رواد مصر الرقمية

وزارة الاتصالات وتكنولوجيا المعلومات

Project Title:

Implementing VPN Solutions With FortiGate

Track Name:

Infrastructure and Security - Fortinet Cybersecurity Engineer

FORTINET

Prepared By:

Name	Student Number
Shahd Yesen Salah Abdelmoamen	21036617
Nada Ahmed Abo-Bakr Abdelnaser	21067671
Jana Hany Salah Eldin	21069871
Shams Ibrahem Ali Mohamed	21044658
Mohamed Ahmed Mohamed Haridy	
Merna medhat hamdy rabia	

Table of Contents

1. Project Overview

1.1 Project Purpose

The purpose of this project is to design and implement a simple site-to-site enterprise network using PNETLab, simulating an HQ office and a Branch office connected securely over the internet through an IPsec VPN tunnel. The design uses FortiGate firewalls at both sites, each with a single internal LAN and dual WAN connections via two simulated ISP routers (Vodafone and WE).

1.2 Objectives

- Design and build an HQ–Branch network in PNETLab with FortiGate firewalls at both sites.
- Establish secure site-to-site connectivity between HQ and Branch using an IPsec VPN tunnel.
- Configure basic routing and firewall policies to allow controlled communication between the two LANs and the internet.
- Use dual simulated ISPs per site to test basic link redundancy and manual failover (no SD-WAN).
- Document the network topology, addressing plan, configurations, and troubleshooting steps.

1.3 Topology Used

The enterprise network consists of:

- One HQ site (Fortinet1 firewall + internal LAN 172.16.0.0/24 + VPC1 client).
- One Branch site (Fortinet2 firewall + internal LAN 192.168.0.0/24 + VPC2 client).
- Two ISP routers (Vodafone and WE) providing two separate public networks between HQ and Branch.
- IPsec VPN tunnel between Fortinet1 and Fortinet2 over the public links.
- No internal VLAN segmentation, no HA, and no SD-WAN in this design.

---

2. Network Topology

2.1 Topology Diagram

The topology consists of Fortinet1 at HQ and Fortinet2 at the Branch, each connected to both ISPs (Vodafone and WE) using separate WAN interfaces, and to a single internal LAN where the VPC hosts reside. The IPsec VPN tunnel is configured between the public IPs of Fortinet1 and Fortinet2 so that 172.16.0.0/24 at HQ can securely reach 192.168.0.0/24 at Branch.

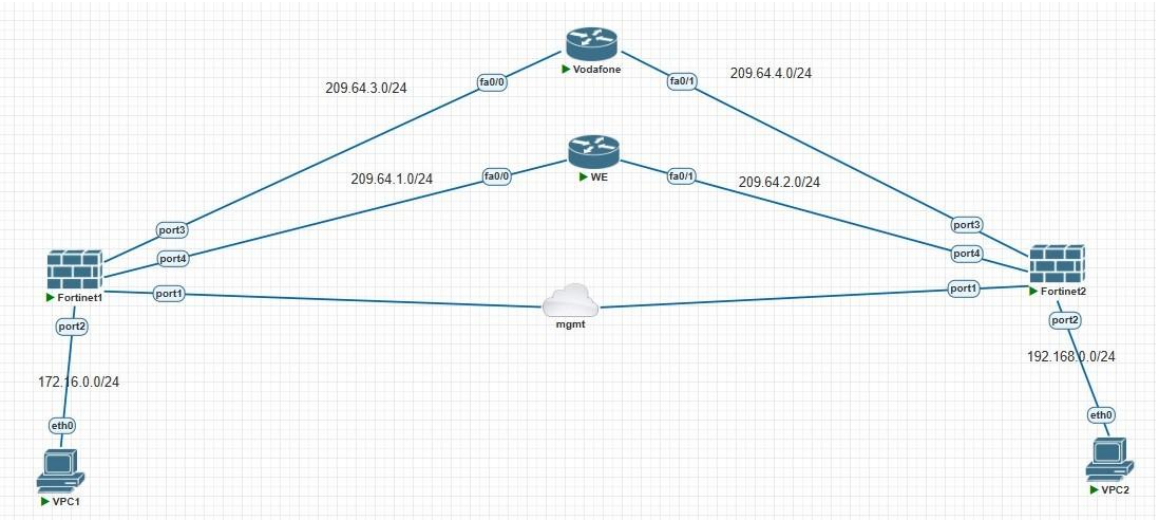

Figure 2.1 – Full Network Topology in PNETLab

2.2 Network Components Description

Headquarters (HQ)

- Fortinet1 firewall acting as the default gateway for LAN 172.16.0.0/24 and terminating the VPN tunnel.
- One internal client (VPC1) connected to Fortinet1 port2 in subnet 172.16.0.0/24.

Branch (BR)

- Fortinet2 firewall acting as the default gateway for LAN 192.168.0.0/24 and terminating the VPN tunnel.
- One internal client (VPC2) connected to Fortinet2 port2 in subnet 192.168.0.0/24.

---

3. IP Addressing Scheme

3.1 IP Table

HQ (Fortinet1)

Interface	IP Address	Purpose
port1	209.64.1.2/24	WAN toward WE cloud
port2	172.16.0.1/24	HQ LAN, default gateway for VPC1
port3	209.64.3.2/24	WAN toward Vodafone cloud

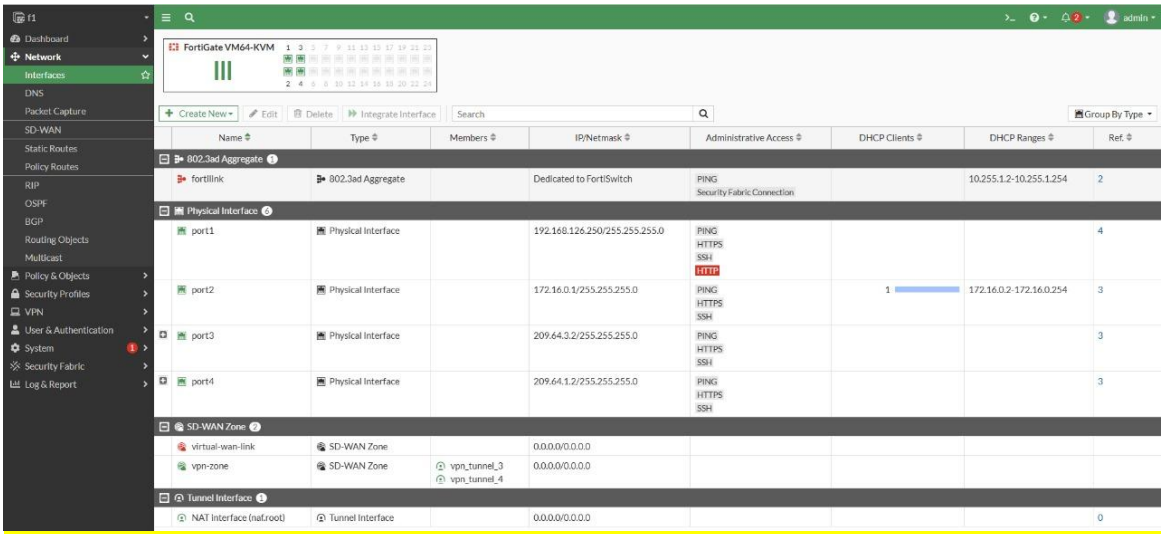

Figure 3.1 – HQ Interface Table (F1)

Branch (F3/F4 HA Pair)

Interface	IP Address	Purpose
port1	209.64.2.2/24	WAN toward WE cloud
port2	192.168.0.1/24	Branch LAN, default gateway for VPC2
port3	209.64.4.2/24	WAN toward Vodafone cloud

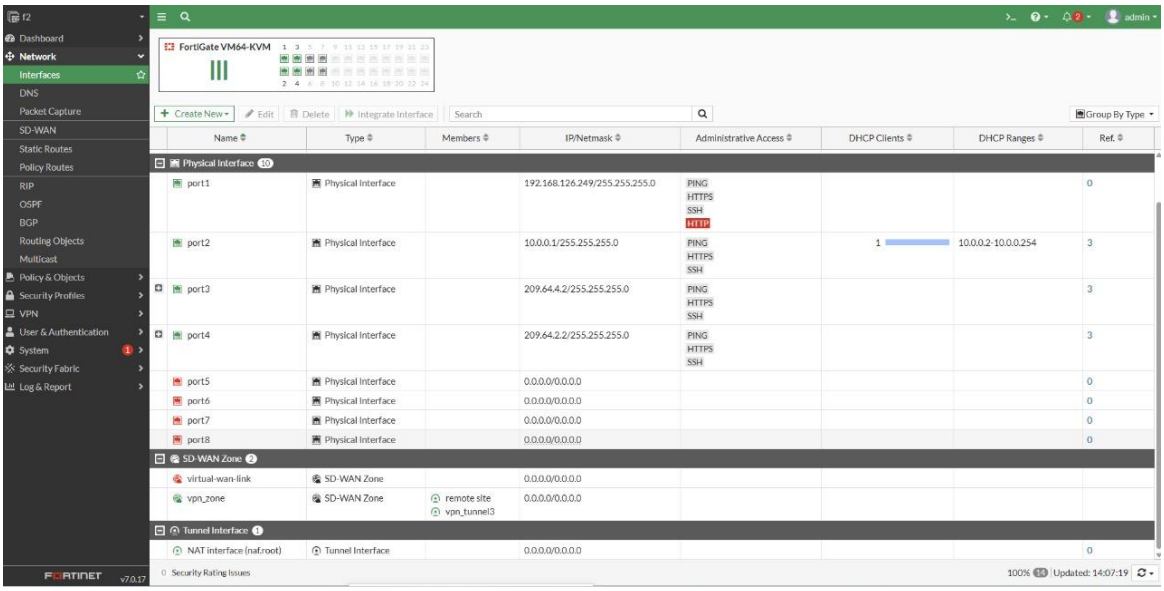

Figure 3.2 – Branch Interface Table (F3)

3.2 Addressing Plan Summary

- Private IP addressing is used for internal LANs: the HQ site uses network 172.16.0.0/24 and the Branch site uses network 192.168.0.0/24, with the FortiGate at each site acting as the default gateway.
- Public subnets from the 209.64.x.x range are used on the WAN links between the FortiGates and the ISP routers (Vodafone and WE), with a separate subnet for each physical link.
- Static routes are configured on both FortiGates so that the HQ LAN (172.16.0.0/24) can reach the Branch LAN (192.168.0.0/24) through the IPsec VPN tunnel, and vice versa.
- Default routes on both FortiGates point to the appropriate ISP next-hop addresses, allowing internet access from both sites when required.
- The addressing plan is kept simple: one internal subnet per site and multiple public subnets on the WAN side, which makes routing and troubleshooting easier while still supporting dual-ISP connectivity.

---

4. Device Configuration

This section summarizes the configuration applied to all devices in the topology: the two ISP routers (Vodafone and WE) and the two FortiGate firewalls (Fortinet1 and Fortinet2).

4.1 ISP Router Configuration

- Each ISP router is configured with two interfaces, one facing the HQ firewall and one facing the Branch firewall, in separate 209.64.x.x subnets.

- Static routes are configured so that each ISP knows how to reach the remote FortiGate's public IP over its own network, allowing the IPsec tunnel to be established over either path.

4.3 Firewall Configuration

- Basic interface configuration for WAN and LAN ports, including IP addresses and administrative access (HTTPS/SSH) for management.
- **Static routes:**
  - Default route on each FortiGate pointing to the local ISP next-hop on the active WAN link.
  - Route for the remote LAN through the IPsec tunnel interface (e.g. 192.168.0.0/24 via VPN interface on Fortinet1, and 172.16.0.0/24 via VPN interface on Fortinet2).
- **Security policies:**
  - LAN-to-VPN policy allowing traffic from the local LAN subnet to the remote LAN subnet through the IPsec tunnel.
  - VPN-to-LAN policy allowing return traffic from the remote site.
  - Optional LAN-to-Internet policy to allow clients to access the internet via the default route.

---

5. VPN Configuration

5.1 Phase 1 (IKE) Settings

- Mode: Interface mode (tunnel used as a logical interface).
- Authentication: Pre-shared key between Fortinet1 and Fortinet2.
- Encryption: AES-128 or AES-256.
- Hash / Integrity: SHA-1 or SHA-256.
- DH Group: Appropriate group selected on both peers, matching exactly.
- Local interface: WAN interface (e.g. Fortinet1 port3 public IP and Fortinet2 port1/port3 public IP).

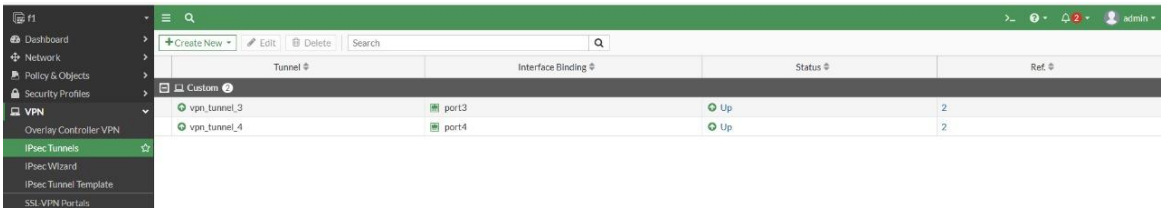

Figure 6.1 – IPsec Tunnel Status (F1)

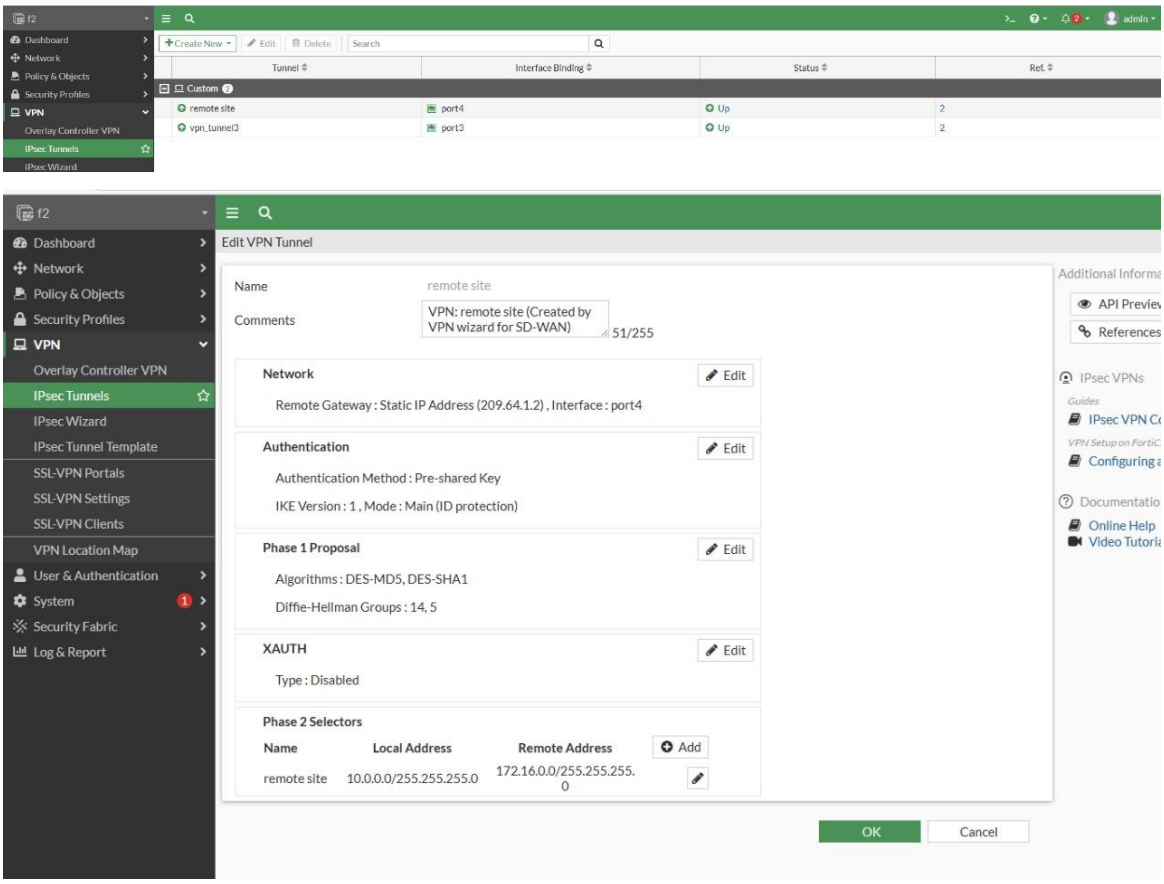

Figure 6.2 – IPsec Tunnel Status (F2)

5.2 Phase 2 (IPsec) Settings

- ESP Encryption: AES-128 or AES-256.
- Authentication: SHA-1 or SHA-256.
- Perfect Forward Secrecy (PFS): Enabled with the same DH group on both sides.
- Quick mode selectors:
    - Local subnet HQ side: 172.16.0.0/24.
    - Remote subnet HQ side: 192.168.0.0/24.
    - Mirrored on the Branch side (local 192.168.0.0/24, remote 172.16.0.0/24).

5.3 VPN Policies

- On Fortinet1 (HQ):
    - Policy from LAN (172.16.0.0/24) to VPN interface, destination 192.168.0.0/24, action Allow, with NAT disabled.
    - Reverse policy from VPN interface to LAN to permit return traffic.
- On Fortinet2 (Branch):
    - Policy from LAN (192.168.0.0/24) to VPN interface, destination 172.16.0.0/24, action Allow, NAT disabled.
    - Reverse policy from VPN interface to LAN.

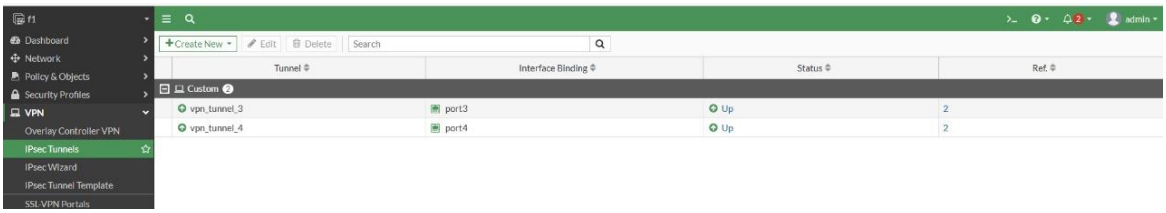

Figure 6.3 – HQ Firewall IPv4 Policies for LAN ↔ IPsec/WAN (F1)

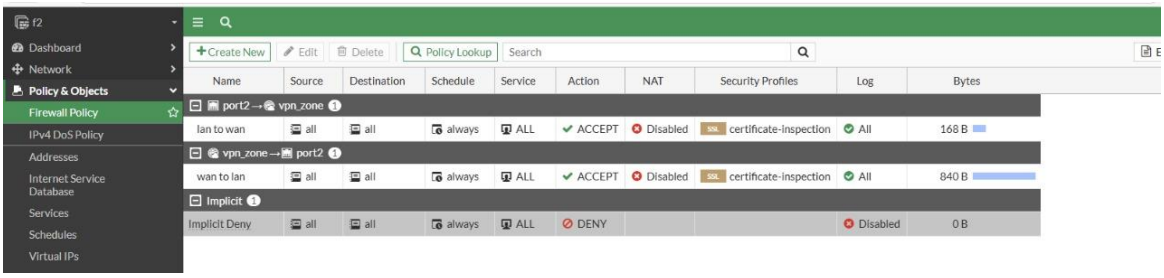

Figure 6.4 – BR Firewall IPv4 Policies for LAN ↔ IPsec/WAN (F2)

---

6. SD-WAN Configuration

6.1 WAN Interfaces

- Each FortiGate has two WAN-facing interfaces connected to Vodafone and WE respectively, using different 209.64.x.x networks.
- Only one WAN link is used as the active path for the VPN and internet by default; the second link can be used for manual failover or for testing.

6.2 Static Routing for Redundancy

- Two default routes can be configured with different priorities/distance values:
  - Primary default route via Vodafone with lower distance.
  - Backup default route via WE with higher distance, used if the primary gateway becomes unreachable.

6.3 Manual Failover

- To test failover, the administrator can disable the primary WAN interface or its default route on the FortiGate.
- The firewall then uses the backup default route and the VPN can be re-established over the remaining ISP link, restoring connectivity between HQ and Branch.

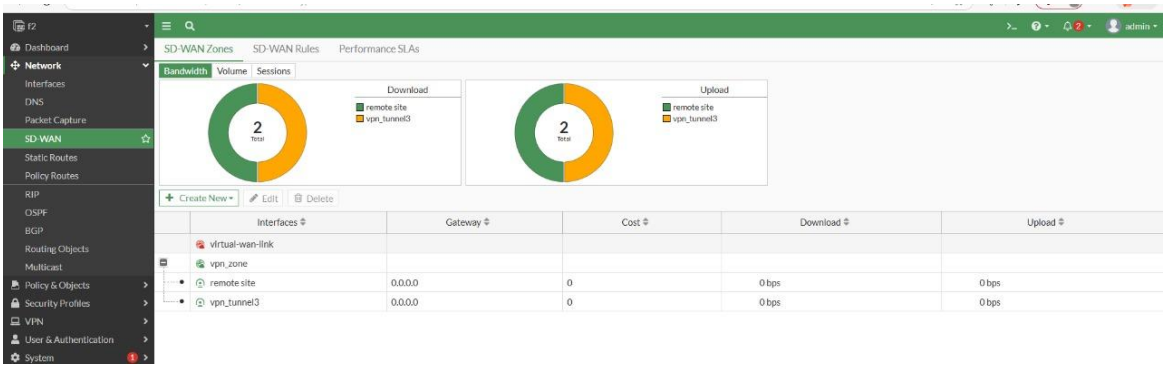

Figure 7.1 – SD-WAN Configuration

---

7. Testing & Verification

7.1 Connectivity Tests

Test 1: Ping HQ LAN to Branch LAN

- Source: VPCS in HQ LAN (172.16.0.x).
- Destination: VPCS in Branch LAN (192.168.0.x).
- Expected Result: All pings succeed over the IPsec tunnel with 0% packet loss and stable RTT, confirming full HQ ↔ Branch reachability.

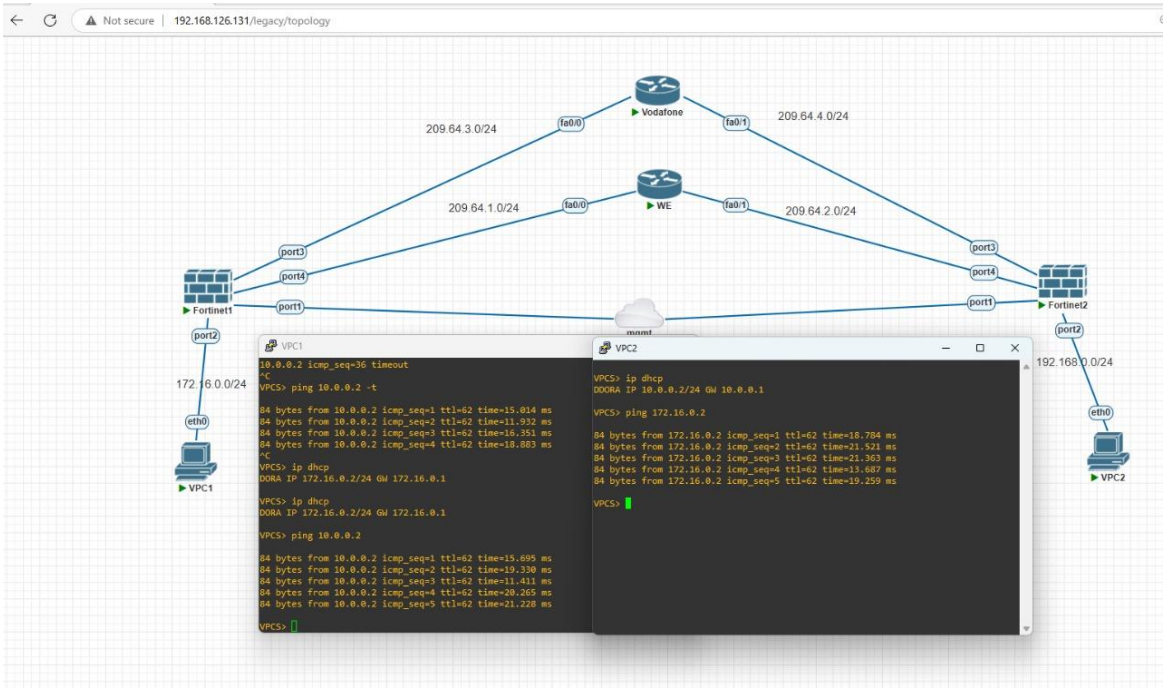

Figure 8.1 – Ping HQ LAN to Branch LAN

Test 2: Ping Branch LAN to HQ LAN

- Source: VPCS in Branch LAN (192.168.0.x).

- Destination: VPCS in HQ LAN (172.16.0.x).
- Expected Result: All pings succeed over the IPsec tunnel with consistent latency, confirming bidirectional routing and policies.

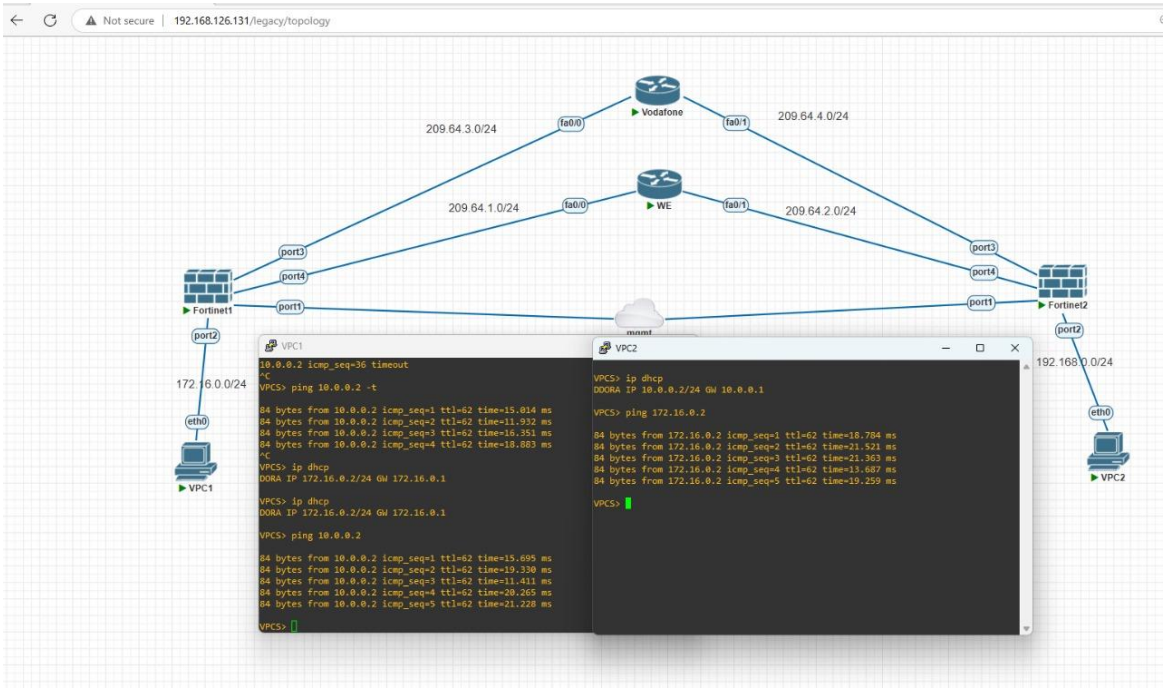

Figure 8.2 – Ping Branch LAN to HQ LAN.

Test 3: Internet Access Test from HQ

- Source: HQ client (172.16.0.x).
- Destination: Public IP (for example 8.8.8.8) or another reachable internet host.
- Expected Result: Successful ping or reachability, proving that the HQ default route and WAN NAT are working.

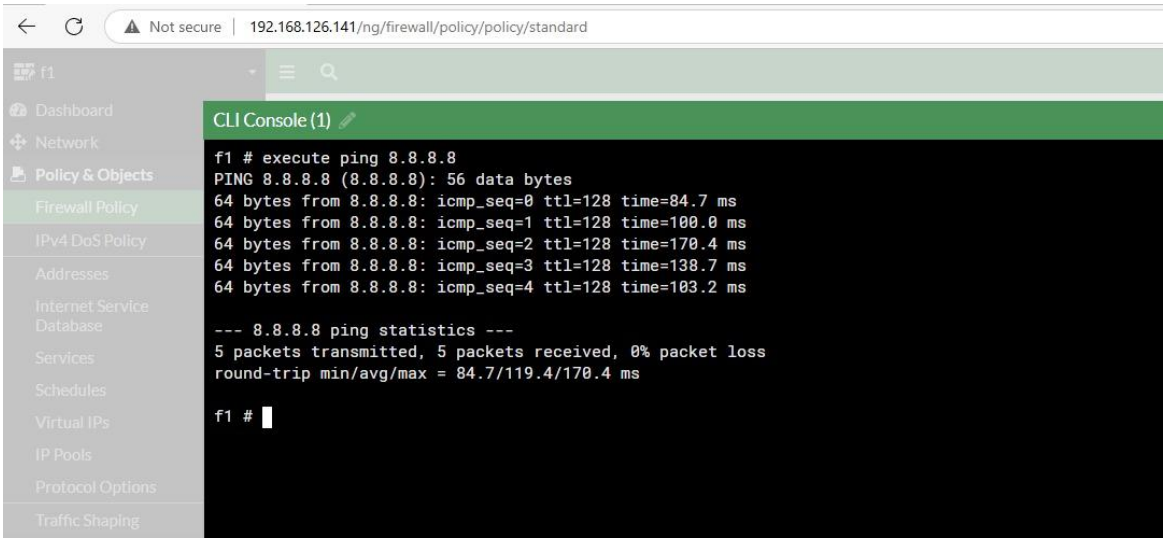

Figure 8.3 – Internet Access Test

---

8. Conclusion

8.1 Summary

This project successfully implemented a simulated enterprise network with one HQ site and one Branch site connected over an IPsec site-to-site VPN tunnel in PNETLab. The design uses FortiGate firewalls at both locations, dual ISP routers, and a simple addressing plan with one LAN subnet per site, providing secure and reliable connectivity between 172.16.0.0/24 and 192.168.0.0/24. Testing confirmed end-to-end communication between HQ and Branch clients, stable VPN operation, and working internet access from both sites, demonstrating correct routing, NAT, and security policy configuration.

8.2 Lessons Learned

1. Careful IP addressing and clear separation between LAN and WAN subnets greatly simplify VPN and routing configuration.

2. Matching Phase-1 and Phase-2 parameters on both FortiGates is critical for bringing the IPsec tunnel up and keeping it stable.

3. Continuous ping and GUI monitoring provide a simple but effective way to validate connectivity, latency, and tunnel health during testing.

4. Even with a flat network (single LAN per site), centralizing security and routing on the firewalls makes the design easier to manage and extend later (for example, adding VLANs or SD-WAN).