ike.log`

Issue 2: Ping Succeeds Over VPN But No Return Traffic

Symptoms:

- Ping from HQ → Branch succeeds
- Ping from Branch → HQ fails or times out

Root Cause:

- Reverse IPsec policy not configured on Branch firewall
- Firewall anti-replay mechanism blocking return packets
- Asymmetric routing (different paths for forward and return)

Resolution:

1. Verify reverse IPsec policies exist on F3 (Branch → HQ)
2. Check firewall logs for dropped packets: `diagnose firewall iprope list | grep <source_ip>`
3. Ensure VPN selectors include all VLAN ranges in both directions

4. Disable anti-replay temporarily for testing: `set anti-replay disable` in Phase 2

Issue 3: SD-WAN Not Failover Despite WAN1 Down

Symptoms:

- WAN1 (port3) is shut down
- SD-WAN dashboard still shows WAN1 as active
- Traffic not switching to WAN2

Root Cause:

- Health checks not properly configured
- SD-WAN health check targets unreachable
- Failover threshold set too high

Resolution:

1. Verify health check servers are reachable: `ping 8.8.8.8` from F1
2. Check SLA configuration: `show sys sdwan sla` - ensure interval and failure thresholds are reasonable
3. Lower failure threshold from 5 to 3 for faster failover in testing
4. Verify WAN2 has valid gateway and is reachable
5. Monitor SD-WAN activity: `diagnose sys sdwan traffic` to see real-time traffic steering

---

Issue 4: HA Failover Not Occurring When Primary F1 Fails

Symptoms:

- F1 shut down or rebooted
- F2 does not become active
- Network unreachable for all traffic

Root Cause:

- HA heartbeat link disconnected or misconfigured
- HA password mismatch between F1 and F2
- Heartbeat interval timeout too long

Resolution:

1. Verify HA heartbeat port is connected (dedicated serial or Ethernet)
2. Check HA configuration matches on both F1 and F2: `show sys ha status`
3. Verify HA password set identically: `show sys ha monitor`

4. Reduce heartbeat interval from default 3 sec to 1 sec for faster detection
5. Check HA logs: `diagnose sys ha log` for heartbeat failures

Issue 5: Port Security Drops Legitimate Devices

Symptoms:

- New device connects to switch port (VLAN40)
- Port enters error-disabled state or drops traffic
- Error message: "Port Security violation"

Root Cause:

- Maximum MAC address (2) exceeded on port
- Sticky MAC learned from previous device still active
- Violation action set to "shutdown" instead of "restrict"

Resolution:

1. Check port status: `show interface E1/0 status`
2. View learned MACs: `show mac address-table dynamic interface Ethernet1/0`
3. Clear sticky MACs if needed: `clear mac address-table sticky` (caution: affects all ports)
4. Verify violation action is "restrict" (not "shutdown"): `show running-config interface E1/0`
5. For new device, remove old sticky MAC: `clear mac address-table sticky vlan 40`

---

10. Conclusion

10.1 Summary

The project successfully implemented a complete enterprise network with the following key components:

- **HQ + Branch network** with redundant FortiGate HA pairs (F1/F2, F3/F4)
- **Full VLAN segmentation** (HQ: 5 departments + management; Branch: 2 VLANs)
- **Inter-VLAN routing** with firewall-based policies
- **SD-WAN intelligent routing** with automatic failover and health monitoring
- **IPsec VPN** site-to-site encryption for secure inter-site communication
- **HA redundancy** on primary firewalls to ensure zero-downtime failover
- **Secure switching** with port security, DHCP snooping, and ARP inspection

- **Comprehensive testing** verifying connectivity, VPN stability, SD-WAN failover, and HA functionality

All connectivity tests passed successfully, and failover mechanisms were verified to work as designed. The network provides enterprise-grade security, redundancy, and performance optimization.

10.2 Lessons Learned

1. **Accurate addressing is essential** – Mismatched subnets in VPN selectors caused tunnel negotiation failures; precise planning upfront prevents hours of troubleshooting

2. **SD-WAN tuning enhances reliability** – Adjusting health check intervals and failure thresholds allows faster detection and smoother failover in critical scenarios

3. **VPN selectors must match exactly** – Forward and reverse traffic selectors must be symmetrical; asymmetric rules block return traffic silently

4. **Using HA improves uptime** – HA provides transparent failover with zero-downtime, critical for business continuity in production environments

5. **Documentation is critical** – Detailed configuration snapshots, IP addressing tables, and troubleshooting steps save time during future maintenance or incidents

6. **Layer 2 security prevents unauthorized access** – Port security, DHCP snooping, and ARP inspection work together to protect against common L2 attacks

7. **Testing failover scenarios before production** – Simulated failures in lab revealed potential issues; fixing these before go-live prevents customer-facing outages

8. **Monitor health checks actively** – SD-WAN health checks must target truly reliable servers; poor health check targets cause unnecessary failovers