رواد مصر الرقمية

Exploring VPN Security Techniques, Protocols, and Attacks

Implementing VPN Solutions Project

Secure Connectivity for Modern Networks

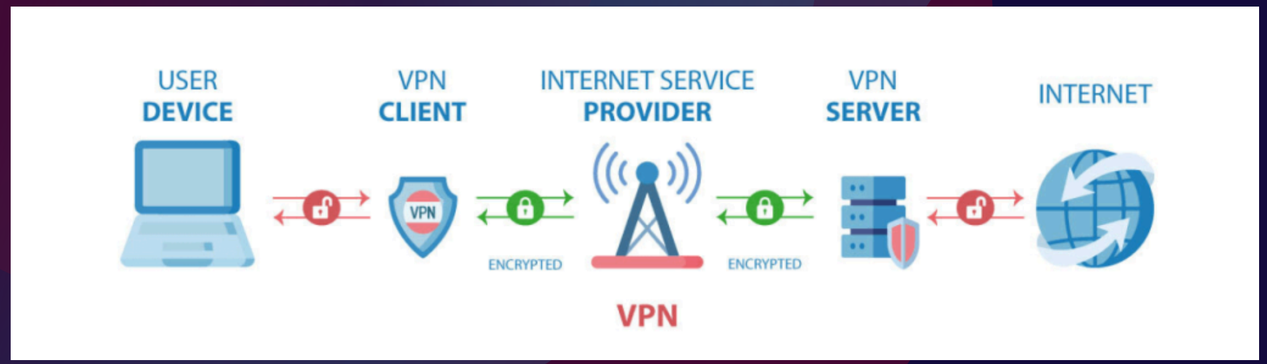
رواد مصر الرقمية

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 Protocoles

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).

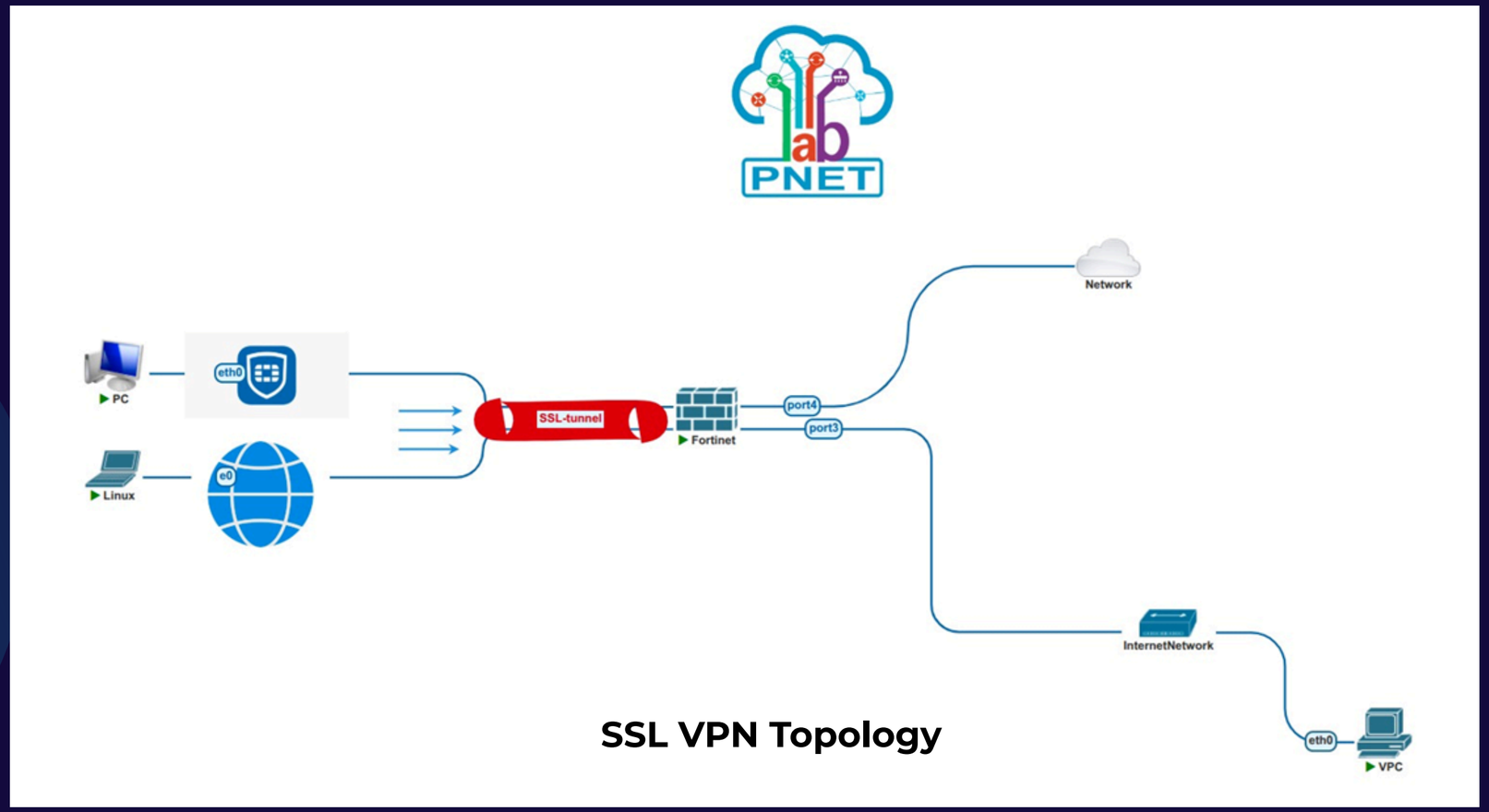
SSL VPN

- **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

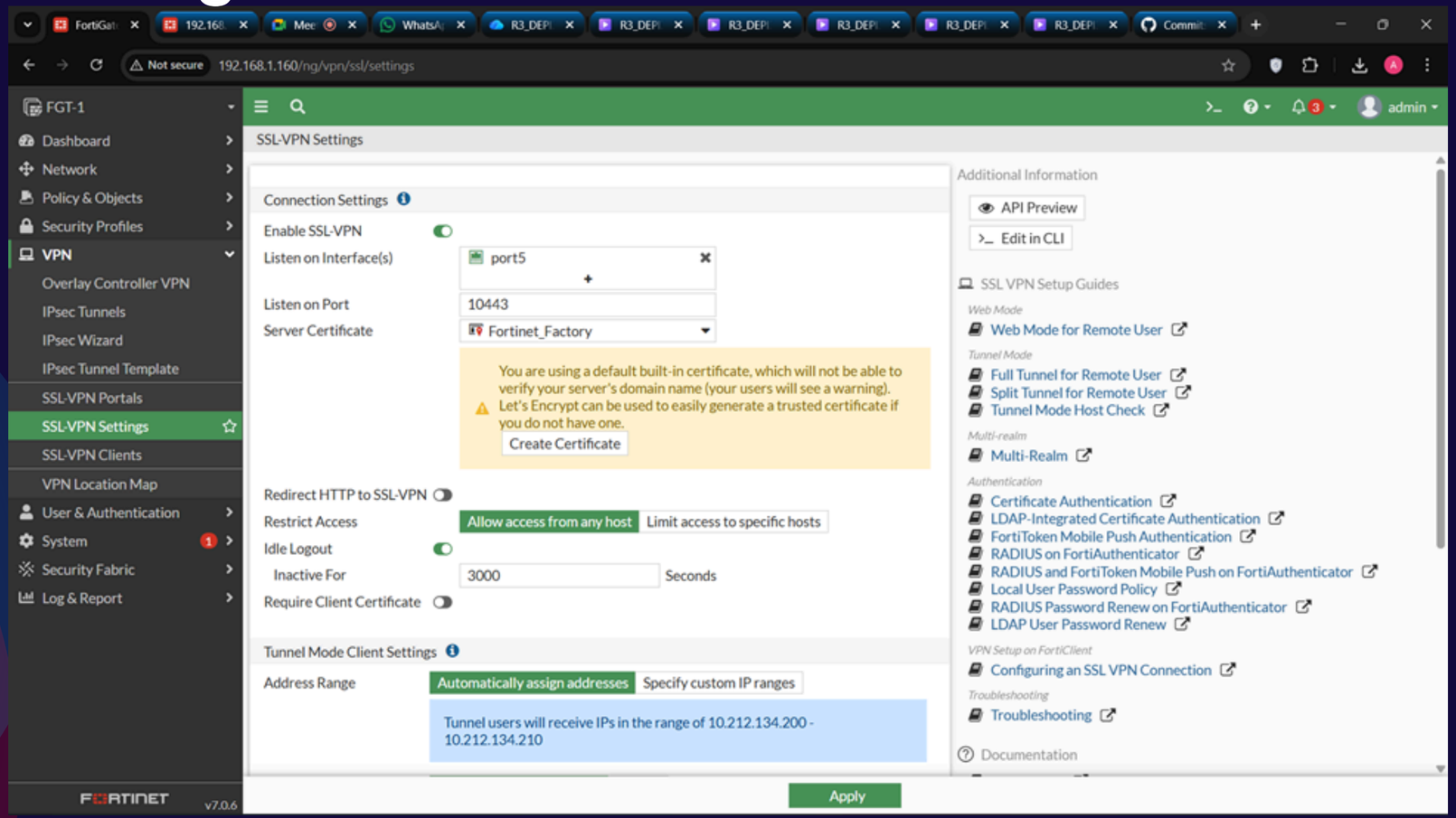
- **Web Mode**
  - Access through a web portal.
  - Users log in via a browser (e.g., https://<public-ip>:443) and can access specific applications like email, file servers, or web-based tools.
  - Suitable for simple, controlled access without installing a VPN client
- **Tunnel Mode**
  - Requires a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



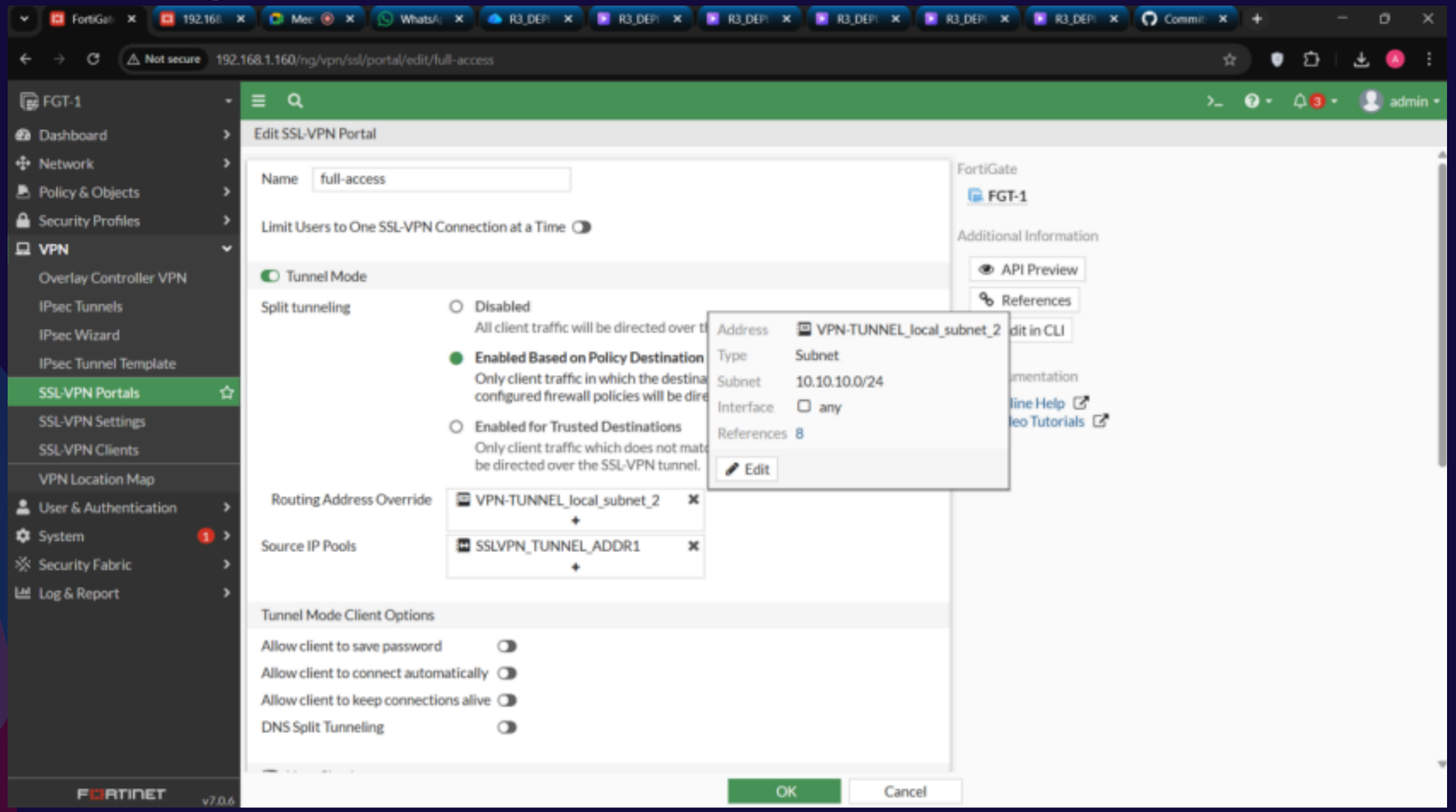
SSL VPN Topology

SSL VPN Configuration on FortiGate



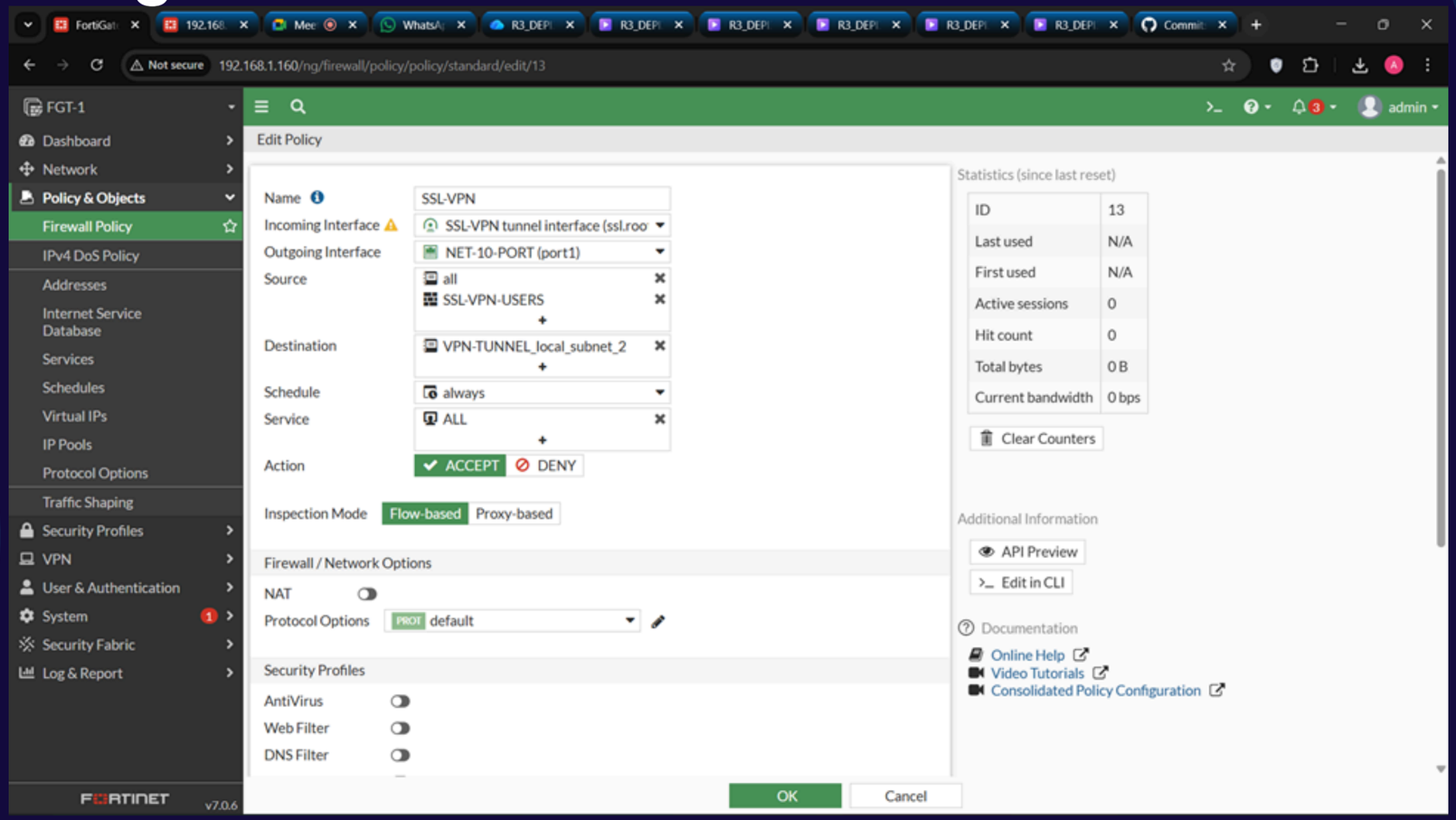
SSL-VPN Setting Configuration

SSL VPN Configuration on FortiGate



SSL-VPN Portal Configuration

SSL VPN Configuration on FortiGate



SSL-VPN-Access Policy Configuration

IPsec VPN

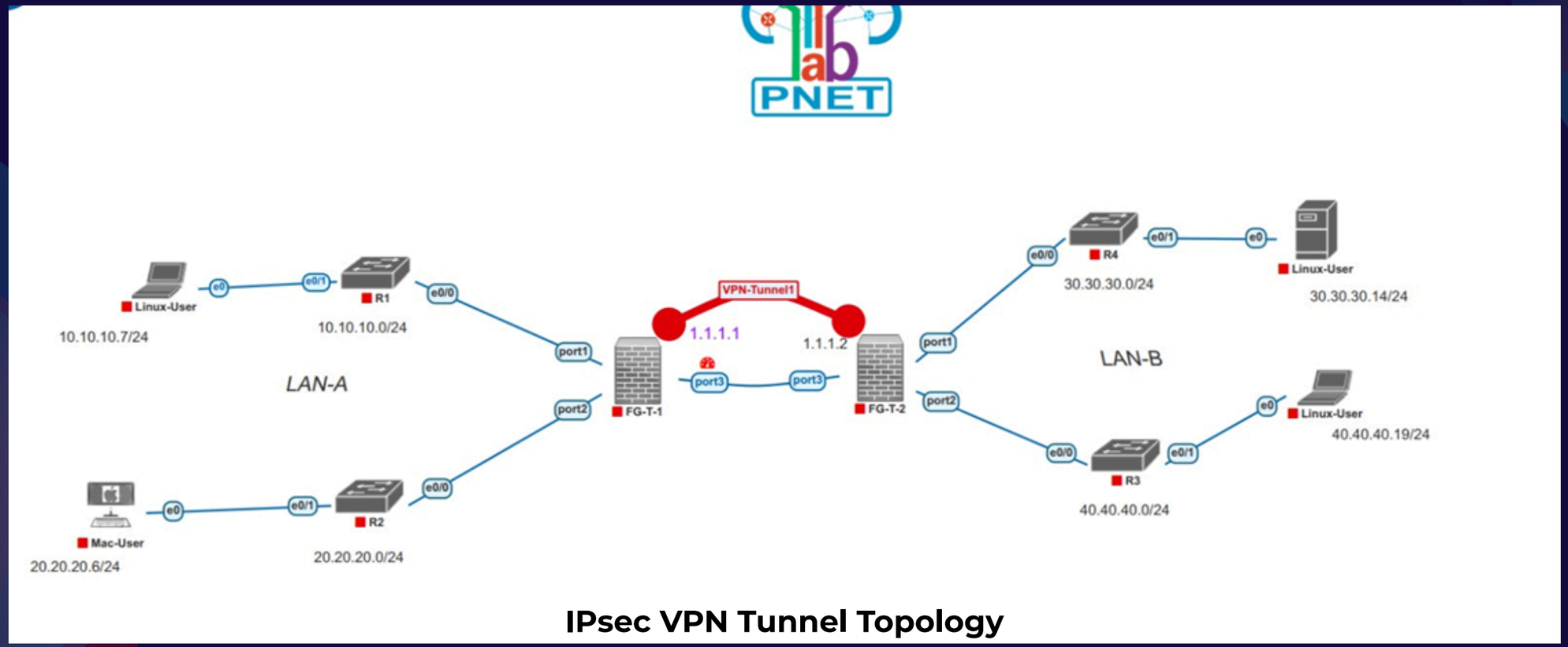
- **Overview**
  - The IPsec (Internet Protocol Security) VPN is a widely used protocol suite that secures network traffic by encrypting and authenticating IP packets at the network layer (Layer 3). It provides site-to-site and remote access solutions that ensure data confidentiality, integrity, and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

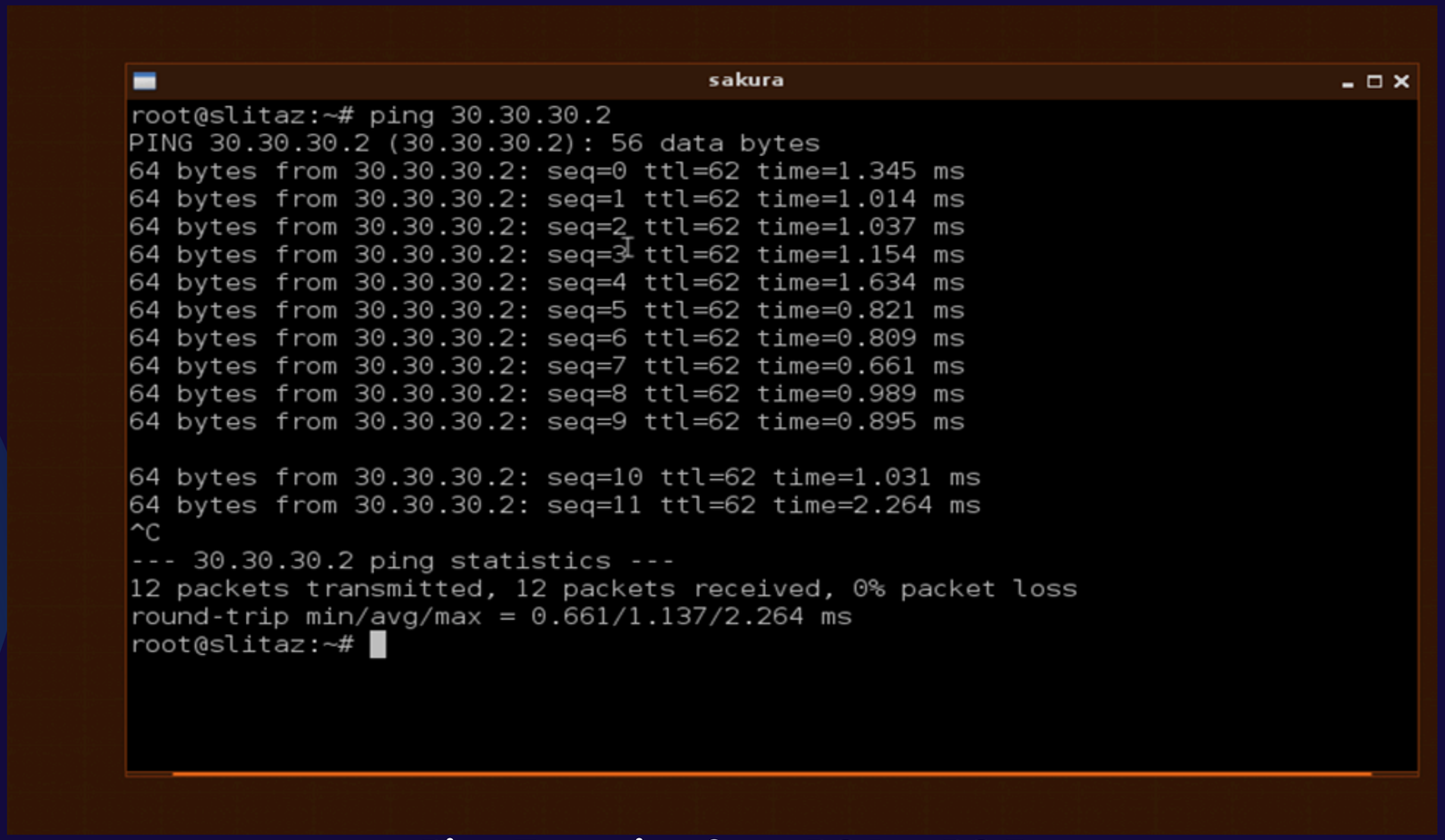
1. Phase 1 (IKE Negotiation):
   - Establishes a secure communication channel.
   - Authenticates the two VPN peers.
   - Negotiates encryption and hashing algorithms (e.g., AES, SHA).
2. Phase 2 (Data Encryption):
   - Defines traffic selectors (networks that will communicate).
   - Encrypts user data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

IPsec Configuration Steps on FortiGate



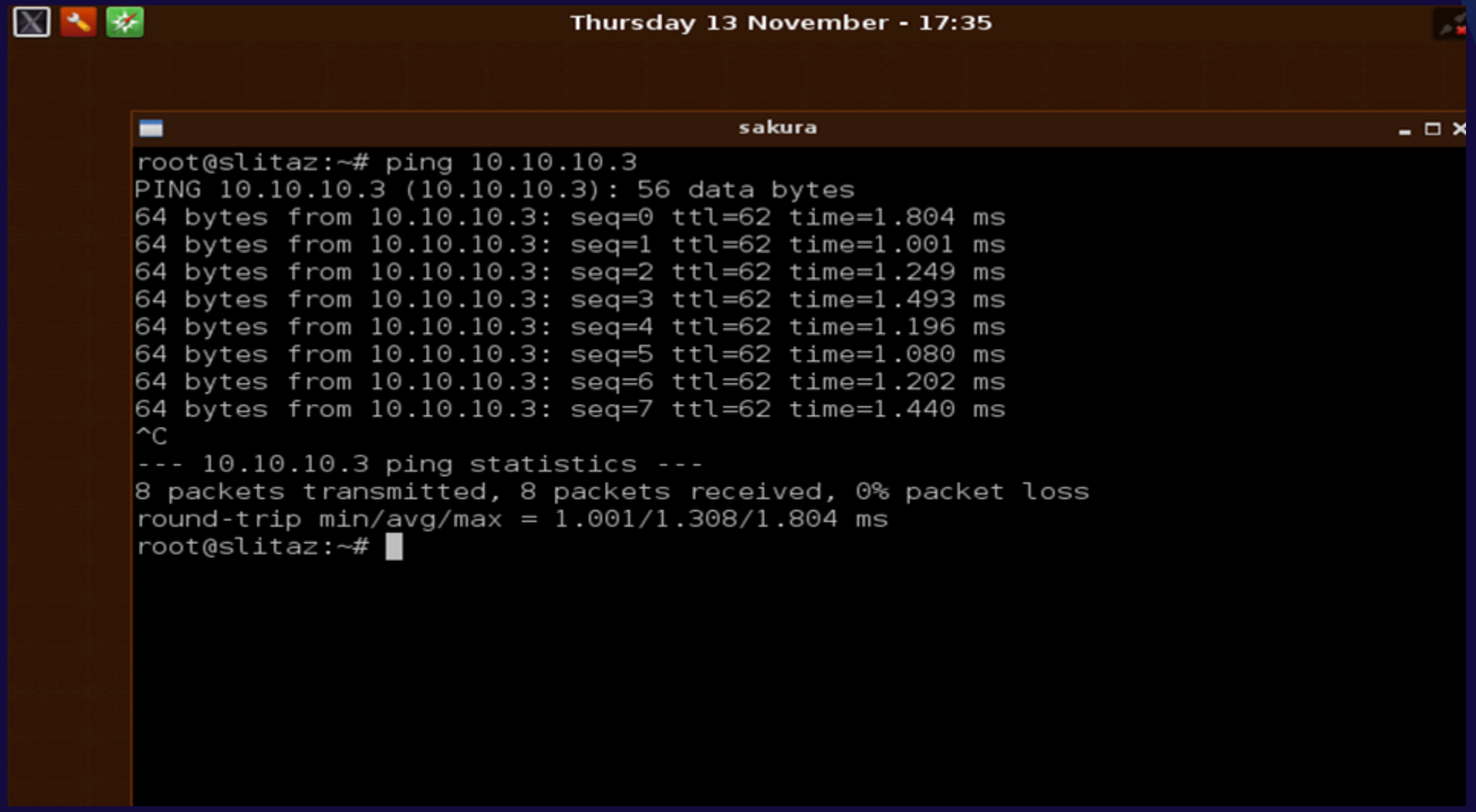
IPsec VPN Tunnel Topology

Testing and Verification



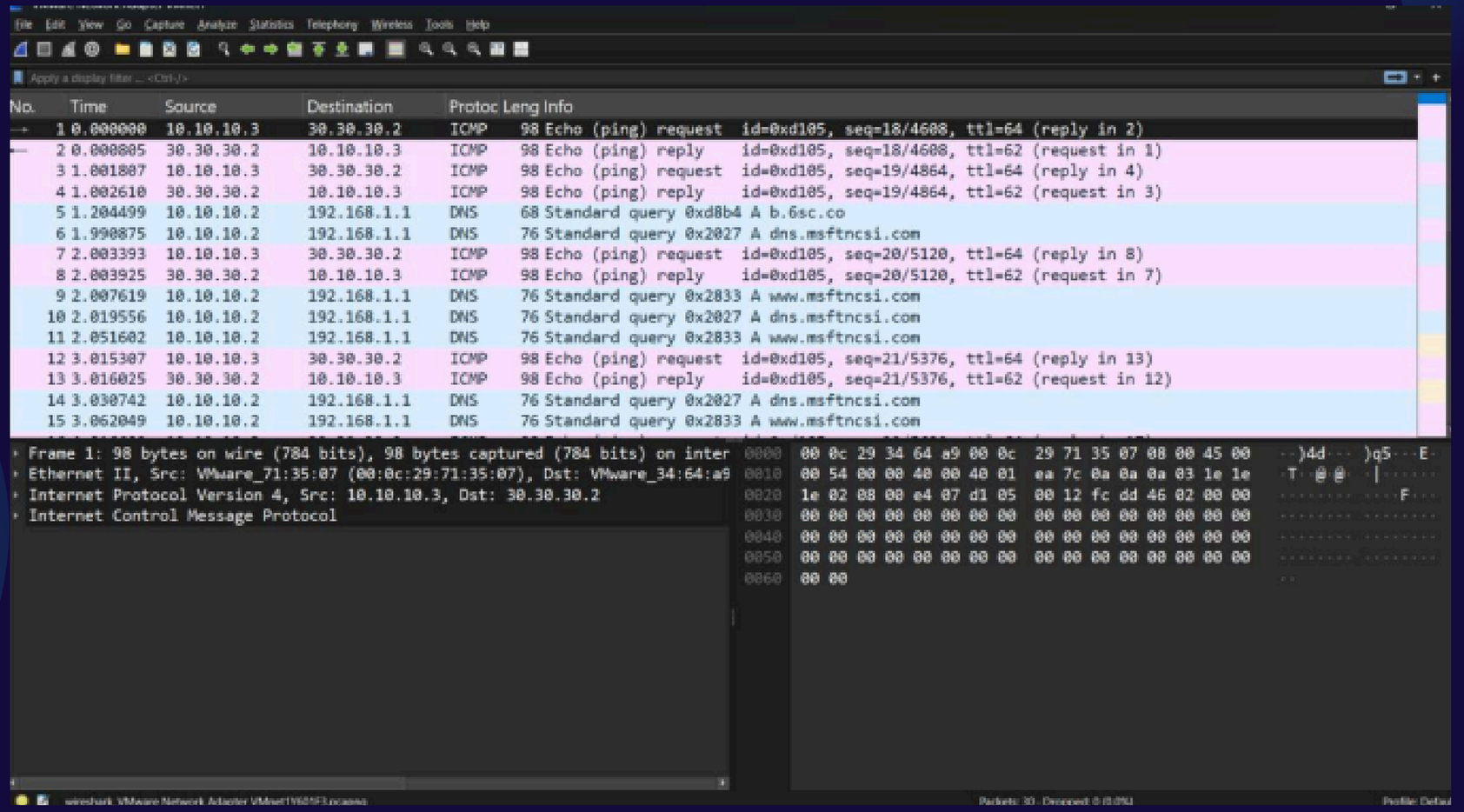
Ping Test: ping from PC-1 to PC-3

Testing and Verification



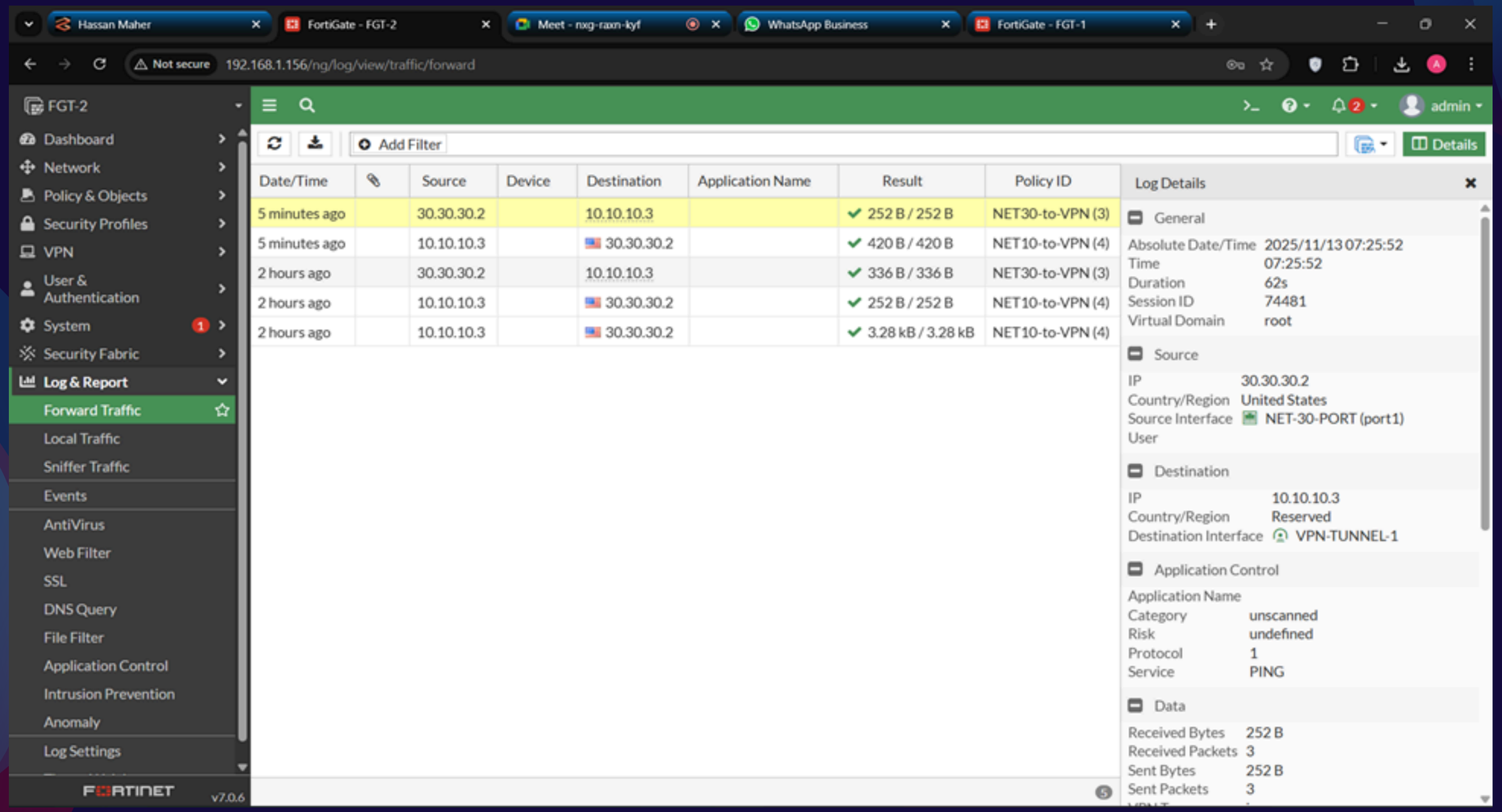
ping from PC-3 to PC-1

Testing and Verification

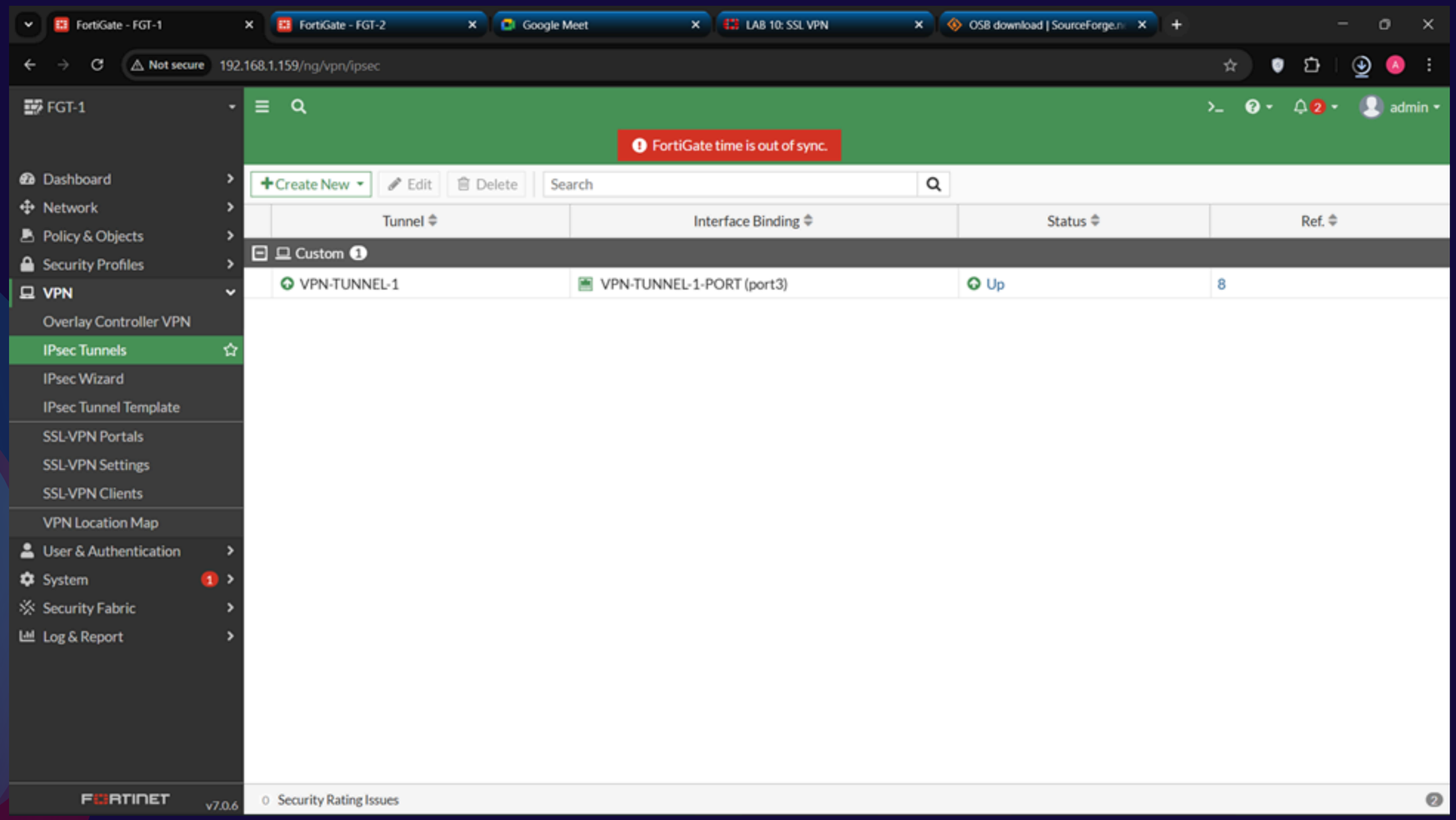


Capturing a traffic between PC-1 and PC-3 using Wireshark

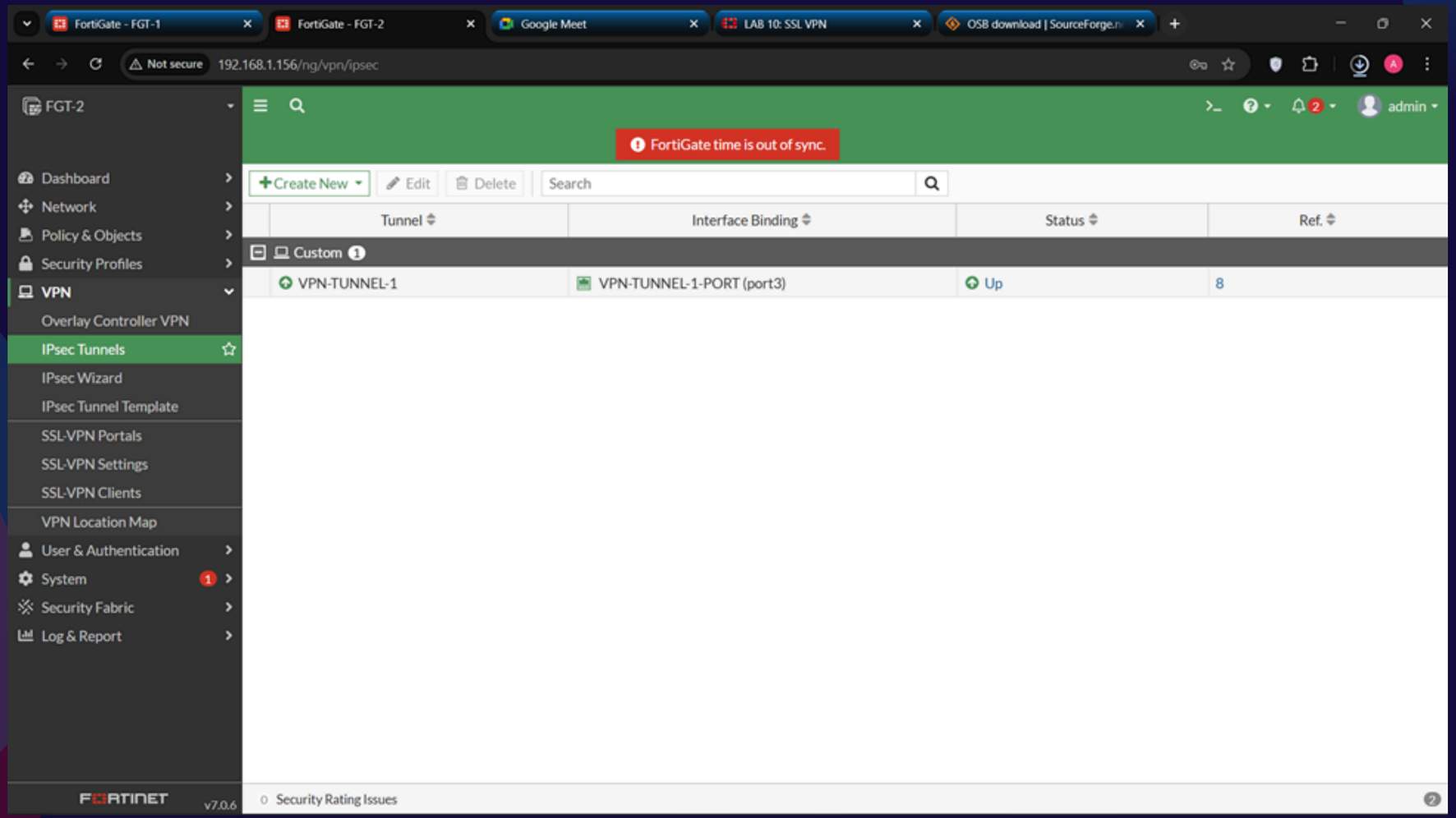
Logs and Events



Tunnel Status



Tunnel Status



FortiGate VPN with SD-WAN Integration

- **Overview**

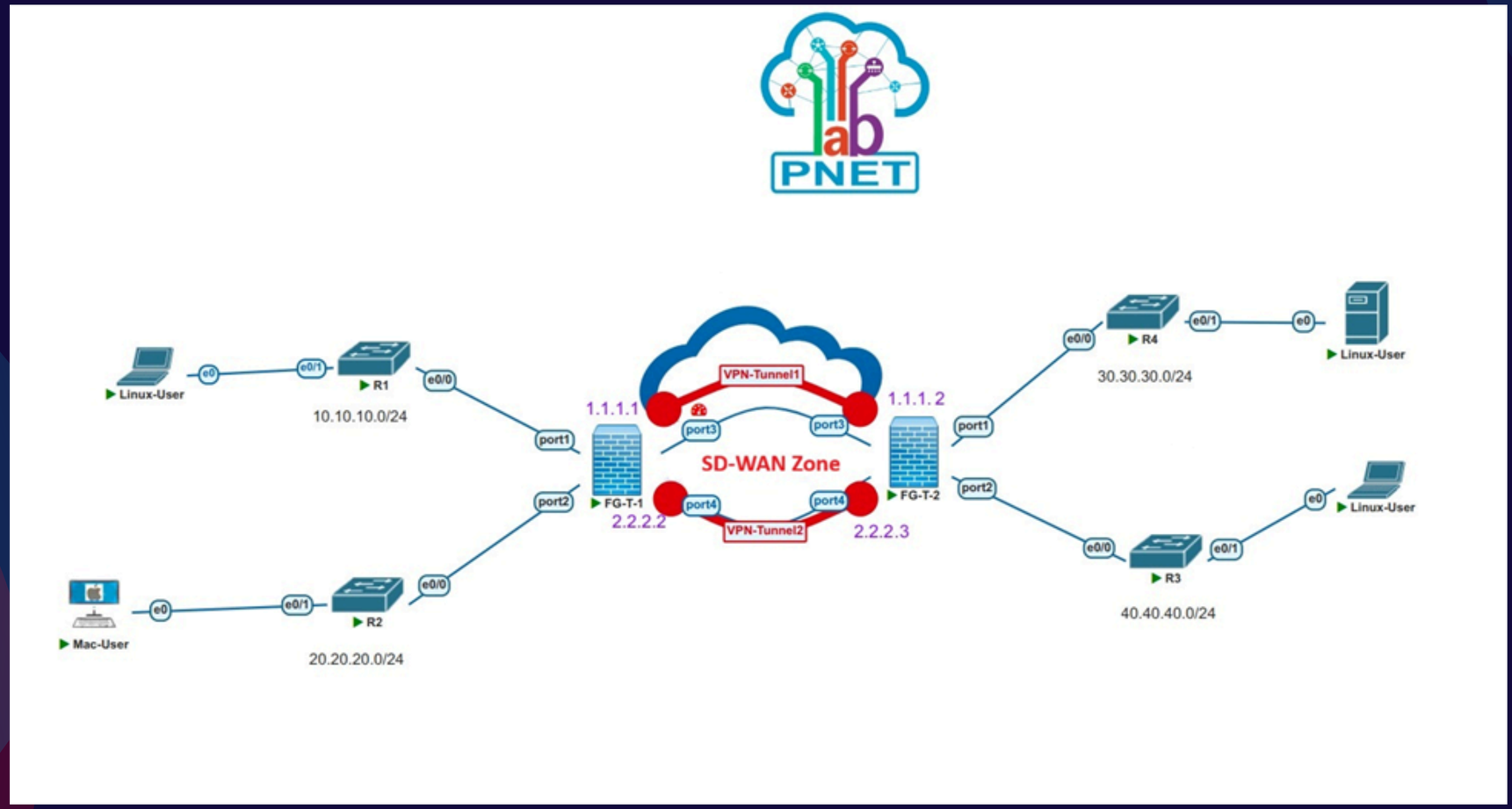
SD-WAN (Software-Defined Wide Area Network) is an advanced networking technology that enhances WAN performance by intelligently directing traffic across multiple WAN connections (such as MPLS, broadband, or LTE). Integrating SD-WAN with VPN allows FortiGate devices to dynamically select the best path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

FortiGate VPN with SD-WAN Integration

- **How SD-WAN Works**

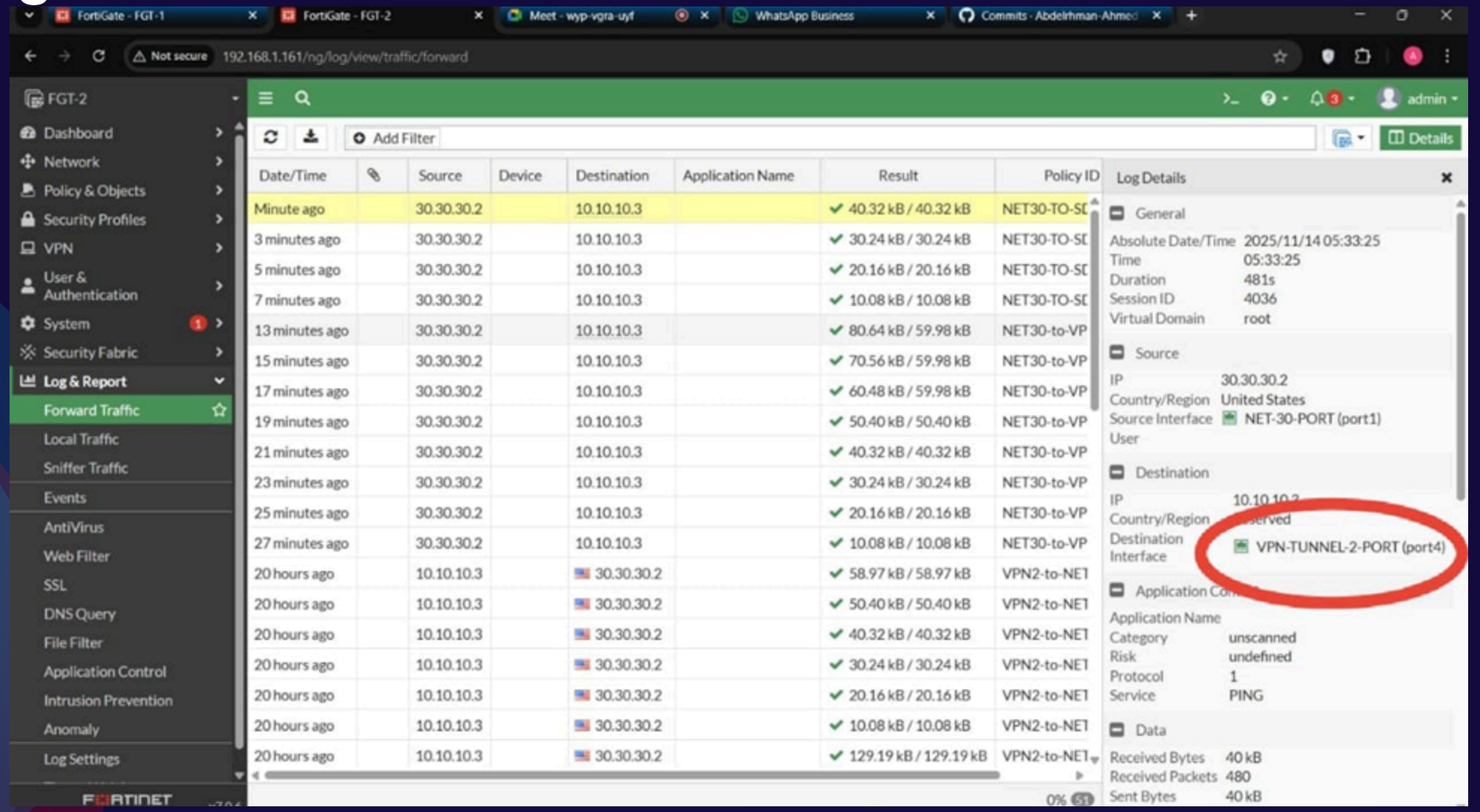
SD-WAN operates by creating a virtual overlay network on top of existing physical connections like broadband, MPLS, or LTE. Edge devices installed at branch offices, data centers, or cloud locations manage and route traffic according to centrally defined policies.

SD-WAN Configuration on FortiGate



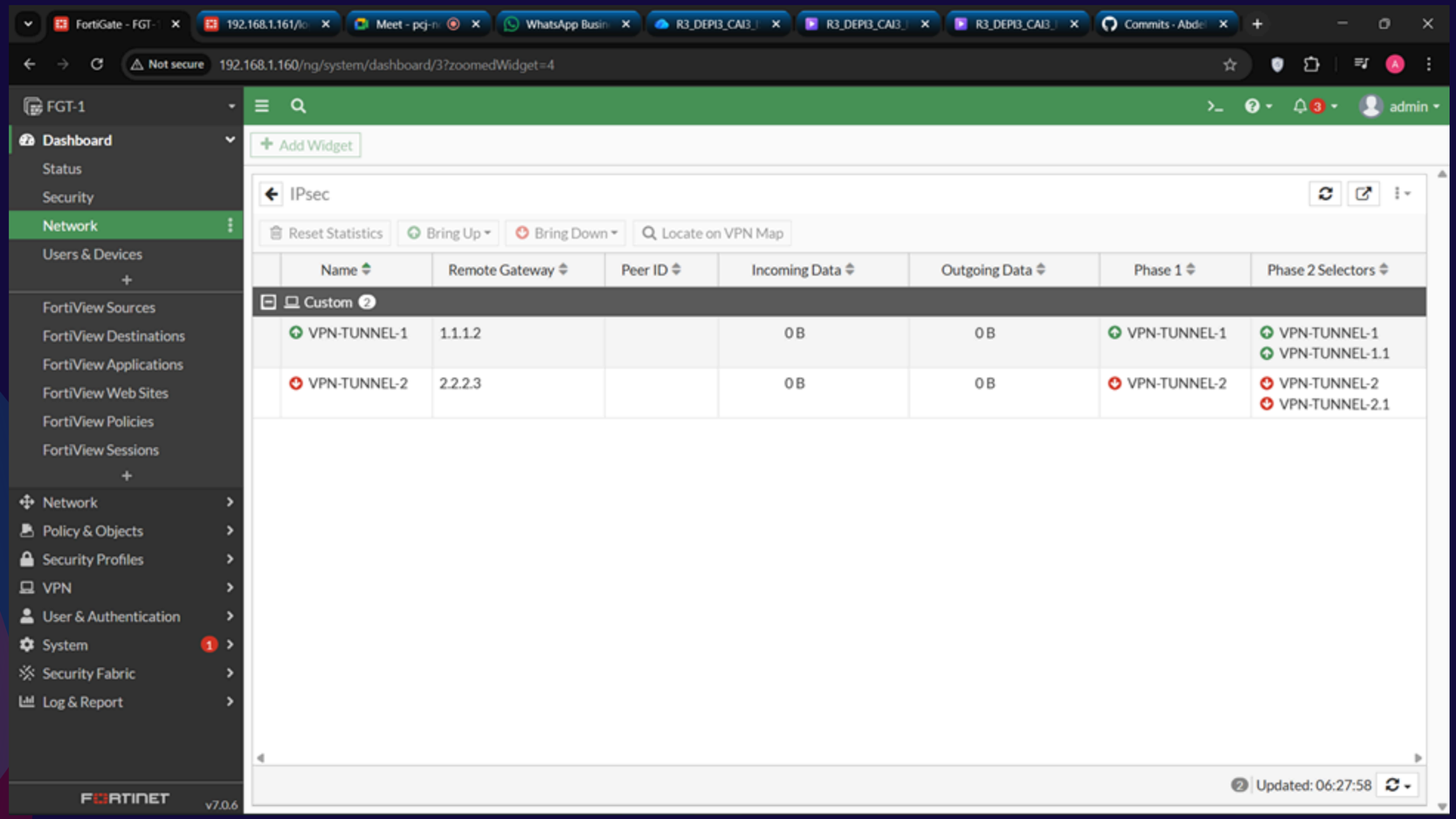
VPN with SD-WAN Integration Topology

Testing and Performance Evaluation



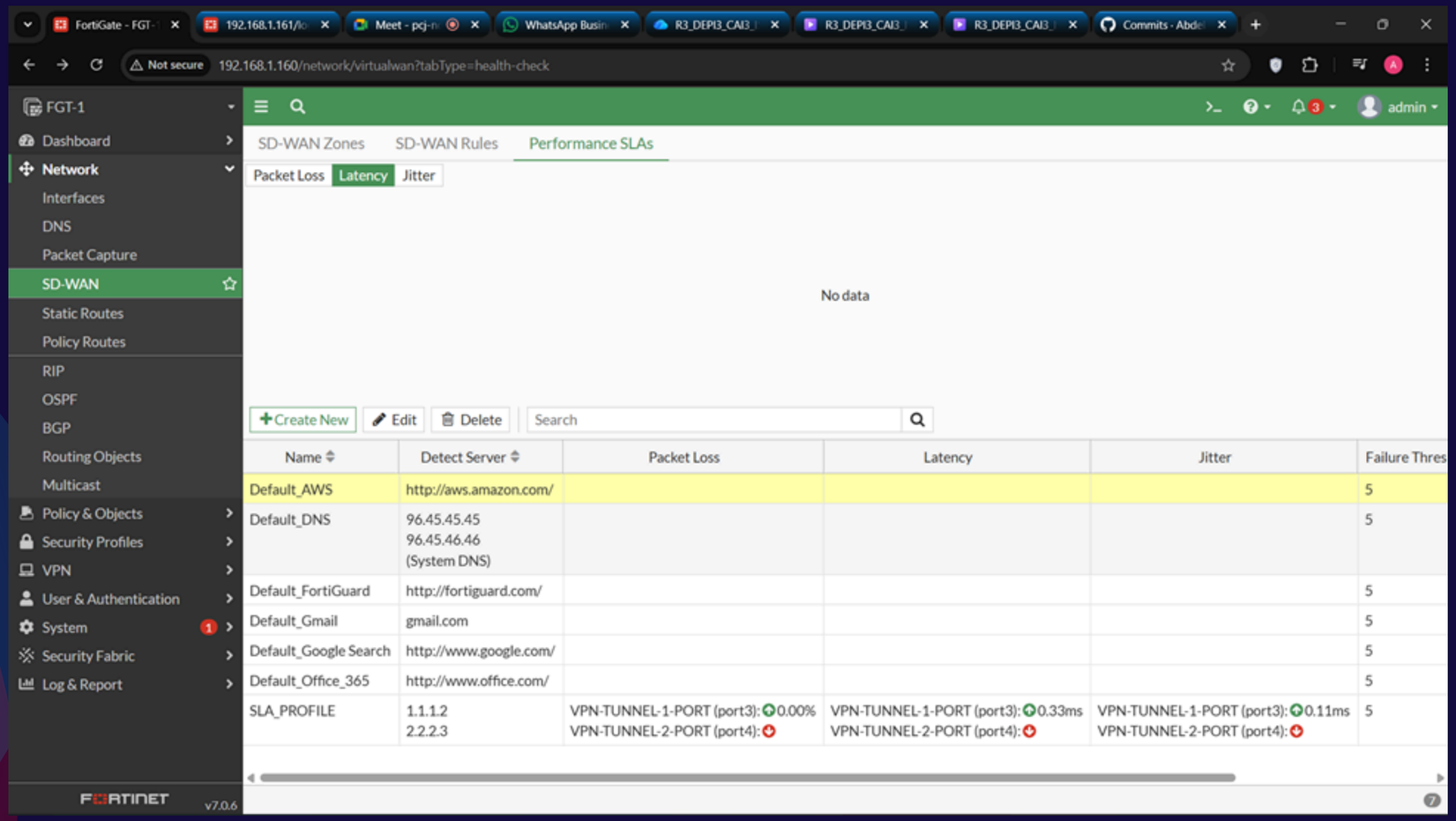
1. Tunnel 1 down and Tunnel 2 up

Testing and Performance Evaluation



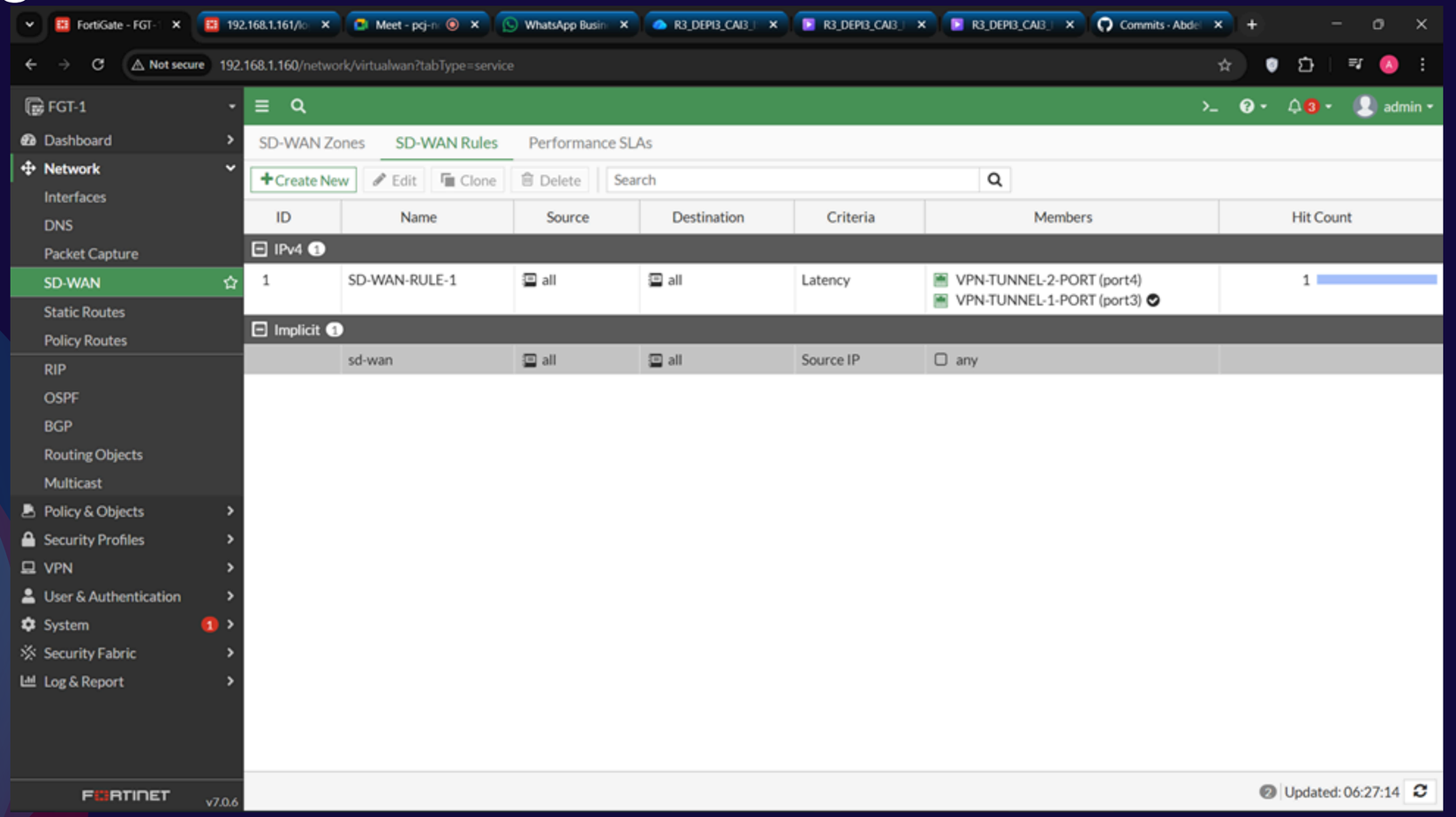
2. Tunnel 1 up and Tunnel 2 down

Testing and Performance Evaluation



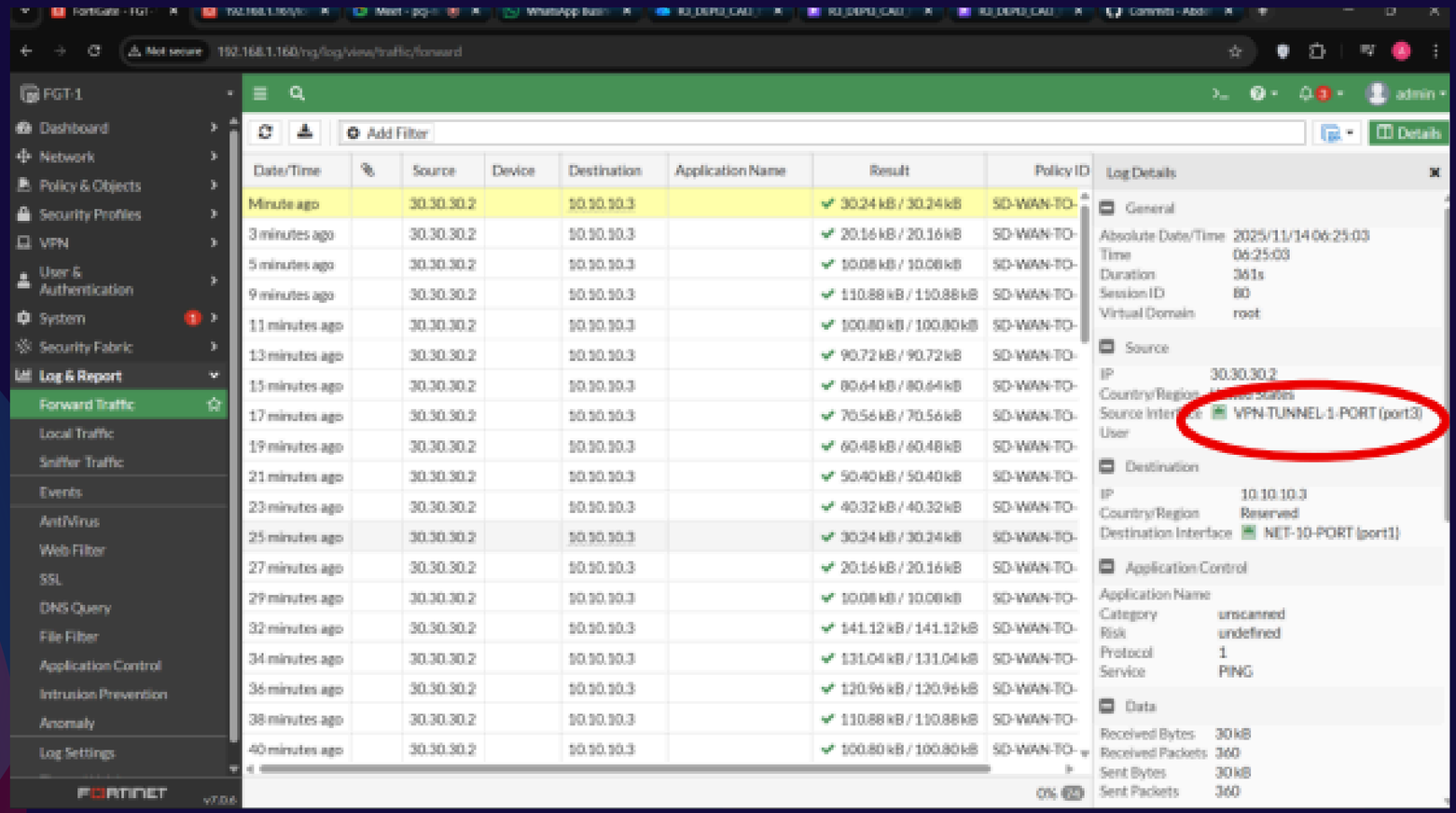
2. Tunnel 1 up and Tunnel 2 down

Testing and Performance Evaluation



2. Tunnel 1 up and Tunnel 2 down

Testing and Performance Evaluation



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

رواد مصر الرقمية

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