Exploring VPN Security Techniques, Protocols, and Attacks

Implementing VPN Solutions Project

Secure Connectivity for Modern Networks

Team Members

Abdelrahman Ali Ghonemy Ayad

Ziad Mohamed Hassan Sultan

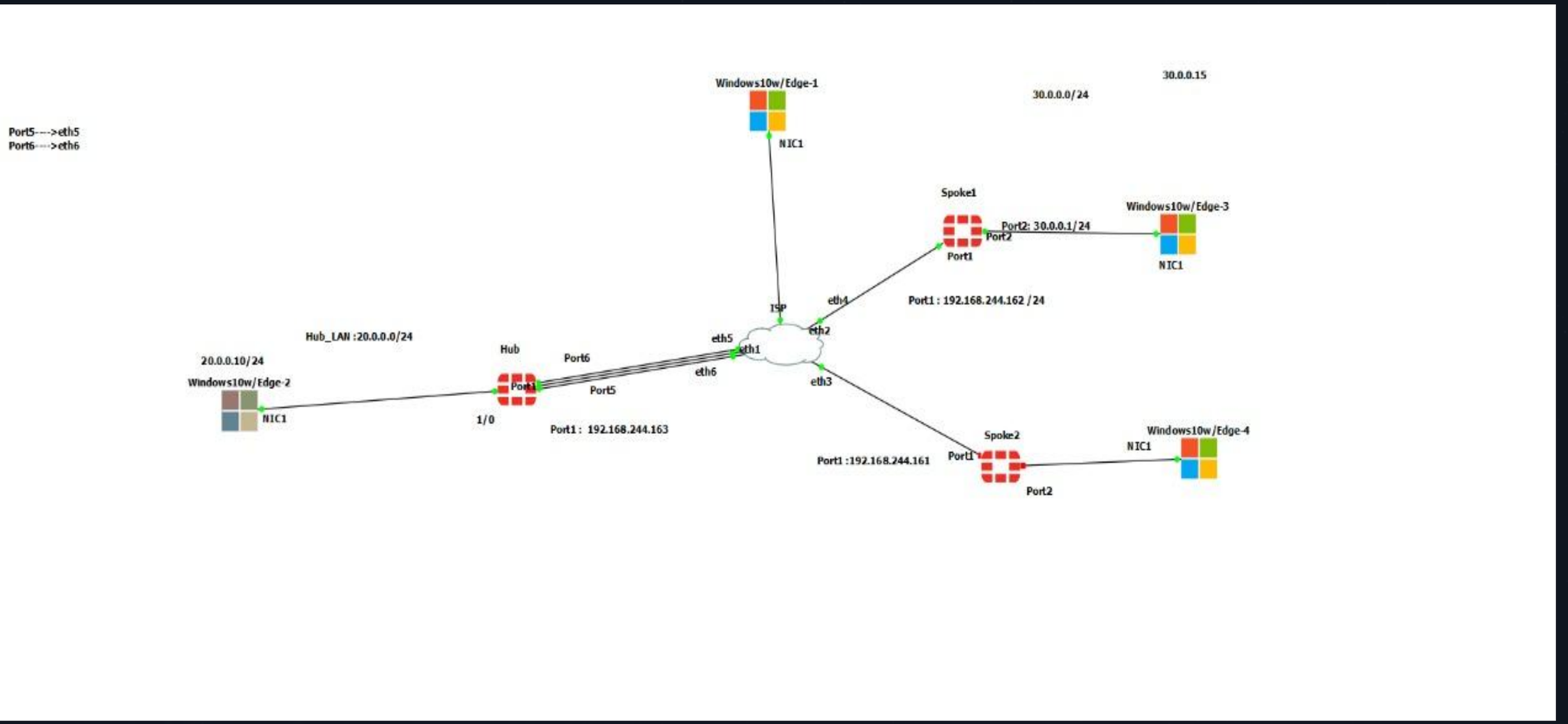
Yazan Abdelfatah Shehata Kholief

Shams Ibrahim Elsayed Salama

Sherif Ayman Ahmed

Ziad Wael Faiz AbdelGaber

Topolgy



Understanding VPNs

A Virtual Private Network (VPN) establishes a secure connection between devices over the internet, creating a private network. It's essential for maintaining privacy, ensuring security, and enabling remote access to private networks.

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, typically implemented between routers or firewalls.

SSL VPN (Secure Sockets Layer VPN)

Uses HTTPS (port 443) for secure remote access via web browser or client, encrypting traffic with SSL/TLS protocols.

IPsec VPN

Uses the IPsec protocol suite to encrypt and authenticate IP packets between sites or devices. It operates at the network layer.

IMPLS VPN (Mulitprotocol Label Switching VPN)

Uses service provider network to create private paths for enterprise traffic, ensuring reliability and Qos

l2TP / IPsec VPN

Combine layer 2 Tunneling Protocol with IPsec encryption. Often used for secure remote access

SSL VPN: Secure Web Access

An SSL VPN enables 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 securing websites (HTTPS).

Because it uses port 443, SSL VPN traffic easily passes through most firewalls without special configurations. Organizations widely use SSL VPNs to allow remote employees, partners, or clients to securely access internal applications, files, or systems over the internet.

Why Choose SSL VPN?

SSL VPNs offer significant advantages due to their flexibility and ease of use. Their reliance on standard web protocols makes them highly compatible with existing network infrastructures.

Firewall Friendly

Uses HTTPS (port 443), allowing it to easily pass through most firewalls.

User-Based Authentication

Provides robust authentication mechanisms tailored to individual users.

Clientless Access

Doesn't require a special client, functioning directly within a web browser.

Flexible Access Modes

Offers both tunnel mode (for full network access) and web mode (for portal-based access).

How SSL VPN Works

The SSL VPN process is straightforward, ensuring secure and authenticated access to internal resources.

User Connection

The user connects to the SSL VPN gateway (e.g., FortiGate) via a web browser or FortiClient VPN application.

Secure Establishment

The connection is established using SSL/TLS encryption, securing data transmission between the user and the VPN gateway.

Authenticated Access

Once authenticated, the user is granted access to internal resources based on their assigned privileges.

Modes of SSL VPN

SSL VPNs offer two primary modes, each designed for different levels of access and user requirements.

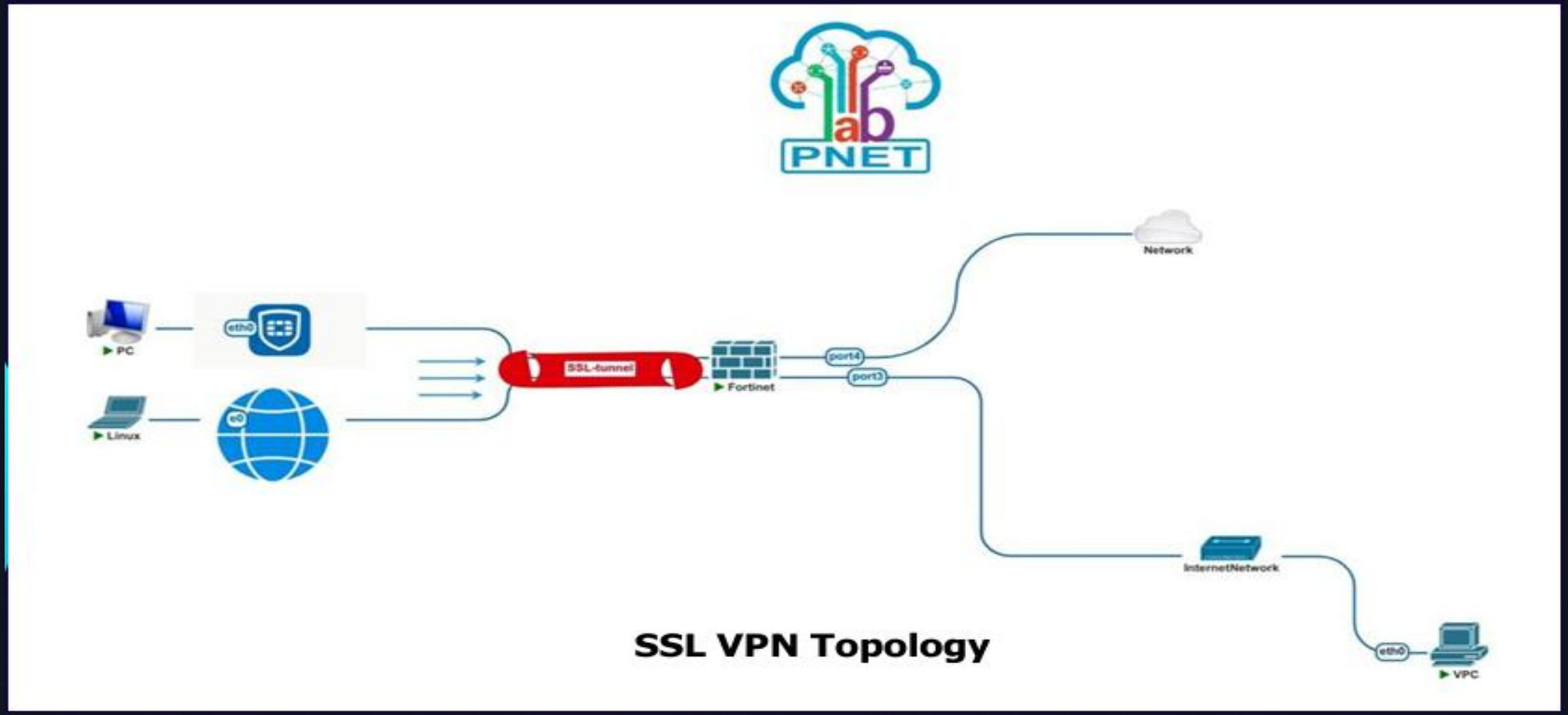
Web Mode

- Access through a web portal.
- Users log in via a browser to access specific applications (email, file servers, web tools).
- Suitable for simple, controlled access without installing a VPN client.

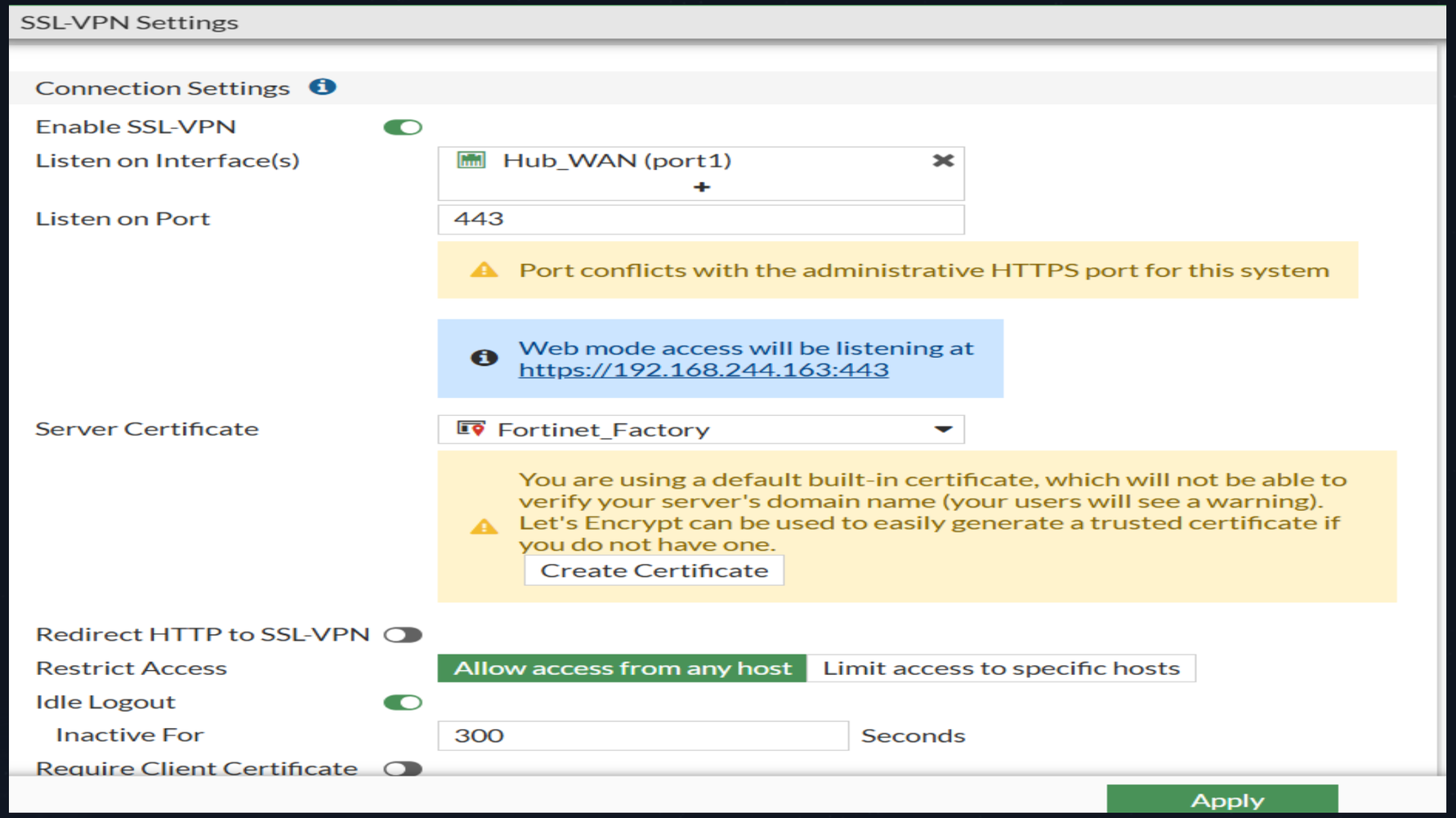
Tunnel Mode

- 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 onsite.
- Ideal for IT staff or employees needing broader network access.

SSL VPN Configuration on FortiGate

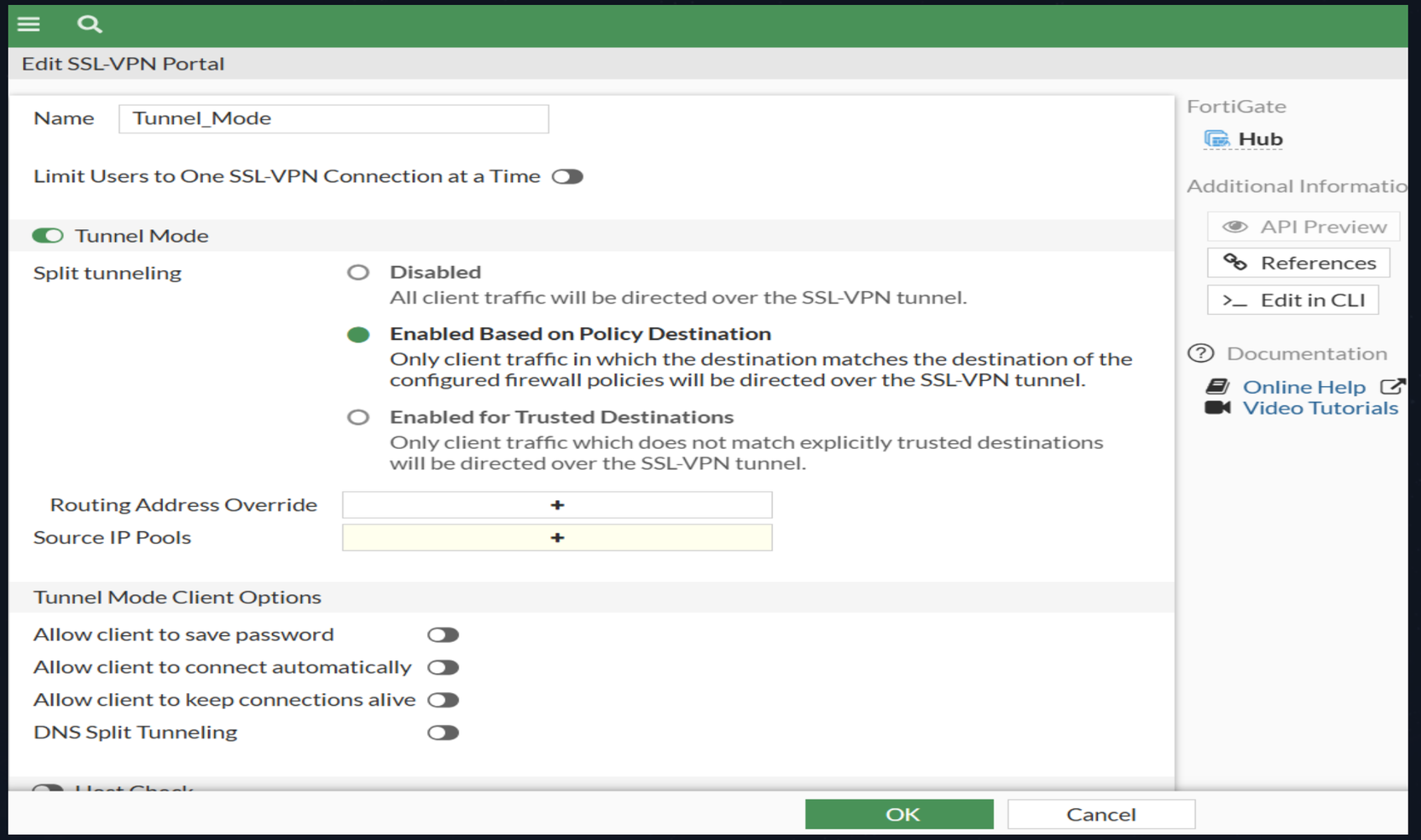


SSL VPN Configuration on FortiGate



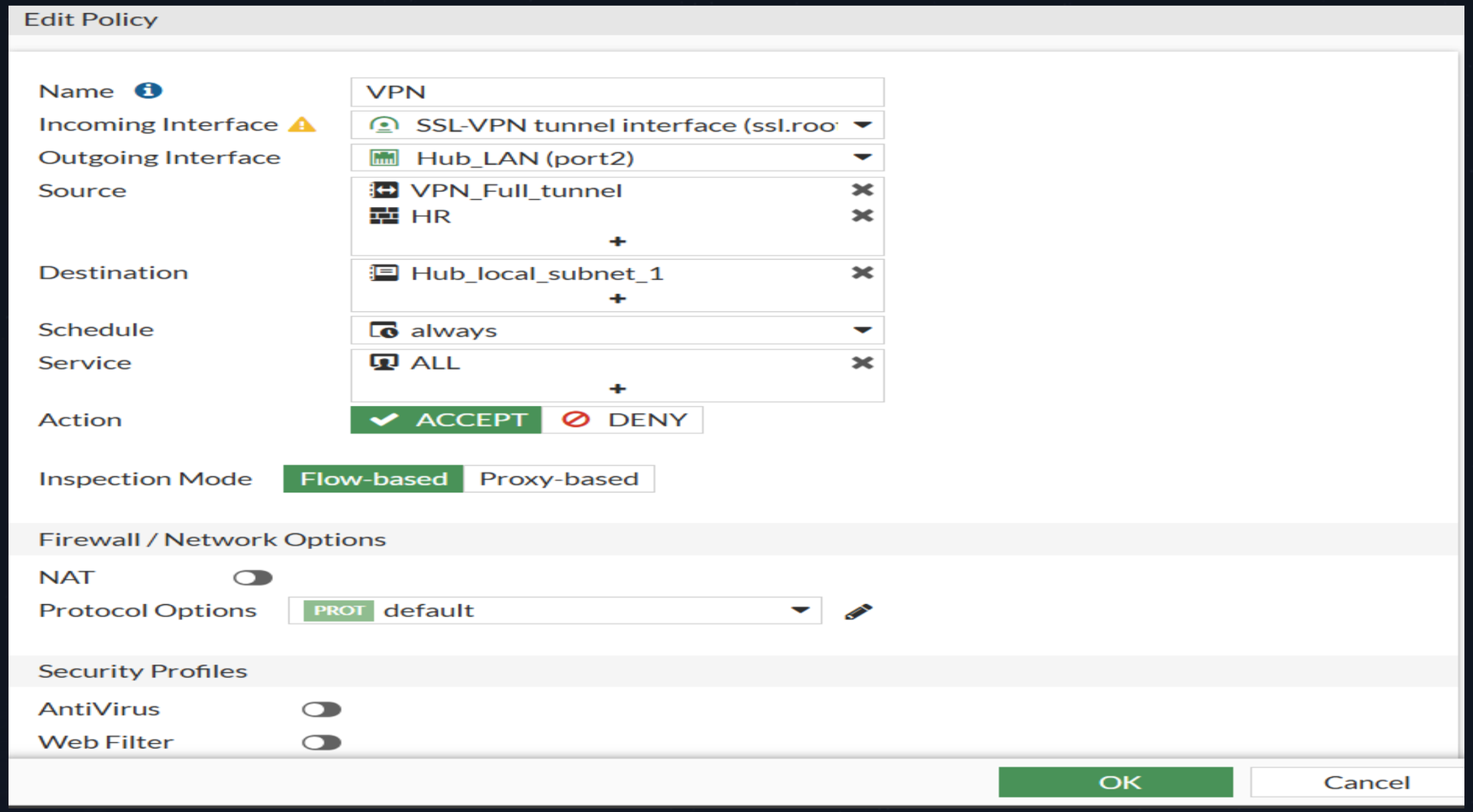
SSL-VPN Setting Configuration

SSL VPN Configuration on FortiGate



SSL-VPN Portal Configuration

SSL VPN Configuration on FortiGate



SSL-VPN-Access Policy Configuration

IPsec VPN

Over View

- The IPsec (Internet Protocol Security) VPN is a 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, ensuring data confidentiality, integrity, and authenticity between two or more networks.

- IPsec VPNs are ideal for organizations requiring permanent, secure connections between branches, headquarters, or data centers.

- Unlike SSL VPNs, IPsec VPNs operate transparently for entire subnets and devices, offering a more comprehensive network-level security solution.

How IPsec VPN Works

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

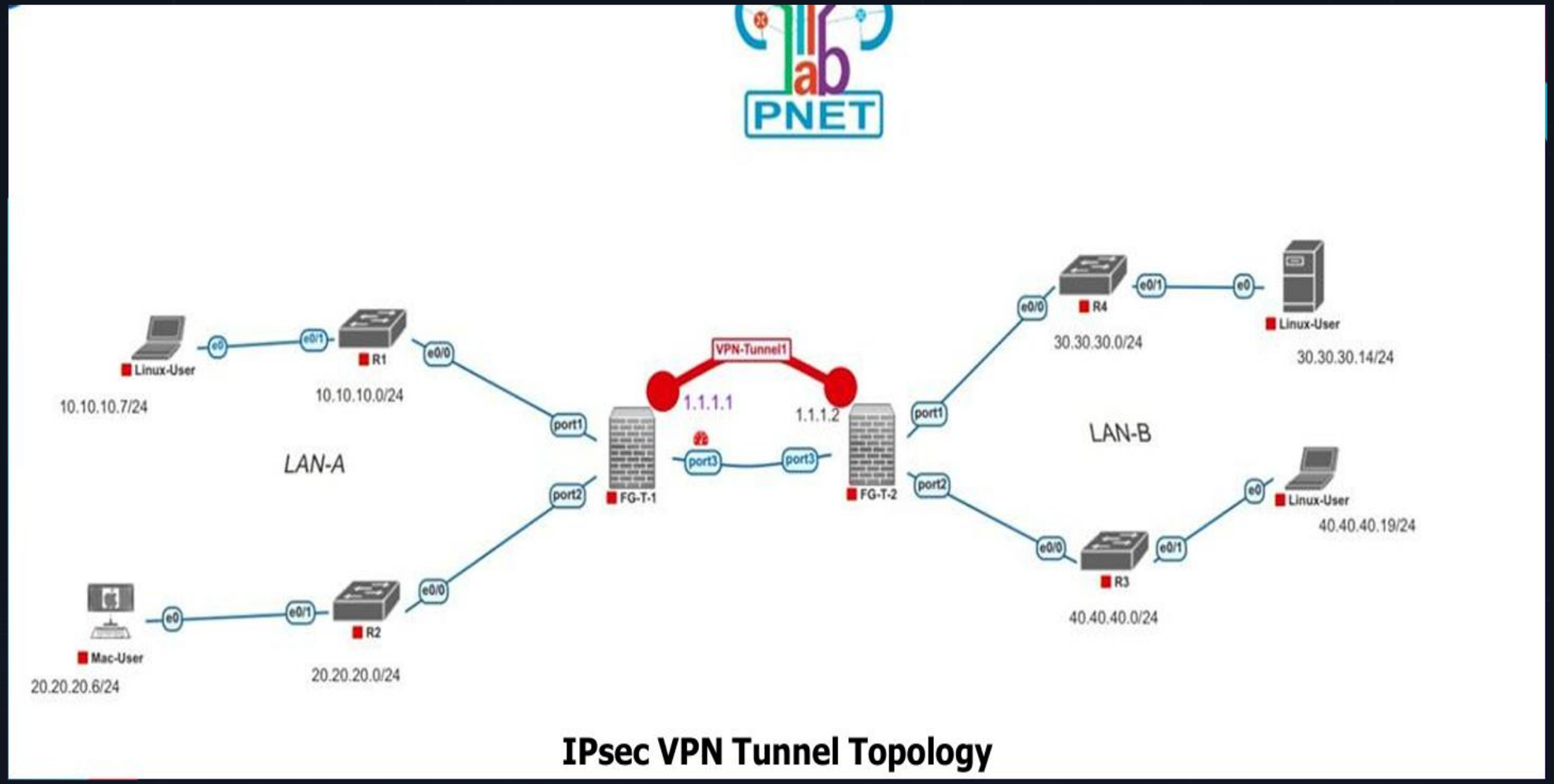
Phase 1: IKE Negotiation

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

Phase 2: Data Encryption

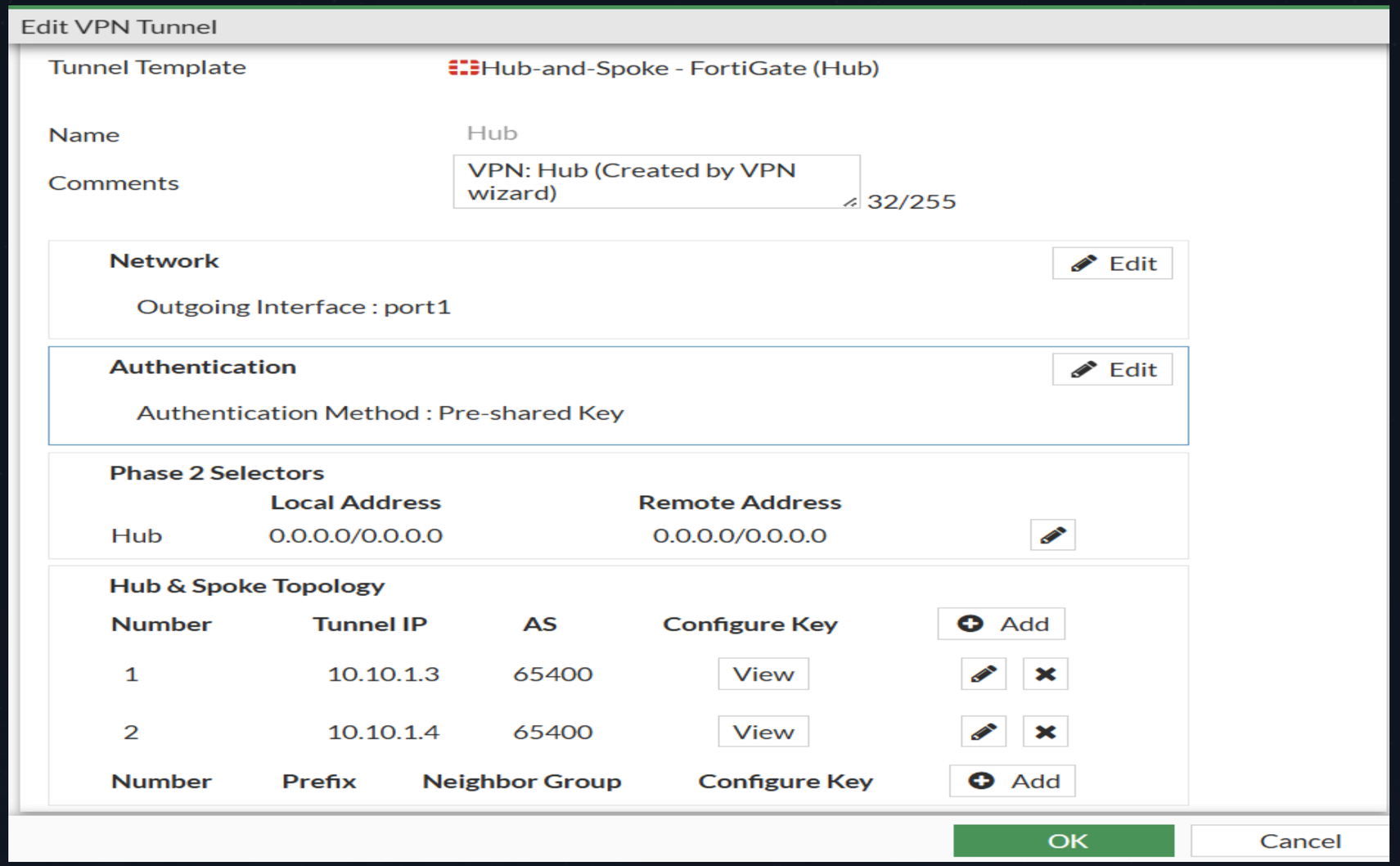
- Defines traffic selectors (networks that will communicate)
- Encrypts user data packets through the established tunnel.

IPsec Configuration Steps on FortiGate

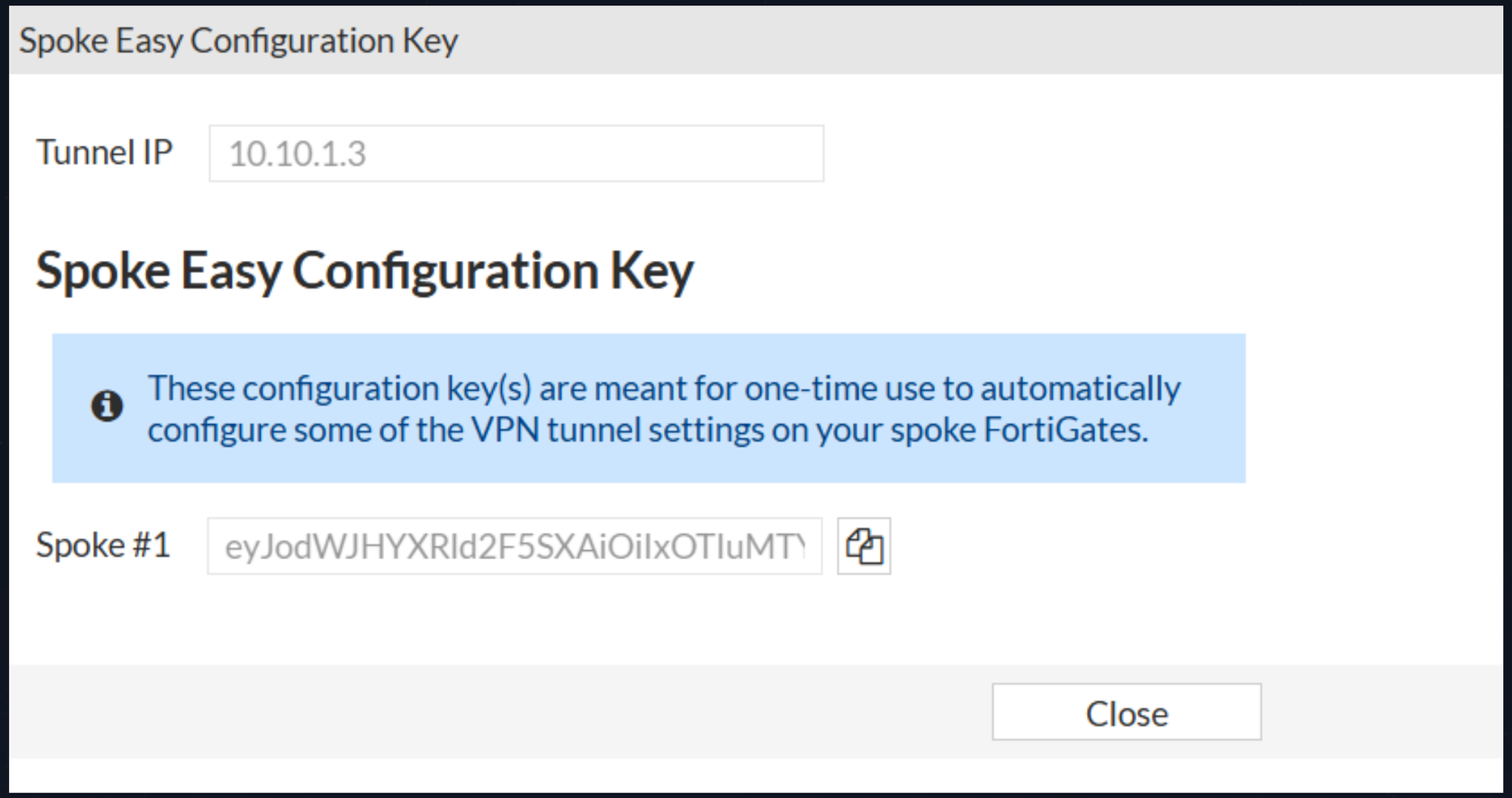


IPsec VPN Tunnel Topology

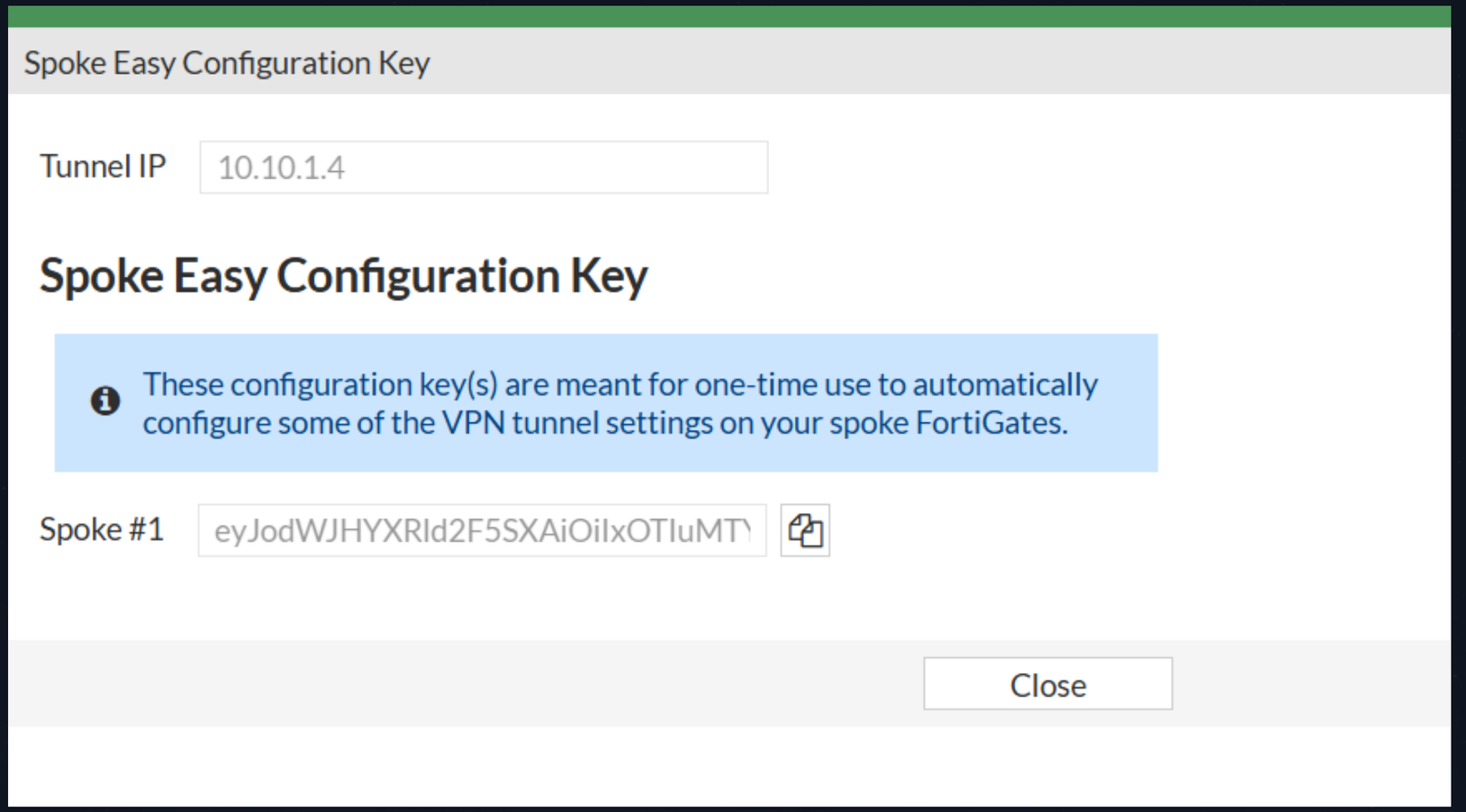
IPsec Configuration Steps on FortiGate



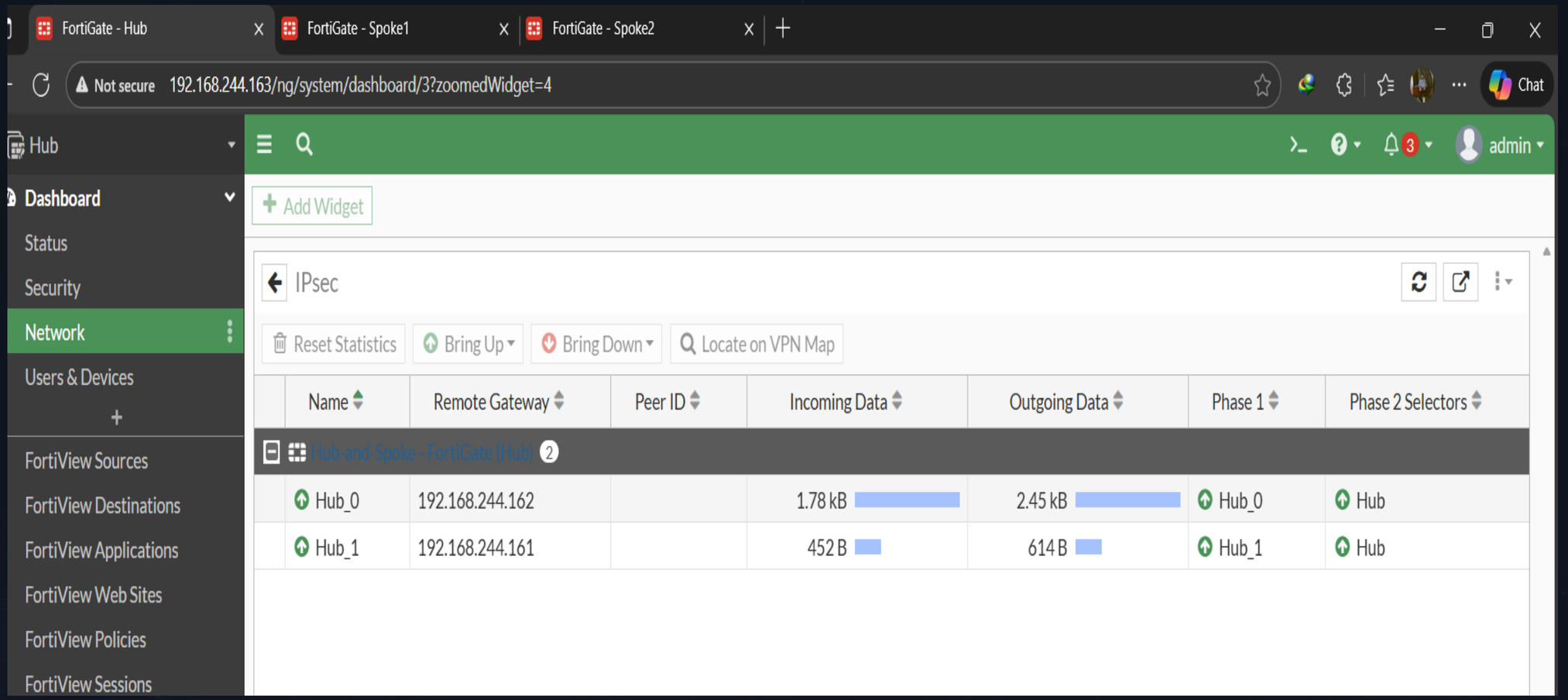
IPsec Configuration Steps on FortiGate



IPsec Configuration Steps on FortiGate

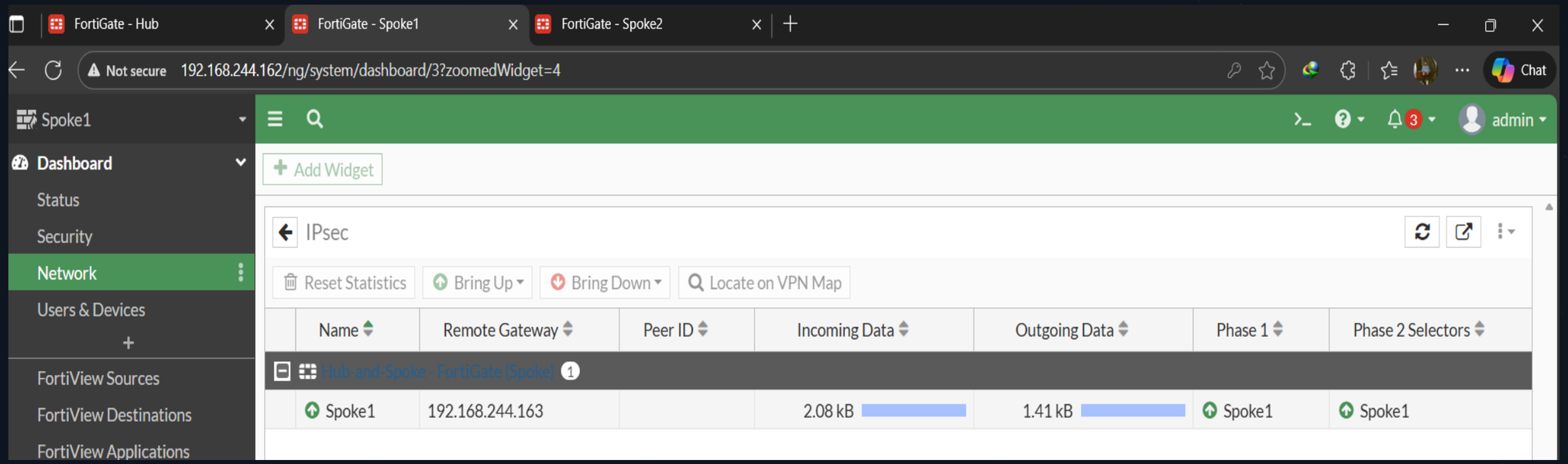


IPsec Configuration Steps on FortiGate



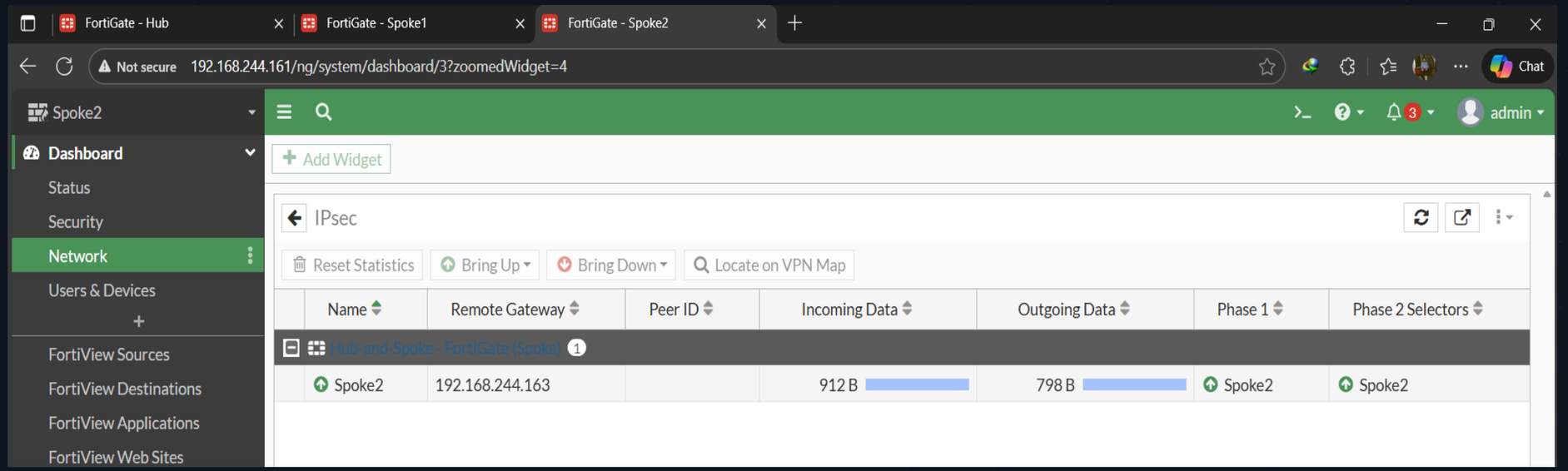
Connection on Hubs

IPsec Configuration Steps on FortiGate



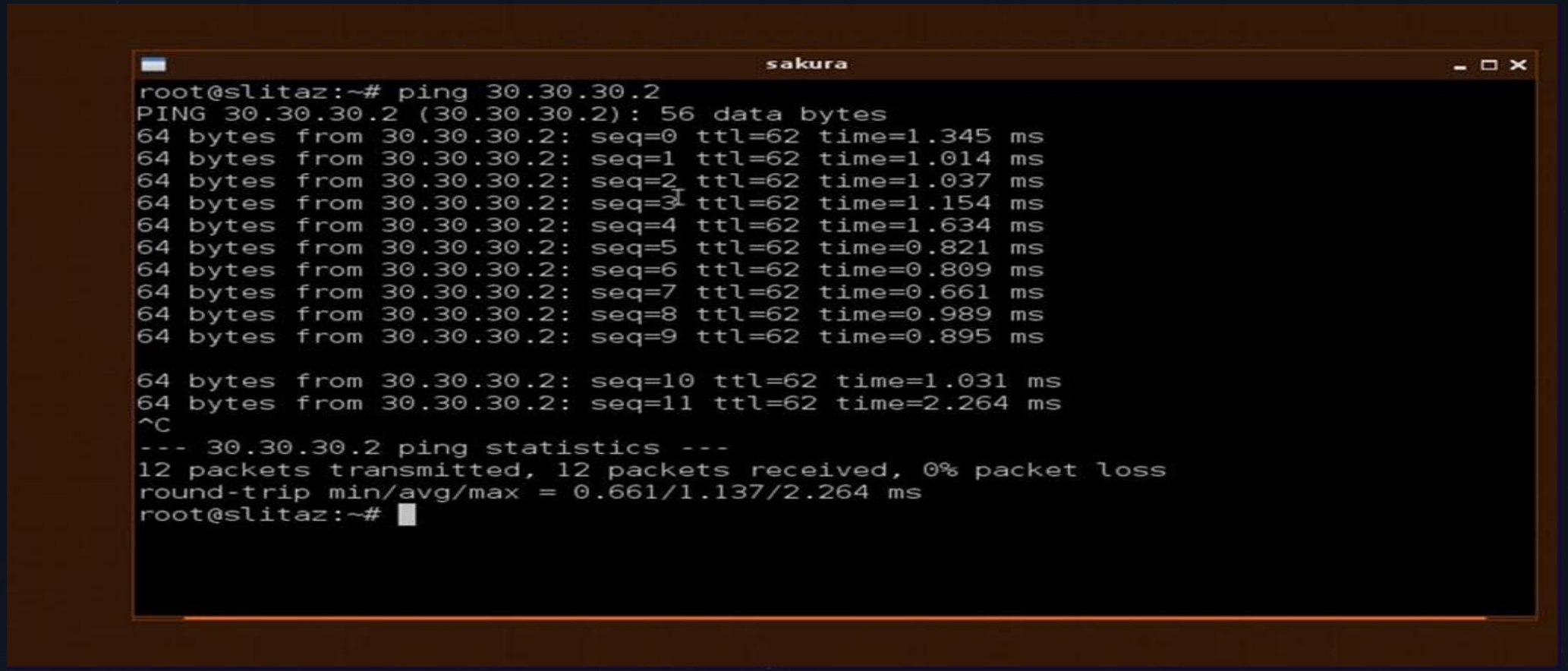
Spoke 1

IPsec Configuration Steps on FortiGate



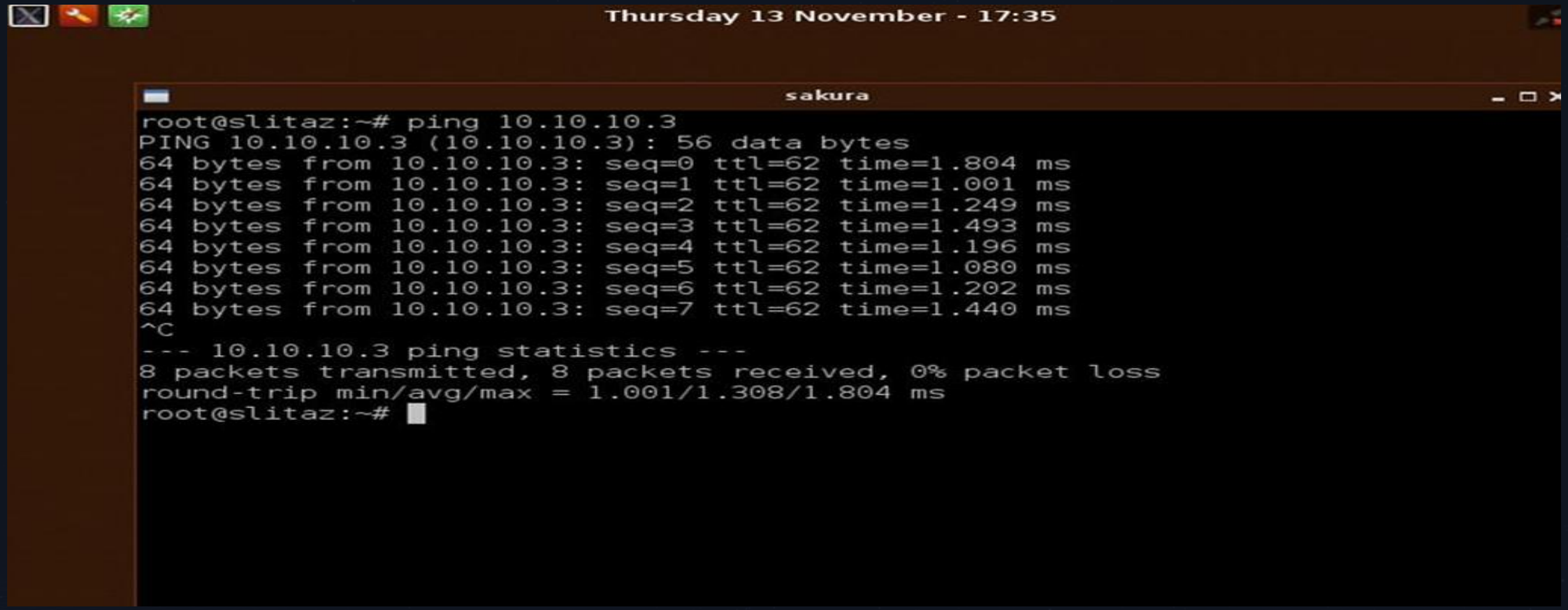
Spoke 2

Testing and Verification



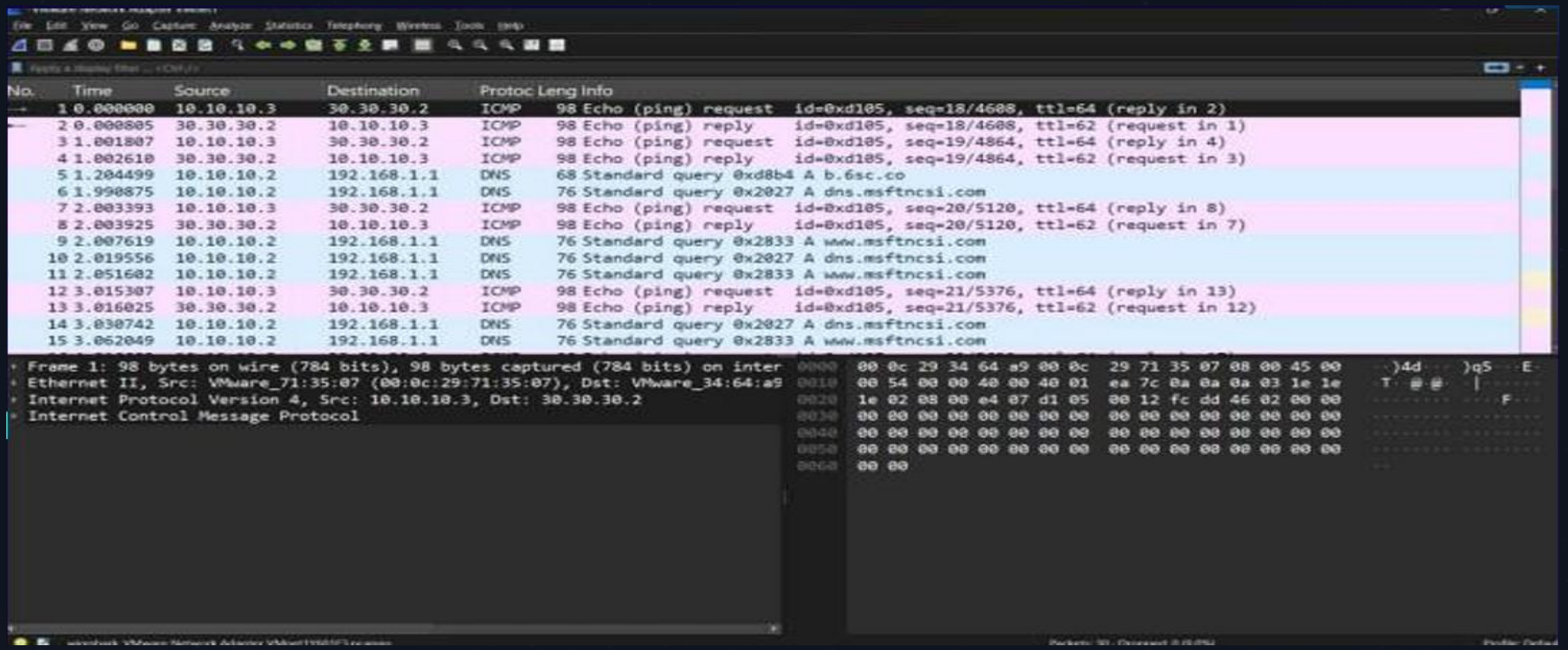
Ping Test: ping from PC-1 To PC-3

Testing and Verification



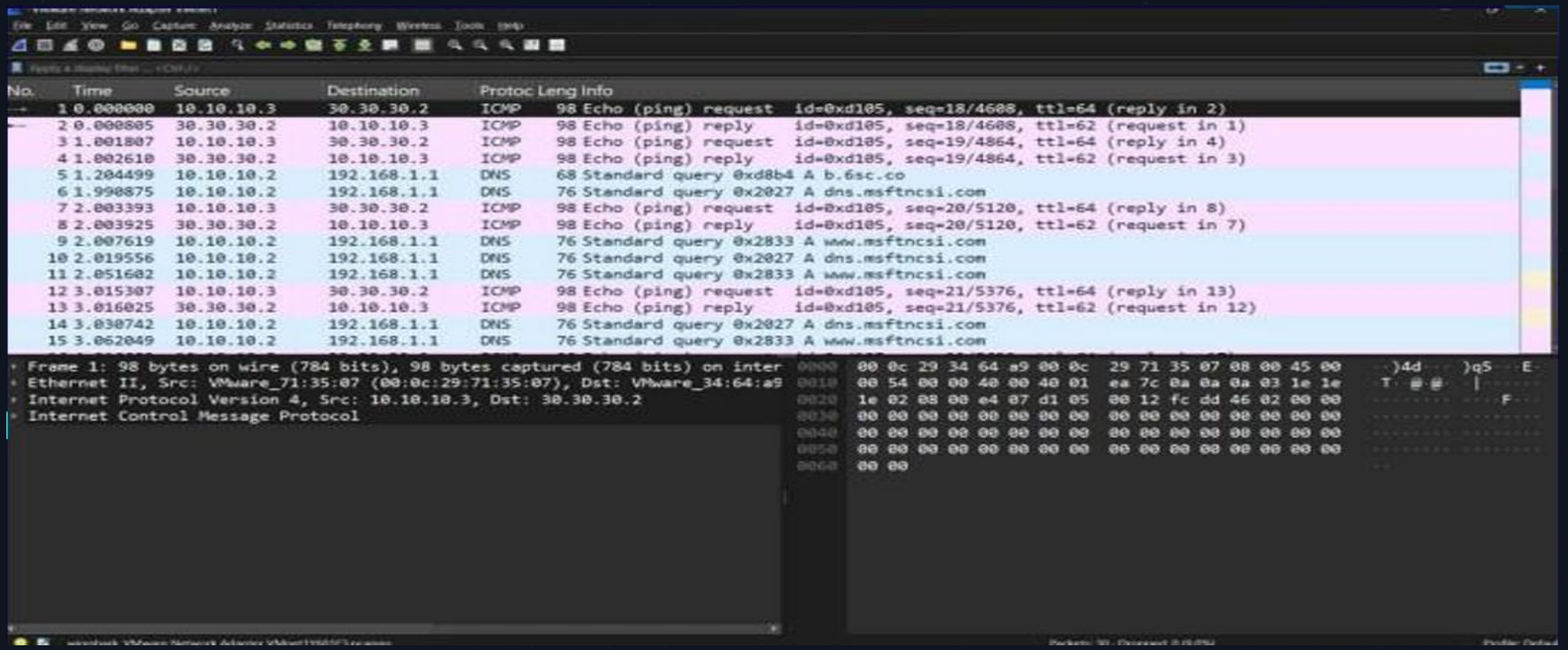
Ping Test: ping from PC-3 To PC-1

Testing and Verification



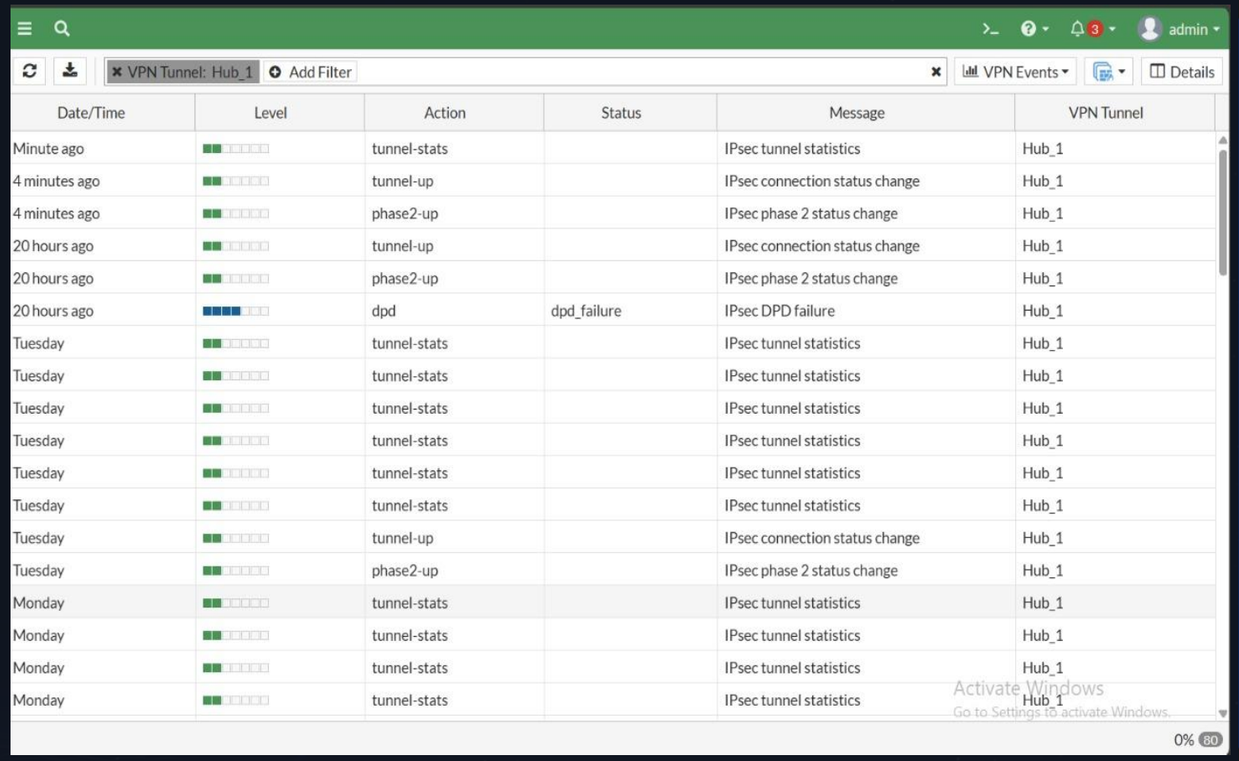
Capturing a traffic between PC-1 and PC-3 Using WireShark

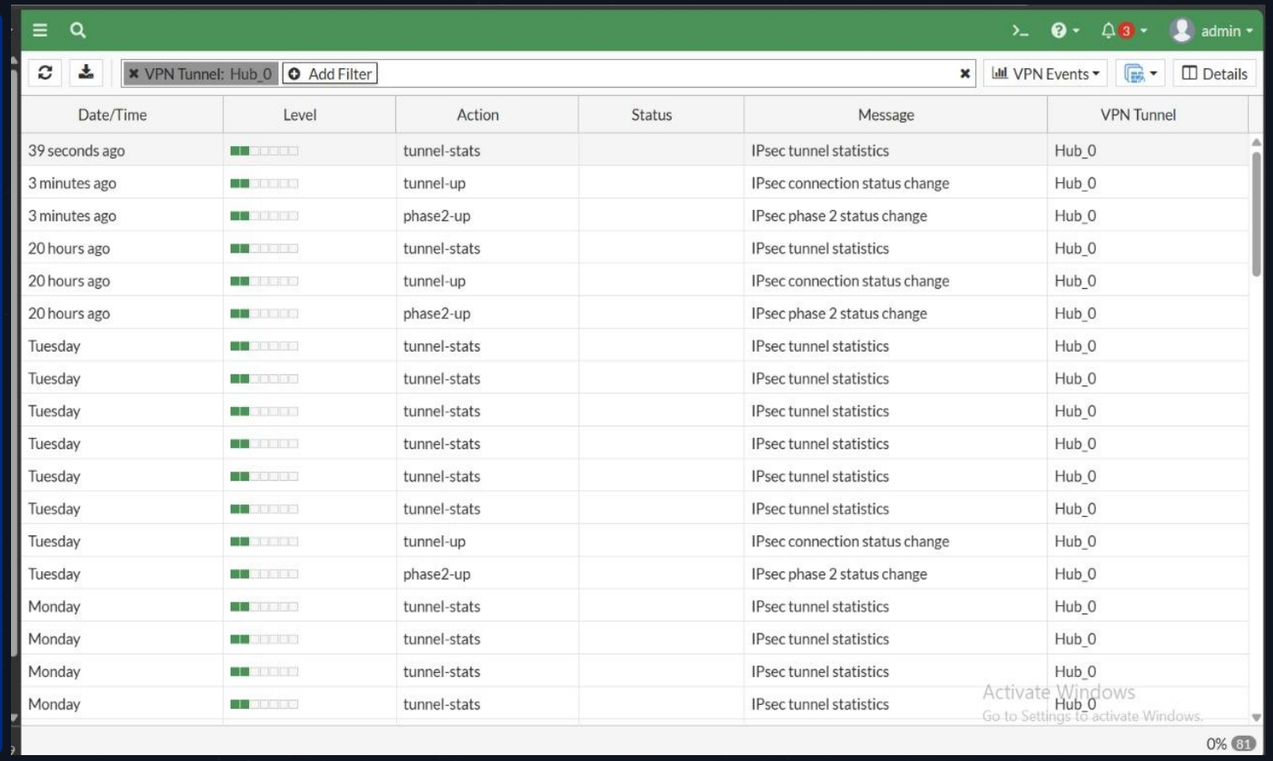
Testing and Verification



Capturing a traffic between PC-1 and PC-3 Using WireShark

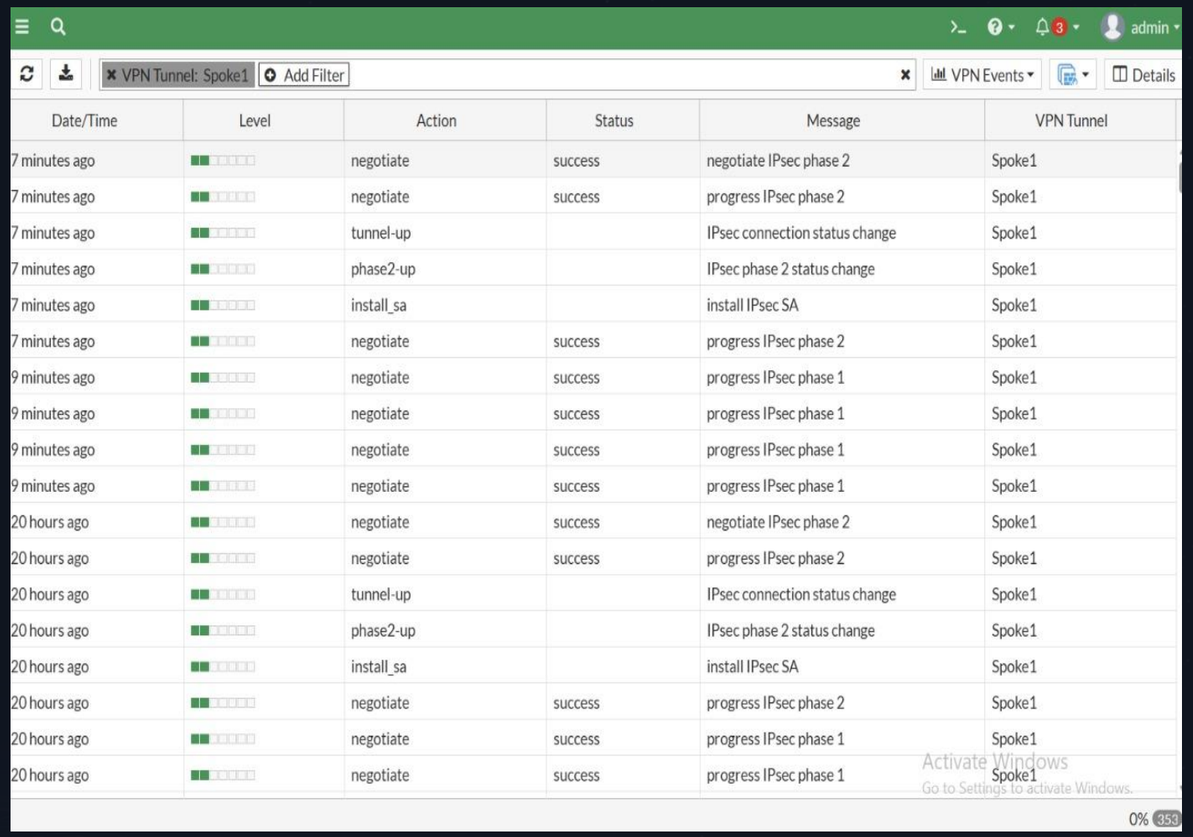
Logs and Events

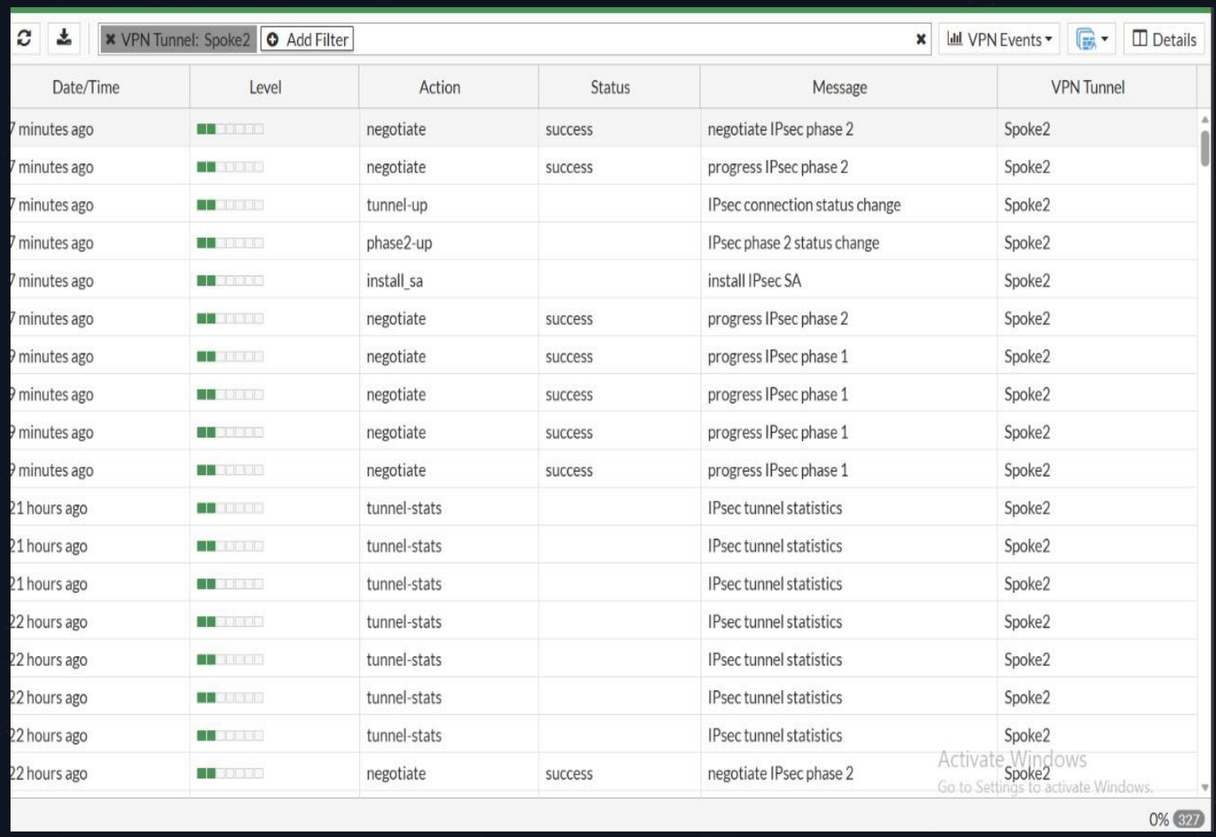




IPsec Logs on Hub

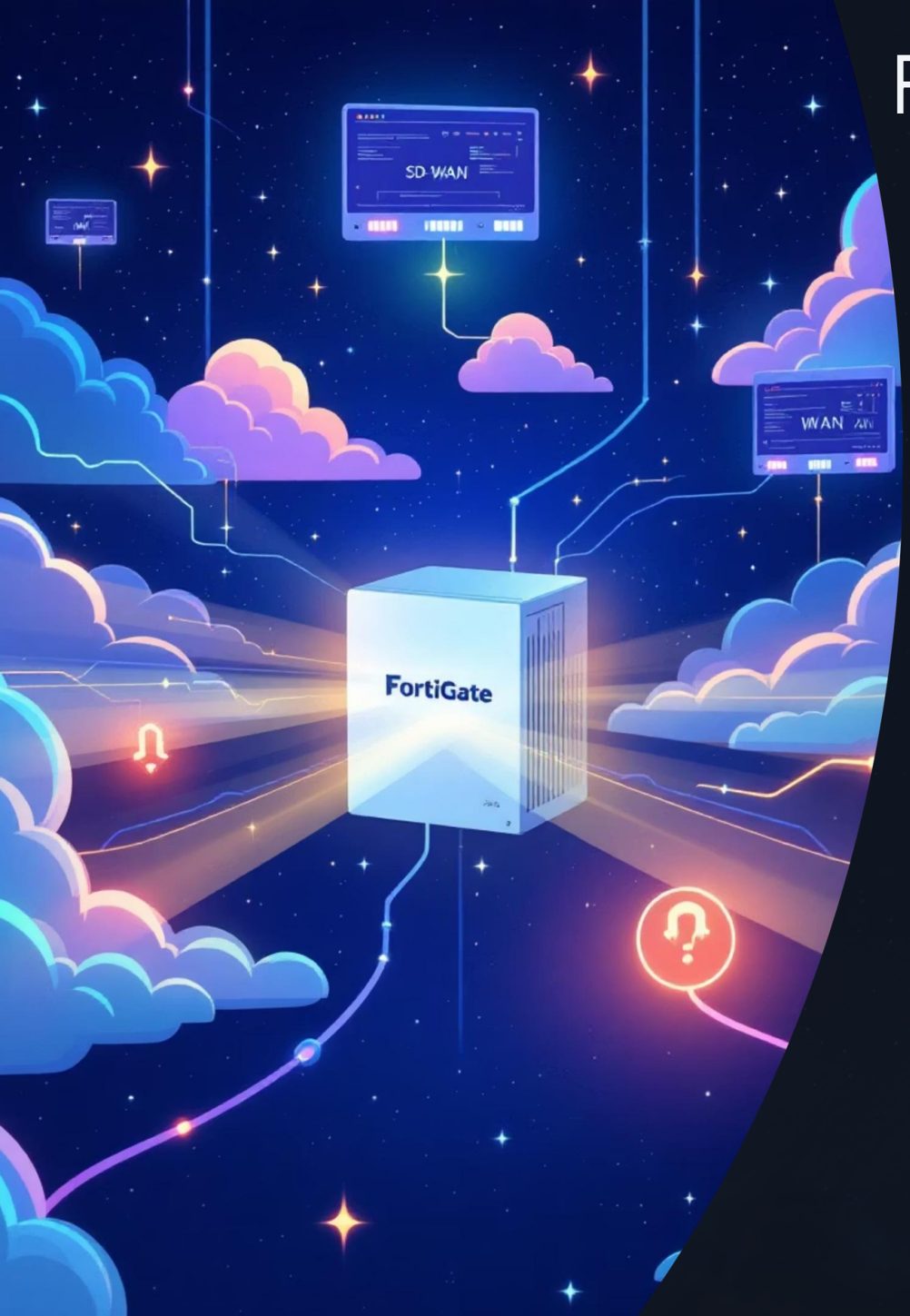
Logs and Events





IPsec Logs on Spoke 1

IPsec Logs on Spoke 2

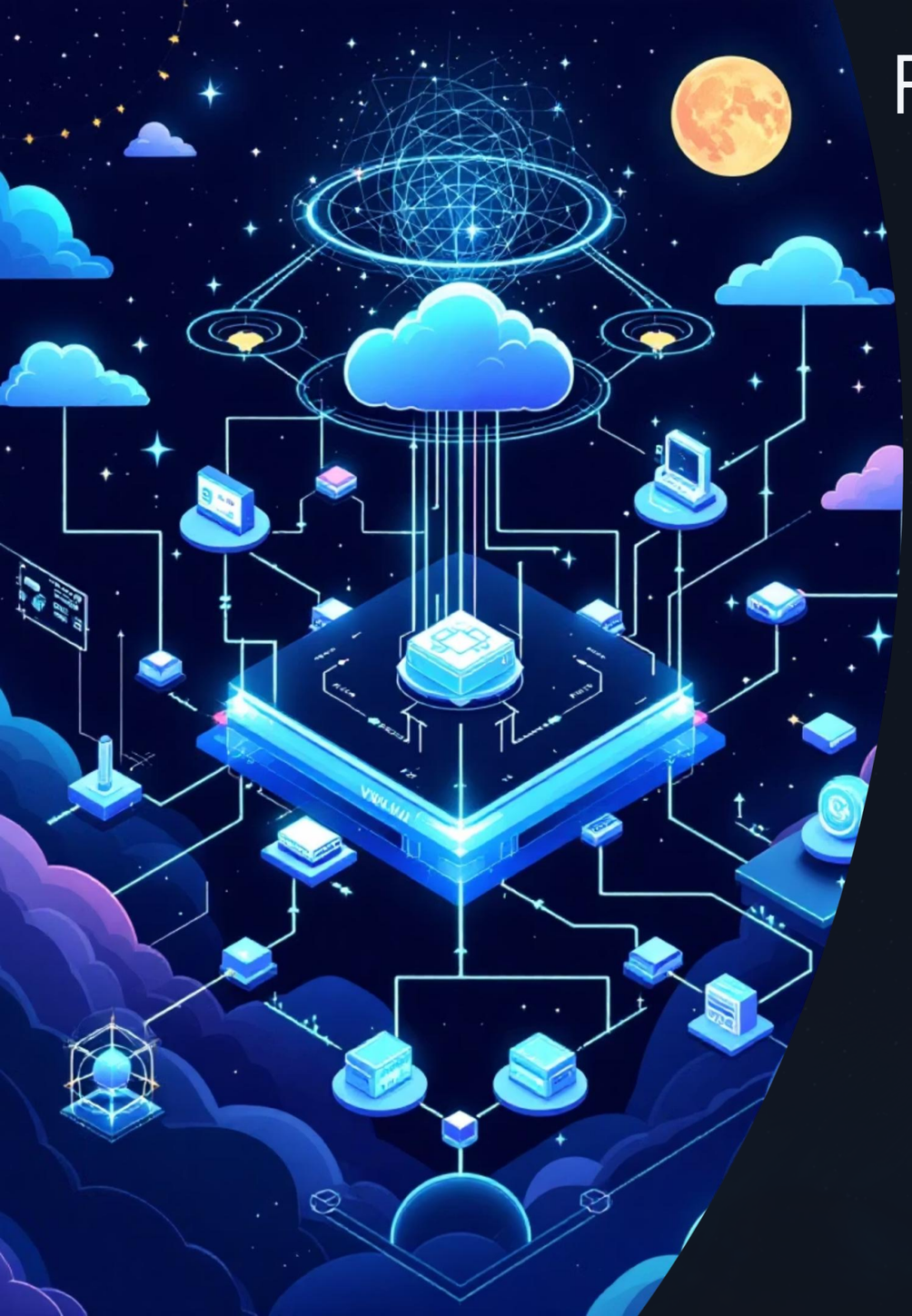


FortiGate VPN with SD-WAN Integration

Over View :

- SD-WAN (Software-Defined Wide Area Network) 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.

- This integration optimizes network efficiency, reduces latency, and ensures high availability for critical applications, making it a powerful solution for modern enterprise networking.



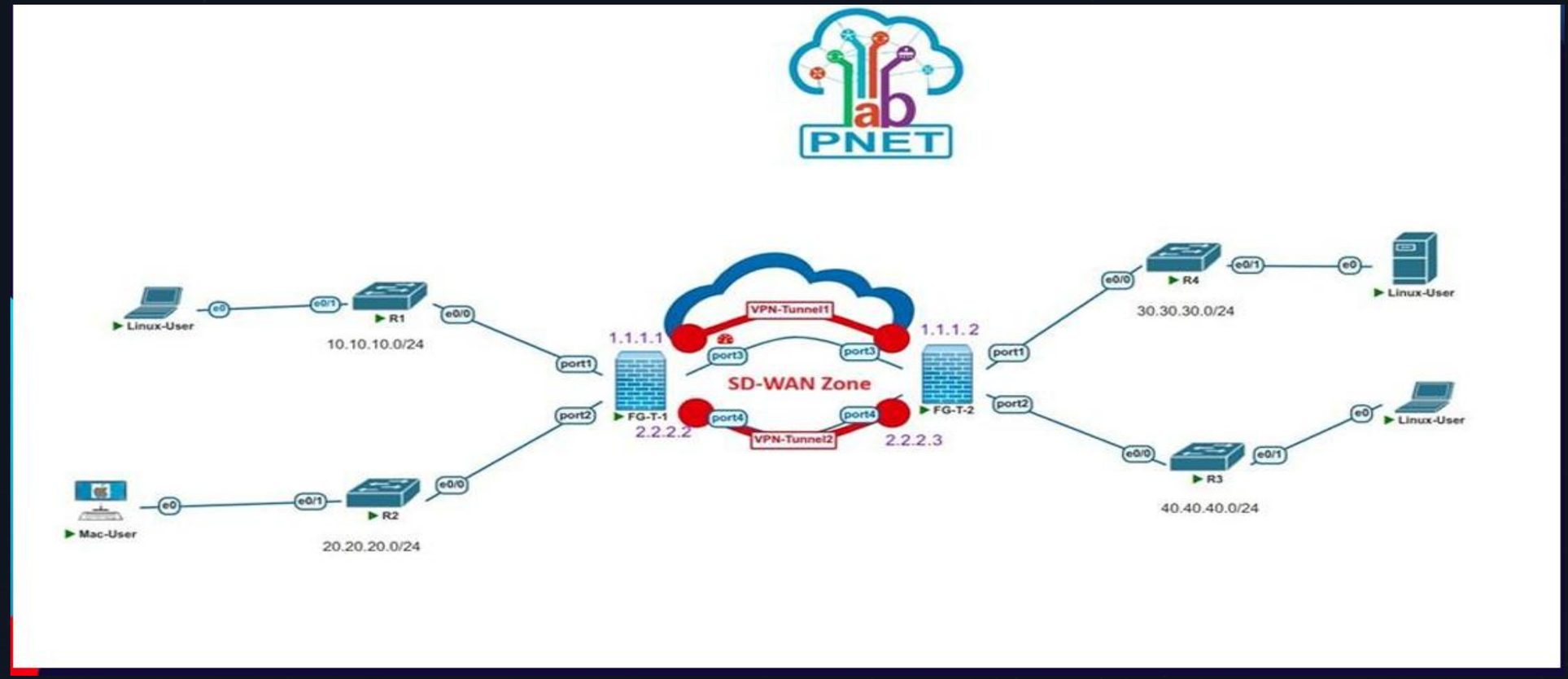
FortiGate VPN with SD-WAN Integration

How SD-WAN Works :

- SD-WAN creates 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.

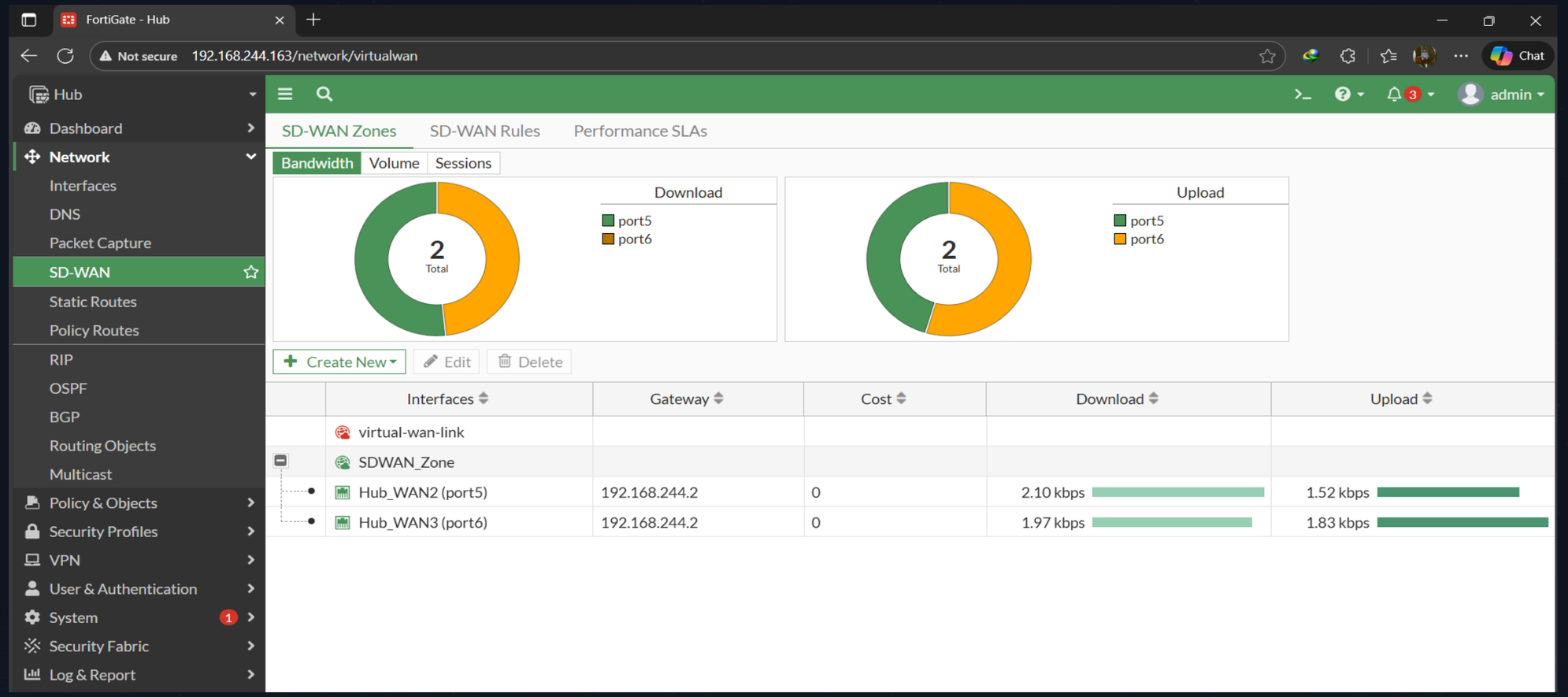
- This intelligent routing ensures that applications receive the necessary bandwidth and performance, adapting to network conditions in real-time. It provides a flexible, cost-effective, and high-performing solution for distributed organizations.

SD-WAN Configuration on FortiGate



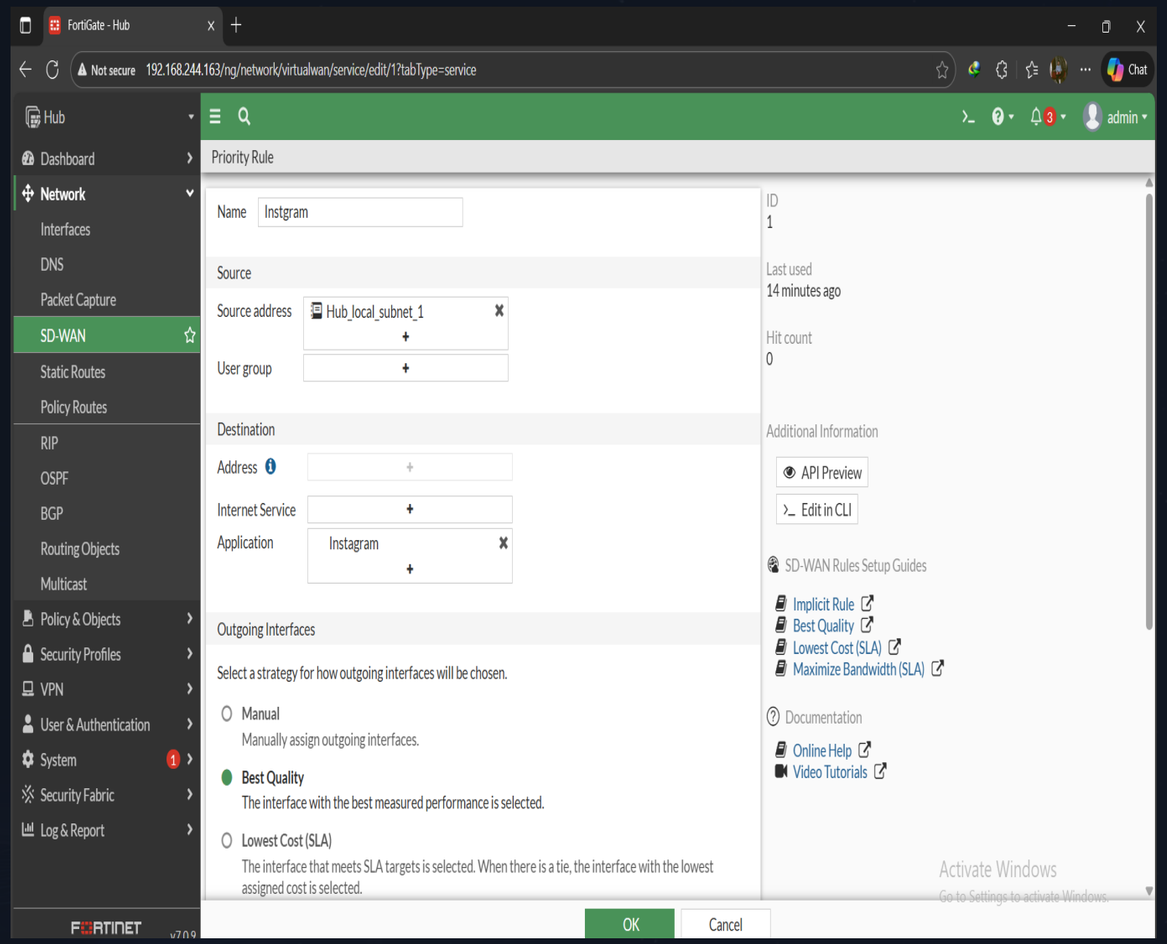
VPN with SD-WAN Integration Topolgy

SD-WAN Configuration on FortiGate

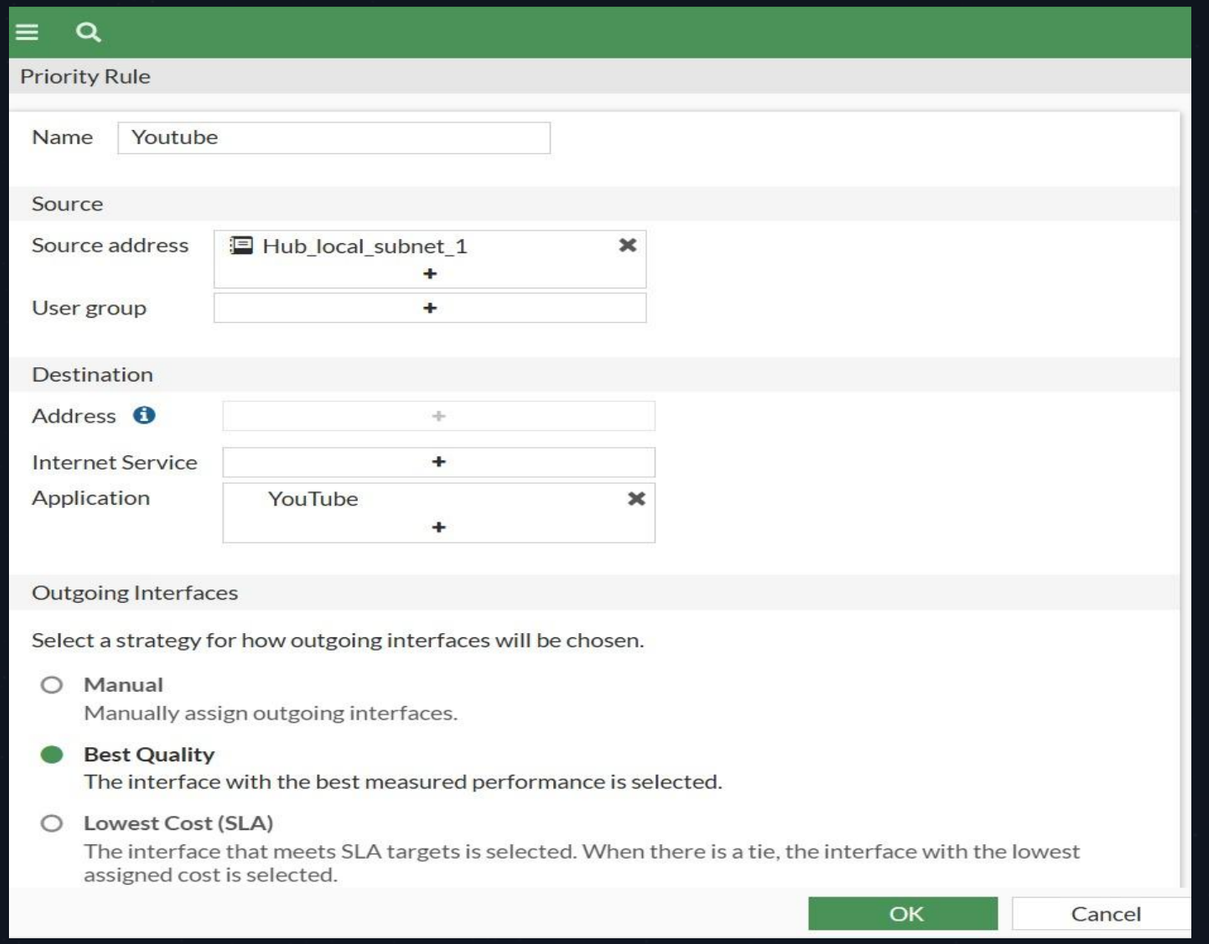


SD-WAN Zones and members

SD-WAN Configuration on FortiGate



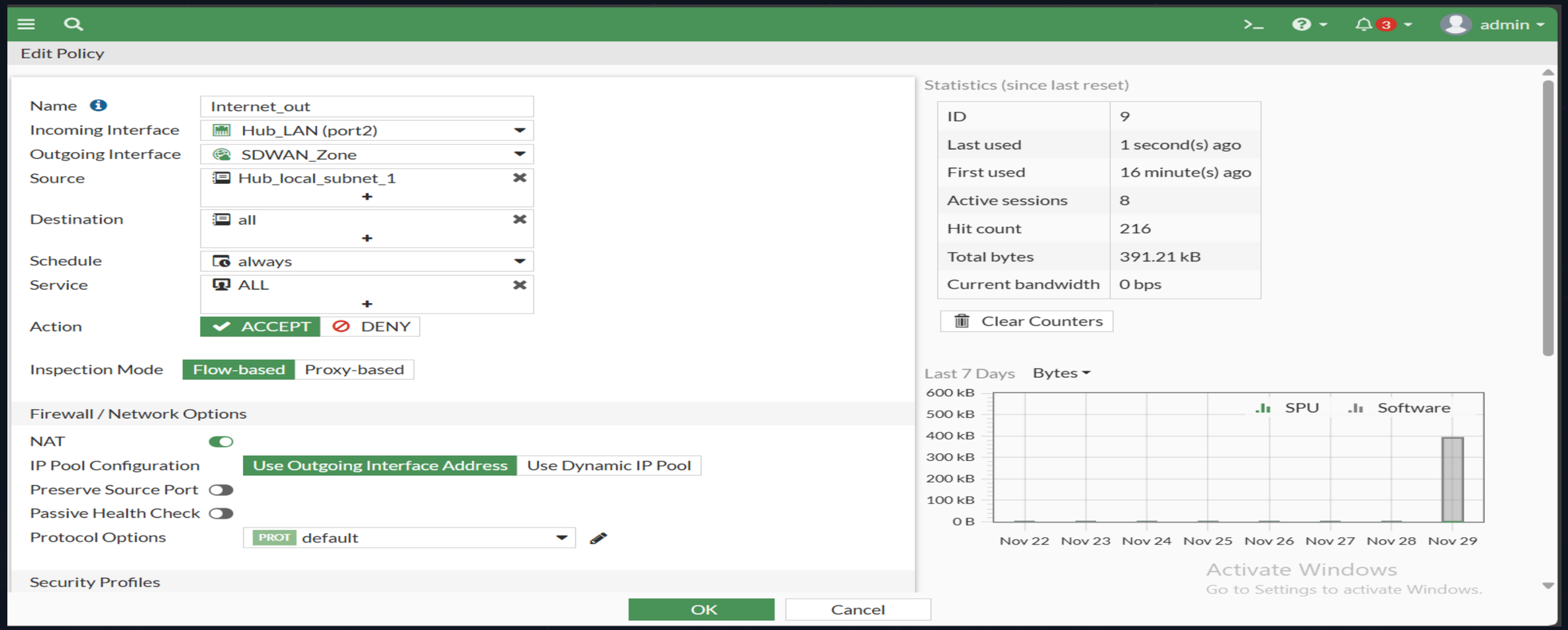
Instgram



Youtube

SD-WAN Rules

SD-WAN Configuration on FortiGate



SD-WAN Policy

SD-WAN Configuration on FortiGate

admin

Policy UUID: 9c19f6a0-cc7b-51f0-bb2f-4e996c987b17 | Add Filter | Details

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
Minute ago	20.0.0.10		40.69.42.241 (fe3.delivery.mp.microsoft.com)		384 B / 1.34 kB	Internet_out (9)
Minute ago	20.0.0.10		8.8.8.8		75 B / 216 B	Internet_out (9)
Minute ago	20.0.0.10		40.69.42.241 (fe3.delivery.mp.microsoft.com)		18.33 kB / 27.19 kB	Internet_out (9)
2 minutes ago	20.0.0.10		52.178.17.234 (v10.events.data.microsoft.com)			Internet_out (9)
2 minutes ago	20.0.0.10		8.8.8.8		75 B / 215 B	Internet_out (9)
2 minutes ago	20.0.0.10		8.8.8.8		75 B / 145 B	Internet_out (9)
3 minutes ago	20.0.0.10		40.69.42.241 (fe3.delivery.mp.microsoft.com)		18.21 kB / 27.11 kB	Internet_out (9)
3 minutes ago	20.0.0.10		52.178.17.234 (v10.events.data.microsoft.com)			Internet_out (9)
4 minutes ago	20.0.0.10		13.89.179.8 (v10.events.data.microsoft.com)			Internet_out (9)
5 minutes ago	20.0.0.10		8.8.8.8		62 B / 157 B	Internet_out (9)
5 minutes ago	20.0.0.10		8.8.8.8		70 B / 154 B	Internet_out (9)
5 minutes ago	20.0.0.10		134.33.185.99 (fe2.update.microsoft.com)			Internet_out (9)
6 minutes ago	20.0.0.10		134.33.185.99 (fe2.update.microsoft.com)		35.55 kB / 19.08 kB	Internet_out (9)
7 minutes ago	20.0.0.10		8.8.8.8		62 B / 157 B	Internet_out (9)
8 minutes ago	20.0.0.10		8.8.8.8		70 B / 154 B	Internet_out (9)
8 minutes ago	20.0.0.10		8.8.8.8		75 B / 212 B	Internet_out (9)
8 minutes ago	20.0.0.10		8.8.8.8		62 B / 157 B	Internet_out (9)
8 minutes ago	20.0.0.10		134.33.4.20 (fe2.update.microsoft.com)		35.75 kB / 27.00 kB	Internet_out (9)

0% 721

FortiGate - Hub

Not secure 192.168.244.163/ng/log/view/traffic/forward?filter=poluuid%3D*"9c19f6a0-cc7b-51f0-bb2f-4e996c987b17"

Summarize | Chat

Hub

- Dashboard
- Network
- Policy & Objects
- Security Profiles
- VPN

admin

Policy UUID: 9c19f6a0-cc7b-51f0-bb2f-4e996c987b17 | Add Filter | Details

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
32 seconds ago	20.0.0.10		102.132.97.18 (instgram.com)		240 B / 240 B	Internet_out (9)
46 seconds ago	20.0.0.10		142.250.200.238 (youtube.com)		240 B / 240 B	Internet_out (9)

SD-WAN Logs

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 connectivity for modern networks.

Secure Implementation

Successfully deployed FortiGate firewall solutions with comprehensive VPN configurations

Enhanced Connectivity

Established reliable and encrypted connections across distributed networks

Project Success

Achieved all objectives in exploring VPN security techniques, protocols, and attack mitigation

Thank You