



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

---

<b>Project 3: Implementing VPN Solutions with FortiGate .....</b>	2
<b>Introduction.....</b>	2
<b>Week 1: VPN Concepts and SSL VPN Configuration .....</b>	3
<b>a) VPN Overview.....</b>	3
<b>b) Types of VPNs and Their Use Cases .....</b>	3
<b>c) SSL VPN.....</b>	4
<b>d) SSL VPN Configuration on FortiGate .....</b>	7
<b>Week 2: IPsec VPN Configuration.....</b>	10
<b>a) Overview .....</b>	10
<b>b) How IPsec VPN Works .....</b>	10
<b>c) Key Components .....</b>	11
<b>d) IPsec Configuration Steps on FortiGate.....</b>	11
<b>e) Testing and Verification .....</b>	16
<b>f) Advantages of IPsec VPN .....</b>	20
<b>Week 3: FortiGate VPN with SD-WAN Integration .....</b>	20
<b>a) Overview .....</b>	20
<b>b) Benefits of SD-WAN Integration.....</b>	20
<b>c) SD-WAN Configuration on FortiGate .....</b>	20
<b>d) Testing and Performance Evaluation .....</b>	26
<b>Conclusion.....</b>	29
<b>References .....</b>	29

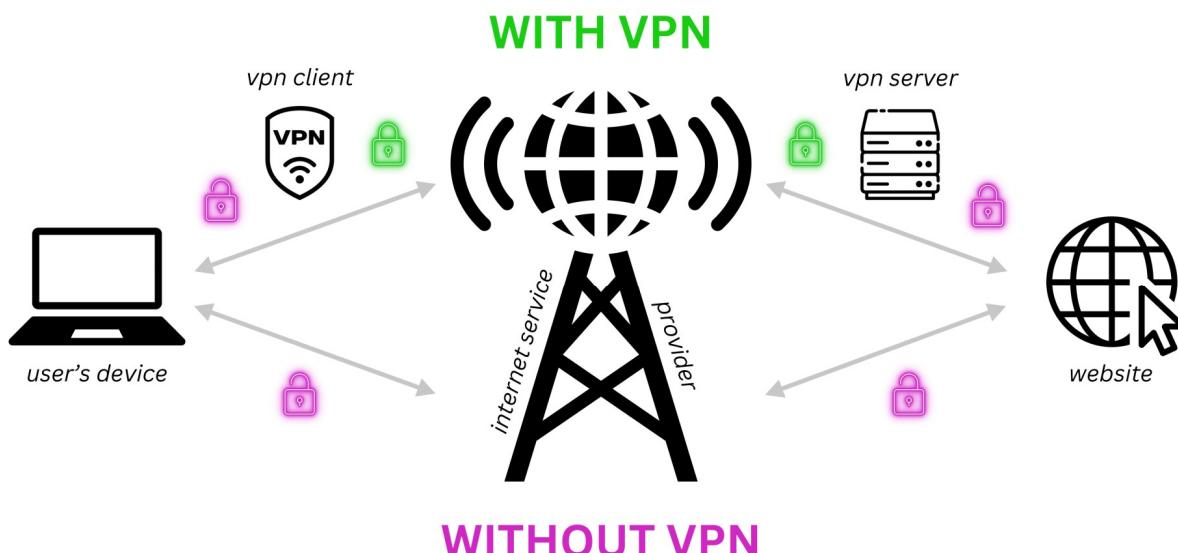
## Project 3: Implementing VPN Solutions with FortiGate

### 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
<b>Remote Access VPN (Client-to-Site VPN)</b>	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.
<b>Site-to-Site VPN</b>	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.
<b>SSL VPN (Secure Sockets Layer VPN)</b>	Uses HTTPS (port 443) to provide secure remote access via a web browser.	Users who need access without installing special VPN software.

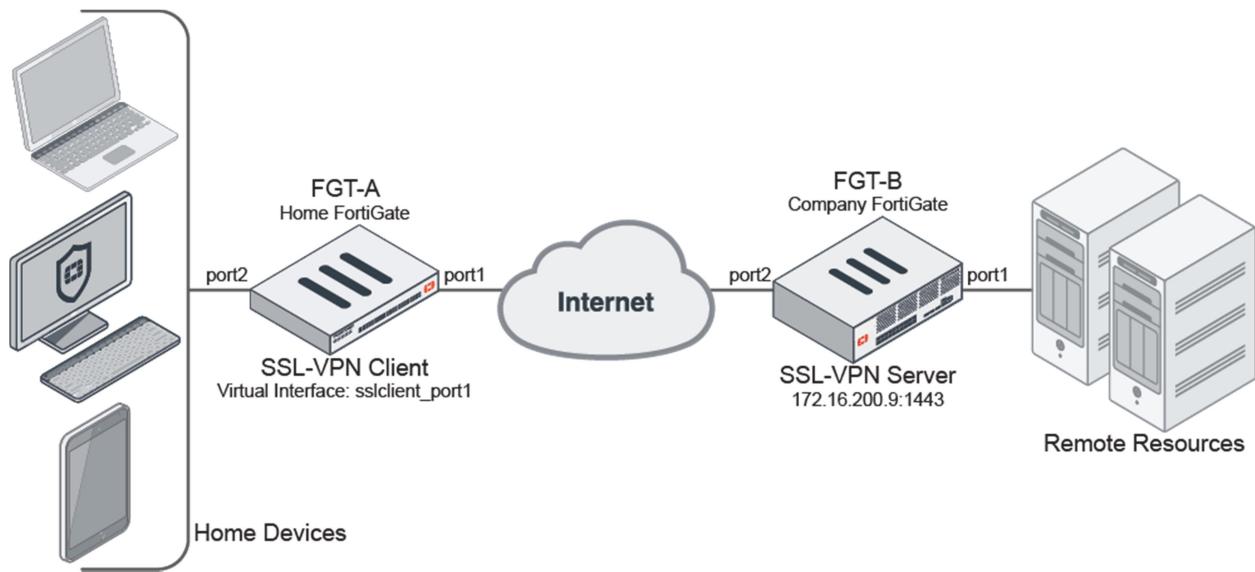
	browser or client. It encrypts traffic using SSL/TLS protocols.	clients (works through browsers).
<b>IPsec VPN (Internet Protocol Security VPN)</b>	Uses the IPsec protocol suite to encrypt and authenticate IP packets between sites or devices. It operates at the network layer.	Permanent, secure tunnels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

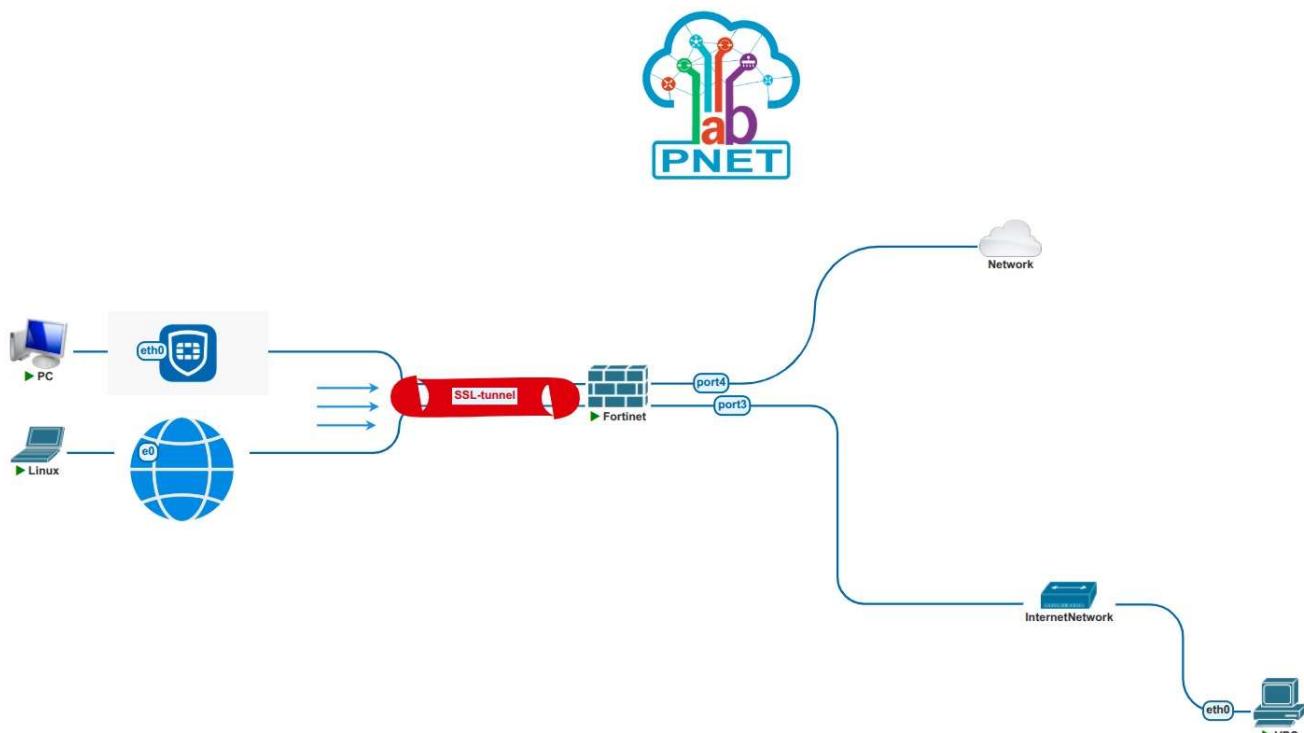
## Common Use Cases

- 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

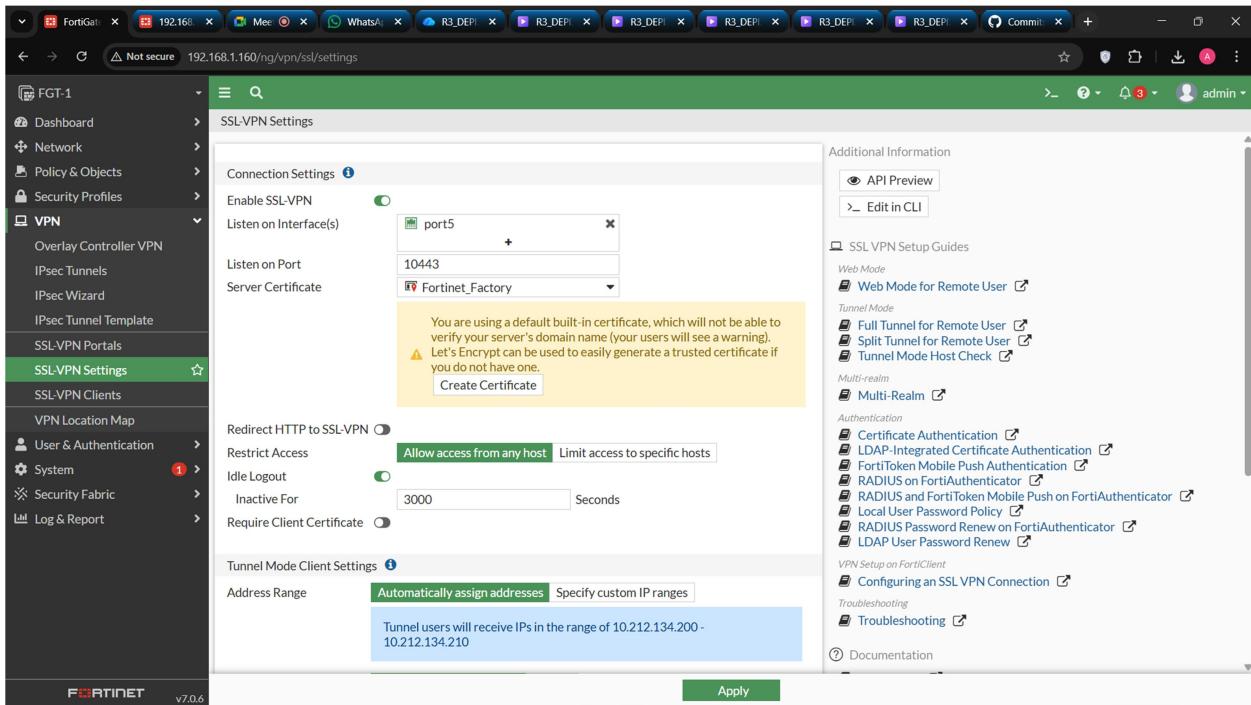
#### Objective:

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):

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

#### Phase 2 (Data Encryption):

- Defines traffic selectors (networks that will communicate).

b. Encrypts user data packets through the established tunnel.

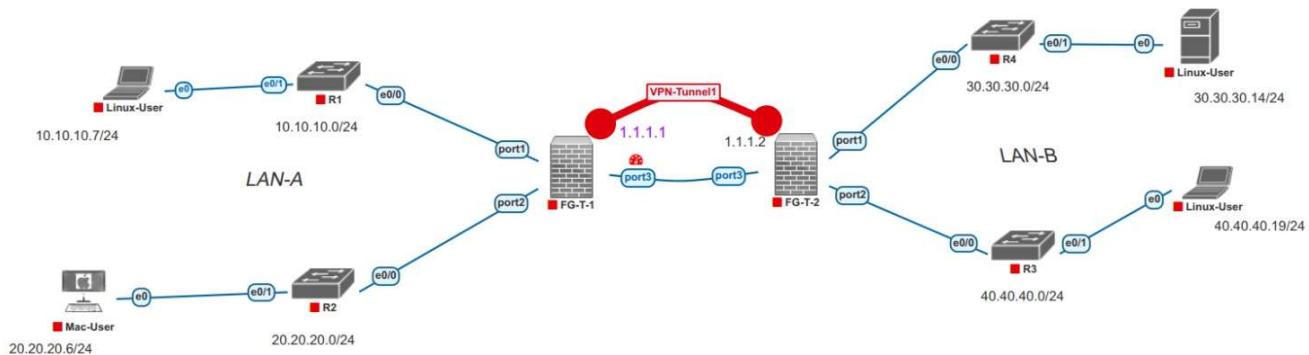
### c) Key Components

- 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

**Name:** VPN-TUNNEL-1

**Comments:**

**Network**

- IP Version: IPv4
- Remote Gateway: Static IP Address (1.1.1.2)
- IP Address: 1.1.1.2
- Interface: VPN-TUNNEL-1-PORT (port3)
- Local Gateway: Primary IP (1.1.1.1)
- Mode Config: (checkbox unchecked)
- NAT Traversal: Enable
- Keepalive Frequency: 10
- Dead Peer Detection: On Demand
- DPD retry count: 3
- DPD retry interval: 20 s
- Forward Error Correction: Egress, Ingress (checkboxes unchecked)

**Authentication**

- Method: Pre-shared Key
- Pre-shared Key: FORTINET

**Name:** VPN-TUNNEL-1

**Comments:**

**Network**

Remote Gateway: Static IP Address (1.1.1.2), Local Gateway: 1.1.1.1, Interface: port3

**Authentication**

- Method: Pre-shared Key
- Pre-shared Key: FORTINET
- IKE**
- Version: 1
- Mode: Aggressive

**Phase 1 Proposal**

- Algorithms: DES-SHA256
- Diffie-Hellman Groups: 32, 31, 30

**XAUTH**

Type: Disabled

**Phase 2 Selectors**

**Name:** VPN-TUNNEL-1

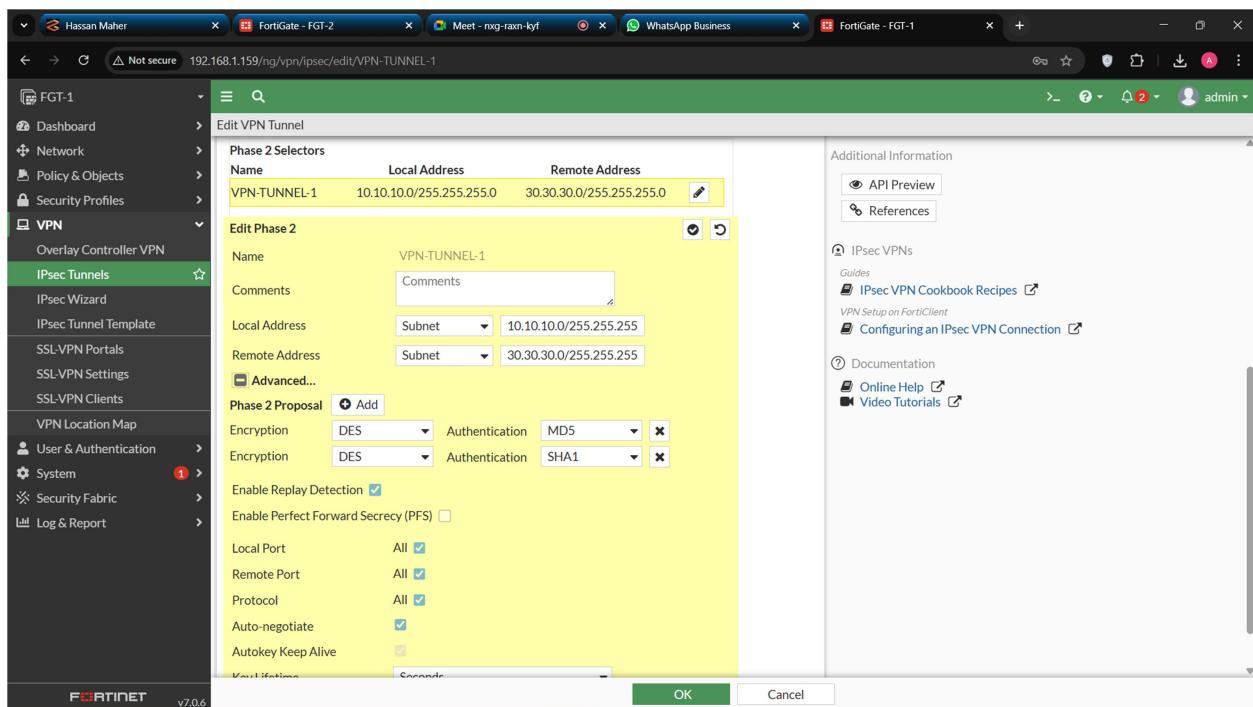
**Comments:**

**Network**

Remote Gateway: Static IP Address (1.1.1.2), Local Gateway: 1.1.1.1, Interface: port3

**Authentication**

Authentication Method: Pre-shared Key (FORTINET)



Not secure 192.168.1.159/ng vpn/ipsec/edit/VPN-TUNNEL-1

FGT-1

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

FGT-1

Edit VPN Tunnel

Phase 2 Selectors

Name	Local Address	Remote Address
VPN-TUNNEL-1	10.10.0/255.255.255.0	30.30.0/255.255.255.0

Edit Phase 2

Name: VPN-TUNNEL-1

Comments: Comments

Local Address: Subnet 10.10.0/255.255.255

Remote Address: Subnet 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:

Keepalive: Seconds

OK Cancel

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

## Step 2: Set Static Routes

The screenshot shows the FortiGate web interface for FGT-1. The left sidebar is expanded, showing the Network section with 'Static Routes' selected. The main content area displays a table of static routes. One route is listed:

Destination	Gateway IP	Interface	Status	Comments
30.30.30.0/24	1.1.1.2	VPN-TUNNEL-1	Enabled	

The screenshot shows the FortiGate web interface for FGT-2. The left sidebar is expanded, showing the Network section with 'Static Routes' selected. The main content area displays a table of static routes. One route is listed:

Destination	Gateway IP	Interface	Status	Comments
10.10.10.0/24	1.1.1.1	VPN-TUNNEL-1	Enabled	

## Step 3: Configure Policies

The screenshot shows the FortiGate management interface with the URL [192.168.1.159/ng/firewall/policy/policy/standard/edit/3](http://192.168.1.159/ng/firewall/policy/policy/standard/edit/3). The left sidebar is the navigation menu, and the main area is the 'Edit Policy' dialog for a policy named 'NET10-to-VPN'. The policy details are as follows:

- Name:** NET10-to-VPN
- Incoming Interface:** NET-10-PORT (port1)
- Outgoing Interface:** VPN-TUNNEL-1
- Source:** VPN-TUNNEL-1\_local\_subnet\_2
- Destination:** VPN-TUNNEL-1\_remote\_subnet\_1
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (selected)
- Inspection Mode:** Flow-based

The dialog also displays statistics since the last reset:

ID	3
Last used	4 minute(s) ago
First used	3 hour(s) ago
Active sessions	0
Hit count	5
Total bytes	9.07 kB
Current bandwidth	0 bps

Below the dialog, there is a chart titled 'Last 7 Days Bytes' showing traffic distribution between SPU and Software over time from Nov 06 to Nov 13.

The screenshot shows the FortiGate management interface with the URL [192.168.1.156/ng/firewall/policy/policy/standard?showInList=%7B%22origin\\_key%22%7D](http://192.168.1.156/ng/firewall/policy/policy/standard?showInList=%7B%22origin_key%22%7D). The left sidebar is the navigation menu, and the main area is the 'List Policies' dialog. It shows a single policy entry:

Name	Source	Destination	Schedule	Action	NAT	Security Profiles	Log
NET30-PORT (port1) → VPN-TUNNEL-1	NET30-to-VPN	VPN-TUNNEL-1_local_subnet_2	VPN-TUNNEL-1_remote_subnet_1	always	ALL	ACCEPT	Disabled

## e) Testing and Verification

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

The screenshot shows a terminal window titled "sakura" running on a Linux system. The terminal displays the output of a "ping" command to an IP address. The output shows 12 packets transmitted, all received, with no packet loss. The round-trip time statistics are provided at the end.

```
Thursday 13 November - 17:34

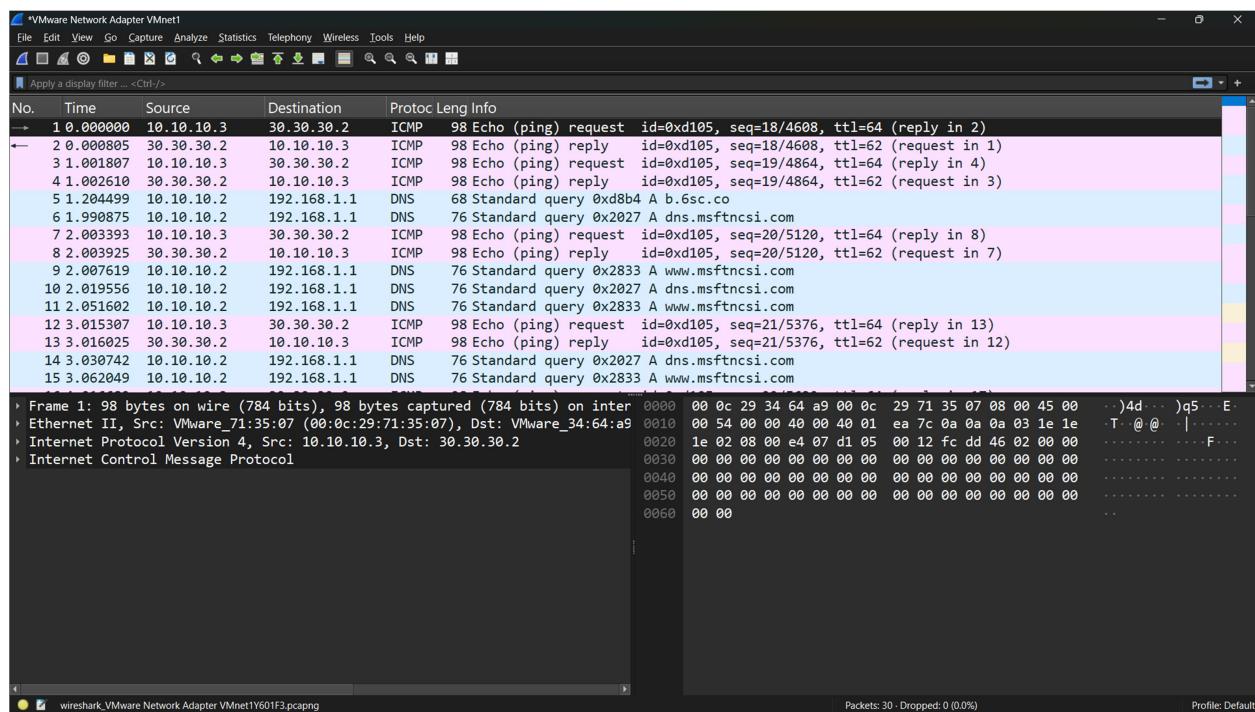
root@slitaz:~# ping 30.30.30.2
PING 30.30.30.2 (30.30.30.2): 56 data bytes
64 bytes from 30.30.30.2: seq=0 ttl=62 time=1.345 ms
64 bytes from 30.30.30.2: seq=1 ttl=62 time=1.014 ms
64 bytes from 30.30.30.2: seq=2 ttl=62 time=1.037 ms
64 bytes from 30.30.30.2: seq=3 ttl=62 time=1.154 ms
64 bytes from 30.30.30.2: seq=4 ttl=62 time=1.634 ms
64 bytes from 30.30.30.2: seq=5 ttl=62 time=0.821 ms
64 bytes from 30.30.30.2: seq=6 ttl=62 time=0.809 ms
64 bytes from 30.30.30.2: seq=7 ttl=62 time=0.661 ms
64 bytes from 30.30.30.2: seq=8 ttl=62 time=0.989 ms
64 bytes from 30.30.30.2: seq=9 ttl=62 time=0.895 ms

64 bytes from 30.30.30.2: seq=10 ttl=62 time=1.031 ms
64 bytes from 30.30.30.2: seq=11 ttl=62 time=2.264 ms
^C
--- 30.30.30.2 ping statistics ---
12 packets transmitted, 12 packets received, 0% packet loss
round-trip min/avg/max = 0.661/1.137/2.264 ms
root@slitaz:~#
```

## ping from PC-3 to PC-1

```
root@slitaz:~# ping 10.10.10.3
PING 10.10.10.3 (10.10.10.3): 56 data bytes
64 bytes from 10.10.10.3: seq=0 ttl=62 time=1.804 ms
64 bytes from 10.10.10.3: seq=1 ttl=62 time=1.001 ms
64 bytes from 10.10.10.3: seq=2 ttl=62 time=1.249 ms
64 bytes from 10.10.10.3: seq=3 ttl=62 time=1.493 ms
64 bytes from 10.10.10.3: seq=4 ttl=62 time=1.196 ms
64 bytes from 10.10.10.3: seq=5 ttl=62 time=1.080 ms
64 bytes from 10.10.10.3: seq=6 ttl=62 time=1.202 ms
64 bytes from 10.10.10.3: seq=7 ttl=62 time=1.440 ms
^C
--- 10.10.10.3 ping statistics ---
8 packets transmitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 1.001/1.308/1.804 ms
root@slitaz:~#
```

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



- Logs and Events

Hassan Maher - Not secure - 192.168.1.156/ng/log/view/traffic/forward

FGT-2

Log Details

Date/Time: 5 minutes ago, Source: 30.30.30.2, Destination: 10.10.10.3, Application Name: 252 B / 252 B, Result: NET30-to-VPN (3)

General

- Absolute Date/Time: 2025/11/13 07:25:52
- Time: 07:25:52
- Duration: 62s
- Session ID: 74481
- Virtual Domain: root

Source

- IP: 30.30.30.2
- Country/Region: United States
- Source Interface: NET-30-PORT (port1)
- User:

Destination

- IP: 10.10.10.3
- Country/Region: Reserved
- Destination Interface: VPN-TUNNEL-1

Application Control

- Application Name:
- Category: unscanned
- Risk: undefined
- Protocol: 1
- Service: PING

Data

- Received Bytes: 252 B
- Received Packets: 3
- Sent Bytes: 252 B
- Sent Packets: 3

- Tunnel Status:

The screenshot shows the FortiGate FGT-1 interface. The left sidebar is open, showing the navigation menu with 'IPsec Tunnels' selected. The main pane displays a table titled 'Custom' with one entry: 'VPN-TUNNEL-1' (Status: Up). A red banner at the top indicates 'FortiGate time is out of sync.'

The screenshot shows the FortiGate FGT-2 interface. The left sidebar is open, showing the navigation menu with 'IPsec Tunnels' selected. The main pane displays a table titled 'Custom' with one entry: 'VPN-TUNNEL-1' (Status: Up). A red banner at the top indicates 'FortiGate time is out of sync.'

## 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.

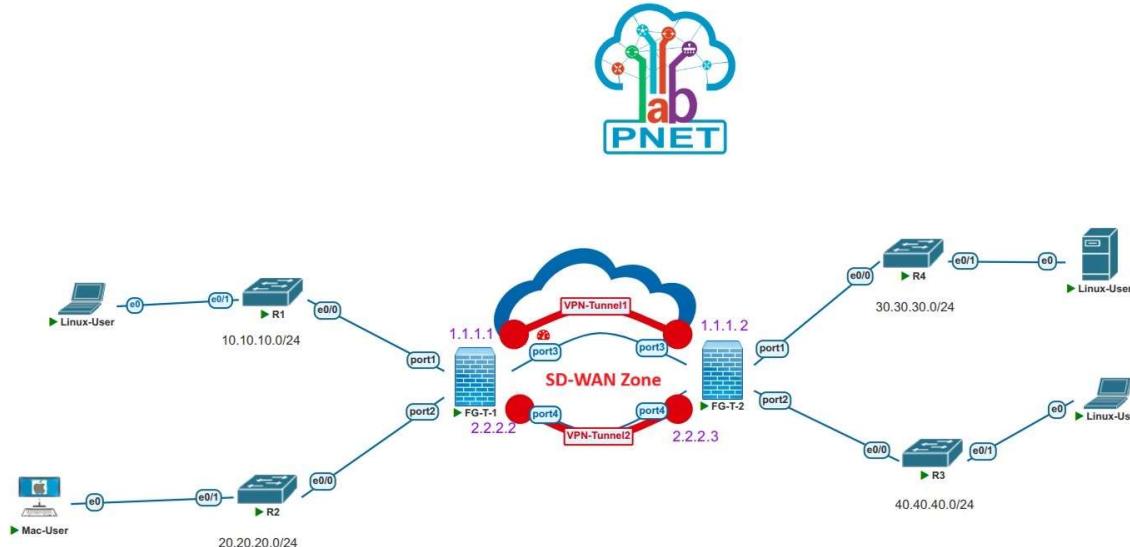
## b) Benefits of SD-WAN Integration

- 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

Member	Port	IP Address	Cost	Download	Upload
VPN-TUNNEL-1-PORT	port3	1.1.1.1	0	0 bps	0 bps
VPN-TUNNEL-2-PORT	port4	2.2.2.2	0	856 bps	810 bps
port3	port3	-	-	-	-
port4	port4	-	-	-	-

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

The screenshot shows the FortiGate FGT-1 interface. The left sidebar is expanded to show the Network section, specifically the SD-WAN tab. The main pane displays the SD-WAN Rules table. There are two entries:

ID	Name	Source	Destination	Criteria	Members	Hit Count
1	SD-WAN-RULE-1	VPN-TUNNEL_local_subnet_2	VPN-TUNNEL_remote_subnet_1		VPN-TUNNEL-2-PORT (port4) VPN-TUNNEL-1-PORT (port3)	1
2	SD-WAN-RULE-2	VPN-TUNNEL_remote_subnet_1	VPN-TUNNEL_local_subnet_2		VPN-TUNNEL-2-PORT (port4) VPN-TUNNEL-1-PORT (port3)	0

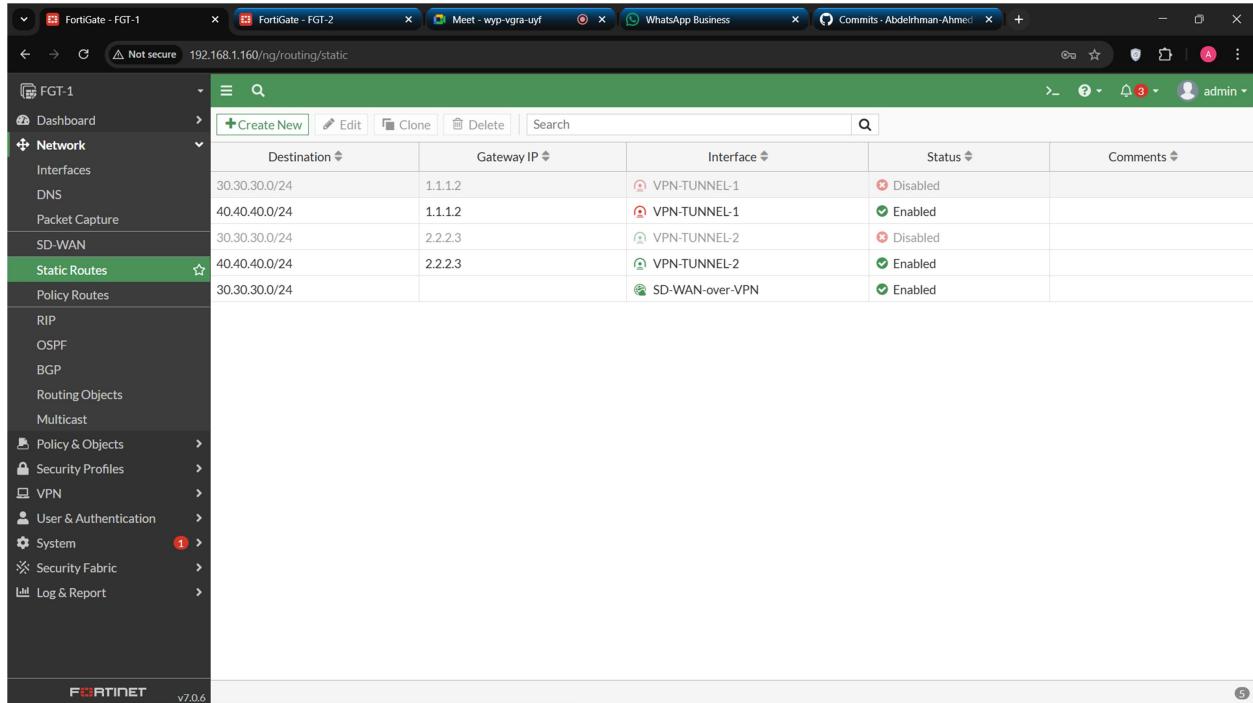
The interface is v7.0.6 and was updated at 05:28:50.

The screenshot shows the FortiGate FGT-2 interface, which is identical to FGT-1 in terms of SD-WAN configuration. It also has two SD-WAN rules listed in the table:

ID	Name	Source	Destination	Criteria	Members	Hit Count
1	SD-WAN-RULE-1	VPN-TUNNEL_local_subnet_2	VPN-TUNNEL_remote_subnet_1		VPN-TUNNEL-2-PORT (port4) VPN-TUNNEL-1-PORT (port3)	3
2	SD-WAN-RULE-2	VPN-TUNNEL_remote_subnet_1	VPN-TUNNEL_local_subnet_2		VPN-TUNNEL-2-PORT (port4) VPN-TUNNEL-1-PORT (port3)	0

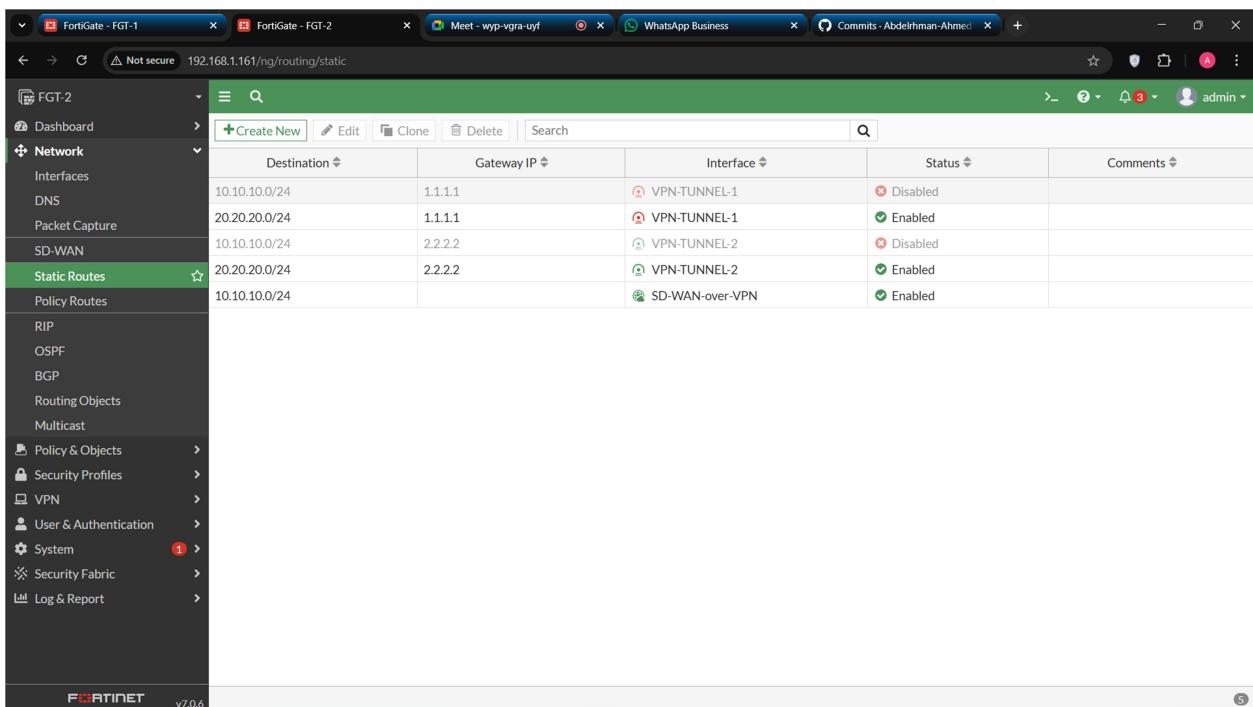
The interface is v7.0.6 and was updated at 05:28:29.

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



The screenshot shows the FortiGate FGT-1 web interface. The left sidebar is collapsed, and the main content area displays the 'Static Routes' table. The table has columns for Destination, Gateway IP, Interface, Status, and Comments. There are six entries:

Destination	Gateway IP	Interface	Status	Comments
30.30.30.0/24	1.1.1.2	VPN-TUNNEL-1	Disabled	
40.40.40.0/24	1.1.1.2	VPN-TUNNEL-1	Enabled	
30.30.30.0/24	2.2.2.3	VPN-TUNNEL-2	Disabled	
40.40.40.0/24	2.2.2.3	VPN-TUNNEL-2	Enabled	
30.30.30.0/24		SD-WAN-over-VPN	Enabled	



The screenshot shows the FortiGate FGT-2 web interface. The left sidebar is collapsed, and the main content area displays the 'Static Routes' table. The table has columns for Destination, Gateway IP, Interface, Status, and Comments. There are five entries:

Destination	Gateway IP	Interface	Status	Comments
10.10.10.0/24	1.1.1.1	VPN-TUNNEL-1	Disabled	
20.20.20.0/24	1.1.1.1	VPN-TUNNEL-1	Enabled	
10.10.10.0/24	2.2.2.2	VPN-TUNNEL-2	Disabled	
20.20.20.0/24	2.2.2.2	VPN-TUNNEL-2	Enabled	
10.10.10.0/24		SD-WAN-over-VPN	Enabled	

## Step 4: Configure Policies

**Edit Policy**

**Name:** NET10-TO-SD-WAN

**Incoming Interface:** NET-10-PORT (port1)

**Outgoing Interface:** SD-WAN-over-VPN

**Source:** VPN-TUNNEL\_local\_subnet\_2

**Destination:** VPN-TUNNEL\_remote\_subnet\_1

**Schedule:** always

**Action:** ✓ ACCEPT

**Inspection Mode:** Flow-based

**Statistics (since last reset):**

ID	11
Last used	N/A
First used	N/A
Active sessions	0
Hit count	0
Total bytes	0 B
Current bandwidth	0 bps

**Additional Information:**

- API Preview
- Edit in CLI
- Documentation
  - Online Help
  - Video Tutorials
  - Consolidated Policy Configuration

**Edit Policy**

**Name:** SD-WAN-TO-NET10

**Incoming Interface:** SD-WAN-over-VPN

**Outgoing Interface:** NET-10-PORT (port1)

**Source:** VPN-TUNNEL\_remote\_subnet\_1

**Destination:** VPN-TUNNEL\_local\_subnet\_2

**Schedule:** always

**Action:** ✓ ACCEPT

**Inspection Mode:** Flow-based

**Statistics (since last reset):**

ID	12
Last used	4 minute(s) ago
First used	4 minute(s) ago
Active sessions	1
Hit count	1
Total bytes	43.51 kB
Current bandwidth	0 bps

**Additional Information:**

Last 7 Days Bytes

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

### 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

**Action**:  ACCEPT  DENY

**Inspection Mode**: Flow-based

**Firewall / Network Options**

**NAT**:

**Protocol Options**: PROT default

**Security Profiles**

- AntiVirus:
- Web Filter:
- DNS Filter:
- Application Control:

**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

**Additional Information**

- [API Preview](#)
- [Edit in CLI](#)
- [Documentation](#)
- [Online Help](#)
- [Video Tutorials](#)
- [Consolidated Policy Configuration](#)

OK Cancel

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

### 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

**Action**:  ACCEPT  DENY

**Inspection Mode**: Flow-based

**Firewall / Network Options**

**NAT**:

**Passive Health Check**:

**Protocol Options**: PROT default

**Security Profiles**

- AntiVirus:
- Web Filter:
- DNS Filter:

**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

**Last 7 Days Bytes**

0 B 10 kB 20 kB 30 kB 40 kB 50 kB 60 kB

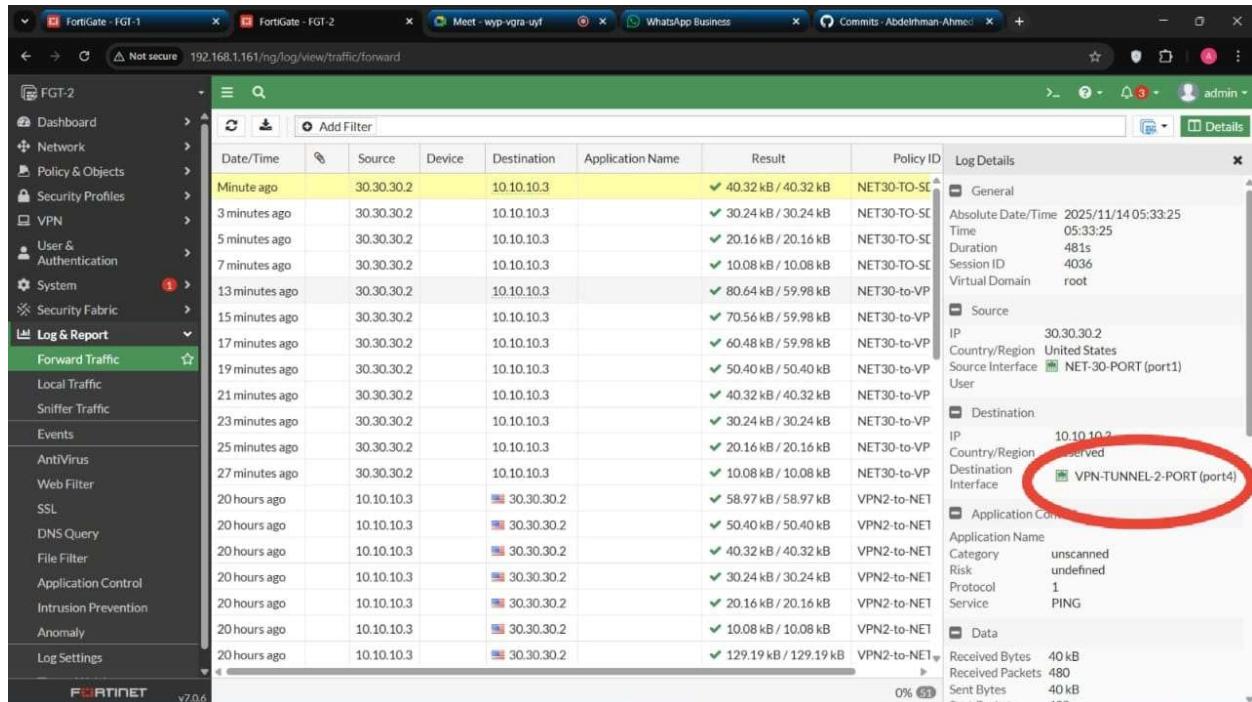
Nov 07 Nov 08 Nov 09 Nov 10 Nov 11 Nov 12 Nov 13 Nov 14

**Additional Information**

OK Cancel

## d) Testing and Performance Evaluation

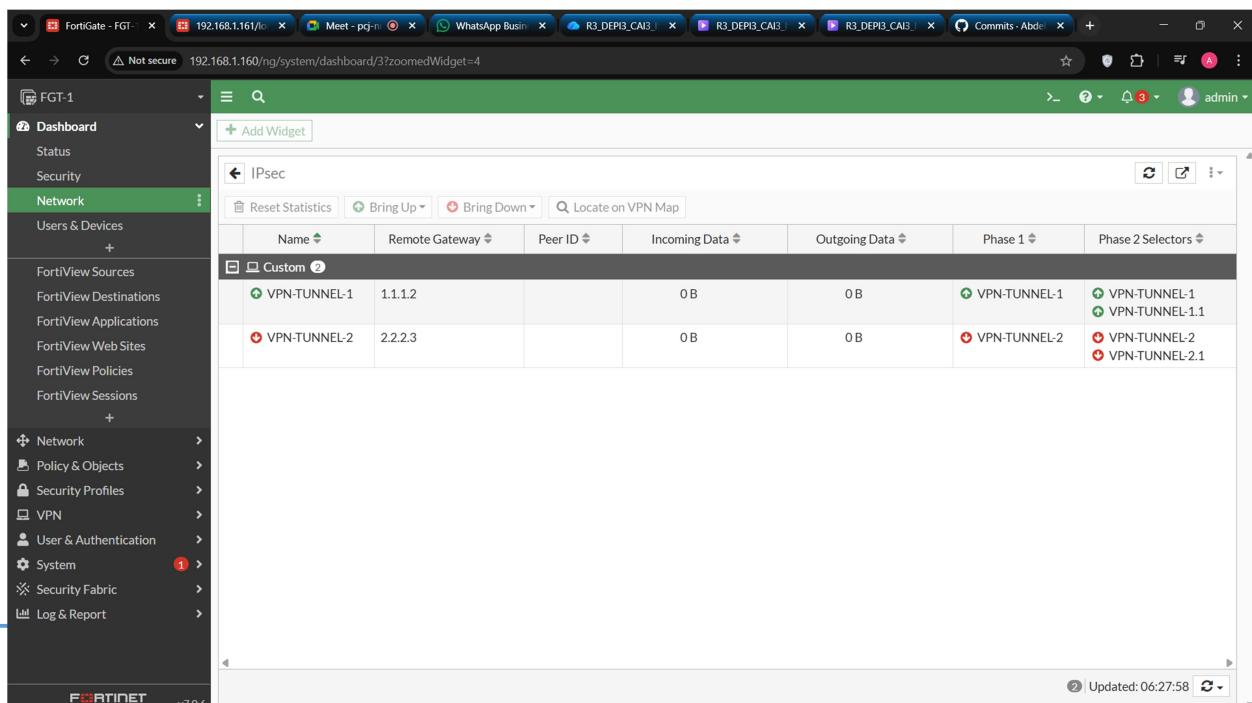
### 1. Tunnel 1 down and Tunnel 2 up



The screenshot shows the FortiGate FGT-2 interface. In the left sidebar, 'Forward Traffic' is selected under 'Log & Report'. The main area displays a table of forward traffic logs. The 'Destination Interface' column for the last entry is circled in red, showing 'VPN-TUNNEL-2-PORT (port4)'. The right panel shows detailed log information for this specific entry.

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID	Log Details
Minute ago	30.30.30.2		10.10.10.3		✓ 40.32 kB / 40.32 kB	NET30-TO-SE	General
3 minutes ago	30.30.30.2		10.10.10.3		✓ 30.24 kB / 30.24 kB	NET30-TO-SE	Source
5 minutes ago	30.30.30.2		10.10.10.3		✓ 20.16 kB / 20.16 kB	NET30-TO-SE	Destination
7 minutes ago	30.30.30.2		10.10.10.3		✓ 10.08 kB / 10.08 kB	NET30-TO-SE	Application
13 minutes ago	30.30.30.2		10.10.10.3		✓ 80.64 kB / 59.98 kB	NET30-to-VP	Data
15 minutes ago	30.30.30.2		10.10.10.3		✓ 70.56 kB / 59.98 kB	NET30-to-VP	
17 minutes ago	30.30.30.2		10.10.10.3		✓ 60.48 kB / 59.98 kB	NET30-to-VP	
19 minutes ago	30.30.30.2		10.10.10.3		✓ 50.40 kB / 50.40 kB	NET30-to-VP	
21 minutes ago	30.30.30.2		10.10.10.3		✓ 40.32 kB / 40.32 kB	NET30-to-VP	
23 minutes ago	30.30.30.2		10.10.10.3		✓ 30.24 kB / 30.24 kB	NET30-to-VP	
25 minutes ago	30.30.30.2		10.10.10.3		✓ 20.16 kB / 20.16 kB	NET30-to-VP	
27 minutes ago	30.30.30.2		10.10.10.3		✓ 10.08 kB / 10.08 kB	NET30-to-VP	
20 hours ago	10.10.10.3		30.30.30.2		✓ 58.97 kB / 58.97 kB	VPN2-to-NET	
20 hours ago	10.10.10.3		30.30.30.2		✓ 50.40 kB / 50.40 kB	VPN2-to-NET	
20 hours ago	10.10.10.3		30.30.30.2		✓ 40.32 kB / 40.32 kB	VPN2-to-NET	
20 hours ago	10.10.10.3		30.30.30.2		✓ 30.24 kB / 30.24 kB	VPN2-to-NET	
20 hours ago	10.10.10.3		30.30.30.2		✓ 20.16 kB / 20.16 kB	VPN2-to-NET	
20 hours ago	10.10.10.3		30.30.30.2		✓ 10.08 kB / 10.08 kB	VPN2-to-NET	
20 hours ago	10.10.10.3		30.30.30.2		✓ 129.19 kB / 129.19 kB	VPN2-to-NET	

### 2. Tunnel 1 up and Tunnel 2 down



The screenshot shows the FortiGate FGT-1 interface. In the left sidebar, 'Network' is selected. The main area displays an 'IPsec' table with two entries: 'VPN-TUNNEL-1' (status: up) and 'VPN-TUNNEL-2' (status: down). The right panel shows a summary of tunnel status with green and red indicators for each tunnel.

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
VPN-TUNNEL-1	1.1.1.2		0 B	0 B	VPN-TUNNEL-1	VPN-TUNNEL-1 VPN-TUNNEL-1.1
VPN-TUNNEL-2	2.2.2.3		0 B	0 B	VPN-TUNNEL-2	VPN-TUNNEL-2 VPN-TUNNEL-2.1

FortGate - FGT- 192.168.1.160/... Meet - pq-n WhatsApp Business R3\_DEP13\_CAI3\_ R3\_DEP13\_CAI3\_ Commits - Abdel +

Not secure 192.168.1.160/network/virtualwan?tabType=health-check

F GT-1 admin

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); 0	VPN-TUNNEL-1-PORT (port3); 0.33ms VPN-TUNNEL-2-PORT (port4); 0	VPN-TUNNEL-1-PORT (port3); 0.11ms VPN-TUNNEL-2-PORT (port4); 0	5

FORTINET v7.0.6 7

FortGate - FGT- 192.168.1.160/... Meet - pq-n WhatsApp Business R3\_DEP13\_CAI3\_ R3\_DEP13\_CAI3\_ Commits - Abdel +

Not secure 192.168.1.160/network/virtualwan?tabType=service

F GT-1 admin

SD-WAN Zones SD-WAN Rules Performance SLAs

Create New Edit Clone Delete Search

ID	Name	Source	Destination	Criteria	Members	Hit Count
1	SD-WAN-RULE-1	all	all	Latency	VPN-TUNNEL-2-PORT (port4) VPN-TUNNEL-1-PORT (port3)	1
	Implicit 1	sd-wan	all	Source IP	any	

FORTINET v7.0.6 Updated: 06:27:14

Not secure 192.168.1.160/ng/log/view/traffic/forward

admin

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID	Log Details
Minute ago	30.30.30.2		10.10.10.3		✓ 30.24 kB / 30.24 kB	SD-WAN-TO-	<b>General</b> Absolute Date/Time: 2025/11/14 06:25:03 Time: 06:25:03 Duration: 361s Session ID: 80 Virtual Domain: root
3 minutes ago	30.30.30.2		10.10.10.3		✓ 20.16 kB / 20.16 kB	SD-WAN-TO-	<b>Source</b> IP: 30.30.30.2 Country/Region: United States Source Interface: VPN-TUNNEL-1-PORT (port3) <b>Destination</b> IP: 10.10.10.3 Country/Region: Reserved Destination Interface: NET-10-PORT (port1)
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-	

FORTINET v7.0.6

0% 74

## 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)*