Digital Egyptian Pioneers initiative (DEPI)

Implementing VPN Solutions with FortiGate

R3_DEPI3_CAI3_ISS8_S3 Fortinet Cybersecurity Engineer

Team names:
Esraa Mahmoud Gaber
Martina Safwat
Ahmed Alaa
Seif Sameh
Mohamed Salah
Ali Mohamed

1- Introduction

1.1 Project Overview

1.2 Technology Stack

1.3 Project Goals

2- Lab Topology and Network Configuration

2.1 Design Rationale

2.2 Network Components

2.3 Topology Diagram

2.4 IP Addressing Scheme

Chapter 3: Implementation and Verification

3.1 LAN Configuration

3.2 WAN Connectivity Verification

3.3 Management Network Setup

3.4 IPsec Site-to-Site VPN Implementation

3.5 SSL-VPN Remote Access

3.6 SD-WAN Deployment

Chapter 4: Configurations (HQ and Branch)

4.1 Headquarters (FGT-HQ)

4.2 Branch (FGT-BR)

Chapter 5: Conclusion

Chapter 1: Introduction and Project Objectives

1.1 Project Overview

Modern enterprises require secure communication between distributed locations. This project simulates an enterprise network that connects HQ and Branch offices using encrypted VPN technologies and intelligent routing. The environment was built entirely in GNS3 and accurately represents real-world FortiGate firewall deployments.

1.2 Technology Stack

• **FortiGate Next-Generation Firewalls** — Firewall enforcement, routing, IPsec, SSL-VPN, SD-WAN

• **GNS3 Emulator** — Full emulation of FortiGate appliances, WAN clouds, LAN switches, and PCs

1.3 Project Goals

• Establish LAN/WAN connectivity

• Deploy IPsec Site-to-Site VPN

• Implement SSL-VPN remote access

• Configure SD-WAN across dual WANs

• Provide a dedicated management network

Chapter 2: Lab Topology and Network Design

2.1 Design Rationale

The topology models a realistic two-site enterprise network with dual WAN uplinks, LAN networks, VPN encryption, and a secure management segment.

2.2 Network Components

• FGT-HQ and FGT-BR firewalls

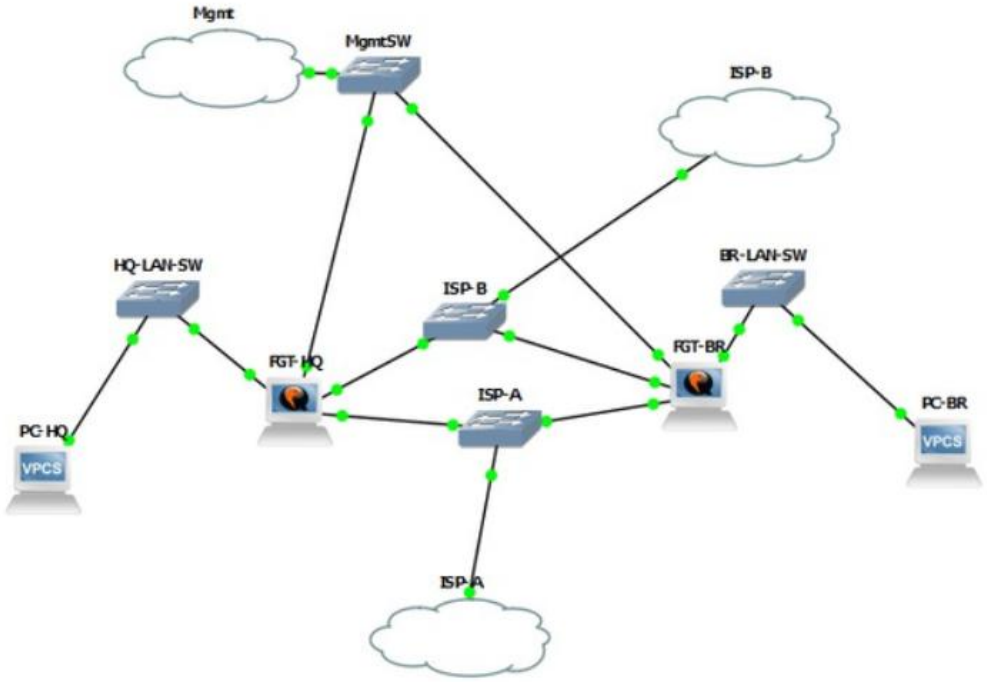
• HQ-LAN-SW and BR-LAN-SW switches

• PC-HQ and PC-BR hosts

• ISP-A and ISP-B simulated WAN clouds

• Management switch and dedicated management cloud

2.3 Topology Diagram



2.4 IP Addressing Scheme

Management Network: 172.16.1.0/24

HQ LAN: 10.0.1.0/24

Branch LAN: 10.0.2.0/24

ISP-A WAN: 198.51.100.0/24

ISP-B WAN: 203.0.113.0/24

GUI addresses:

• HQ: 172.16.1.10:8443

• Branch: 172.16.1.11:8443

Chapter 3: Implementation and Feature Verification

3.1 LAN Configuration

Static addressing applied to PC-HQ and PC-BR. ICMP tests confirmed LAN connectivity and gateway reachability.

3.2 WAN Connectivity

Each FortiGate connected to ISP-A and ISP-B. WAN reachability verified using ping.

3.3 Management Network

Deployed via port4 on both firewalls. GUI access validated using HTTPS over port 8443.

3.4 IPsec Site-to-Site VPN

Encrypted tunnel configured between HQ and Branch.

Phase 1 established the secure control channel; Phase 2 defined LAN-to-LAN selectors.

Verification:

10.0.1.10 ↔ 10.0.2.10 communication succeeded over the encrypted tunnel.

3.5 SSL-VPN Remote Access

SSL-VPN portal, address pool (10.10.10.0/24), user authentication, and firewall policies were configured.

FortiClient connected successfully:

• SSL handshake

• Authentication

• Tunnel establishment

3.6 SD-WAN Deployment

WAN interfaces (port2, port3) added to SD-WAN zone.

SLAs configured to monitor 8.8.8.8 and 1.1.1.1.

Chapter 4: Device Configuration (HQ and Branch)

4.1 Headquarters (FGT-HQ)

Interfaces

port1: 10.0.1.1/24
port2: 198.51.100.10/24
port3: 203.0.113.10/24
port4: 172.16.1.10/24

Address Objects

HQ_LAN: 10.0.1.0/24
BR_LAN: 10.0.2.0/24
SSL_VPN_POOL: 10.10.10.0/24

IPsec

Phase1: IPSEC_TO_BRANCH → 198.51.100.11
Phase2: HQ_to_BR (10.0.1.0/24 → 10.0.2.0/24)

SSL-VPN

Portal: SSL-VPN-Portal
Pool: SSL_VPN_POOL
User: remoteuser1
Group: SSLVPN_Users
Firewall policy: SSL-VPN → HQ LAN

SD-WAN

Members: port2, port3
SLAs: SLA_ISP_A, SLA_ISP_B
Routing: Internet_Traffic

4.2 Branch (FGT-BR)

Interfaces

port1: 10.0.2.1/24
port2: 198.51.100.11/24
port3: 203.0.113.11/24
port4: 172.16.1.11/24

Address Objects

BR_LAN: 10.0.2.0/24
HQ_LAN: 10.0.1.0/24

IPsec

Phase1: IPSEC_TO_HQ → 198.51.100.10
Phase2: BR_to_HQ (10.0.2.0/24 → 10.0.1.0/24)

SD-WAN

Members, SLAs, and rules mirrored from HQ.

Chapter 5: Conclusion

The project successfully delivered a complete secure enterprise connectivity solution. All implemented components—LAN/WAN, management network, IPsec Site-to-Site VPN, SSL-VPN remote access, and SD-WAN—performed as expected. The final environment reflects production-grade FortiGate deployments and provides a strong foundation for advanced enterprise networking.