

Exploring VPN Security  
Techniques, Protocols, and  
Attacks

# Implementing VPN Solutions Project

**Secure Connectivity for  
Modern Networks**



# VPN

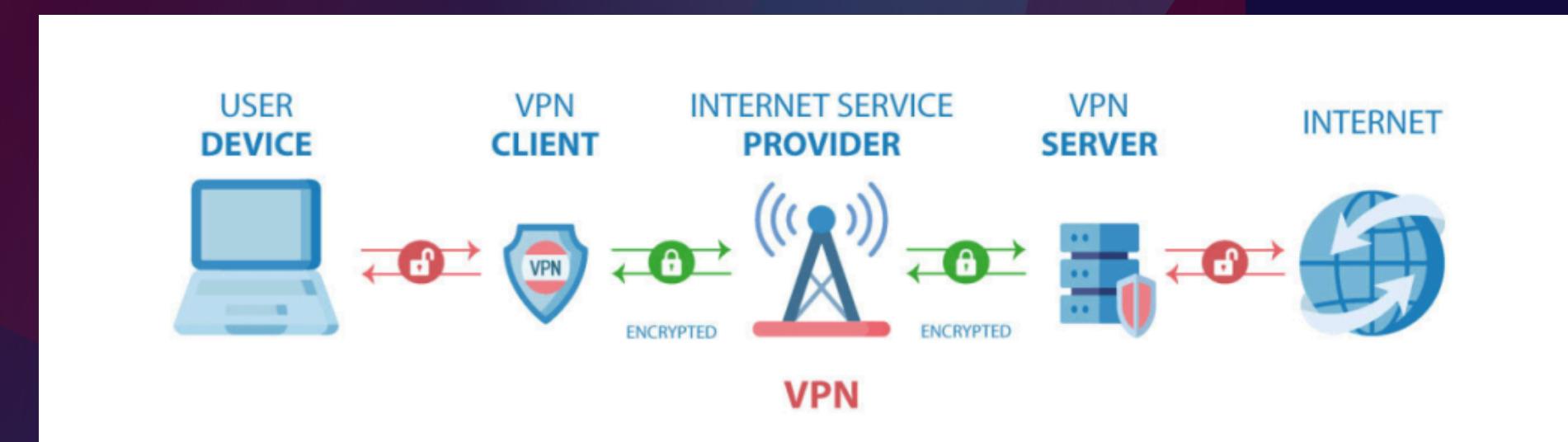
A Virtual Private Network (VPN) is a secure connection between two or more devices over the internet, creating a private network

- **Purpose:**

- Privacy: Hides your IP address.
- Security: Encrypts data to prevent interception.
- Remote Access: Allows secure access to private networks.

- **Key Components:**

- Encryption: Secures data.
- Tunneling: Encapsulates data packets.
- Authentication: Verifies user identity.



# VPN Types and Protocols

## **Remote Access VPN (Client-to-Site VPN)**

Connects individual users securely to a company's internal network using VPN client software

## **Site-to-Site VPN**

Connects two or more networks (e.g., branch offices) securely over the internet. Usually implemented between routers or firewalls

## **SSL VPN (Secure Sockets Layer VPN)**

Uses HTTPS (port 443) to provide secure remote access via web browser or client. It encrypts traffic using SSL/TLS protocols.

## **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

## **IMPLS VPN (Multiprotocol Label Switching VPN)**

Uses service provider networks to create private paths for enterprise traffic, ensuring reliability and QoS.

## **L2TP/IPsec VPN**

Combines Layer 2 Tunneling Protocol with IPsec encryption. Often used for secure remote access

# 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.

# SSL VPN

- **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).

# SSL VPN

- **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

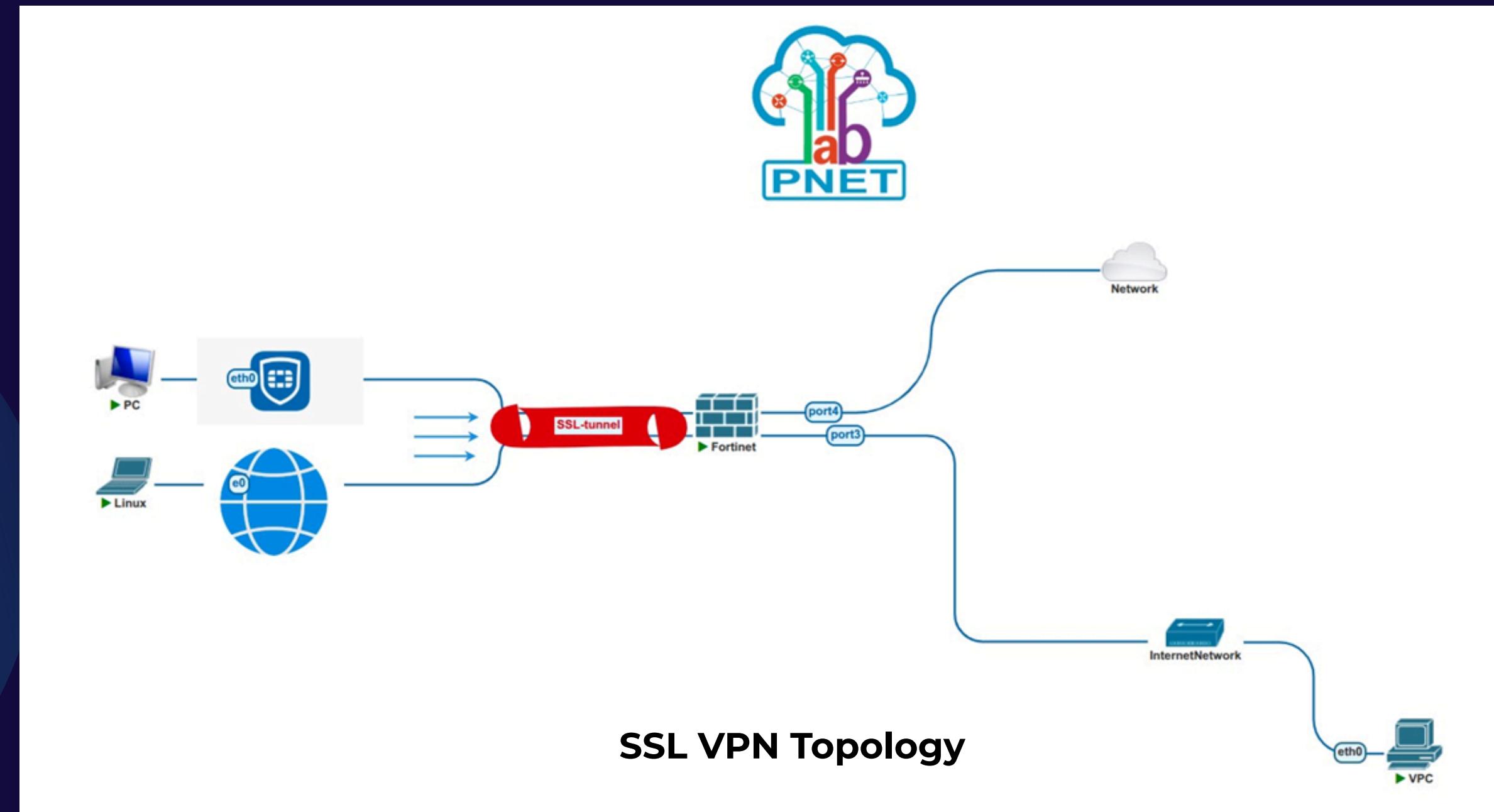
- **Web Mode**

- 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

- **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.

# SSL VPN Configuration on FortiGate



# SSL VPN Configuration on FortiGate

The screenshot shows the SSL-VPN Settings configuration page on a FortiGate device (version v7.0.6). The left sidebar navigation includes: 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 (with a red notification dot), Security Fabric, and Log & Report.

**SSL-VPN Settings**

**Connection Settings**

- Enable SSL-VPN:
- Listen on Interface(s): port5
- Listen on Port: 10443
- Server Certificate: Fortinet\_Factory

A yellow warning box states: "You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). Let's Encrypt can be used to easily generate a trusted certificate if you do not have one." It includes a "Create Certificate" button.

**Redirect HTTP to SSL-VPN**

- Restrict Access: Allow access from any host
- Idle Logout: Inactive For: 3000 Seconds
- Require Client Certificate:

**Tunnel Mode Client Settings**

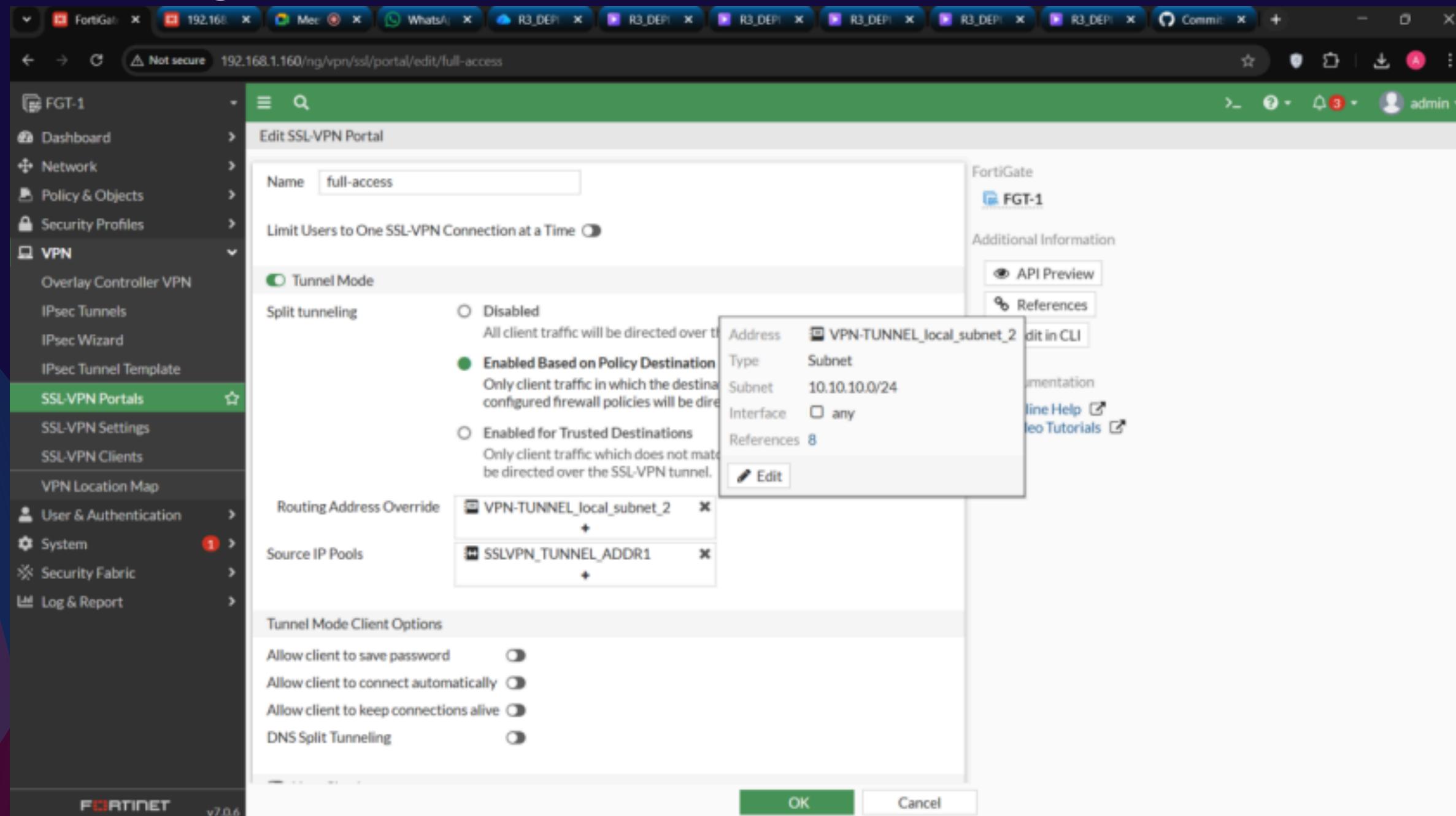
- Address Range: Automatically assign addresses
- Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210

**Additional Information**

- API Preview
- Edit in CLI
- SSL VPN Setup Guides**
  - Web Mode
  - Web Mode for Remote User
  - Tunnel Mode
  - Full Tunnel for Remote User
  - Split Tunnel for Remote User
  - Tunnel Mode Host Check
  - Multi-realm
  - Multi-Realm
- Authentication**
  - Certificate Authentication
  - LDAP-Integrated Certificate Authentication
  - FortiToken Mobile Push Authentication
  - RADIUS on FortiAuthenticator
  - RADIUS and FortiToken Mobile Push on FortiAuthenticator
  - Local User Password Policy
  - RADIUS Password Renew on FortiAuthenticator
  - LDAP User Password Renew
- VPN Setup on FortiClient
- Configuring an SSL VPN Connection
- Troubleshooting**
- Troubleshooting
- Documentation

SSL-VPN Setting Configuration

# SSL VPN Configuration on FortiGate



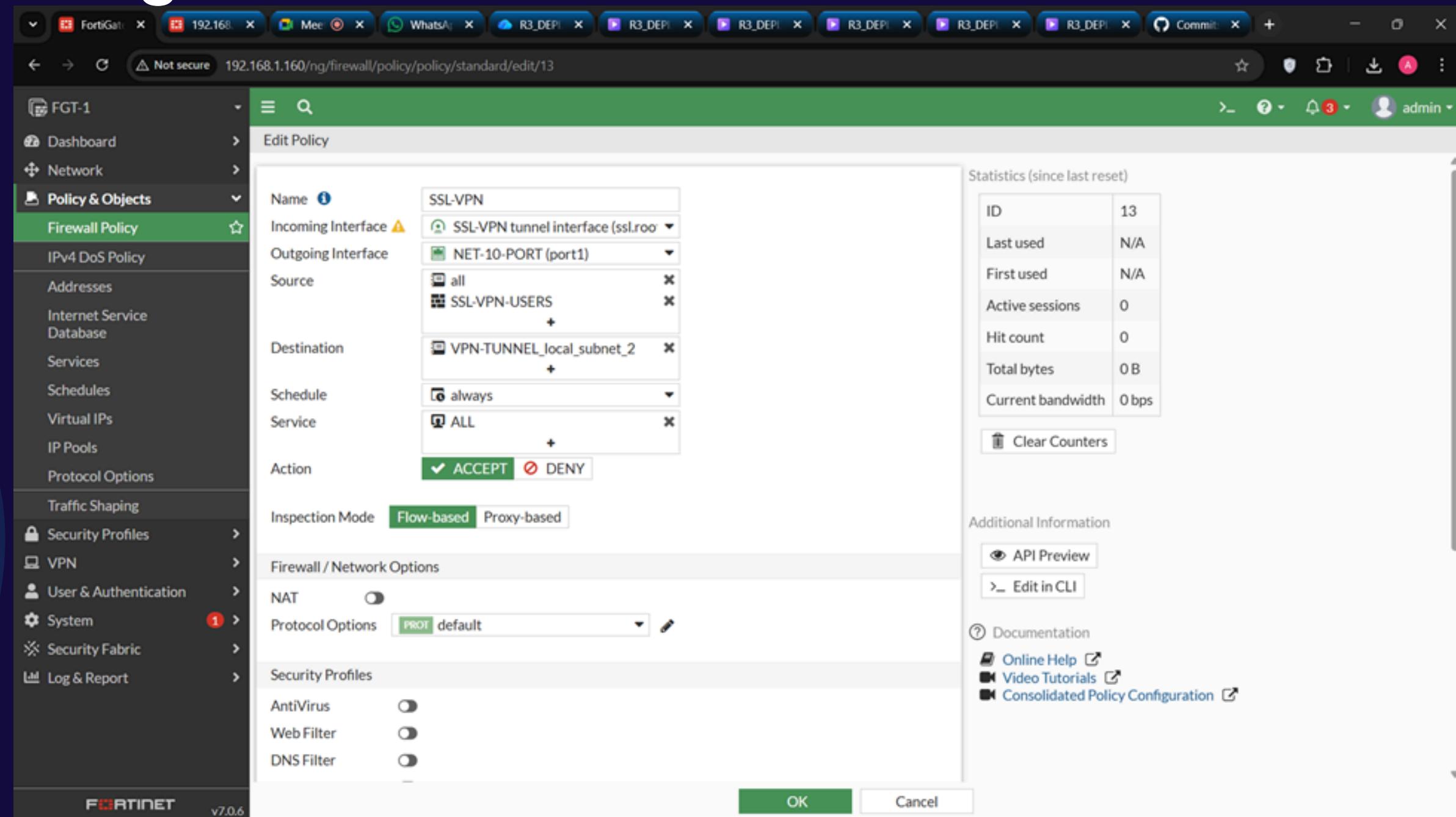
The screenshot shows the FortiGate management interface for configuring an SSL-VPN portal. The left sidebar navigation includes: Dashboard, Network, Policy & Objects, Security Profiles, VPN (Overlay Controller VPN, IPsec Tunnels, IPsec Wizard, IPsec Tunnel Template), SSL-VPN Portals (selected), SSL-VPN Settings, SSL-VPN Clients, VPN Location Map, User & Authentication, System (with a red notification dot), Security Fabric, and Log & Report.

The main content area displays the 'Edit SSL-VPN Portal' dialog for a portal named 'full-access'. The 'Tunnel Mode' is set to 'Enabled Based on Policy Destination'. In the 'Routing Address Override' section, there is a configuration for 'VPN-TUNNEL\_local\_subnet\_2' which is a subnet of '10.10.10.0/24' on 'any' interface. The 'Source IP Pools' section lists 'SSLVPN\_TUNNEL\_ADDR1'.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

SSL-VPN Portal Configuration

# SSL VPN Configuration on FortiGate



The screenshot shows the 'Edit Policy' dialog box for an SSL-VPN access policy on a FortiGate device. The policy is named 'SSL-VPN' and has the following configuration:

- Name:** SSL-VPN
- Incoming Interface:** SSL-VPN tunnel interface (ssl.root)
- Outgoing Interface:** NET-10-PORT (port1)
- Source:** all, SSL-VPN-USERS
- Destination:** VPN-TUNNEL\_local\_subnet\_2
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (selected)

Below the main configuration, there are sections for Inspection Mode (Flow-based selected), Firewall / Network Options, NAT (disabled), Protocol Options (PROT default), Security Profiles, AntiVirus, Web Filter, and DNS Filter.

On the right side of the dialog, there are 'Statistics (since last reset)' and 'Additional Information' sections, along with links for API Preview, Edit in CLI, and Documentation.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

SSL-VPN-Access Policy Configuration

# IPsec VPN

- **Overview**

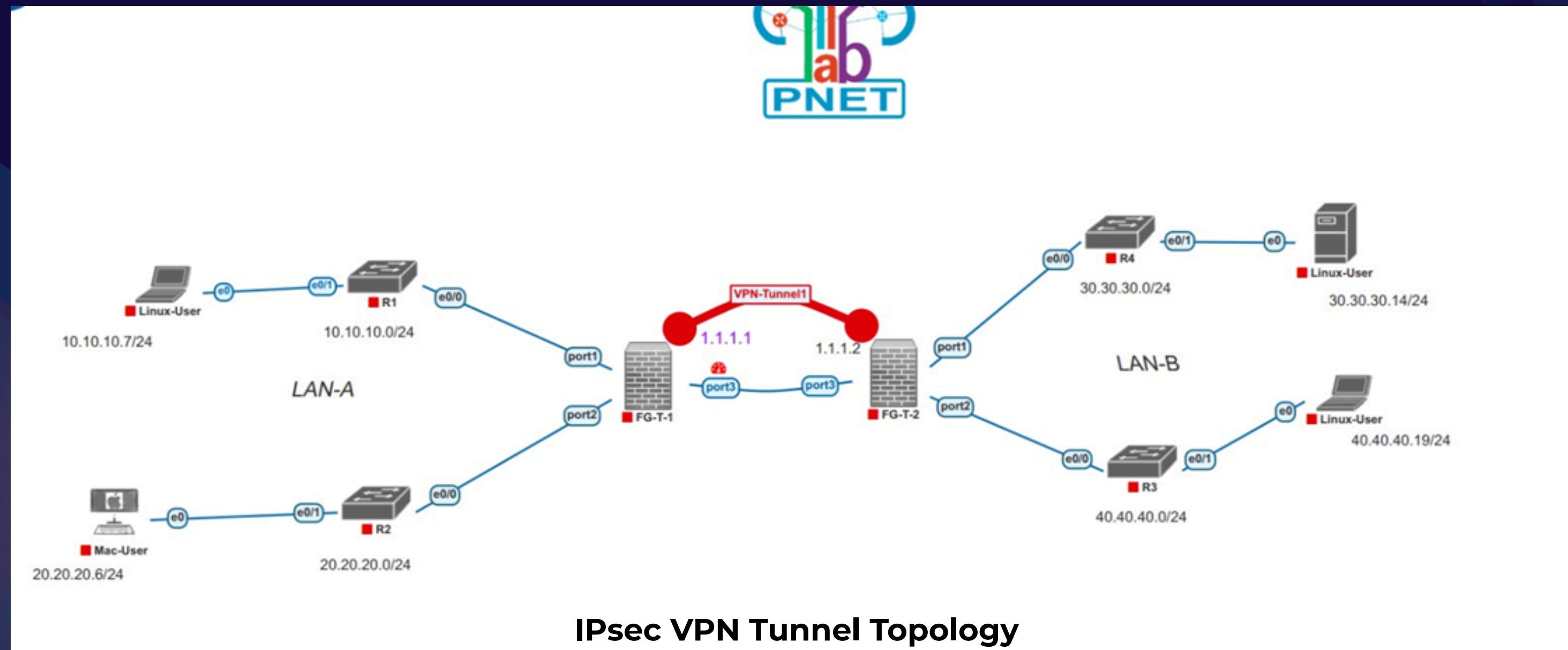
- The IPsec (Internet Protocol Security) VPN is a widely used protocol suite that secures network traffic by encrypting and authenticating IP packets at the network layer (Layer 3). It provides site-to-site and remote access solutions that ensure data confidentiality, integrity, and authenticity between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

# IPsec VPN

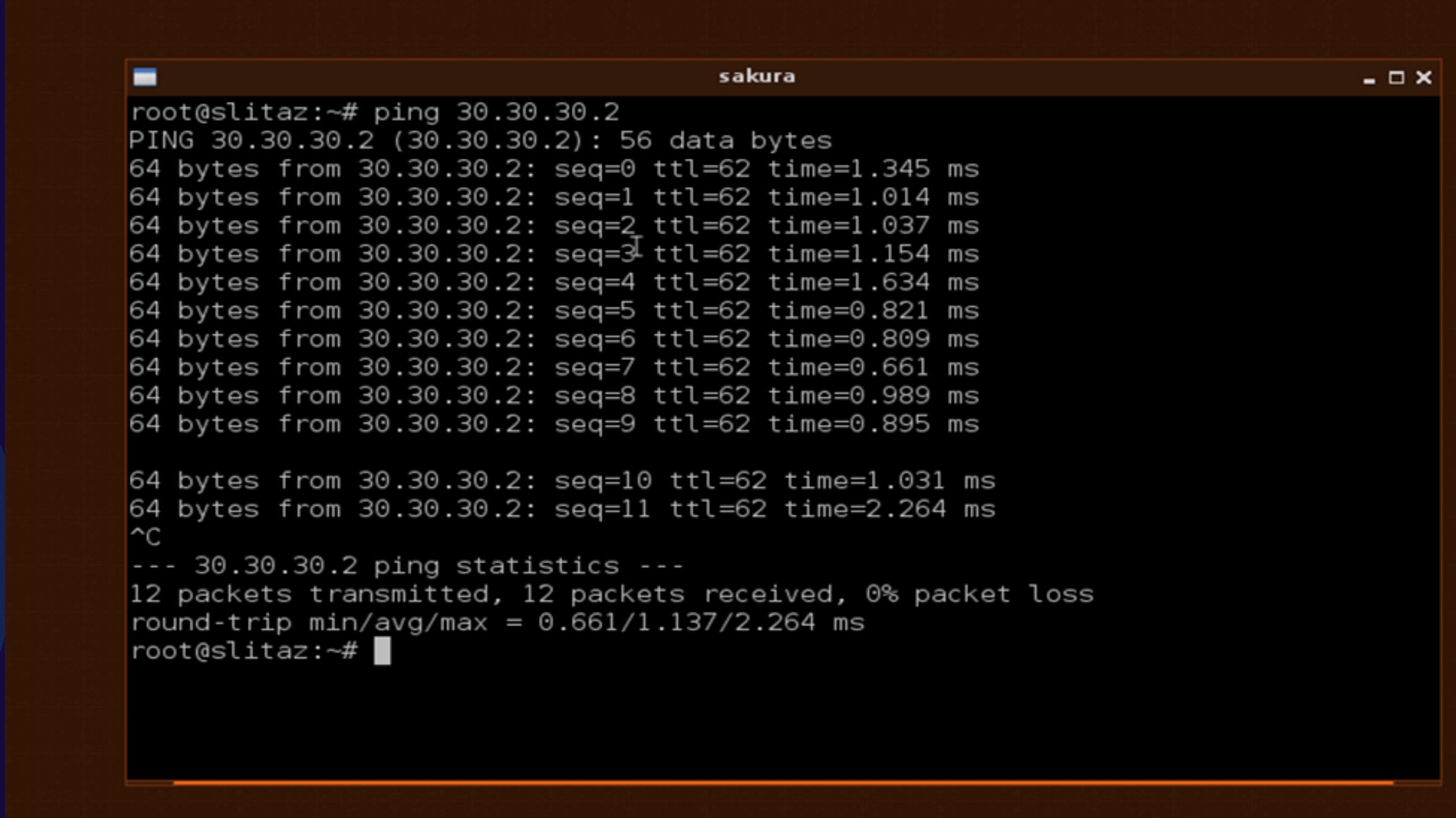
- **How It Works**

- An IPsec VPN establishes a secure tunnel between two FortiGate devices through a two-phase process:
  1. Phase 1 (IKE Negotiation):
    - Establishes a secure communication channel.
    - Authenticates the two VPN peers.
    - Negotiates encryption and hashing algorithms (e.g., AES, SHA).
  2. Phase 2 (Data Encryption):
    - Defines traffic selectors (networks that will communicate).
    - Encrypts user data packets through the established tunnel.

# IPsec Configuration Steps on FortiGate



# Testing and Verification

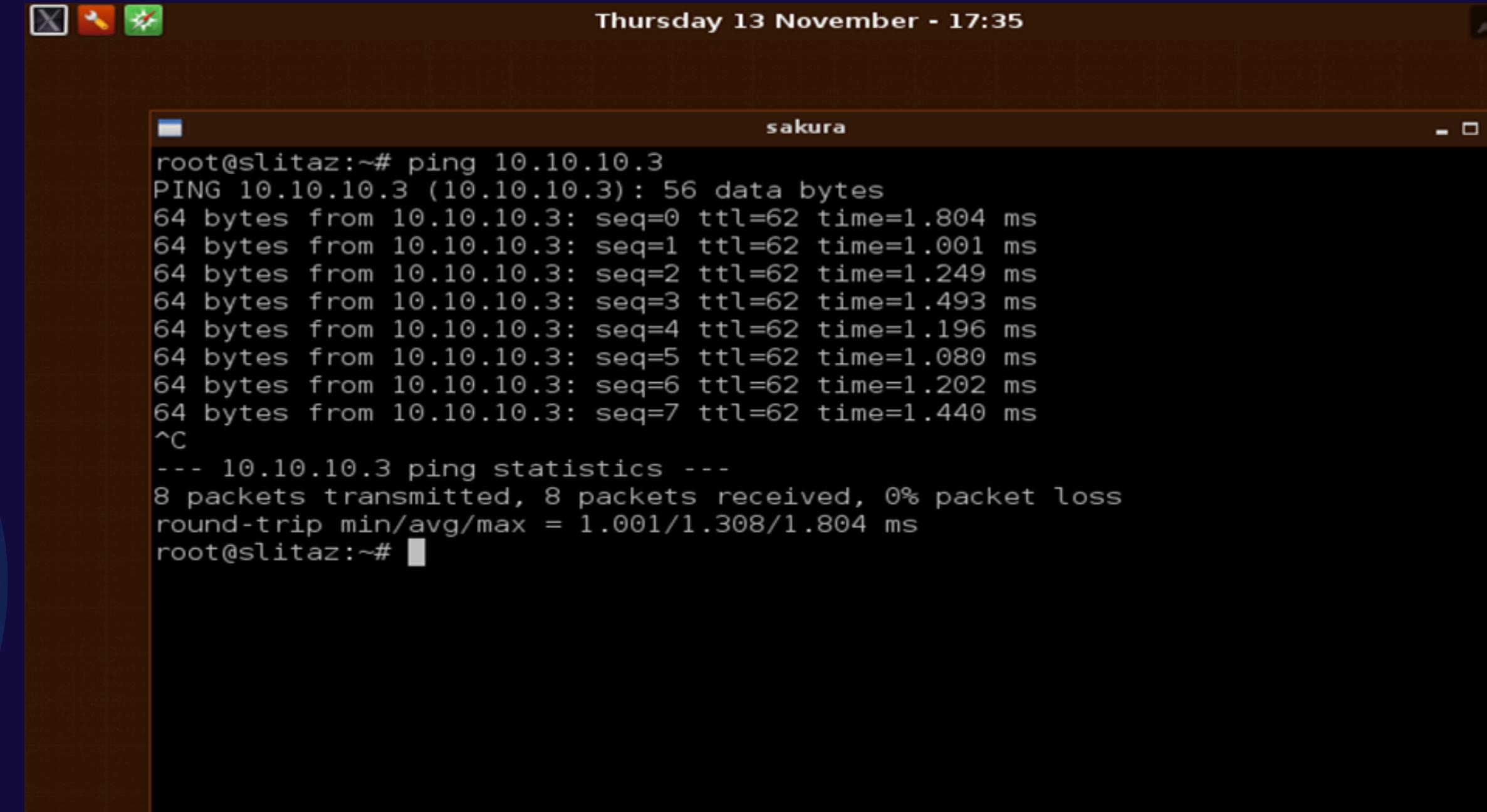


```
root@slitaz:~# ping 30.30.30.2
PING 30.30.30.2 (30.30.30.2): 56 data bytes
64 bytes from 30.30.30.2: seq=0 ttl=62 time=1.345 ms
64 bytes from 30.30.30.2: seq=1 ttl=62 time=1.014 ms
64 bytes from 30.30.30.2: seq=2 ttl=62 time=1.037 ms
64 bytes from 30.30.30.2: seq=3 ttl=62 time=1.154 ms
64 bytes from 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 Test: ping from PC-1 to PC-3

# Testing and Verification

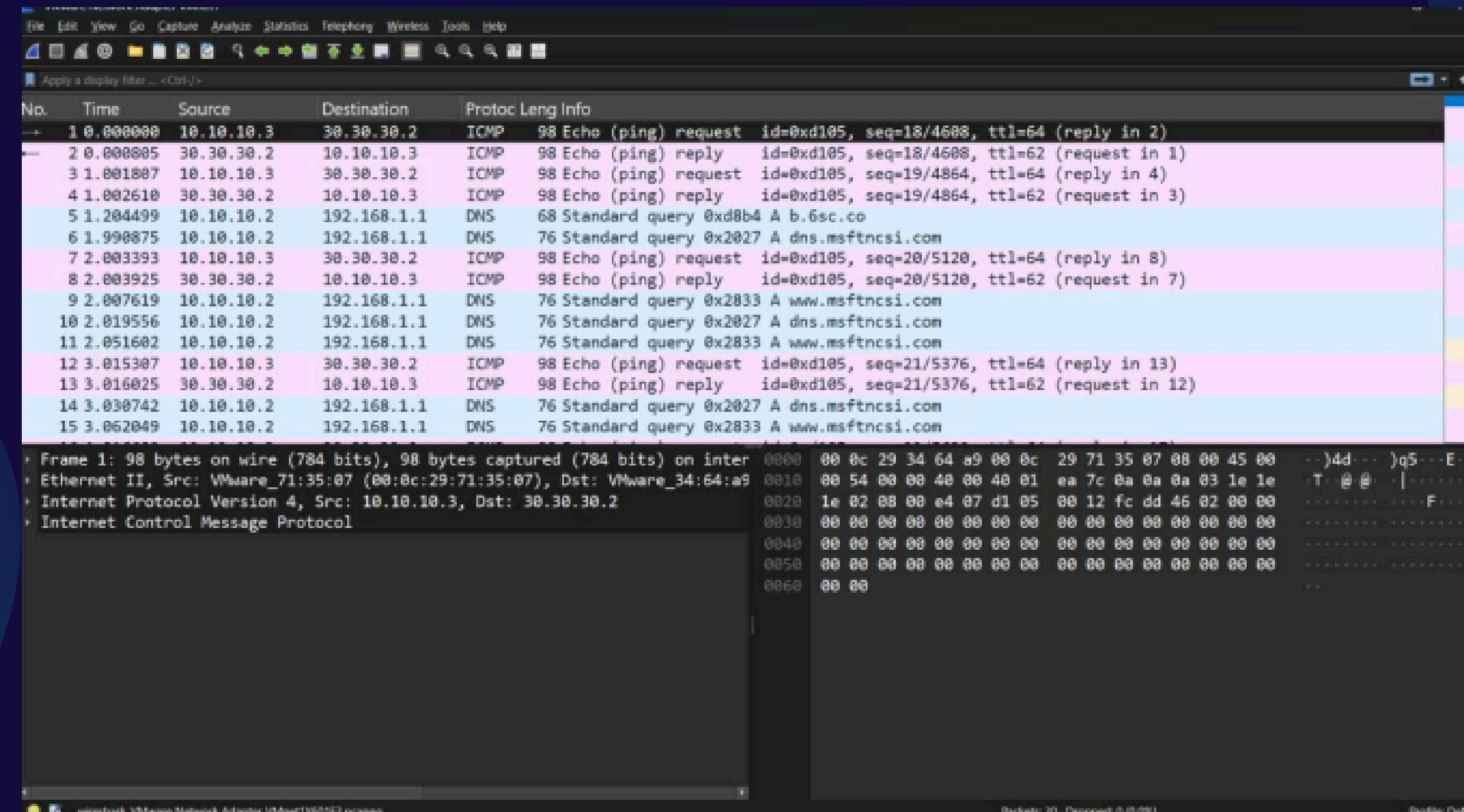


The terminal window shows the following output:

```
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:~#
```

ping from PC-3 to PC-1

# Testing and Verification



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



# Logs and Events

Screenshot of the FortiGate Management Interface showing Forward Traffic logs.

The interface includes a top navigation bar with tabs for Hassan Maher, FortiGate - FGT-2, Meet - nxg-raxm-kyf, WhatsApp Business, and FortiGate - FGT-1. The current tab is "Forward Traffic".

The left sidebar shows the navigation menu under "FGT-2", with "Log & Report" selected and "Forward Traffic" highlighted.

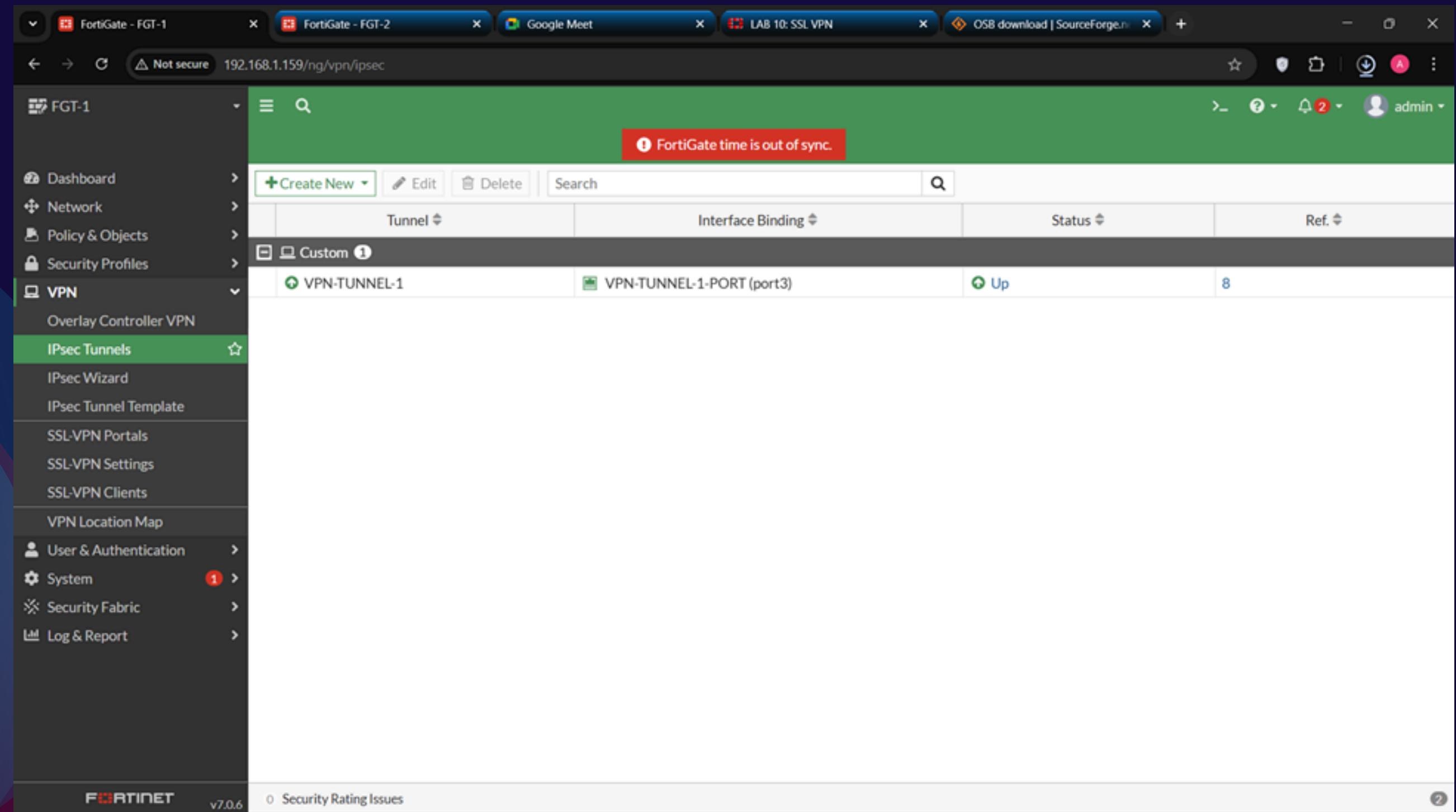
The main content area displays a table of traffic logs:

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
5 minutes ago	30.30.30.2		10.10.10.3		✓ 252 B / 252 B	NET30-to-VPN (3)
5 minutes ago	10.10.10.3		30.30.30.2		✓ 420 B / 420 B	NET10-to-VPN (4)
2 hours ago	30.30.30.2		10.10.10.3		✓ 336 B / 336 B	NET30-to-VPN (3)
2 hours ago	10.10.10.3		30.30.30.2		✓ 252 B / 252 B	NET10-to-VPN (4)
2 hours ago	10.10.10.3		30.30.30.2		✓ 3.28 kB / 3.28 kB	NET10-to-VPN (4)

A detailed log entry for the first row is expanded on the right side:

- 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: (empty)
- Destination**:
  - IP: 10.10.10.3
  - Country/Region: Reserved
  - Destination Interface: VPN-TUNNEL-1
- Application Control**:
  - Application Name: unscanned
  - 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 management interface with the title "Tunnel Status". A red banner at the top right of the main content area displays the message "FortiGate time is out of sync." Below the banner is a table with the following data:

Tunnel	Interface Binding	Status	Ref.
<b>Custom 1</b>			
VPN-TUNNEL-1	VPN-TUNNEL-1-PORT (port3)	Up	8

The left sidebar navigation menu includes the following items under the "VPN" section:

- Overlay Controller VPN
- IPsec Tunnels** (highlighted)
- IPsec Wizard
- IPsec Tunnel Template
- SSL-VPN Portals
- SSL-VPN Settings
- SSL-VPN Clients
- VPN Location Map

The bottom of the interface shows the Fortinet logo and the version v7.0.6.



# Tunnel Status

The screenshot shows the FortiGate management interface with the title "Tunnel Status". The left sidebar menu is open, showing the following navigation paths:

- Dashboard
- Network
- Policy & Objects
- Security Profiles
- VPN
  - Overlay Controller VPN
  - IPsec Tunnels** (highlighted)
  - IPsec Wizard
  - IPsec Tunnel Template
- SSL-VPN Portals
- SSL-VPN Settings
- SSL-VPN Clients
- VPN Location Map
- User & Authentication
- System** (highlighted)
- Security Fabric
- Log & Report

A red banner at the top right indicates: "FortiGate time is out of sync." The main content area displays a table titled "Custom 1" with the following data:

Tunnel	Interface Binding	Status	Ref.
VPN-TUNNEL-1	VPN-TUNNEL-1-PORT (port3)	Up	8

At the bottom of the interface, it says "FORTINET v7.0.6" and "Security Rating Issues".

# FortiGate VPN with SD-WAN Integration

- **Overview**

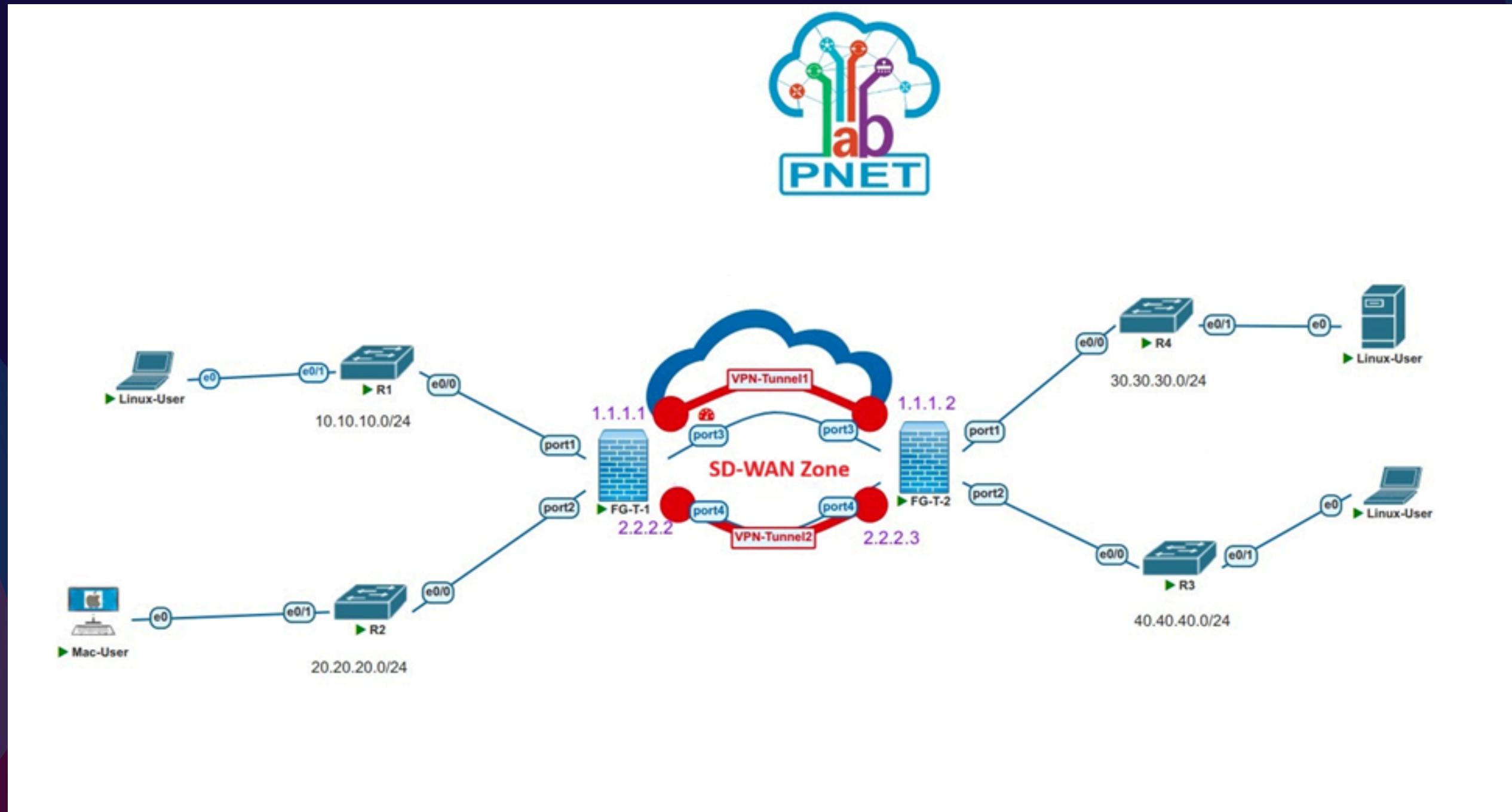
SD-WAN (Software-Defined Wide Area Network) is an advanced networking technology that enhances WAN performance by intelligently directing traffic across multiple WAN connections (such as MPLS, broadband, or LTE). Integrating SD-WAN with VPN allows FortiGate devices to dynamically select the best path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

# FortiGate VPN with SD-WAN Integration

- **How SD-WAN Works**

SD-WAN operates by creating a virtual overlay network on top of existing physical connections like broadband, MPLS, or LTE. Edge devices installed at branch offices, data centers, or cloud locations manage and route traffic according to centrally defined policies.

# SD-WAN Configuration on FortiGate



VPN with SD-WAN Integration Topology

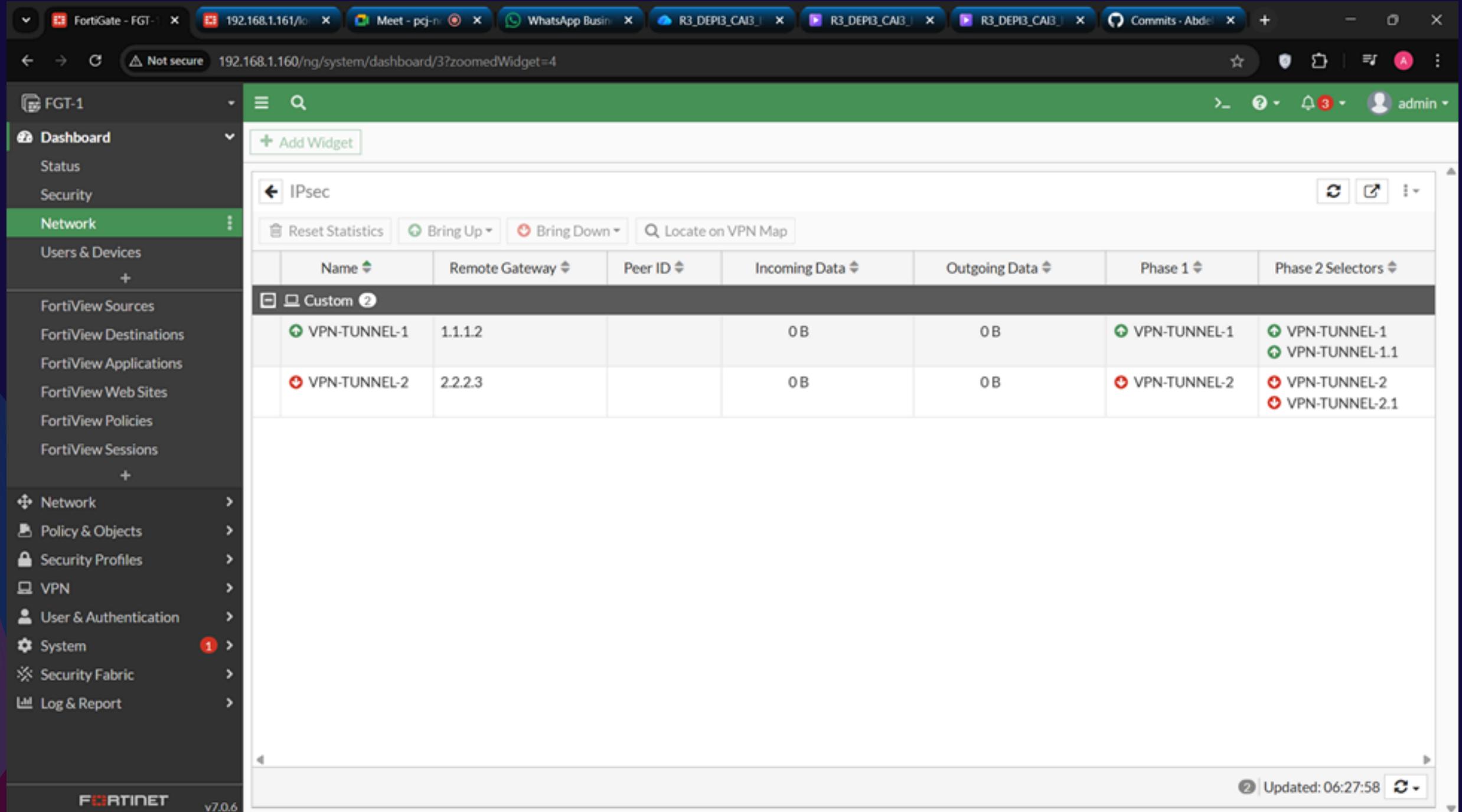
# Testing and Performance Evaluation

The screenshot shows the FortiGate management interface with the URL `192.168.1.161/ng/log/view/traffic/forward`. The left sidebar is the navigation menu for FGT-2, with 'Forward Traffic' selected. The main area displays a table of traffic logs. One specific log entry is highlighted with a red circle around the 'Destination Interface' field in the 'Log Details' pane. The highlighted log entry shows:

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-SC	General Absolute Date/Time: 2025/11/14 05:33:25 Time: 05:33:25 Duration: 481s Session ID: 4036 Virtual Domain: root
3 minutes ago	30.30.30.2		10.10.10.3		✓ 30.24 kB / 30.24 kB	NET30-TO-SC	Source IP: 30.30.30.2 Country/Region: United States Source Interface: NET-30-PORT (port1)
5 minutes ago	30.30.30.2		10.10.10.3		✓ 20.16 kB / 20.16 kB	NET30-TO-SC	Destination IP: 10.10.10.3 Country/Region: Unspecified Destination Interface: VPN-TUNNEL-2-PORT (port4)
7 minutes ago	30.30.30.2		10.10.10.3		✓ 10.08 kB / 10.08 kB	NET30-TO-SC	Application Control Application Name: PING Category: unscanned Risk: undefined Protocol: 1 Service: PING
13 minutes ago	30.30.30.2		10.10.10.3		✓ 80.64 kB / 59.98 kB	NET30-to-VP	Data Received Bytes: 40 kB Received Packets: 480 Sent Bytes: 40 kB
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	

1. Tunnel 1 down and Tunnel 2 up

# Testing and Performance Evaluation



The screenshot shows the FortiGate Management Interface (v7.0.6) with the IPsec dashboard. The left sidebar shows the navigation menu with Network selected. The main panel displays the IPsec configuration for two tunnels:

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

At the bottom right, it says "Updated: 06:27:58".

2. Tunnel 1 up and Tunnel 2 down

# Testing and Performance Evaluation

Screenshot of the FortiGate Management Interface showing the SD-WAN Performance SLAs page.

The URL in the browser is `192.168.1.160/network/virtualwan?tabType=health-check`.

The left sidebar shows the navigation menu with **SD-WAN** selected under Network.

The main content area displays the **Performance SLAs** tab, which includes tabs for **Packet Loss**, **Latency** (selected), and **Jitter**. A message "No data" is displayed below the table.

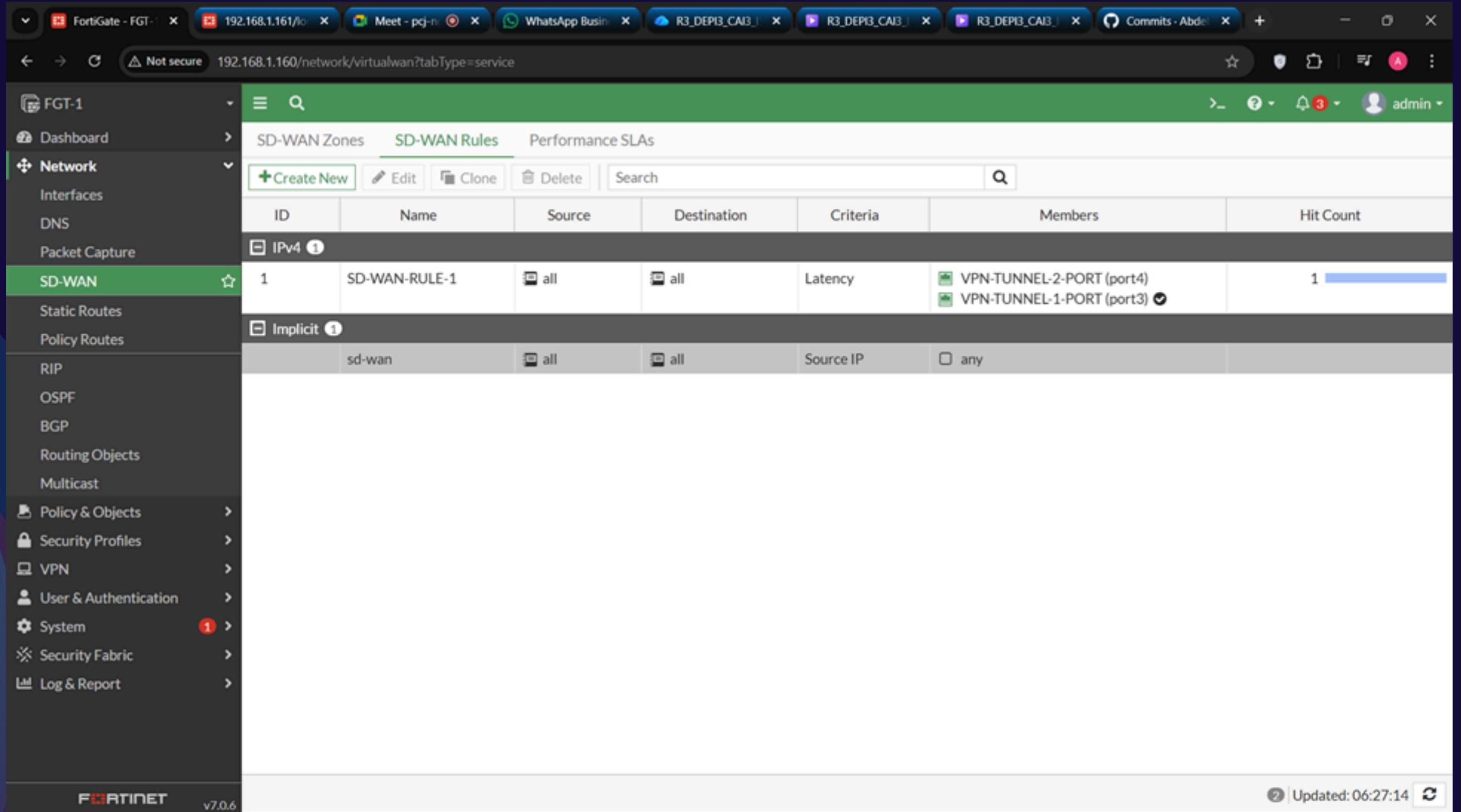
**Latency** table:

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): 0.00%	VPN-TUNNEL-1-PORT (port3): 0.33ms VPN-TUNNEL-2-PORT (port4): 0.11ms	VPN-TUNNEL-1-PORT (port3): 0.11ms VPN-TUNNEL-2-PORT (port4): 0.00%	5

Fortinet v7.0.6

2. Tunnel 1 up and Tunnel 2 down

# Testing and Performance Evaluation



The screenshot shows the FortiGate Management Interface (v7.0.6) with the URL [192.168.1.160/network/virtualwan?tabType=service](http://192.168.1.160/network/virtualwan?tabType=service). The left sidebar is collapsed, and the main content area displays the SD-WAN Rules configuration. The 'SD-WAN Rules' tab is selected, showing a table with one rule entry:

ID	Name	Source	Destination	Criteria	Members	Hit Count
1	SD-WAN-RULE-1	<input type="checkbox"/> all	<input type="checkbox"/> all	Latency	<input checked="" type="checkbox"/> VPN-TUNNEL-2-PORT (port4) <input checked="" type="checkbox"/> VPN-TUNNEL-1-PORT (port3)	1

The 'SD-WAN' option in the sidebar is highlighted with a green star.

2. Tunnel 1 up and Tunnel 2 down

# Testing and Performance Evaluation

Screenshot of the Fortinet FortiLog viewer showing Forward Traffic logs. A red circle highlights the Source Interface field in the log details panel.

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: Unspecified Source Interface: <b>VPN-TUNNEL-1-PORT (port3)</b> User:
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-	

2. Tunnel 1 up and Tunnel 2 down

# 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**

# Thank you

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