رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

Digital Egypt Pioneers Initiative (DEPI)

Implementing VPN Solutions Project

Fortinet Cybersecurity Engineer Track

Team Members:

1. *Abdelrhman Ahmed Abdelmonem*
2. *Mohamed Sameh Saeed*
3. *Hana Emad Isaac*
4. *Roaa Mohamed Said*
5. *Abdullah Tamer Ali*
6. *Raghad Ashraf Ibrahim*

Supervised by:

Eng. Ahmed Mahmoud

Table of Contents

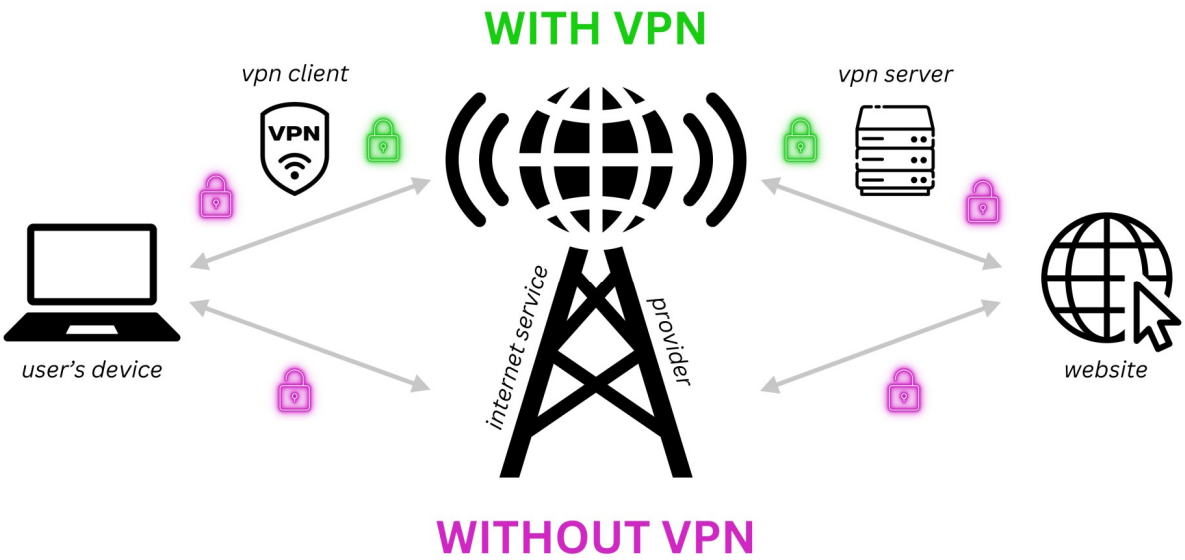
Project 3: Implementing VPN Solutions with FortiGate

Introduction

In today's digital era, secure communication over public networks is a critical requirement for organizations of all sizes. As businesses expand and remote work becomes more common, ensuring data privacy, integrity, and secure access to internal resources has become a major focus in network security.

This project, "Implementing VPN Solutions with FortiGate," aims to explore, design, and implement various VPN technologies using Fortinet's FortiGate firewall platform. The primary goal is to provide secure connectivity between users, branches, and cloud networks by leveraging VPN configurations such as SSL VPN, IPsec VPN, and SD-WAN integration.

Throughout the project, different VPN types will be studied, configured, and tested to evaluate their performance and security capabilities. By the end of the project, a complete and well-documented VPN solution will be presented, demonstrating how FortiGate can effectively secure communication across distributed environments while optimizing network performance through SD-WAN features.



Week 1: VPN Concepts and SSL VPN Configuration

a) VPN Overview

A **Virtual Private Network (VPN)** is a secure communication technology that enables users or entire networks to connect over the public internet as if they were part of a single private network. It achieves this by creating an encrypted "tunnel" that protects data as it travels between devices or sites, preventing unauthorized access or interception. VPNs play a vital role in maintaining **data confidentiality, integrity, and authentication**, ensuring that sensitive information remains secure even when transmitted across untrusted networks.

In modern organizations, VPNs are widely used to allow remote employees to access internal resources safely, to connect multiple branch offices securely, and to enable encrypted communication between data centers or cloud services. By using strong encryption algorithms and authentication methods, VPNs not only enhance network security but also support flexibility and productivity, allowing users to work securely from virtually anywhere.

b) Types of VPNs and Their Use Cases

Type	Description	Use Case
Remote Access VPN (Client-to-Site VPN)	Connects individual users (like employees working remotely) securely to a company's internal network using VPN client software.	Employees accessing company resources securely from home or while traveling.
Site-to-Site VPN	Connects two or more networks (e.g., branch offices) securely over the internet. Usually implemented between routers or firewalls.	Securely connecting branch offices or remote sites to headquarters.
SSL VPN (Secure Sockets Layer VPN)	Uses HTTPS (port 443) to provide secure remote access via a web	Users who need access without installing special VPN

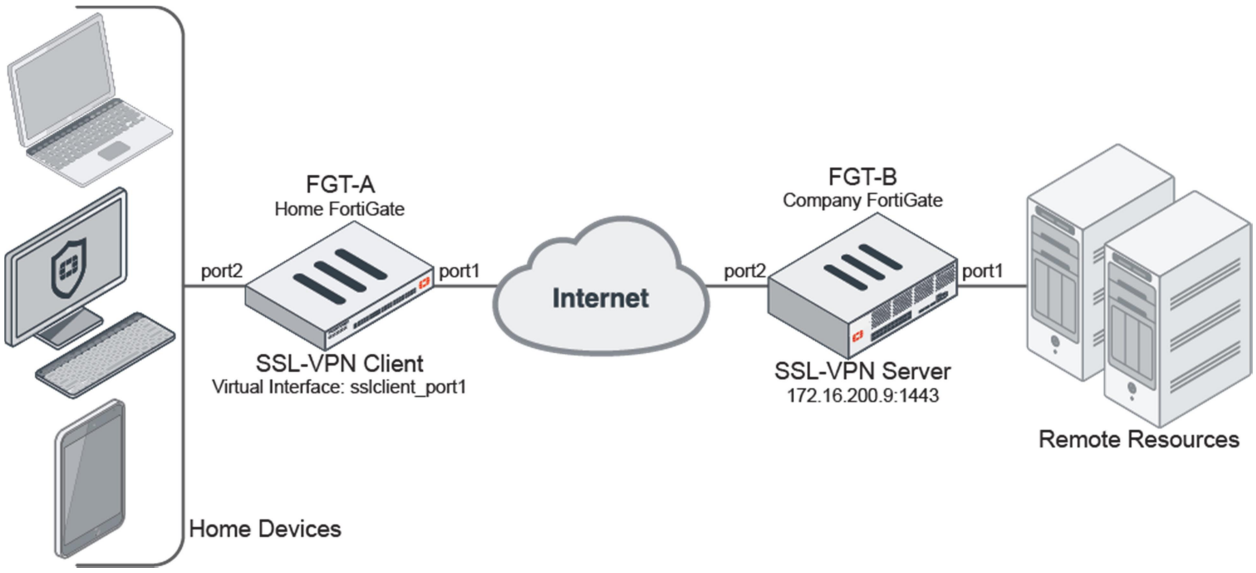
	browser or client. It encrypts traffic using SSL/TLS protocols.	clients (works through browsers).
IPsec VPN (Internet Protocol Security VPN)	Uses the IPsec protocol suite to encrypt and authenticate IP packets between sites or devices. It operates at the network layer.	Permanent, secure tunnels between offices or datacenters.
MPLS VPN (Multiprotocol Label Switching VPN)	Uses service provider networks to create private paths for enterprise traffic, ensuring reliability and QoS.	Large enterprises require scalable and reliable WAN connections.
L2TP/IPsec VPN	Combines Layer 2 Tunneling Protocol with IPsec encryption. Often used for secure remote access.	Legacy systems or networks requiring layer-2 tunneling.
Cloud VPN	Extends on-premises networks securely to cloud services (AWS, Azure, etc.).	Hybrid cloud environments.

c) SSL VPN

Overview

An SSL VPN allows secure remote access to a private network using a standard web browser or a lightweight VPN client. It operates over the SSL/TLS protocol, the same technology used to secure websites (HTTPS). Because it uses port 443, SSL VPN traffic can pass easily through most firewalls and network devices without requiring special configurations.

SSL VPNs are widely used by organizations to enable remote employees, partners, or clients to securely access internal applications, files, or systems over the internet.



Why SSL VPN?

- Uses **HTTPS (port 443)** — easily passes through firewalls.
- Provides **user-based authentication**.
- Doesn't require a special client (can work in a browser).
- Offers **tunnel mode** (for full network access) and **web mode** (for portal-based access).

How It Works

- The user connects to the SSL VPN gateway (e.g., FortiGate) through a **web browser** or **FortiClient VPN application**.
- The connection is established using **SSL/TLS encryption**, ensuring data transmitted between the user and the VPN gateway is secure.
- Once authenticated, the user is granted access to internal resources depending on the assigned privileges.

Modes of SSL VPN

There are typically **two modes** of SSL VPN operation:

a) **Web Mode**

- Access through a web portal.
- Users log in via a browser (e.g., https://<public-ip>:443) and can access specific applications like email, file servers, or web-based tools.
- Suitable for simple, controlled access without installing a VPN client.

b) **Tunnel Mode**

- Requires a VPN client (e.g., FortiClient).
- Creates a full network tunnel between the user's device and the internal network.
- Allows complete access to internal network resources as if the user were on-site.
- Ideal for IT staff or employees who need broader network access.

Advantages of SSL VPN

- **Ease of Use:** Works through browsers and common ports (443).
- **Strong Encryption:** Uses SSL/TLS protocols for secure communication.
- **Flexible Access:** Supports both web-based and full-tunnel connections.
- **Firewall-Friendly:** Easily passes through NAT and firewalls.
- **User-Based Authentication:** Integrates with LDAP, RADIUS, or local users.

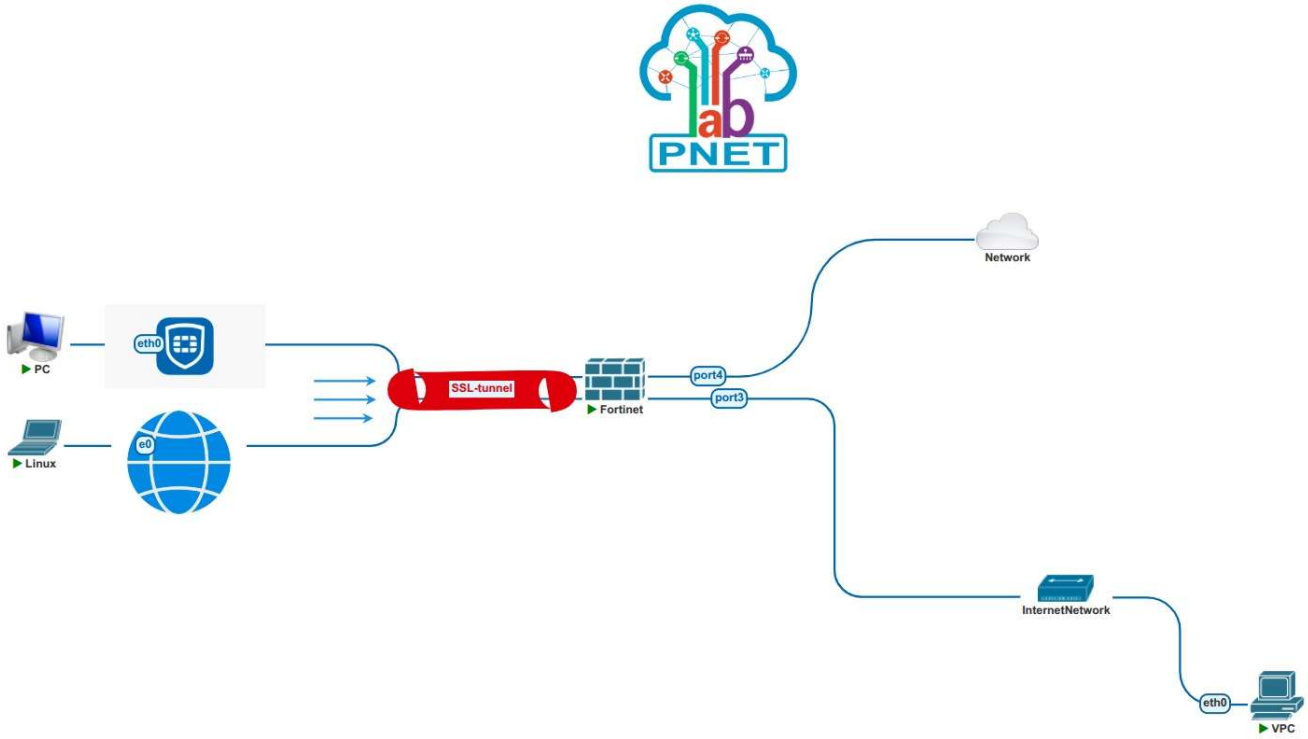
Common Use Cases

- Secure remote access for employees working from home.
- Business partners accessing limited company resources.
- Mobile users connecting from public networks (e.g., hotels, airports).

d) SSL VPN Configuration on FortiGate

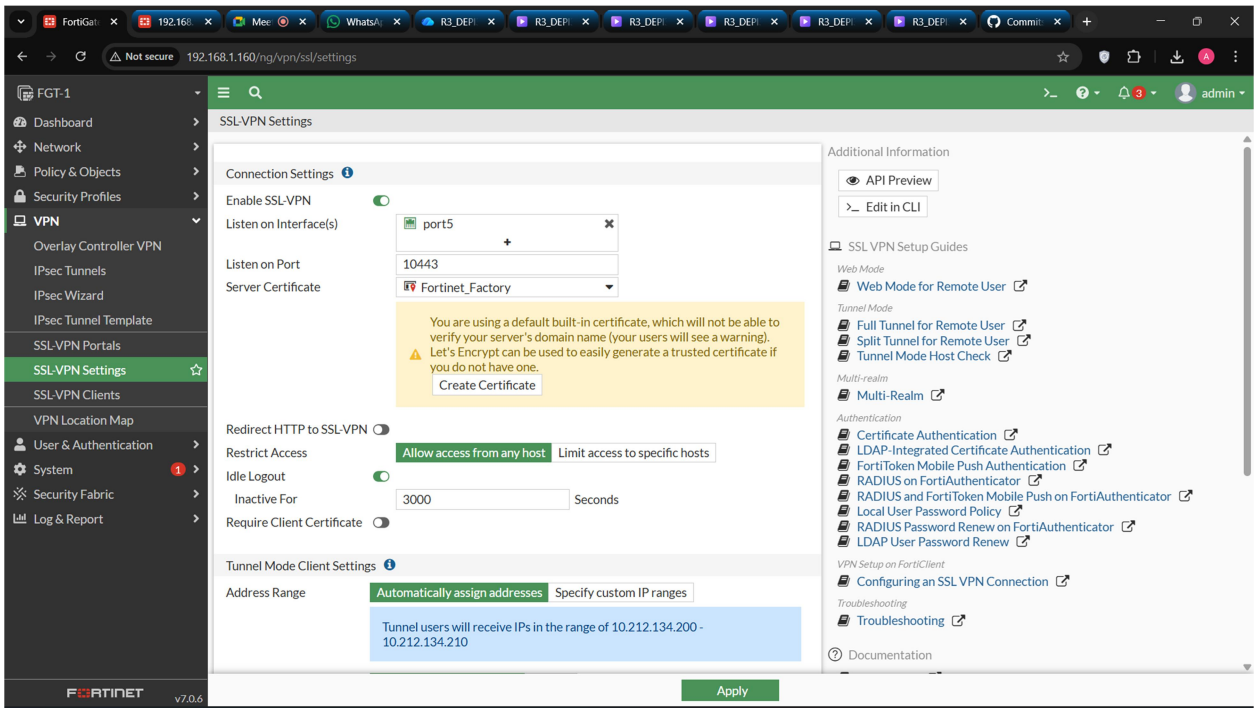
Objective:

Configure an SSL VPN to allow remote users to access internal network resources securely.

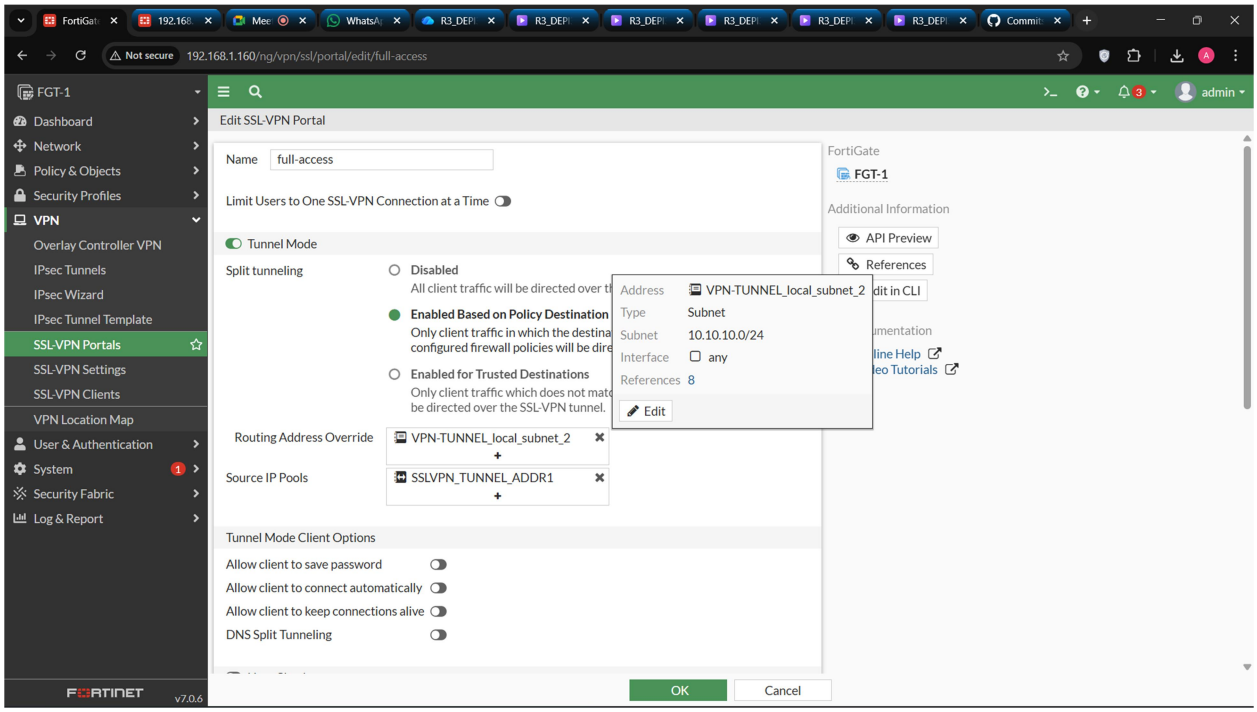


SSL VPN Topology

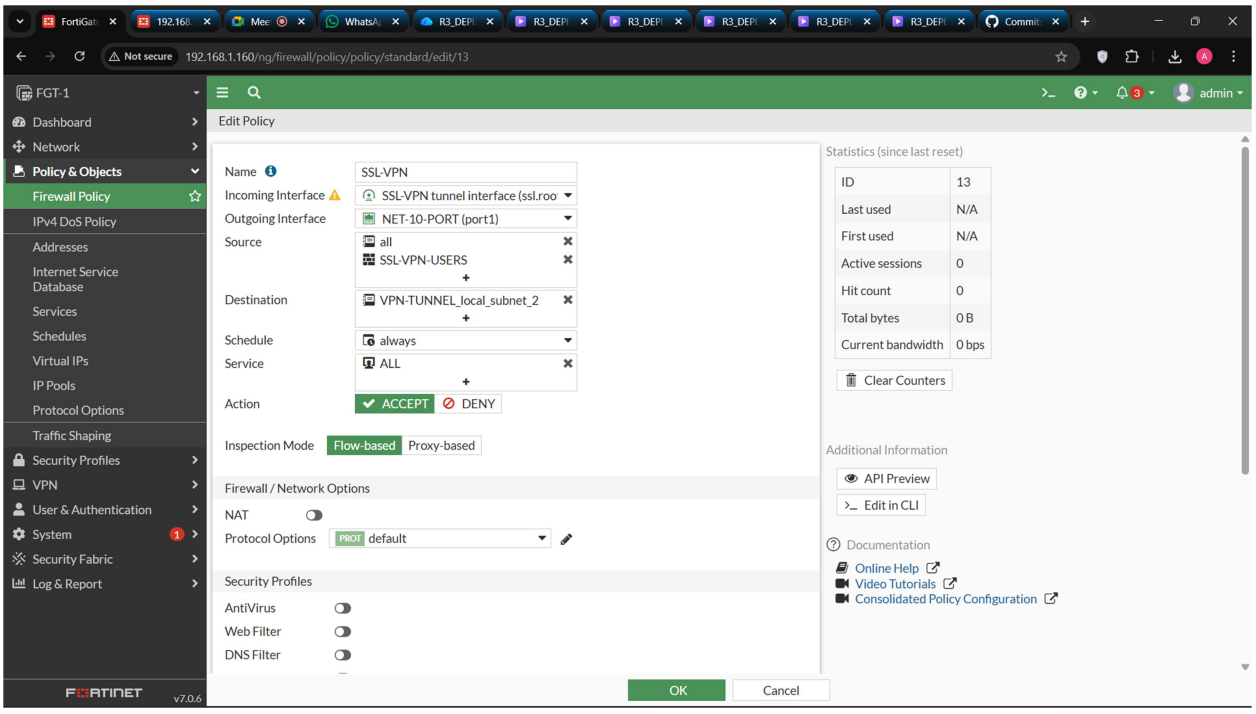
SSL-VPN Setting Configuration:



SSL-VPN Portal Configuration:



SSL-VPN-Access Policy Configuration:



Week 2: IPsec VPN Configuration

a) Overview

The **IPsec (Internet Protocol Security) VPN** is a widely used protocol suite that secures network traffic by encrypting and authenticating IP packets at the **network layer (Layer 3)**. It provides site-to-site and remote access solutions that ensure data confidentiality, integrity, and authenticity between two or more networks.

IPsec VPNs are particularly suitable for organizations that need **permanent, secure connections between branches, headquarters, or data centers**.
Unlike SSL VPNs, which are typically used for individual remote access, IPsec VPNs operate transparently for entire subnets and devices.

b) How IPsec VPN Works

An IPsec VPN establishes a **secure tunnel** between two FortiGate devices through a two-phase process:

Phase 1 (IKE Negotiation):

a. Establishes a secure communication channel.
b. Authenticates the two VPN peers.
c. Negotiates encryption and hashing algorithms (e.g., AES, SHA).

Phase 2 (Data Encryption):

a. Defines traffic selectors (networks that will communicate).

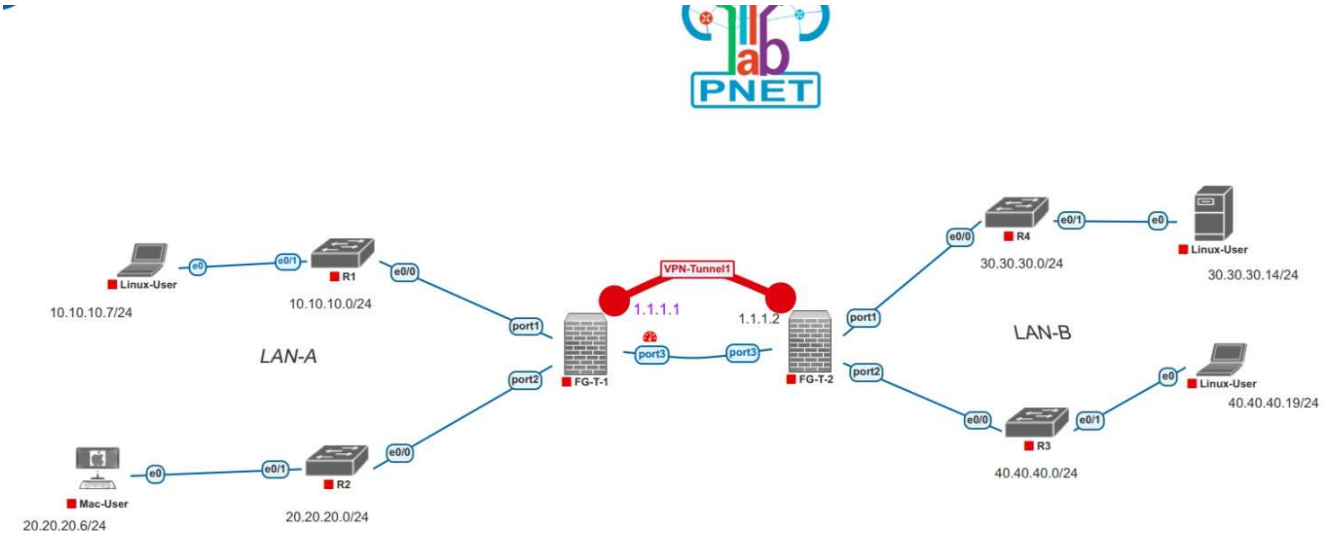
b. Encrypts user data packets through the established tunnel.

c) Key Components

- **IKE (Internet Key Exchange):** Used for secure key exchange.
- **ESP (Encapsulating Security Payload):** Provides encryption and authentication.
- **AH (Authentication Header):** Ensures integrity and authenticity (used optionally).
- **Transform Sets:** Define algorithms for encryption and hashing.

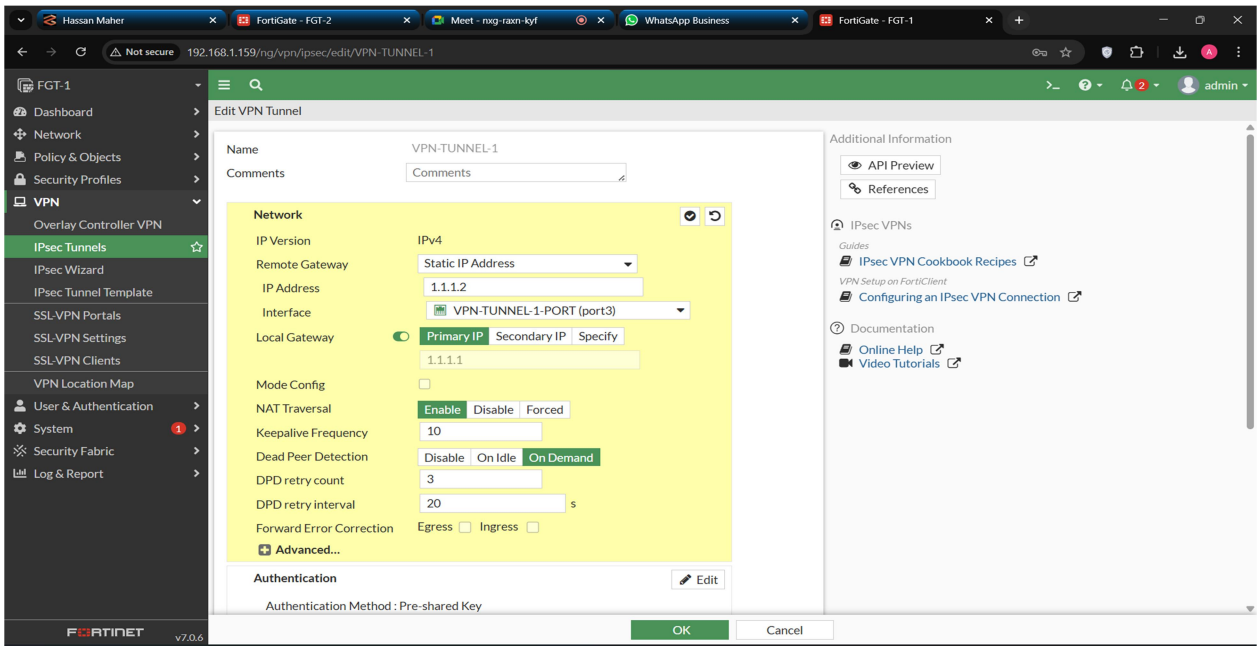
d) IPsec Configuration Steps on FortiGate

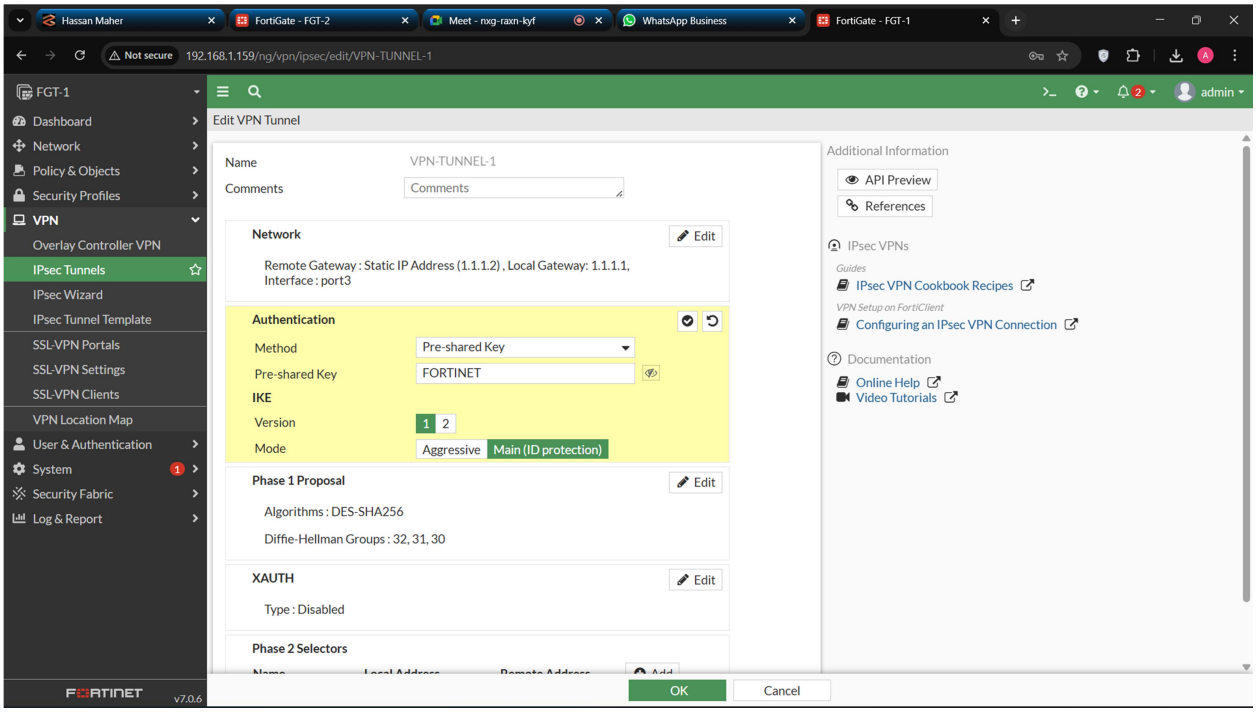
- **Objective:**
  Establish a secure IPsec tunnel between two FortiGate firewalls (e.g., between Head Office and Branch).

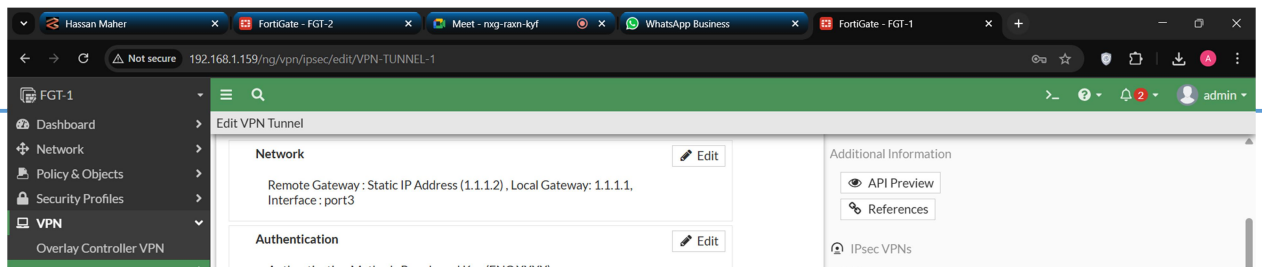


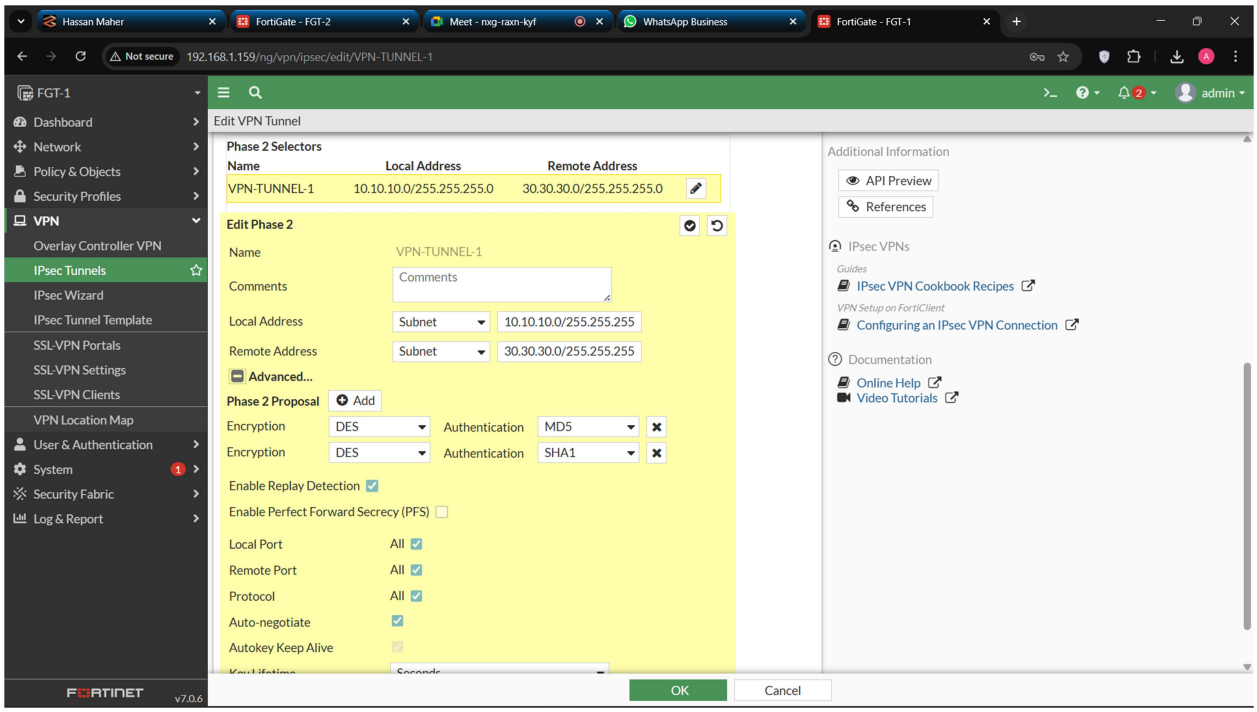
IPsec VPN Tunnel Topology

- **Configuration Steps: Step1: Configure VPN Tunnels**

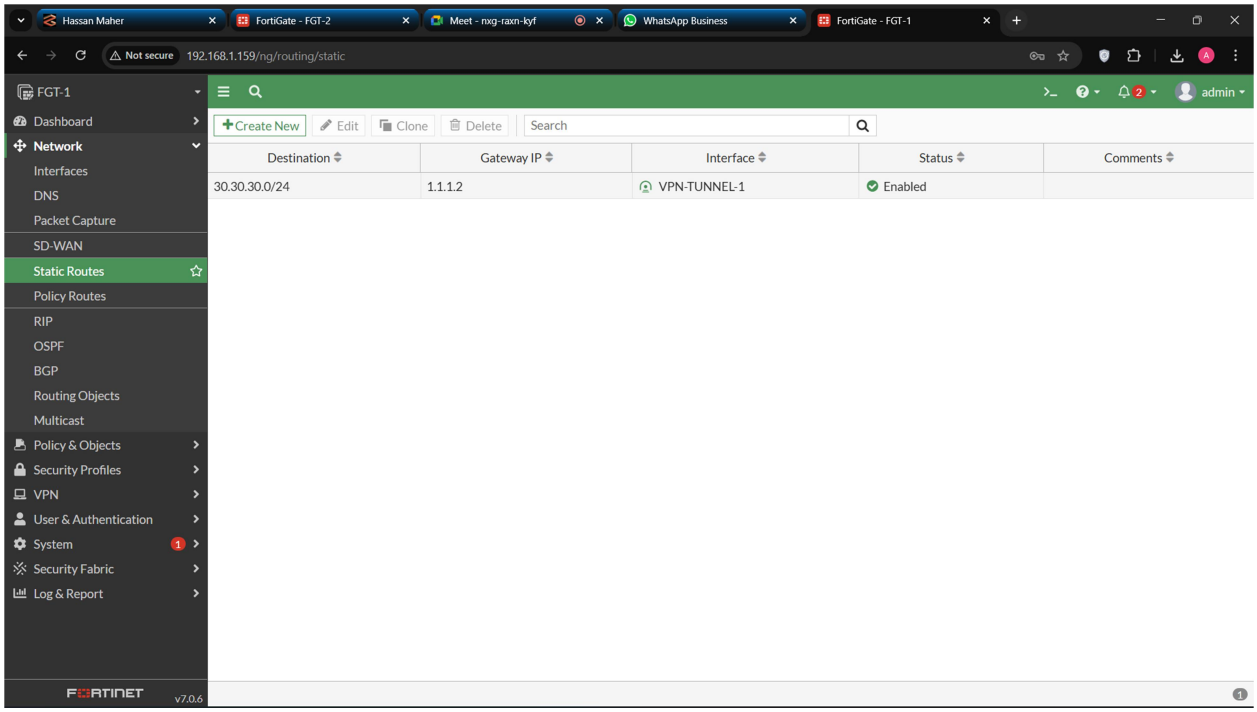


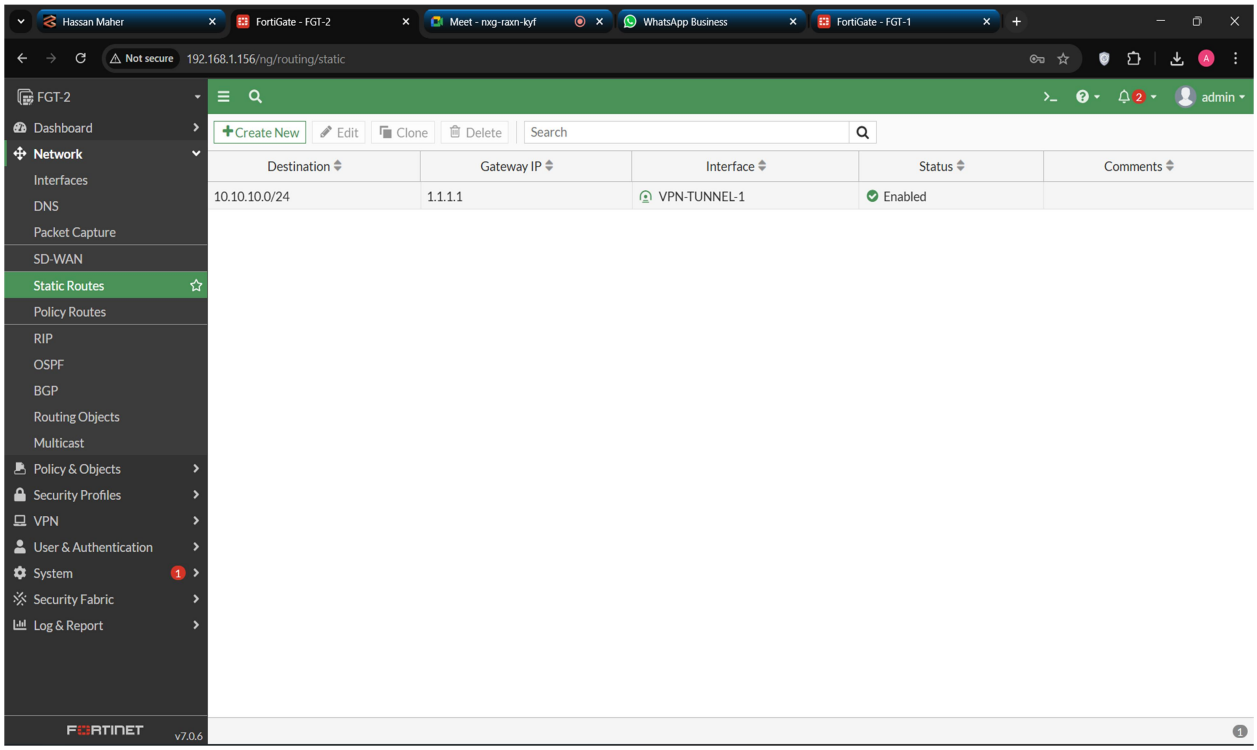




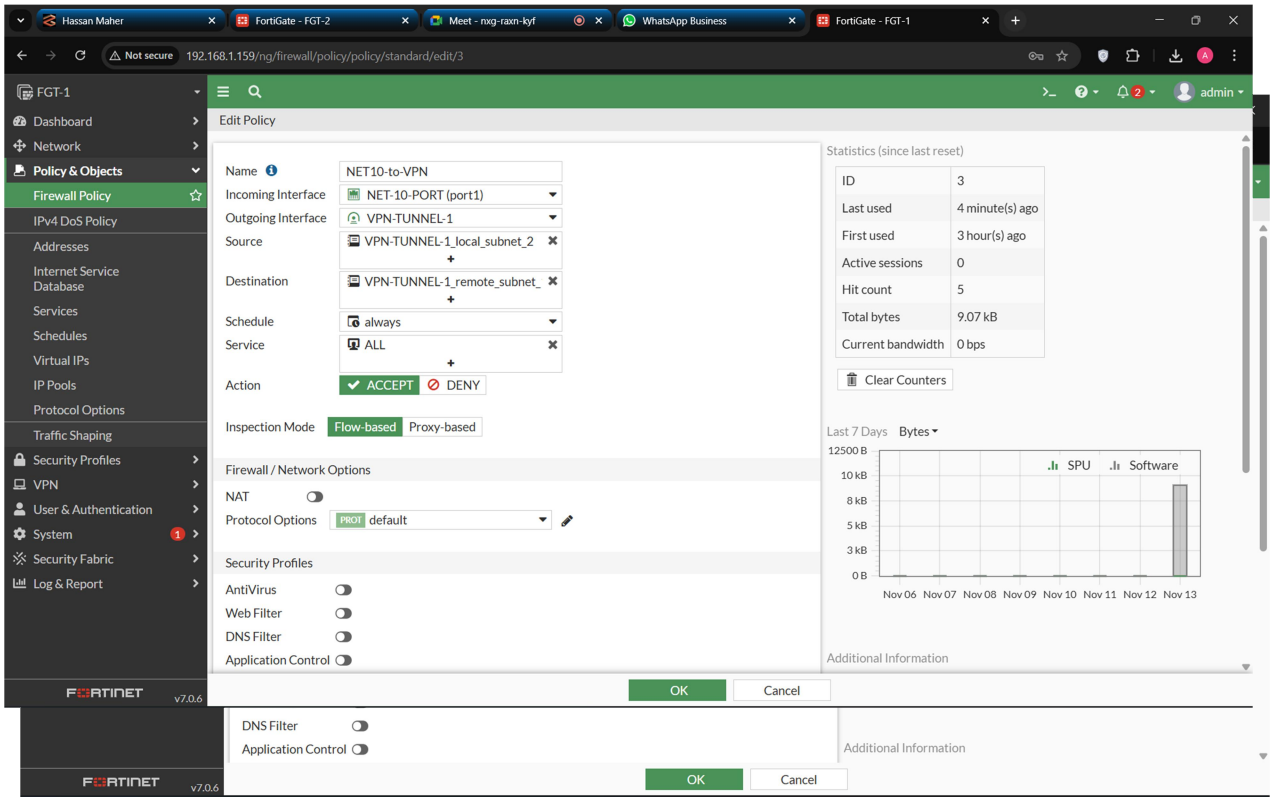

Hassan Maher
FortiGate - FGT-2
Meet - nxg-raxn-kyf
WhatsApp Business
FortiGate - FGT-1
Not secure
192.168.1.159/ng/vpn/ipsec/edit/VPN-TUNNEL-1
FGT-1
admin
Dashboard
Network
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Clients
VPN Location Map
User & Authentication
System
Security Fabric
Log & Report
Edit VPN Tunnel
Phase 2 Selectors
Name
Local Address
Remote Address
VPN-TUNNEL-1
10.10.10.0/255.255.255.0
30.30.30.0/255.255.255.0
Edit Phase 2
Name
VPN-TUNNEL-1
Comments
Comments
Local Address
Subnet
10.10.10.0/255.255.255
Remote Address
Subnet
30.30.30.0/255.255.255
Advanced...
Phase 2 Proposal
Add
Encryption
DES
Authentication
MD5
Encryption
DES
Authentication
SHA1
Enable Replay Detection
Enable Perfect Forward Secrecy (PFS)
Local Port
All
Remote Port
All
Protocol
All
Auto-negotiate
Autokey Keep Alive
Additional Information
API Preview
References
IPsec VPNs
Guides
IPsec VPN Cookbook Recipes
VPN Setup on FortiClient
Configuring an IPsec VPN Connection
Documentation
Online Help
Video Tutorials
OK
Cancel
FORTINET
v7.0.6

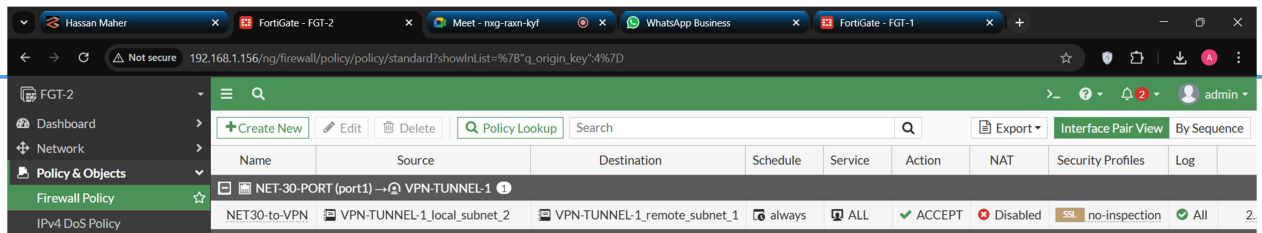
Step 2: Set Static Routes





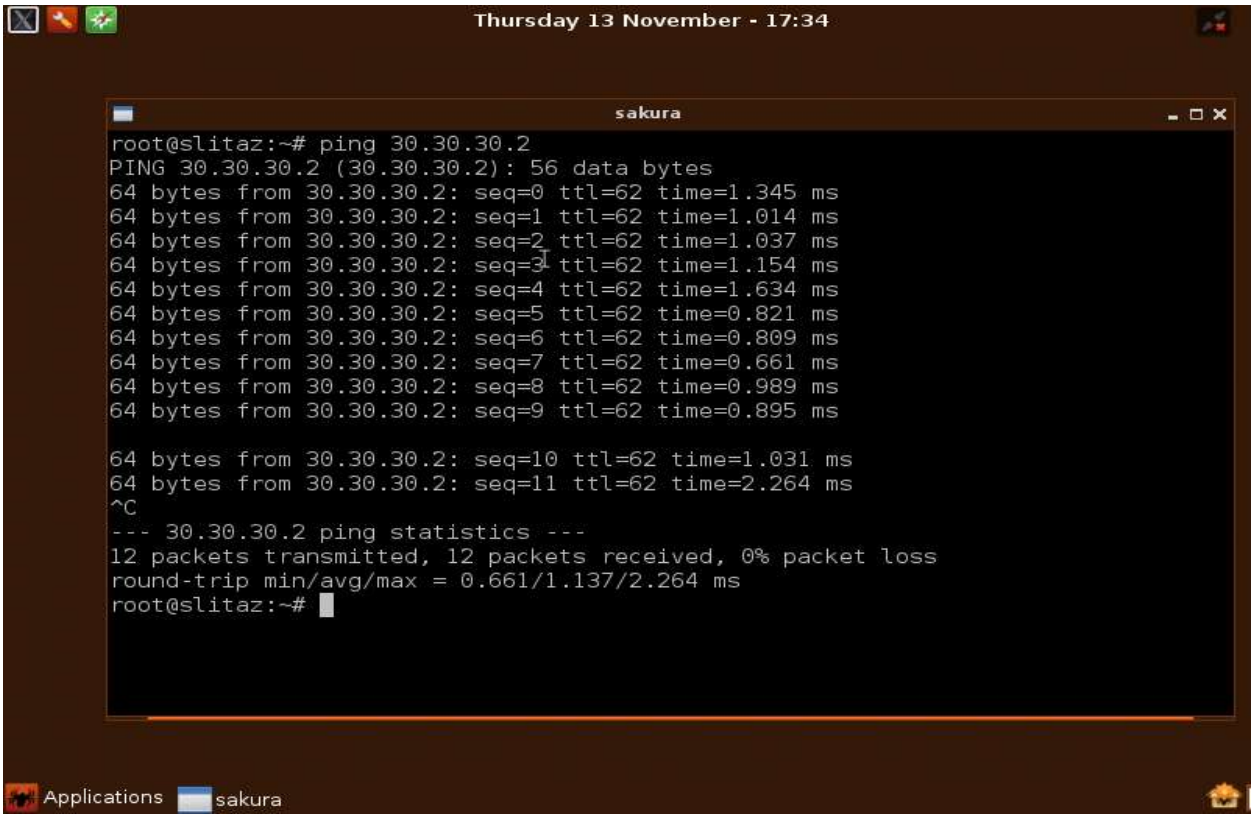
Step 3: Configure Policies



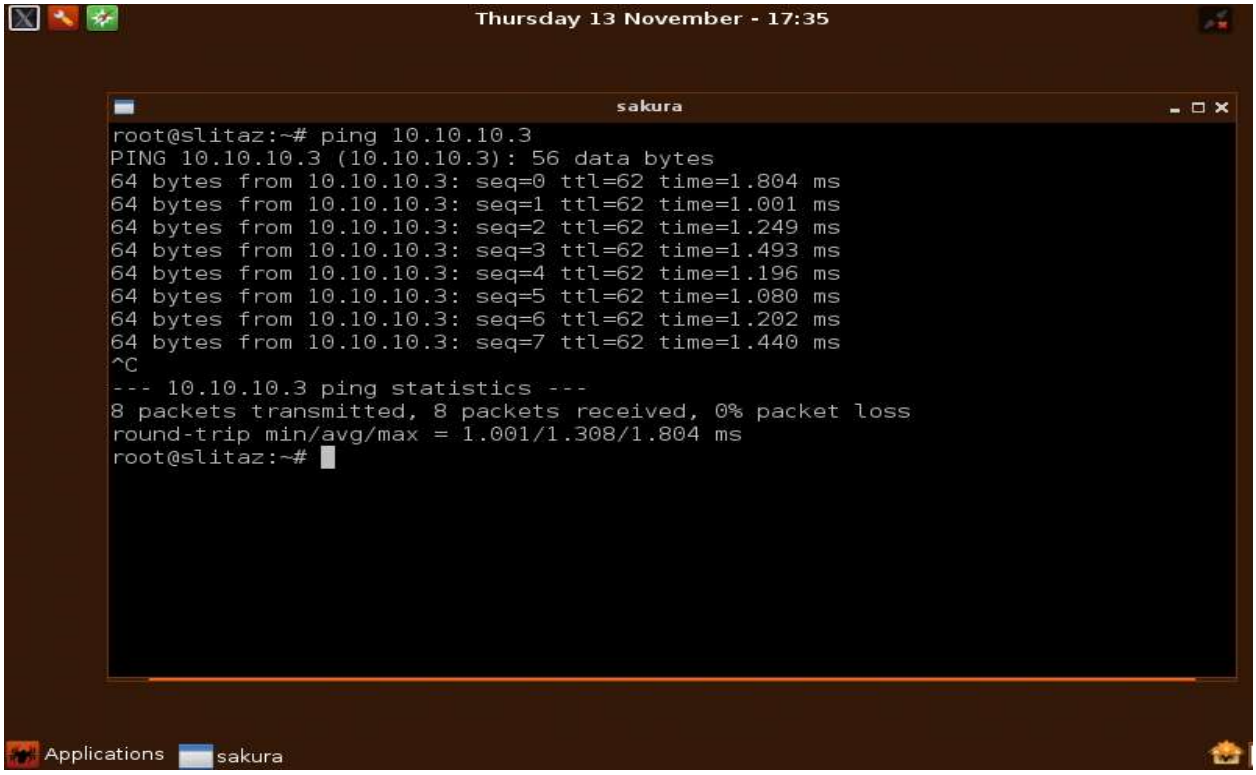


e) Testing and Verification

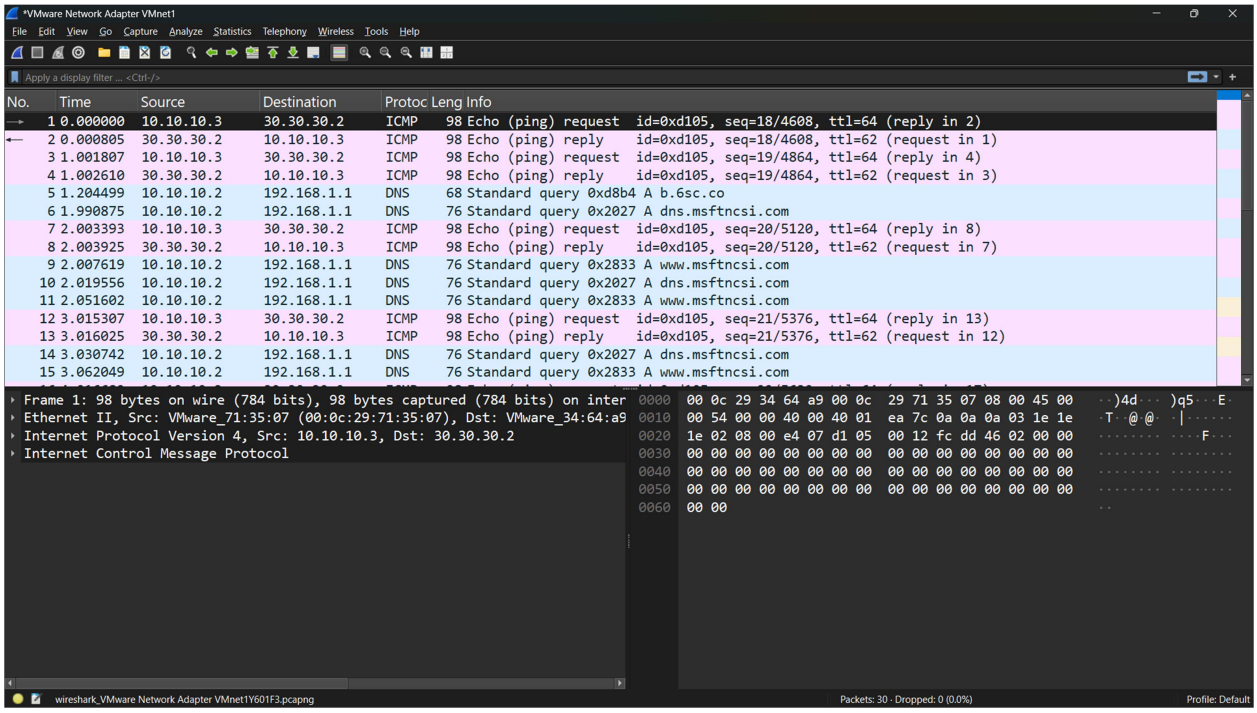
- **Ping Test: ping from PC-1 to PC-3**



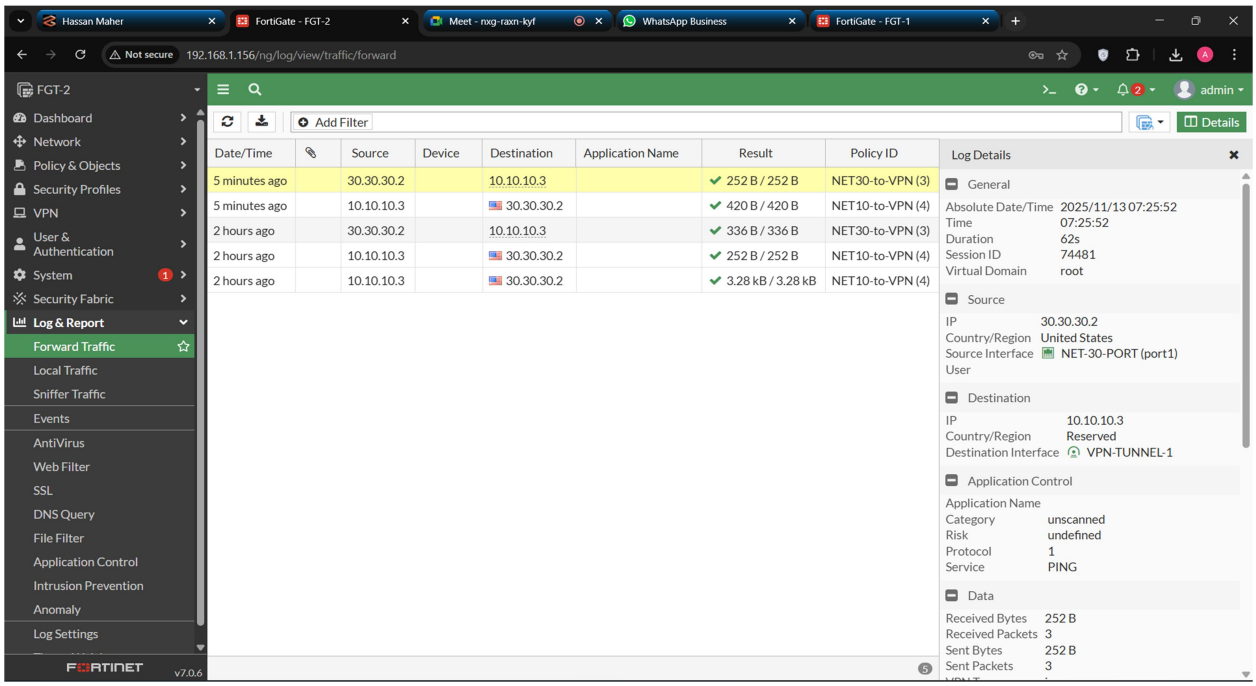
ping from PC-3 to PC-1



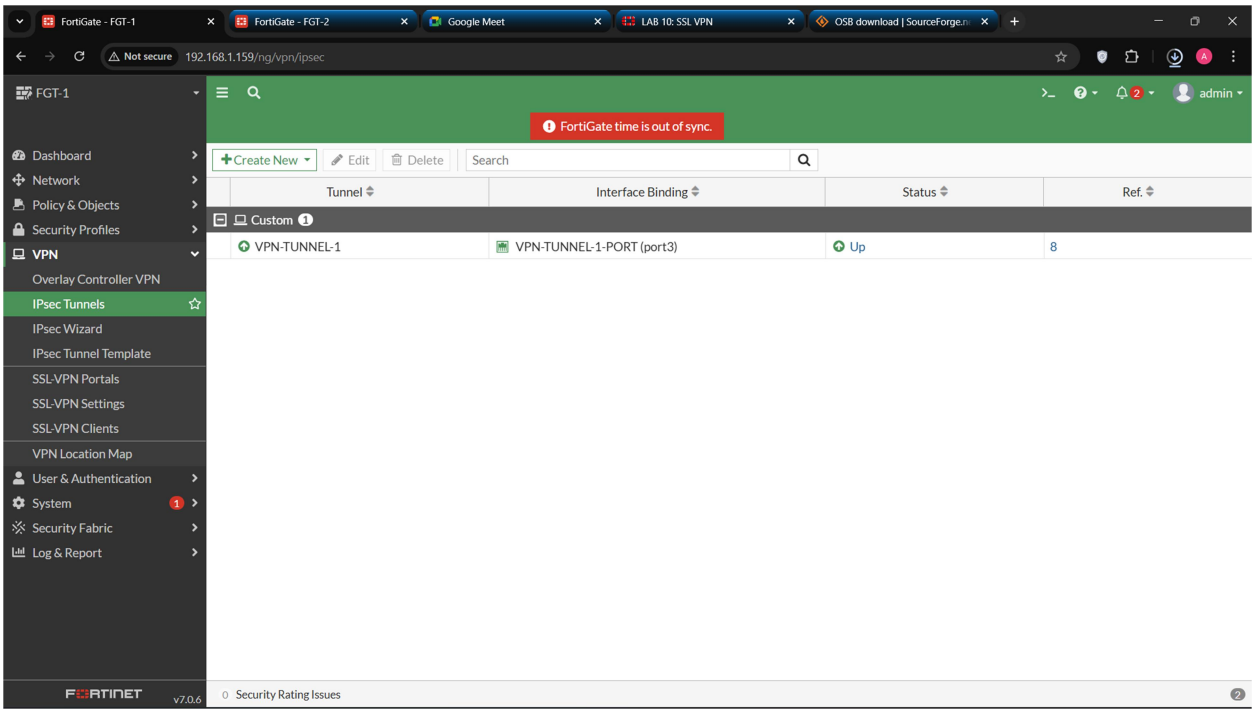
Capturing a traffic between PC-1 and PC-3 using Wireshark

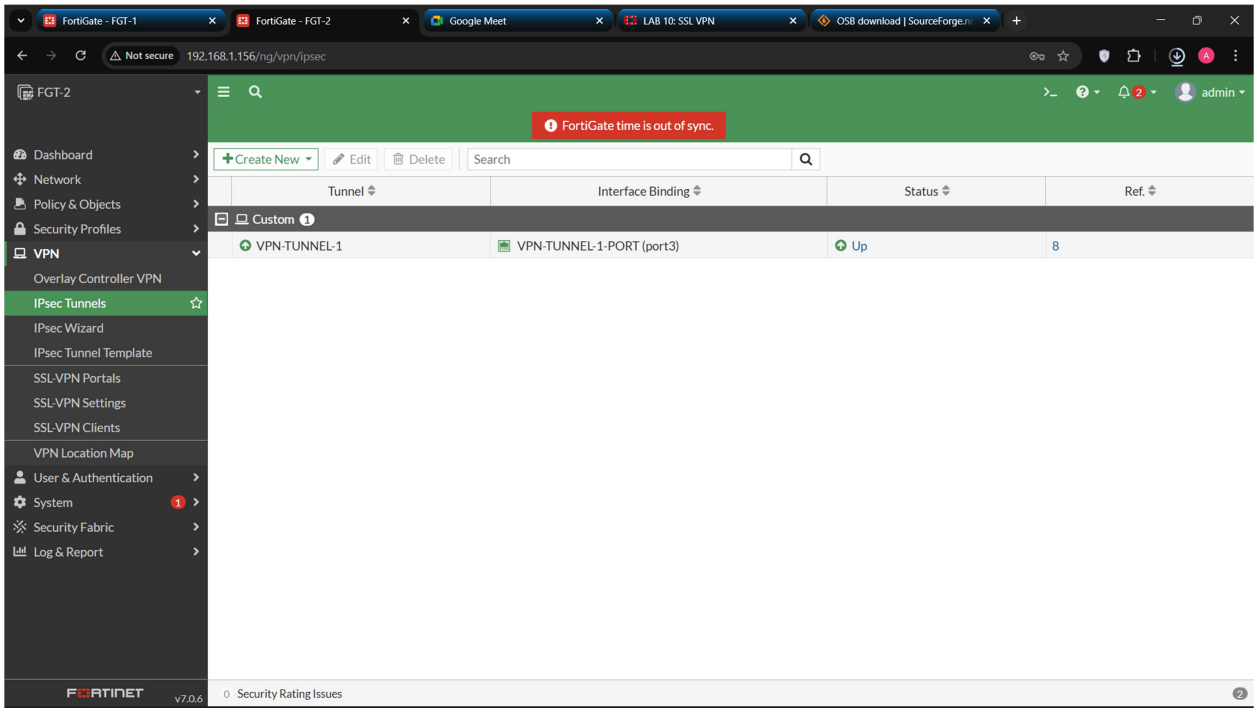


- **Logs and Events**



- **Tunnel Status:**





f) Advantages of IPsec VPN

- Strong encryption and authentication.
- Ideal for permanent site-to-site connections.
- Transparent to users and applications.
- Supports redundancy with multiple WAN links.

Week 3: FortiGate VPN with SD-WAN Integration

a) Overview

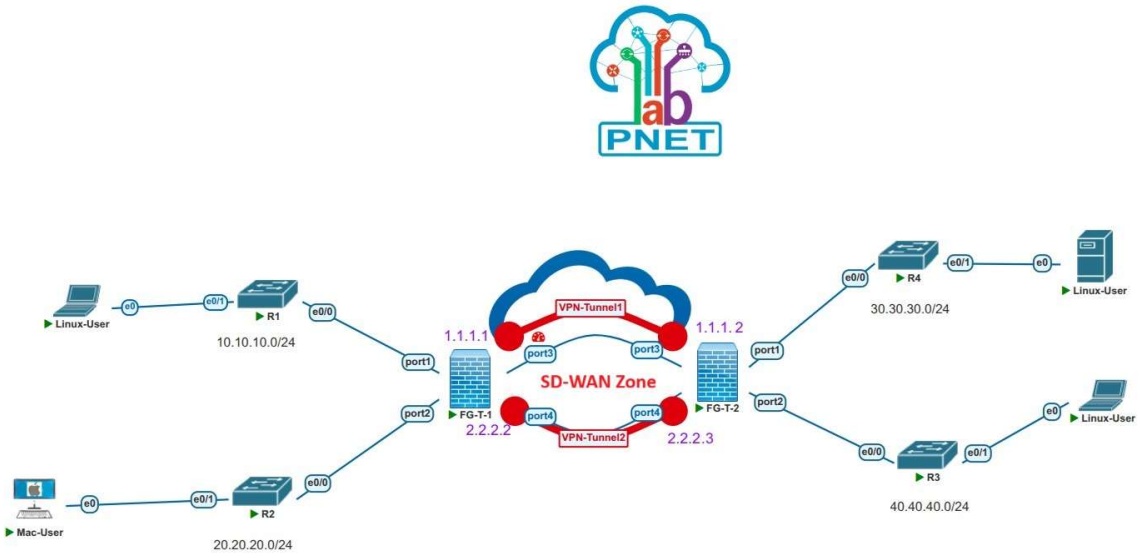
- **SD-WAN (Software-Defined Wide Area Network)** is an advanced networking technology that enhances WAN performance by intelligently directing traffic across multiple WAN connections (such as MPLS, broadband, or LTE). Integrating SD-WAN with VPN allows FortiGate devices to **dynamically select the best path** for VPN traffic based on real-time performance metrics.

b) Benefits of SD-WAN Integration

- Improved VPN performance and stability.
- Intelligent traffic steering based on latency, jitter, and packet loss.
- Cost-efficient use of multiple WAN connections.
- Centralized management and visibility.

c) SD-WAN Configuration on FortiGate

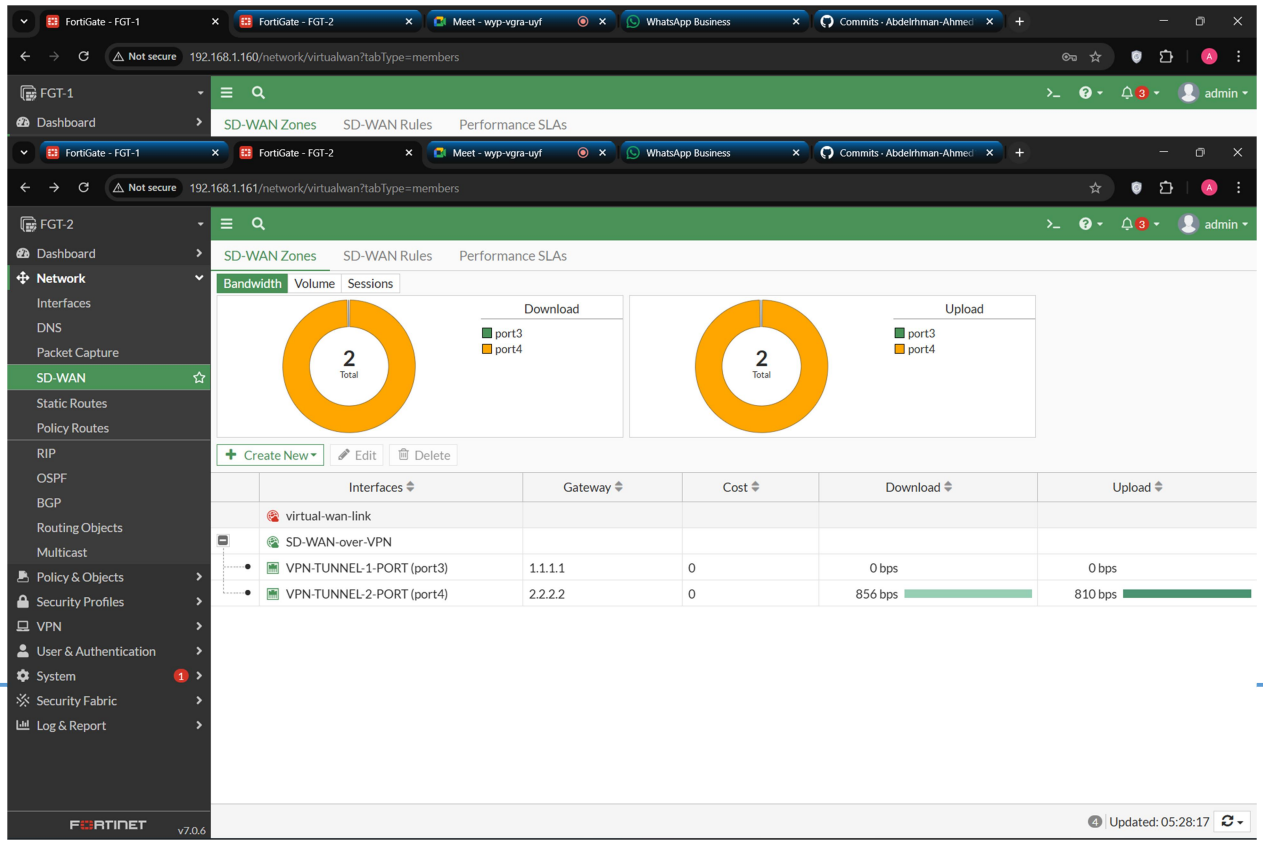
- **Objective:**
  Integrate SD-WAN with VPN tunnels to ensure optimized routing for secure connections.



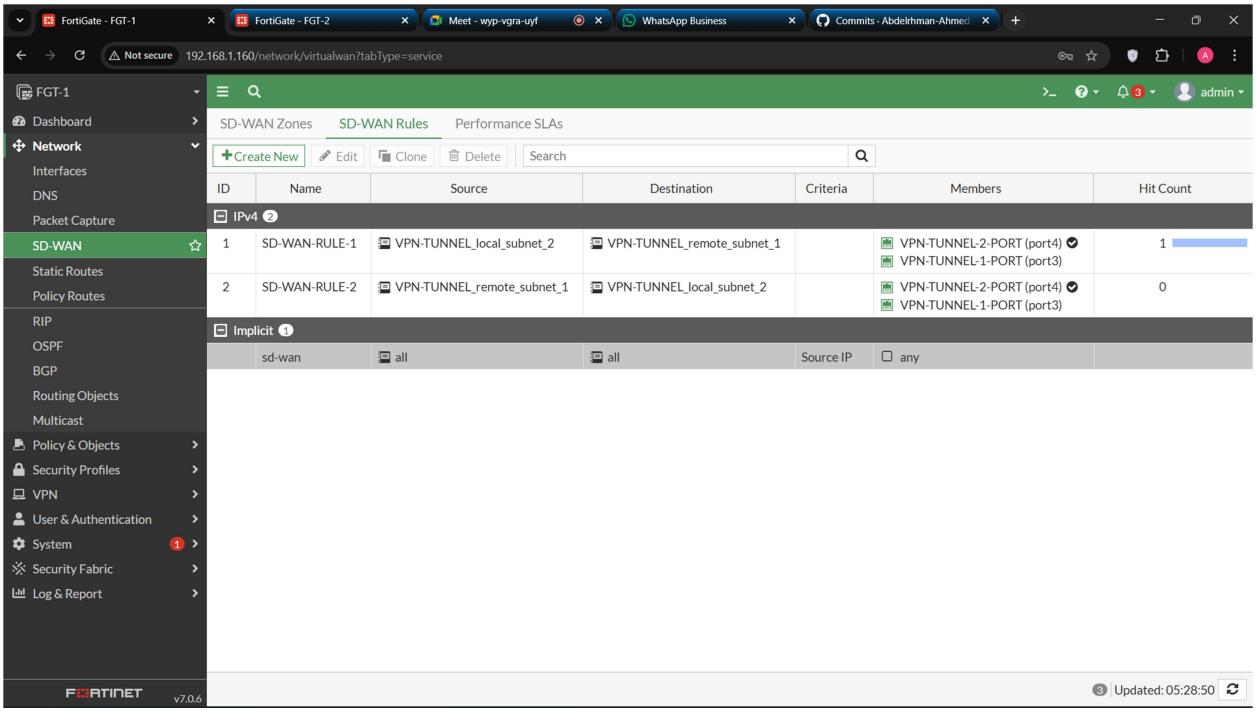
VPN with SD-WAN Integration Topology

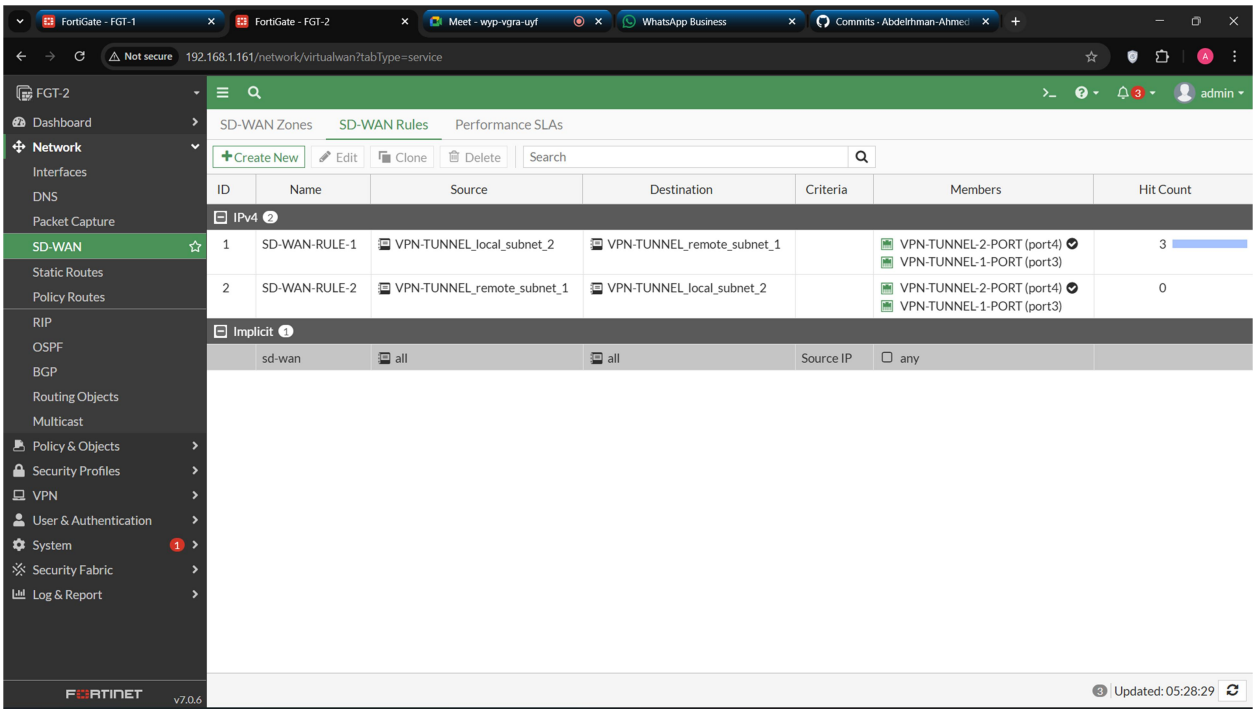
- **Steps:**

Step 1: create SD-wan zone, SD-wan members on FGT-1 and FGT2

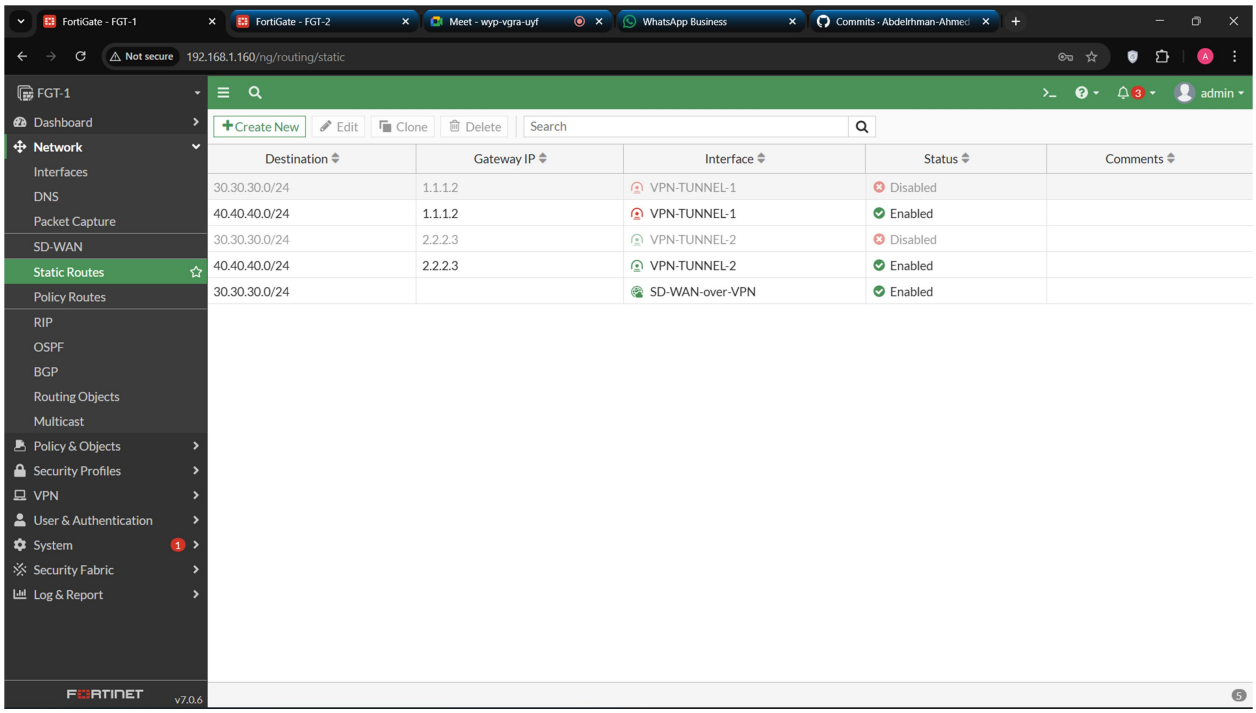


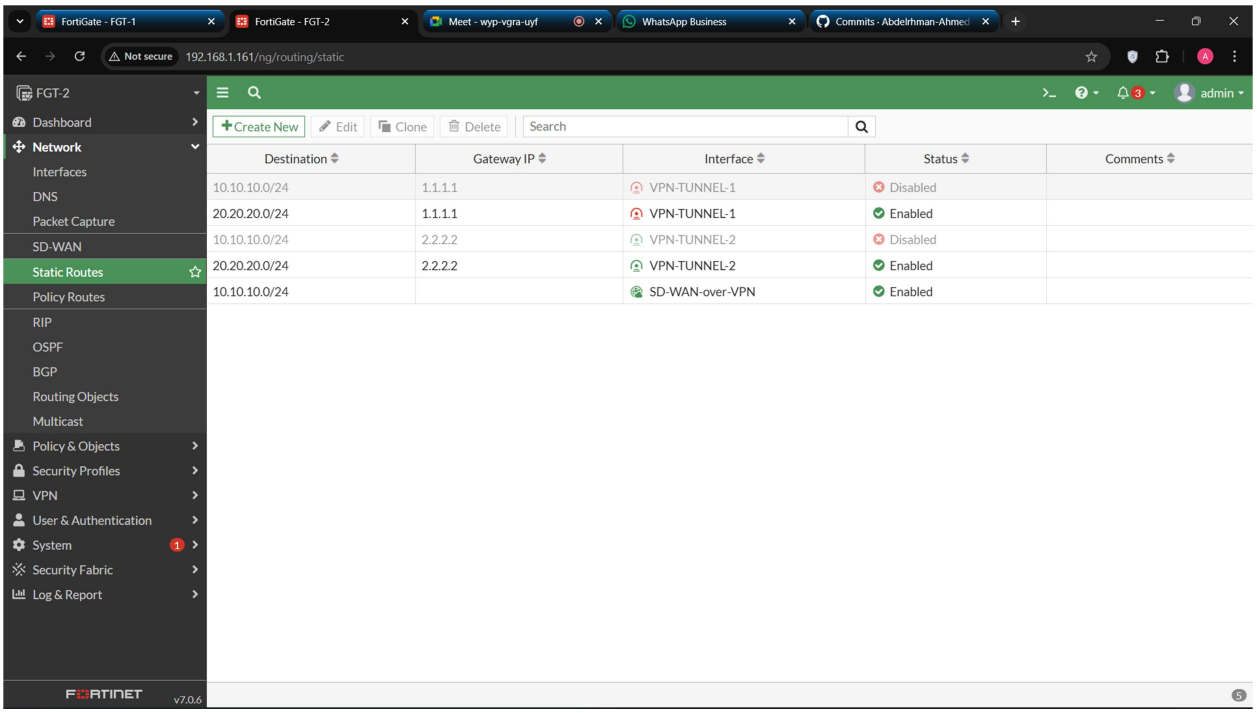
Step 2: Create SD-WAN Rules on FGT-1 and FGT-2



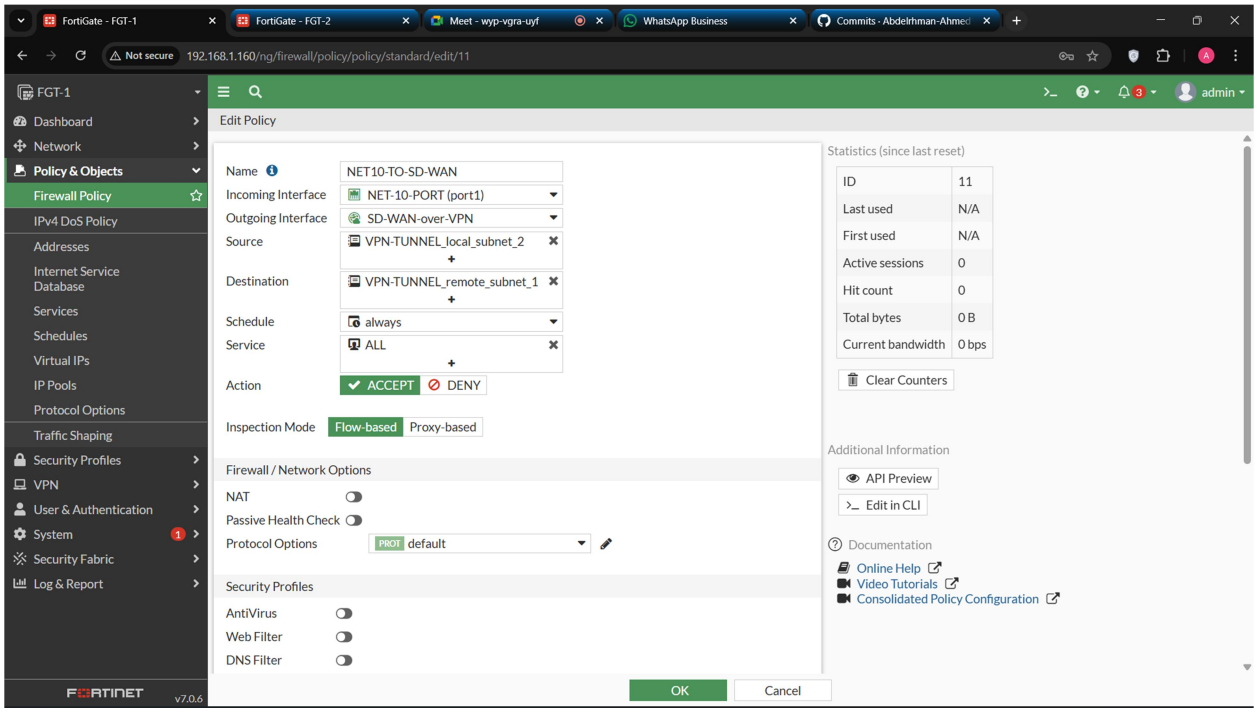


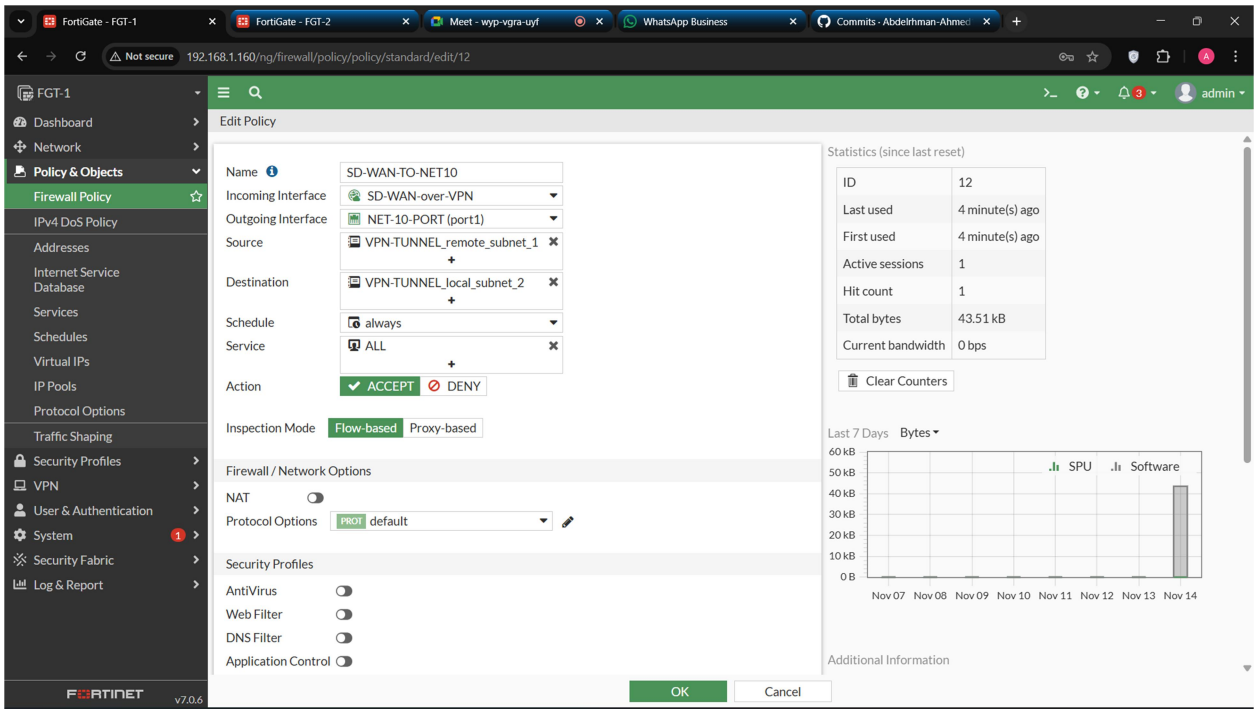
Step 3: Set Static Routes on FGT-1 and FGT-2

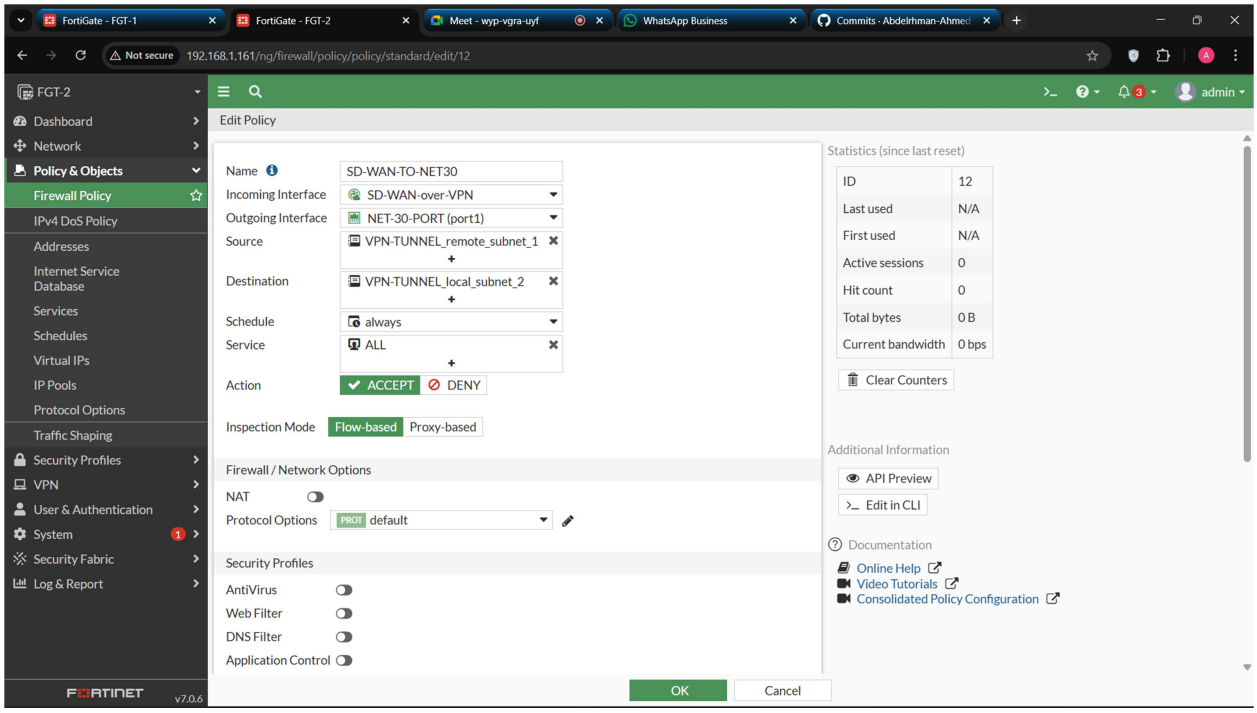


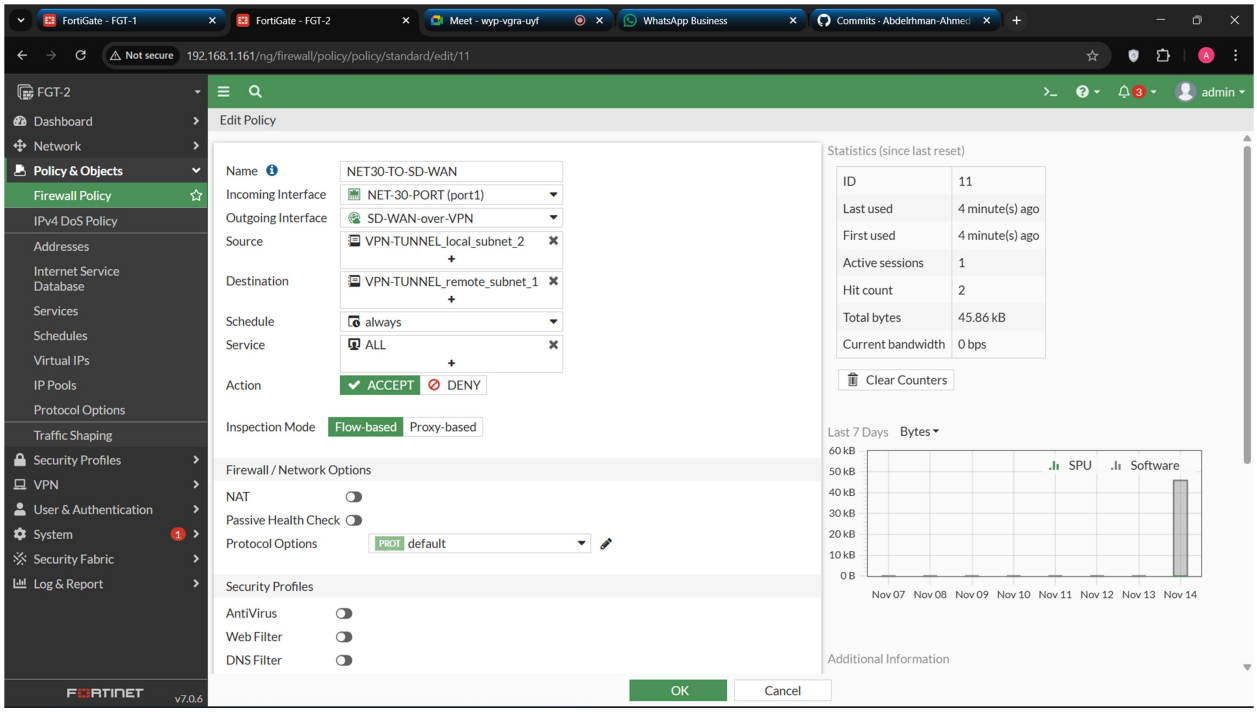


Step 4: Configure Policies



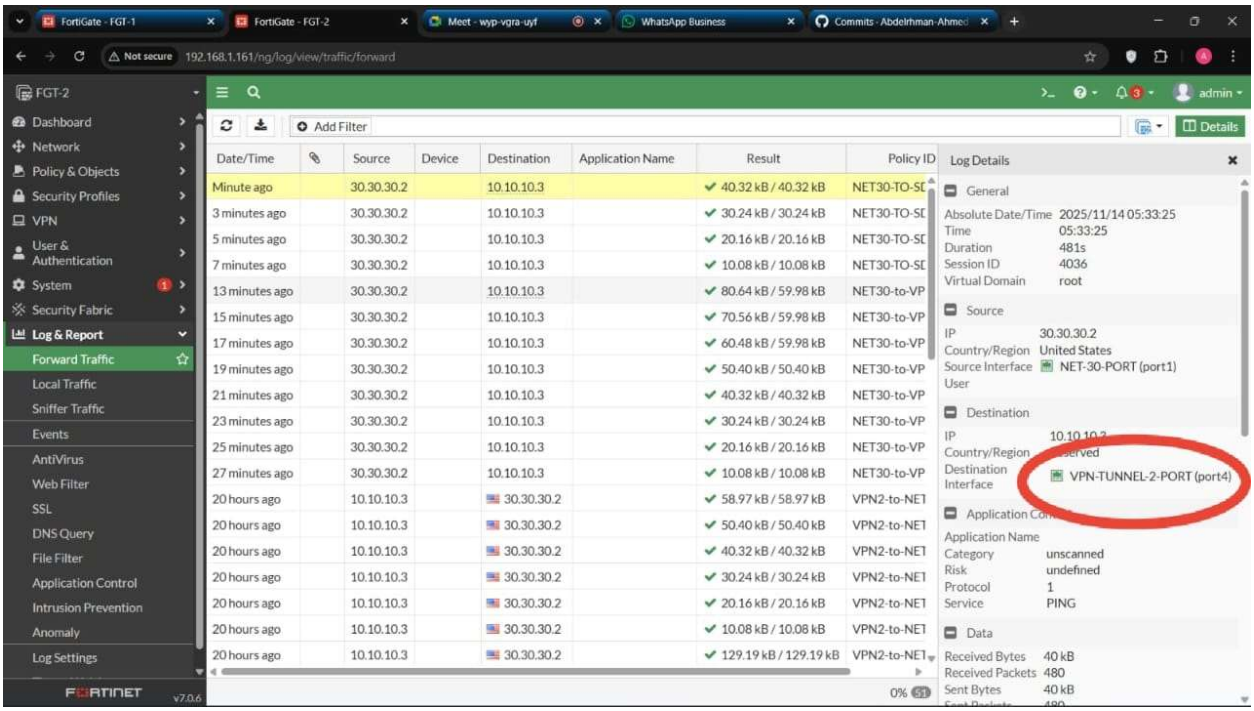



FortiGate - FGT-1
FortiGate - FGT-2
Meet - wyp-vgra-uyf
WhatsApp Business
Commits - Abdelrhman-Ahmed
Not secure
192.168.1.161/ng/firewall/policy/policy/standard/edit/12
FGT-2
admin
Dashboard
Network
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
System
Security Fabric
Log & Report
Edit Policy
Name SD-WAN-TO-NET30
Incoming Interface SD-WAN-over-VPN
Outgoing Interface NET-30-PORT (port1)
Source VPN-TUNNEL_remote_subnet_1
Destination VPN-TUNNEL_local_subnet_2
Schedule always
Service ALL
Action ACCEPT DENY
Inspection Mode Flow-based Proxy-based
Firewall / Network Options
NAT
Protocol Options PROT default
Security Profiles
AntiVirus
Web Filter
DNS Filter
Application Control
OK
Cancel
Statistics (since last reset)
ID 12
Last used N/A
First used N/A
Active sessions 0
Hit count 0
Total bytes 0 B
Current bandwidth 0 bps
Clear Counters
Additional Information
API Preview
Edit in CLI
Documentation
Online Help
Video Tutorials
Consolidated Policy Configuration
FORTINET
v7.0.6

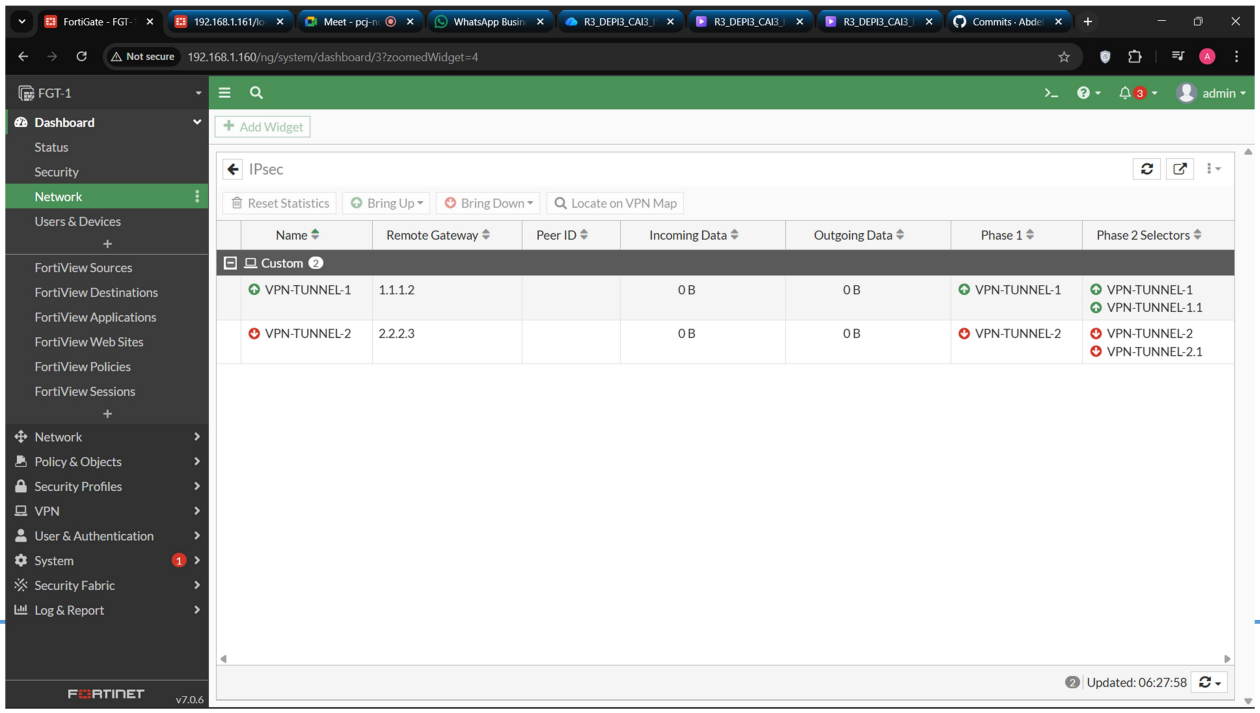

FortiGate - FGT-1
FortiGate - FGT-2
Meet - wyp-vgra-uyf
WhatsApp Business
Commits - Abdelrhman-Ahmed
Not secure
192.168.1.161/ng/firewall/policy/policy/standard/edit/11
FGT-2
admin
Dashboard
Network
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
System
Security Fabric
Log & Report
Edit Policy
Name NET30-TO-SD-WAN
Incoming Interface NET-30-PORT (port1)
Outgoing Interface SD-WAN-over-VPN
Source VPN-TUNNEL_local_subnet_2
Destination VPN-TUNNEL_remote_subnet_1
Schedule always
Service ALL
Action ACCEPT DENY
Inspection Mode Flow-based Proxy-based
Firewall / Network Options
NAT
Passive Health Check
Protocol Options PROT default
Security Profiles
AntiVirus
Web Filter
DNS Filter
OK
Cancel
Statistics (since last reset)
ID 11
Last used 4 minute(s) ago
First used 4 minute(s) ago
Active sessions 1
Hit count 2
Total bytes 45.86 kB
Current bandwidth 0 bps
Clear Counters
Last 7 Days Bytes
60 kB
50 kB
40 kB
30 kB
20 kB
10 kB
0 B
SPU
Software
Nov 07 Nov 08 Nov 09 Nov 10 Nov 11 Nov 12 Nov 13 Nov 14
Additional Information
FORTINET
v7.0.6

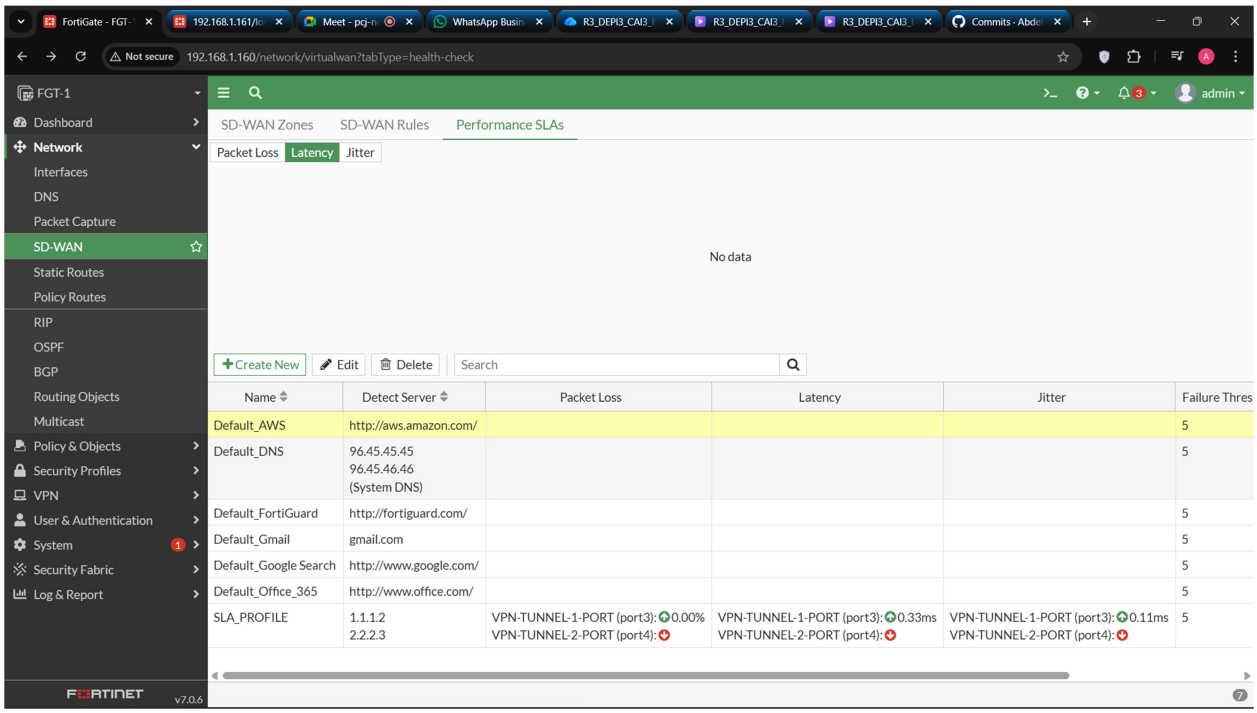
d) Testing and Performance Evaluation

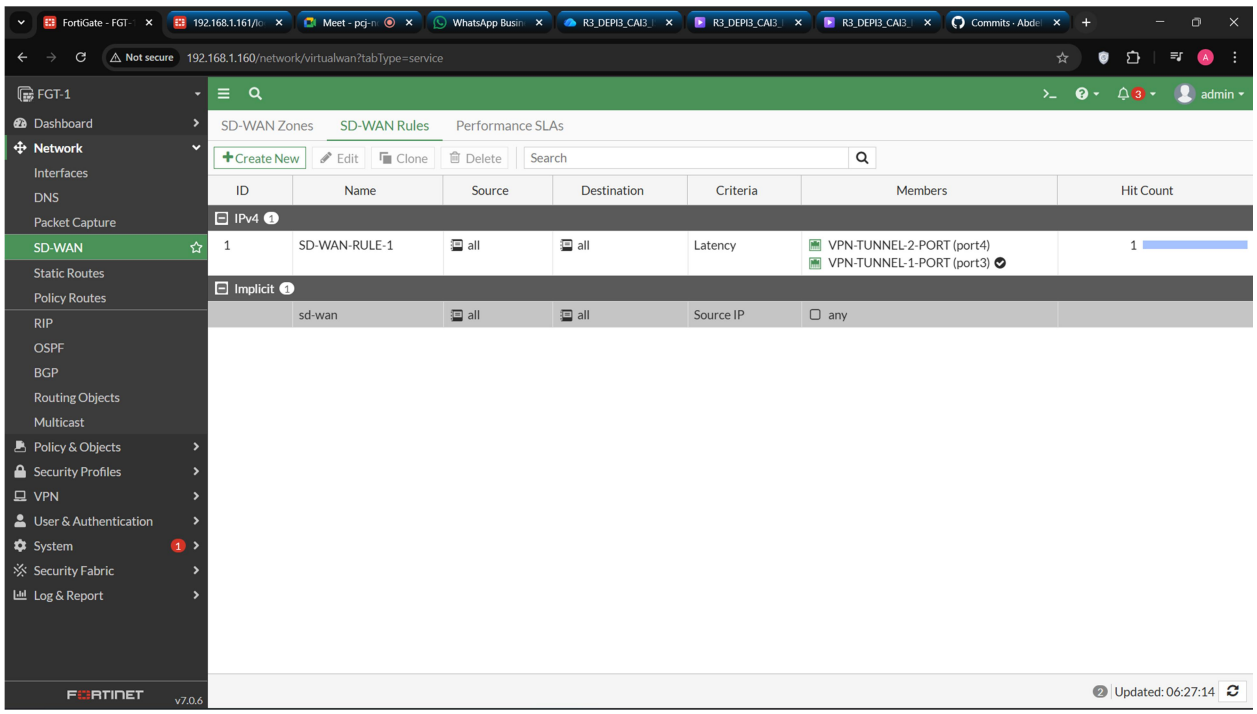
1. Tunnel 1 down and Tunnel 2 up

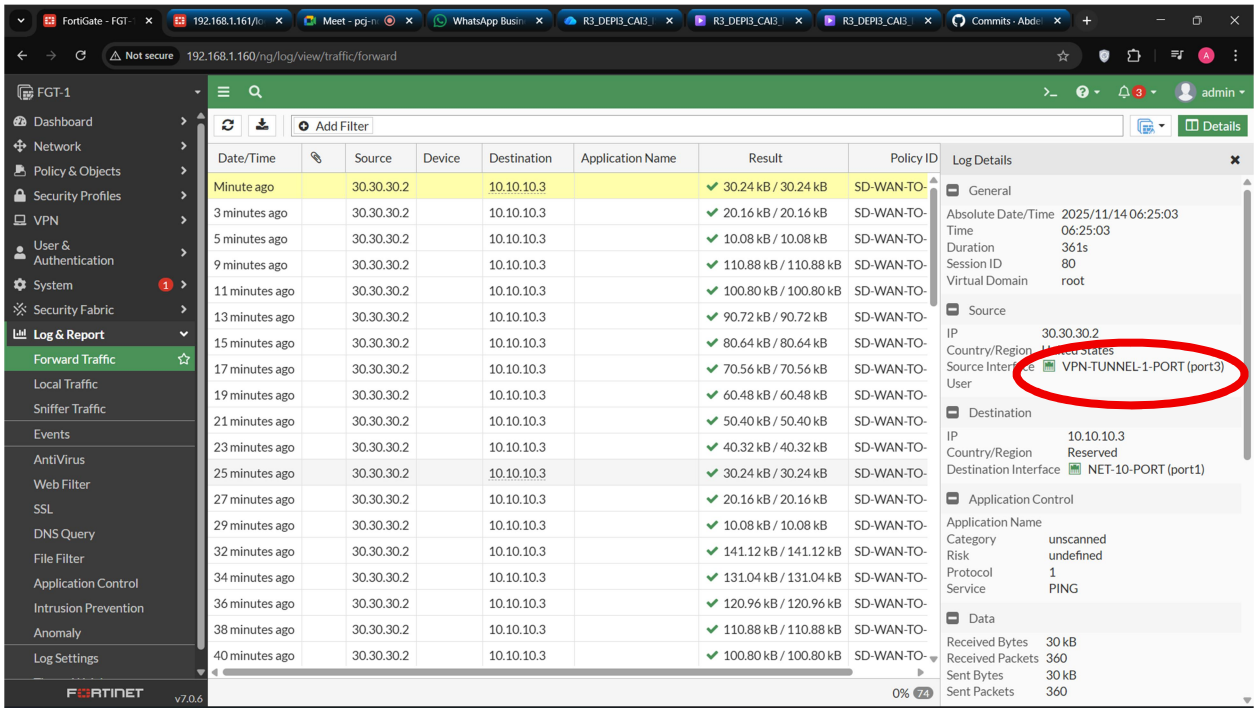


2. Tunnel 1 up and Tunnel 2 down




FortiGate - FGT-
192.168.1.161/lo
Meet - pcj-n
WhatsApp Busin
R3_DEPI3_CAI3_I
R3_DEPI3_CAI3_I
R3_DEPI3_CAI3_I
Commits · Abde
Not secure
192.168.1.160/network/virtualwan?tabType=health-check
FGT-1
admin
Dashboard
Network
Interfaces
DNS
Packet Capture
SD-WAN
Static Routes
Policy Routes
RIP
OSPF
BGP
Routing Objects
Multicast
Policy & Objects
Security Profiles
VPN
User & Authentication
System
Security Fabric
Log & Report
SD-WAN Zones
SD-WAN Rules
Performance SLAs
Packet Loss
Latency
Jitter
No data
Create New
Edit
Delete
Search
Name
Detect Server
Packet Loss
Latency
Jitter
Failure Thres
Default_AWS
http://aws.amazon.com/
5
Default_DNS
96.45.45.45
96.45.46.46
(System DNS)
5
Default_FortiGuard
http://fortiguard.com/
5
Default_Gmail
gmail.com
5
Default_Google Search
http://www.google.com/
5
Default_Office_365
http://www.office.com/
5
SLA_PROFILE
1.1.1.2
2.2.2.3
VPN-TUNNEL-1-PORT (port3): 0.00%
VPN-TUNNEL-2-PORT (port4):
VPN-TUNNEL-1-PORT (port3): 0.33ms
VPN-TUNNEL-2-PORT (port4):
VPN-TUNNEL-1-PORT (port3): 0.11ms
VPN-TUNNEL-2-PORT (port4):
5
FORTINET
v7.0.6


FortiGate - FGT-
192.168.1.161/lo
Meet - pcj-n
WhatsApp Busin
R3_DEPI3_CAI3_I
R3_DEPI3_CAI3_I
R3_DEPI3_CAI3_I
Commits · Abde
Not secure
192.168.1.160/network/virtualwan?tabType=service
FGT-1
admin
Dashboard
Network
Interfaces
DNS
Packet Capture
SD-WAN
Static Routes
Policy Routes
RIP
OSPF
BGP
Routing Objects
Multicast
Policy & Objects
Security Profiles
VPN
User & Authentication
System
Security Fabric
Log & Report
SD-WAN Zones
SD-WAN Rules
Performance SLAs
Create New
Edit
Clone
Delete
Search
ID
Name
Source
Destination
Criteria
Members
Hit Count
IPv4 1
1
SD-WAN-RULE-1
all
all
Latency
VPN-TUNNEL-2-PORT (port4)
VPN-TUNNEL-1-PORT (port3)
1
Implicit 1
sd-wan
all
all
Source IP
any
Updated: 06:27:14
FORTINET
v7.0.6


FortiGate - FGT-
192.168.1.161/lo
Meet - pcj-n
WhatsApp Busin
R3_DEPI3_CAI3_I
R3_DEPI3_CAI3_I
R3_DEPI3_CAI3_I
Commits · Abde
Not secure
192.168.1.160/ng/log/view/traffic/forward
FGT-1
admin
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
System
Security Fabric
Log & Report
Forward Traffic
Local Traffic
Sniffer Traffic
Events
AntiVirus
Web Filter
SSL
DNS Query
File Filter
Application Control
Intrusion Prevention
Anomaly
Log Settings
FORTINET
v7.0.6
Add Filter
Details
Date/Time
Source
Device
Destination
Application Name
Result
Policy ID
Minute ago 30.30.30.2 10.10.10.3 30.24 kB / 30.24 kB SD-WAN-TO-
3 minutes ago 30.30.30.2 10.10.10.3 20.16 kB / 20.16 kB SD-WAN-TO-
5 minutes ago 30.30.30.2 10.10.10.3 10.08 kB / 10.08 kB SD-WAN-TO-
9 minutes ago 30.30.30.2 10.10.10.3 110.88 kB / 110.88 kB SD-WAN-TO-
11 minutes ago 30.30.30.2 10.10.10.3 100.80 kB / 100.80 kB SD-WAN-TO-
13 minutes ago 30.30.30.2 10.10.10.3 90.72 kB / 90.72 kB SD-WAN-TO-
15 minutes ago 30.30.30.2 10.10.10.3 80.64 kB / 80.64 kB SD-WAN-TO-
17 minutes ago 30.30.30.2 10.10.10.3 70.56 kB / 70.56 kB SD-WAN-TO-
19 minutes ago 30.30.30.2 10.10.10.3 60.48 kB / 60.48 kB SD-WAN-TO-
21 minutes ago 30.30.30.2 10.10.10.3 50.40 kB / 50.40 kB SD-WAN-TO-
23 minutes ago 30.30.30.2 10.10.10.3 40.32 kB / 40.32 kB SD-WAN-TO-
25 minutes ago 30.30.30.2 10.10.10.3 30.24 kB / 30.24 kB SD-WAN-TO-
27 minutes ago 30.30.30.2 10.10.10.3 20.16 kB / 20.16 kB SD-WAN-TO-
29 minutes ago 30.30.30.2 10.10.10.3 10.08 kB / 10.08 kB SD-WAN-TO-
32 minutes ago 30.30.30.2 10.10.10.3 141.12 kB / 141.12 kB SD-WAN-TO-
34 minutes ago 30.30.30.2 10.10.10.3 131.04 kB / 131.04 kB SD-WAN-TO-
36 minutes ago 30.30.30.2 10.10.10.3 120.96 kB / 120.96 kB SD-WAN-TO-
38 minutes ago 30.30.30.2 10.10.10.3 110.88 kB / 110.88 kB SD-WAN-TO-
40 minutes ago 30.30.30.2 10.10.10.3 100.80 kB / 100.80 kB SD-WAN-TO-
0%
Log Details
General
Absolute Date/Time 2025/11/14 06:25:03
Time 06:25:03
Duration 361s
Session ID 80
Virtual Domain root
Source
IP 30.30.30.2
Country/Region United States
Source Interface VPN-TUNNEL-1-PORT (port3)
User
Destination
IP 10.10.10.3
Country/Region Reserved
Destination Interface NET-10-PORT (port1)
Application Control
Application Name
Category unscanned
Risk undefined
Protocol 1
Service PING
Data
Received Bytes 30 kB
Received Packets 360
Sent Bytes 30 kB
Sent Packets 360

Conclusion

- This project successfully demonstrated the implementation of **VPN solutions using FortiGate firewalls**.
  By configuring **SSL VPN**, **IPsec VPN**, and **SD-WAN**, the project achieved:

- **Secure remote and site-to-site connectivity**
- **Improved network performance and reliability**
- **Effective utilization of multiple WAN connections**
- Through rigorous testing and documentation, it was confirmed that FortiGate's VPN and SD-WAN features provide an enterprise-grade, secure, and flexible solution for modern networking environments.

References

1. Fortinet Documentation – *FortiGate VPN Configuration Guide*
2. National Telecommunication Institute (NTI) – *Network Security Course Notes*
3. RFC 4301 – *Security Architecture for the Internet Protocol*
4. Fortinet – *SD-WAN Deployment Best Practices (2024)*