

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

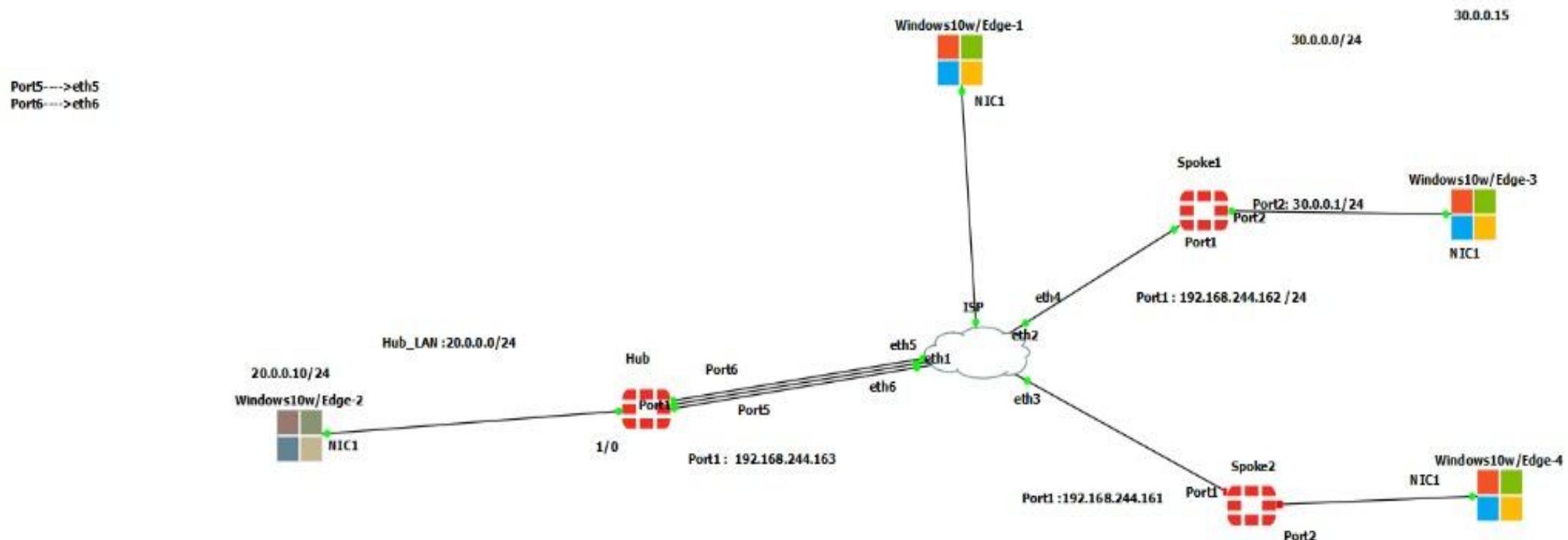
Yazan Abdelfatah Shehata Kholief

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 (Multitprotocol Label Switching VPN)

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

I2TP / 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

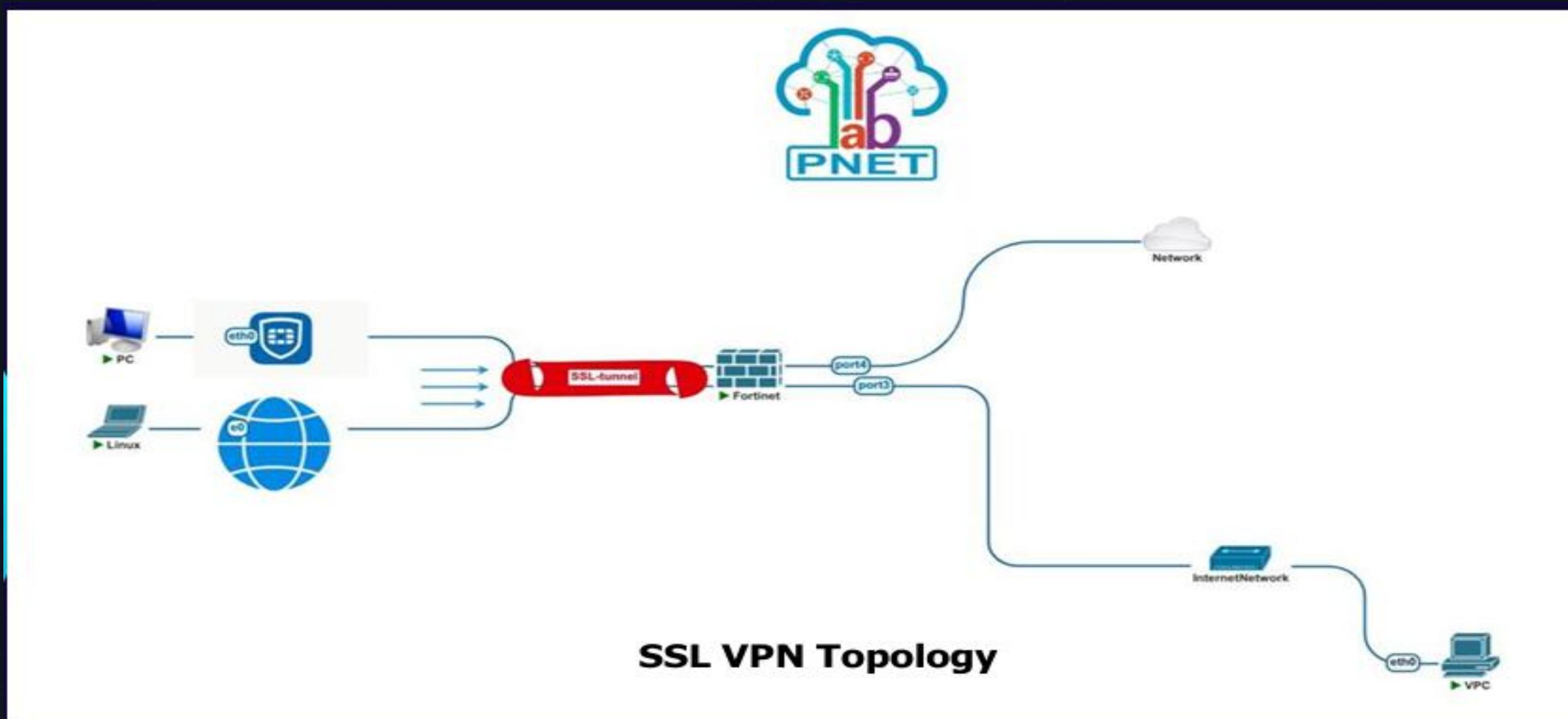
- Access through a web portal.
- Users log in via a browser to access specific applications (email, file servers, web tools).
- Suitable for simple, controlled access without installing a VPN client.

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 Settings

Connection Settings ⓘ

Enable SSL-VPN

Listen on Interface(s)

Hub_WAN (port1)

443

⚠ Port conflicts with the administrative HTTPS port for this system

Listen on Port

ⓘ Web mode access will be listening at <https://192.168.244.163:443>

Server Certificate

Fortinet_Factory

ⓘ 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.
[Create Certificate](#)

Redirect HTTP to SSL-VPN

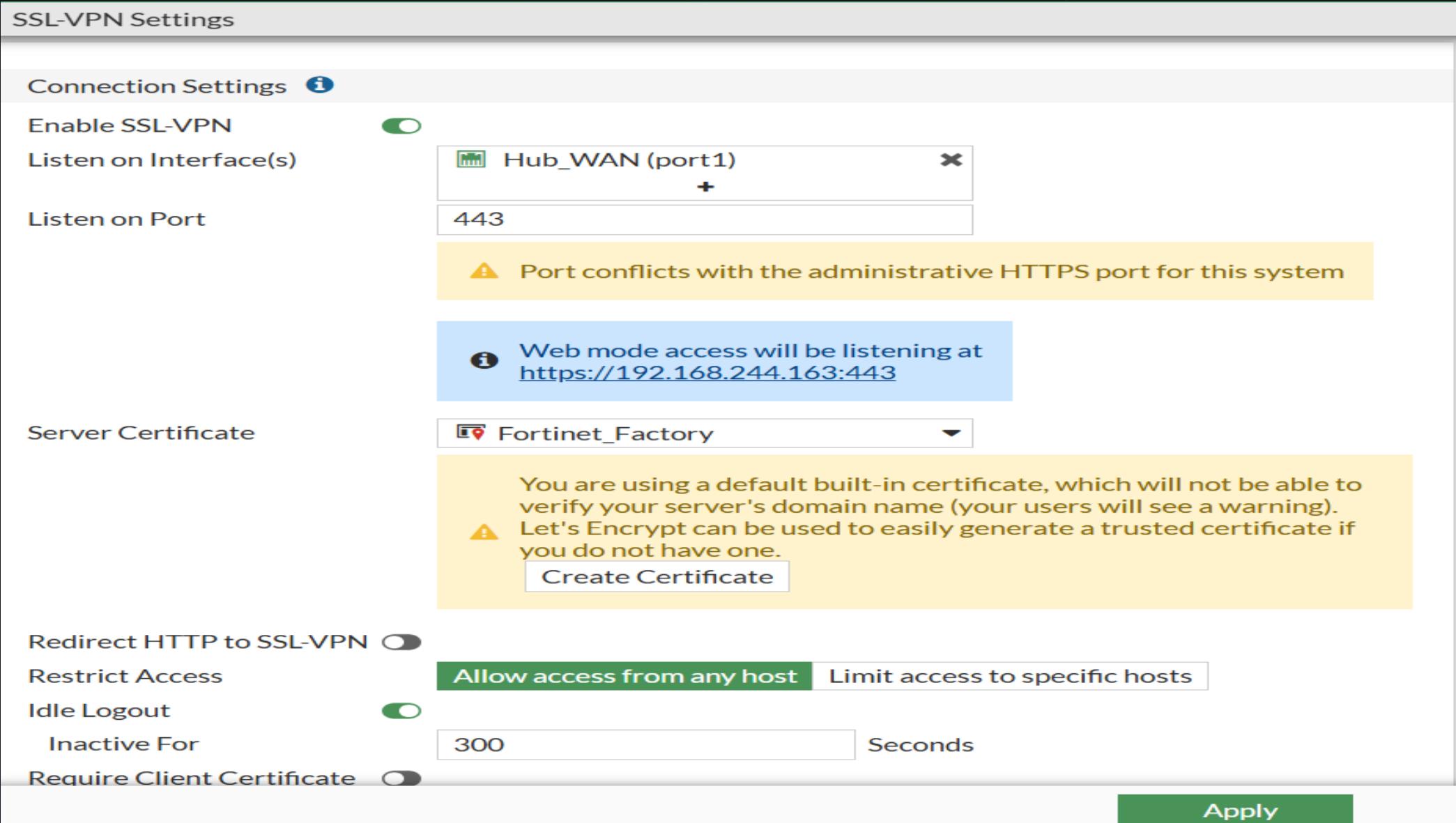
Restrict Access Allow access from any host Limit access to specific hosts

Idle Logout

Inactive For Seconds

Require Client Certificate

Apply



SSL-VPN Setting Configuration

SSL VPN Configuration on FortiGate

The screenshot shows the 'Edit SSL-VPN Portal' configuration page. The 'Name' field is set to 'Tunnel_Mode'. The 'Limit Users to One SSL-VPN Connection at a Time' toggle switch is turned off. Under 'Tunnel Mode', the 'Tunnel Mode' radio button is selected. The 'Split tunneling' section contains three options: 'Disabled' (client traffic over SSL-VPN), 'Enabled Based on Policy Destination' (client traffic matches policy), and 'Enabled for Trusted Destinations' (client traffic from trusted destinations). The 'Routing Address Override' and 'Source IP Pools' fields are empty. In the 'Tunnel Mode Client Options' section, four checkboxes are present: 'Allow client to save password' (unchecked), 'Allow client to connect automatically' (unchecked), 'Allow client to keep connections alive' (unchecked), and 'DNS Split Tunneling' (unchecked). At the bottom, there are 'OK' and 'Cancel' buttons.

FortiGate
Hub

Edit SSL-VPN Portal

Name

Limit Users to One SSL-VPN Connection at a Time

Tunnel Mode

Split tunneling

Disabled
All client traffic will be directed over the SSL-VPN tunnel.

Enabled Based on Policy Destination
Only client traffic in which the destination matches the destination of the configured firewall policies will be directed over the SSL-VPN tunnel.

Enabled for Trusted Destinations
Only client traffic which does not match explicitly trusted destinations will be directed over the SSL-VPN tunnel.

Routing Address Override

Source IP Pools

Tunnel Mode Client Options

Allow client to save password

Allow client to connect automatically

Allow client to keep connections alive

DNS Split Tunneling

Host Check

OK Cancel

Additional Information

API Preview

References

Edit in CLI

Documentation

Online Help Video Tutorials

SSL-VPN Portal Configuration

SSL VPN Configuration on FortiGate

Edit Policy

Name	VPN
Incoming Interface	SSL-VPN tunnel interface (ssl.root)
Outgoing Interface	Hub_LAN (port2)
Source	VPN_Full_tunnel HR
Destination	Hub_local_subnet_1
Schedule	always
Service	ALL
Action	<input checked="" type="button"/> ACCEPT <input type="button"/> DENY
Inspection Mode	<input checked="" type="radio"/> Flow-based <input type="radio"/> Proxy-based
Firewall / Network Options	
NAT	<input type="checkbox"/>
Protocol Options	PROT default
Security Profiles	
AntiVirus	<input type="checkbox"/>
Web Filter	<input type="checkbox"/>
<input type="button"/> OK <input type="button"/> Cancel	

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

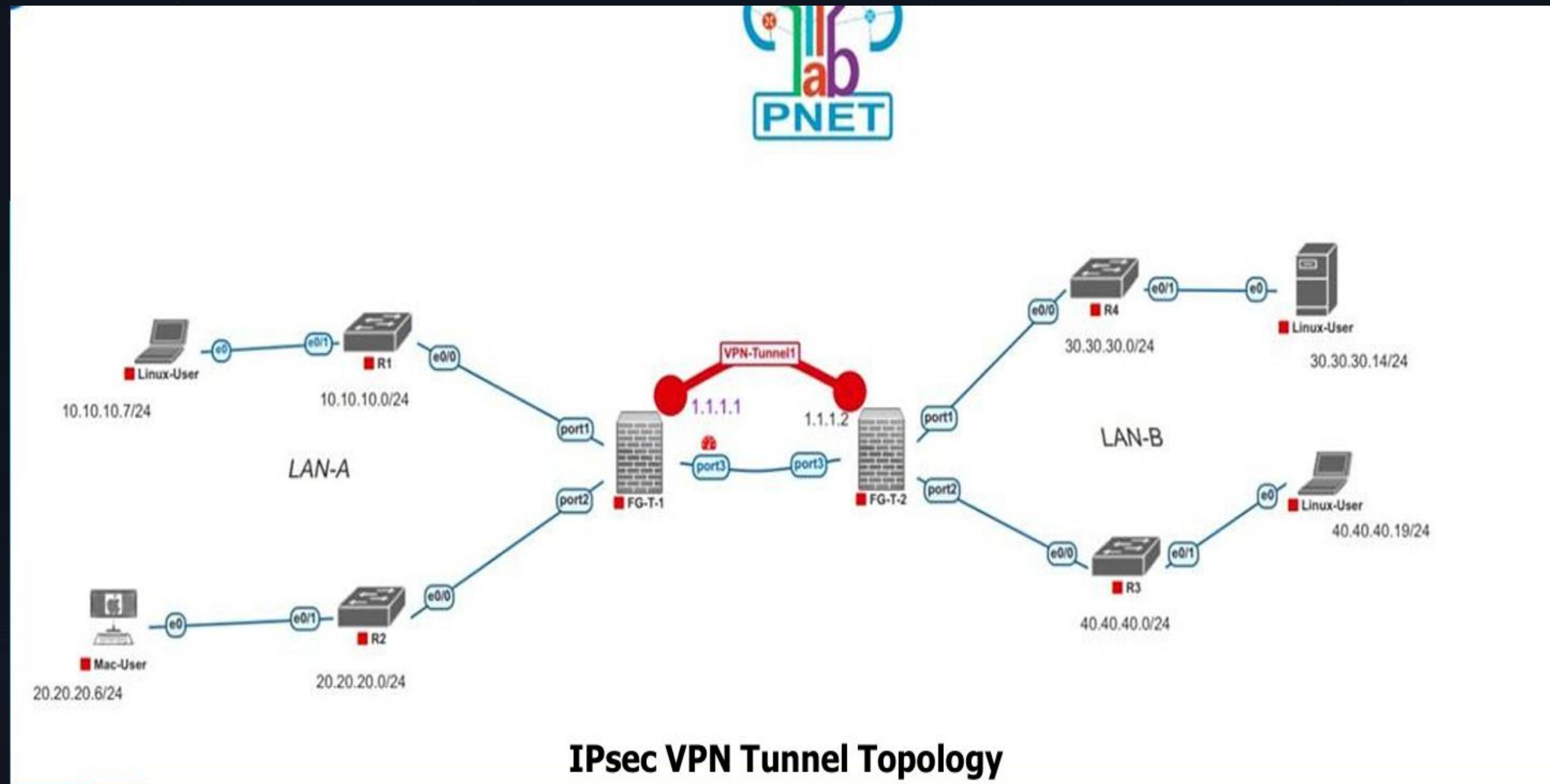
- Establishes a secure communication channel
- Authenticates Two VPN peers
- Negotiates encryption/hashing algorithms (e.g., AES, SHA).



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 Configuration Steps on FortiGate

Edit VPN Tunnel

Tunnel Template: Hub-and-Spoke - FortiGate (Hub)

Name: Hub

Comments: VPN: Hub (Created by VPN wizard) 32/255

Network (Edit): Outgoing Interface : port1

Authentication (Edit): Authentication Method : Pre-shared Key

Phase 2 Selectors

	Local Address	Remote Address	
Hub	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	(Edit)

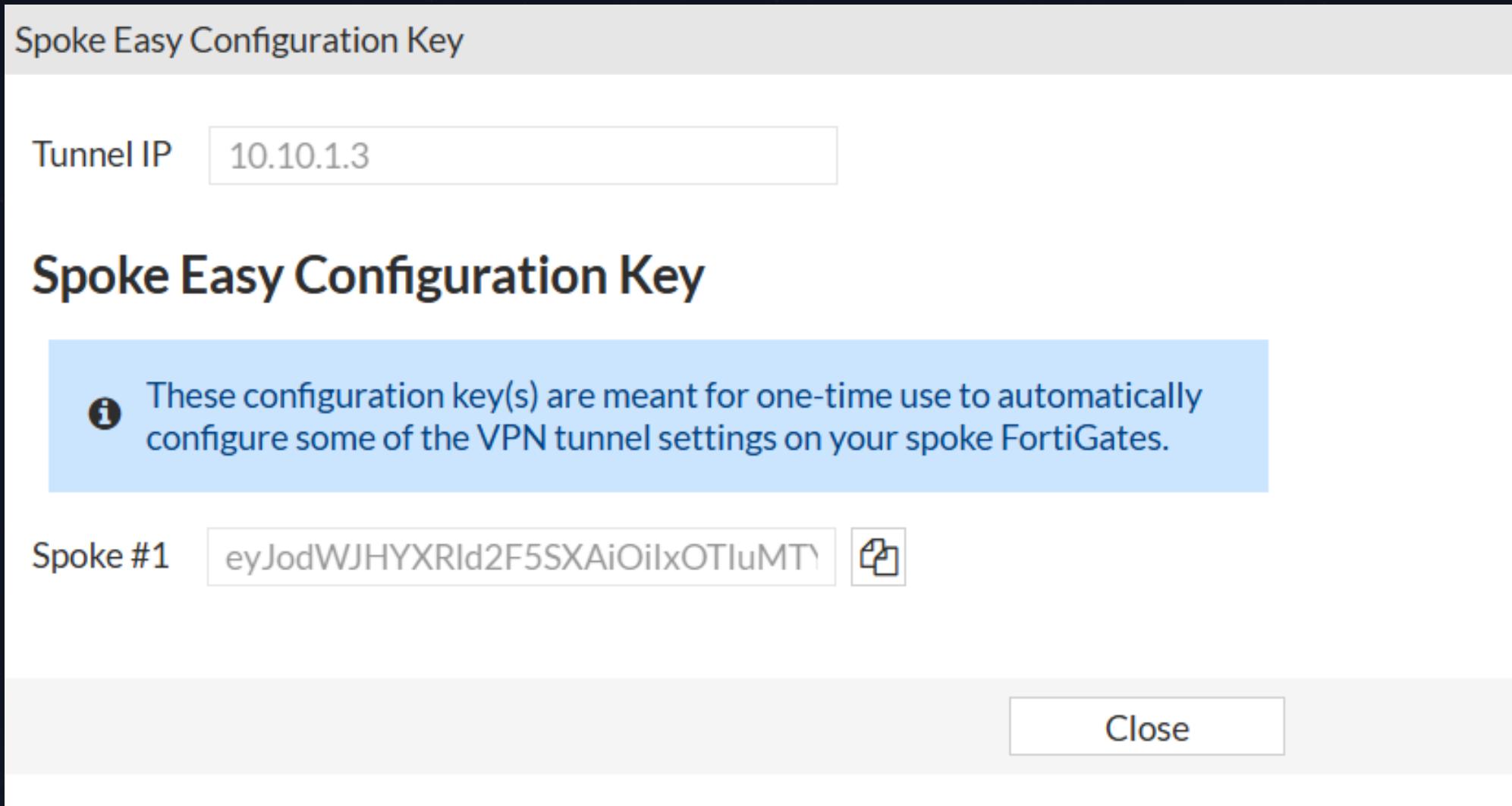
Hub & Spoke Topology

Number	Tunnel IP	AS	Configure Key
1	10.10.1.3	65400	<button>View</button> <button>(Edit)</button> <button>(Delete)</button>
2	10.10.1.4	65400	<button>View</button> <button>(Edit)</button> <button>(Delete)</button>

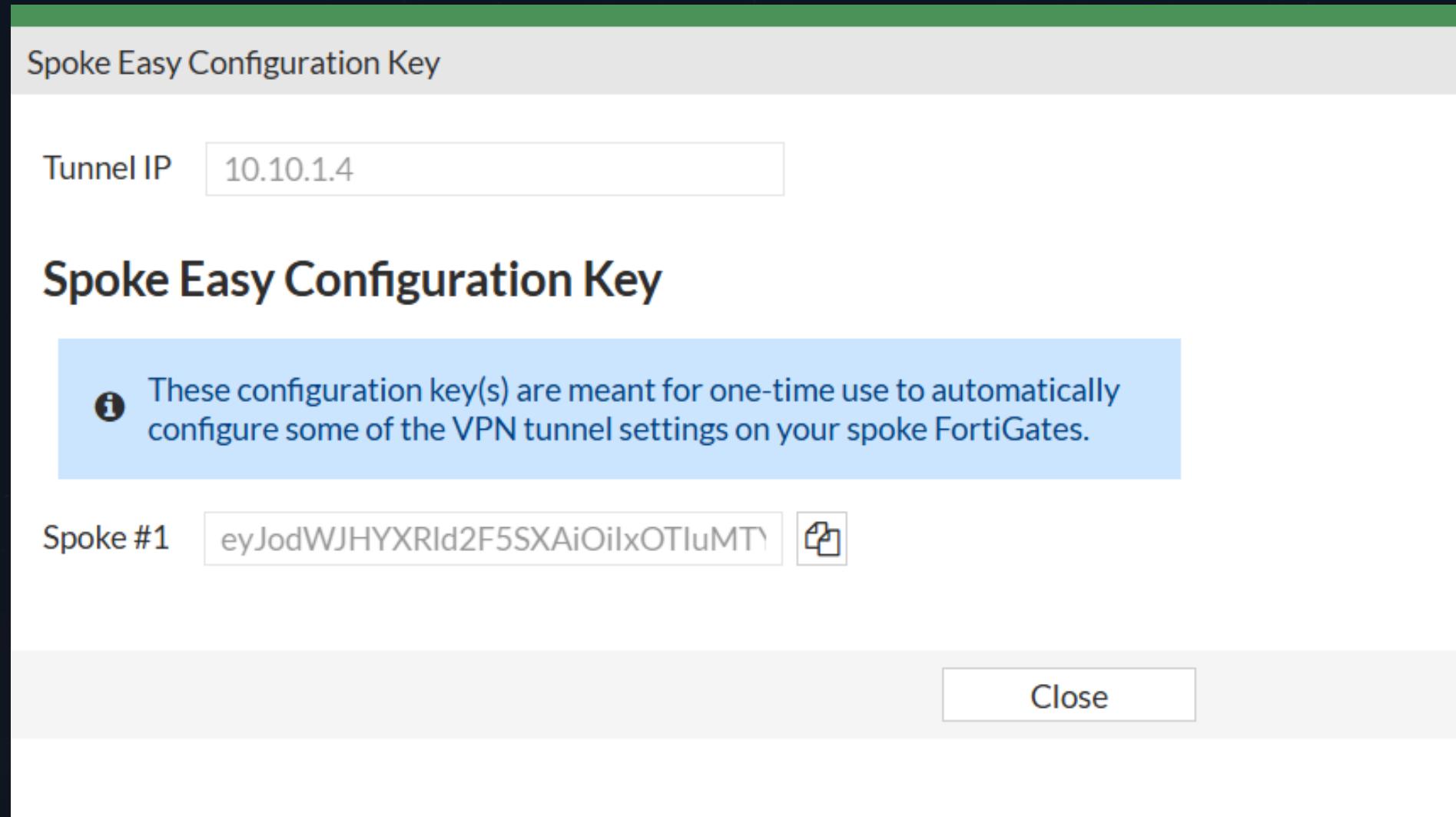
Prefix **Neighbor Group** **Configure Key** **Add**

OK **Cancel**

IPsec Configuration Steps on FortiGate



IPsec Configuration Steps on FortiGate



IPsec Configuration Steps on FortiGate

The screenshot shows the FortiGate management interface with three tabs open: FortiGate - Hub, FortiGate - Spoke1, and FortiGate - Spoke2. The main dashboard has a green header bar with a search icon and an 'Add Widget' button. The left sidebar is titled 'Hub' and includes sections for Dashboard, Status, Security, Network (which is selected), and Users & Devices. The Network section contains a table for IPsec connections.

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Hub-and-Spoke - FortiGate (Hub) 2	192.168.244.162	Hub_0	1.78 kB	2.45 kB	Hub_0	Hub
	192.168.244.161	Hub_1	452 B	614 B	Hub_1	Hub

Connection on Hubs

IPsec Configuration Steps on FortiGate

The screenshot shows the FortiGate web interface with three tabs at the top: "FortiGate - Hub", "FortiGate - Spoke1" (selected), and "FortiGate - Spoke2". The main content area has a green header bar with a search icon and a "Dashboard" section. Below it, a "Network" section is selected in the sidebar. The main pane displays the "IPsec" configuration for "Hub-and-Spoke - FortiGate (Spoke) 1". The table shows the following data:

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Spoke1	192.168.244.163		2.08 kB	1.41 kB	Spoke1	Spoke1

Spoke 1

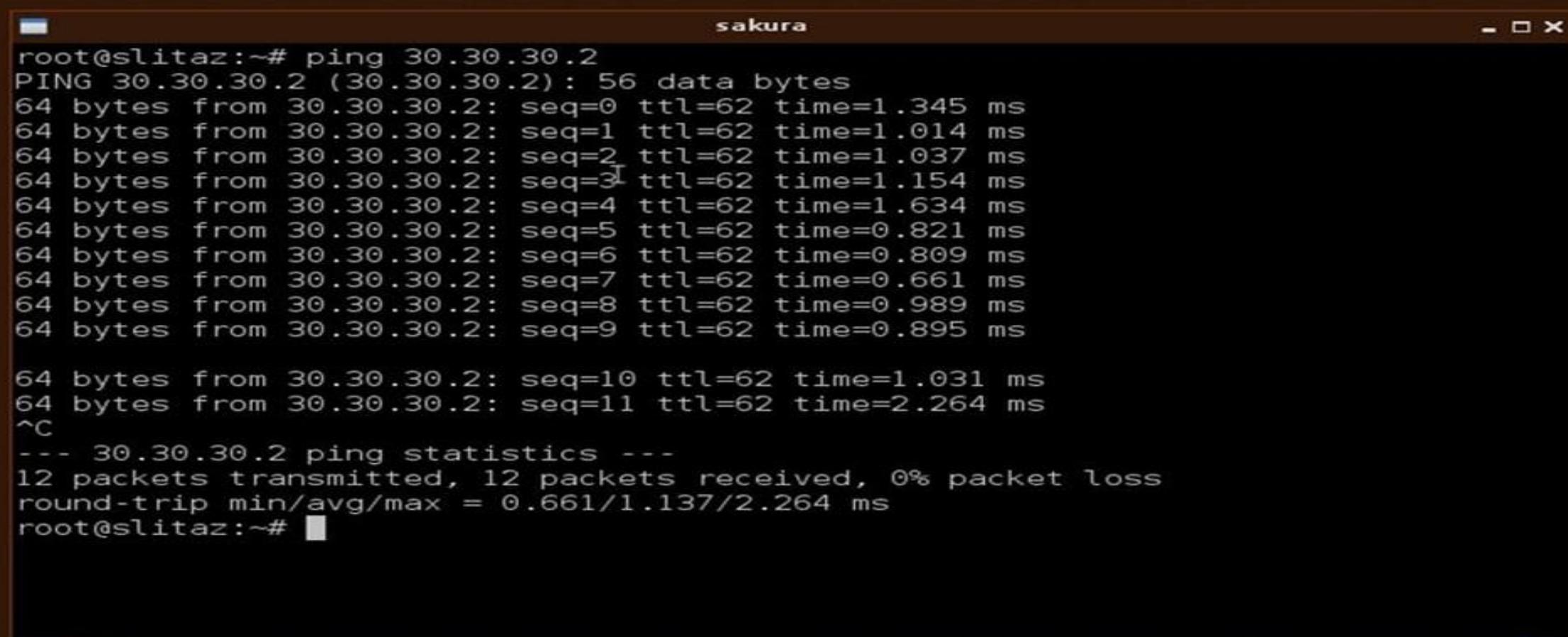
IPsec Configuration Steps on FortiGate

The screenshot shows the FortiGate web interface with three tabs at the top: "FortiGate - Hub", "FortiGate - Spoke1", and "FortiGate - Spoke2". The "FortiGate - Spoke2" tab is active. The left sidebar has a dropdown for "Spoke2" and sections for "Dashboard", "Status", "Security", "Network" (which is selected and highlighted in green), "Users & Devices", "FortiView Sources", "FortiView Destinations", "FortiView Applications", and "FortiView Web Sites". The main content area is titled "IPsec" and displays a table with one row. The table columns are: Name, Remote Gateway, Peer ID, Incoming Data, Outgoing Data, Phase 1, and Phase 2 Selectors. The single entry is "Hub and Spoke - FortiGate (Spoke) 1" with the following details: Spoke2, 192.168.244.163, empty, 912 B, 798 B, empty, and two "Spoke2" entries under Phase 2 Selectors.

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
Hub and Spoke - FortiGate (Spoke) 1	Spoke2	192.168.244.163	912 B	798 B		Spoke2 Spoke2

Spoke 2

Testing and Verification



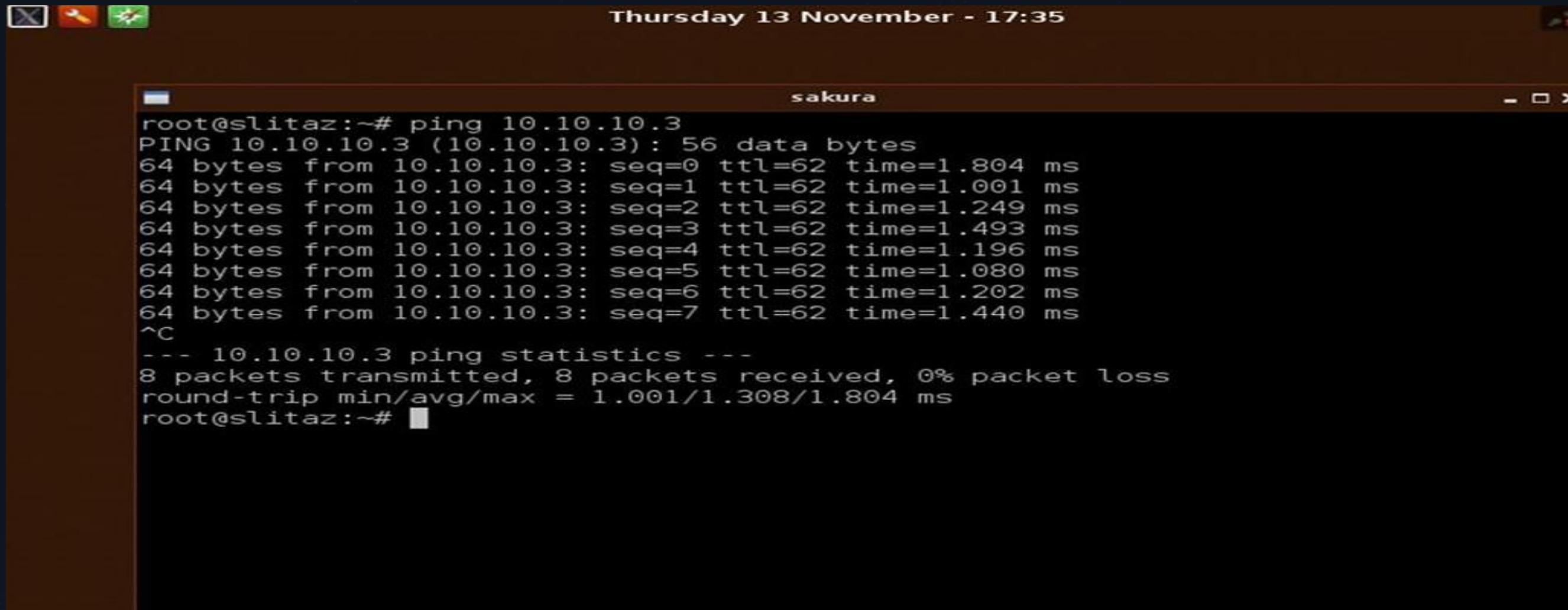
The screenshot shows a terminal window titled "sakura". The terminal output is as follows:

```
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

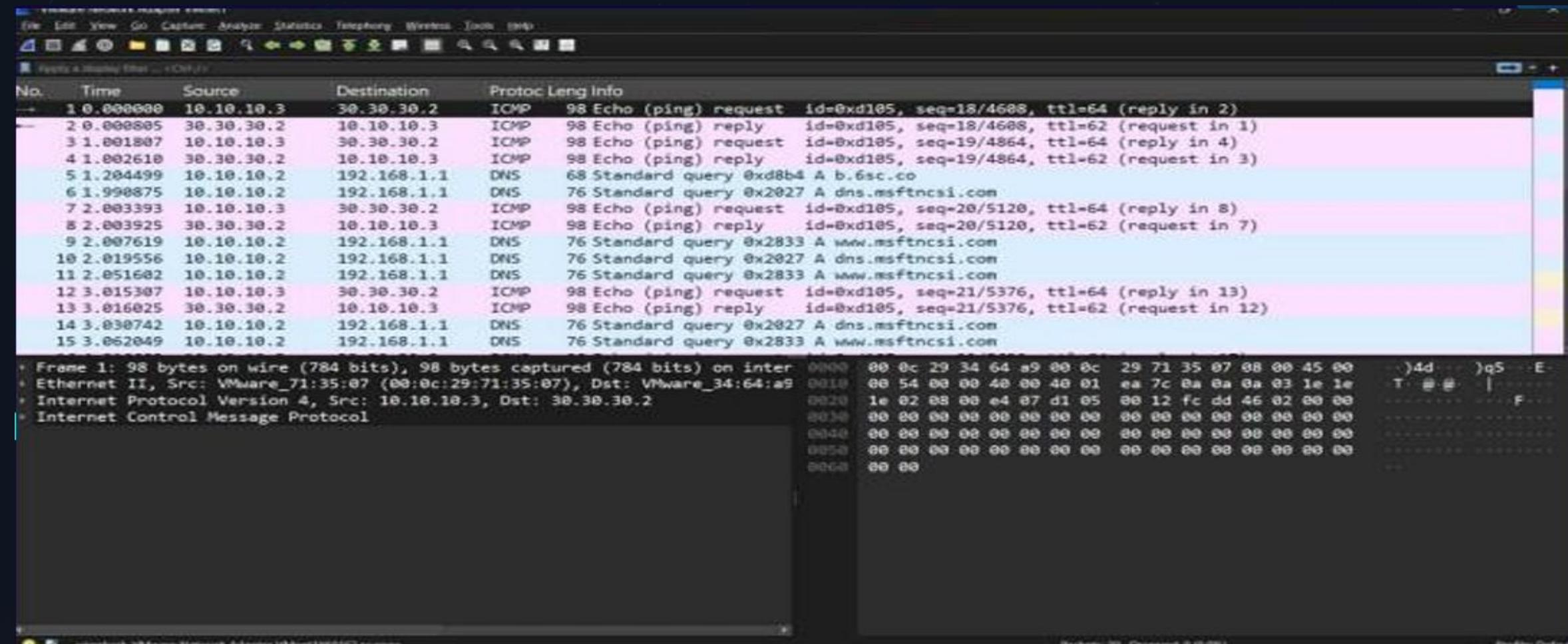


The screenshot shows a terminal window titled "sakura" running on a Linux system. The terminal displays the output of a "ping" command. The command "ping 10.10.10.3" was run from the root prompt "root@slitaz:~#". The output shows 8 packets transmitted, 8 packets received, and 0% packet loss. The round-trip time statistics are listed as min/avg/max = 1.001/1.308/1.804 ms.

```
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:~#
```

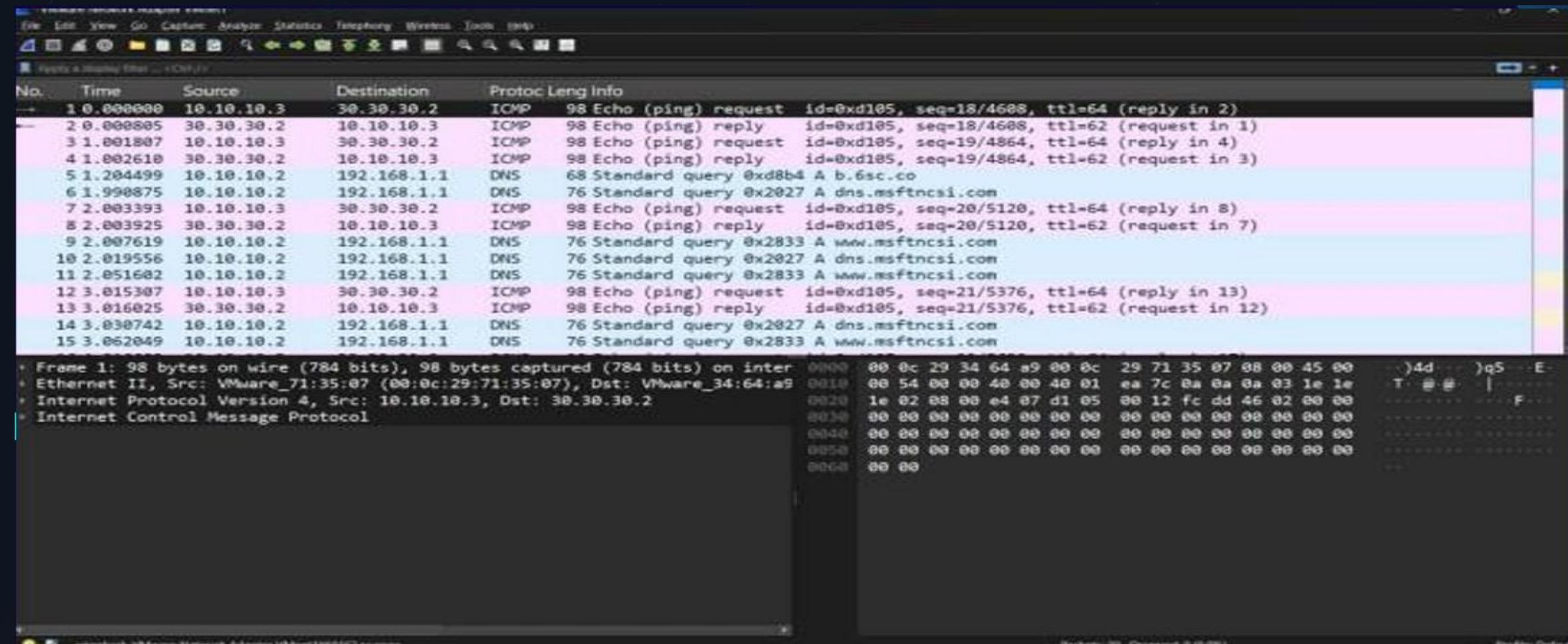
Ping Test: ping from PC-3 To PC-1

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

The image displays two separate log entries from a management interface, each showing a list of events for a specific VPN tunnel. The left window is titled "VPN Tunnel: Hub_1" and the right window is titled "VPN Tunnel: Hub_0". Both windows have a header with "Date/Time", "Level", "Action", "Status", "Message", and "VPN Tunnel" columns. The logs show various IPsec events such as "tunnel-stats", "tunnel-up", and "phase2-up". The "Hub_1" log has 20 entries, and the "Hub_0" log has 18 entries. A watermark for "Activate Windows" is visible at the bottom of both windows.

Date/Time	Level	Action	Status	Message	VPN Tunnel
Minute ago	[green]	tunnel-stats		IPsec tunnel statistics	Hub_1
4 minutes ago	[green]	tunnel-up		IPsec connection status change	Hub_1
4 minutes ago	[green]	phase2-up		IPsec phase 2 status change	Hub_1
20 hours ago	[green]	tunnel-up		IPsec connection status change	Hub_1
20 hours ago	[green]	phase2-up		IPsec phase 2 status change	Hub_1
20 hours ago	[blue]	dpd	dpd_failure	IPsec DPD failure	Hub_1
Tuesday	[green]	tunnel-stats		IPsec tunnel statistics	Hub_1
Tuesday	[green]	tunnel-stats		IPsec tunnel statistics	Hub_1
Tuesday	[green]	tunnel-stats		IPsec tunnel statistics	Hub_1
Tuesday	[green]	tunnel-stats		IPsec tunnel statistics	Hub_1
Tuesday	[green]	tunnel-stats		IPsec tunnel statistics	Hub_1
Tuesday	[green]	tunnel-stats		IPsec tunnel statistics	Hub_1
Tuesday	[green]	tunnel-stats		IPsec tunnel statistics	Hub_1
Tuesday	[green]	tunnel-up		IPsec connection status change	Hub_1
Tuesday	[green]	phase2-up		IPsec phase 2 status change	Hub_1
Monday	[green]	tunnel-stats		IPsec tunnel statistics	Hub_1
Monday	[green]	tunnel-stats		IPsec tunnel statistics	Hub_1
Monday	[green]	tunnel-stats		IPsec tunnel statistics	Hub_1
Monday	[green]	tunnel-stats		IPsec tunnel statistics	Hub_1
39 seconds ago	[green]	tunnel-stats		IPsec tunnel statistics	Hub_0
3 minutes ago	[green]	tunnel-up		IPsec connection status change	Hub_0
3 minutes ago	[green]	phase2-up		IPsec phase 2 status change	Hub_0
20 hours ago	[green]	tunnel-stats		IPsec tunnel statistics	Hub_0
20 hours ago	[green]	tunnel-up		IPsec connection status change	Hub_0
20 hours ago	[green]	phase2-up		IPsec phase 2 status change	Hub_0
Tuesday	[green]	tunnel-stats		IPsec tunnel statistics	Hub_0
Tuesday	[green]	tunnel-stats		IPsec tunnel statistics	Hub_0
Tuesday	[green]	tunnel-stats		IPsec tunnel statistics	Hub_0
Tuesday	[green]	tunnel-stats		IPsec tunnel statistics	Hub_0
Tuesday	[green]	tunnel-stats		IPsec tunnel statistics	Hub_0
Tuesday	[green]	tunnel-up		IPsec connection status change	Hub_0
Tuesday	[green]	phase2-up		IPsec phase 2 status change	Hub_0
Monday	[green]	tunnel-stats		IPsec tunnel statistics	Hub_0
Monday	[green]	tunnel-stats		IPsec tunnel statistics	Hub_0
Monday	[green]	tunnel-stats		IPsec tunnel statistics	Hub_0
Monday	[green]	tunnel-stats		IPsec tunnel statistics	Hub_0

IPsec Logs on Hub

Logs and Events

VPN Tunnel: Spoke1

admin

VPN Events Details

Add Filter

Date/Time	Level	Action	Status	Message	VPN Tunnel
7 minutes ago	[green]	negotiate	success	negotiate IPsec phase 2	Spoke1
7 minutes ago	[green]	negotiate	success	progress IPsec phase 2	Spoke1
7 minutes ago	[green]	tunnel-up		IPsec connection status change	Spoke1
7 minutes ago	[green]	phase2-up		IPsec phase 2 status change	Spoke1
7 minutes ago	[green]	install_sa		install IPsec SA	Spoke1
7 minutes ago	[green]	negotiate	success	progress IPsec phase 2	Spoke1
9 minutes ago	[green]	negotiate	success	progress IPsec phase 1	Spoke1
9 minutes ago	[green]	negotiate	success	progress IPsec phase 1	Spoke1
9 minutes ago	[green]	negotiate	success	progress IPsec phase 1	Spoke1
9 minutes ago	[green]	negotiate	success	progress IPsec phase 1	Spoke1
20 hours ago	[green]	negotiate	success	negotiate IPsec phase 2	Spoke1
20 hours ago	[green]	negotiate	success	progress IPsec phase 2	Spoke1
20 hours ago	[green]	tunnel-up		IPsec connection status change	Spoke1
20 hours ago	[green]	phase2-up		IPsec phase 2 status change	Spoke1
20 hours ago	[green]	install_sa		install IPsec SA	Spoke1
20 hours ago	[green]	negotiate	success	progress IPsec phase 2	Spoke1
20 hours ago	[green]	negotiate	success	progress IPsec phase 1	Spoke1
20 hours ago	[green]	negotiate	success	progress IPsec phase 1	Spoke1

VPN Tunnel: Spoke2

admin

VPN Events Details

Add Filter

Date/Time	Level	Action	Status	Message	VPN Tunnel
7 minutes ago	[green]	negotiate	success	negotiate IPsec phase 2	Spoke2
7 minutes ago	[green]	negotiate	success	progress IPsec phase 2	Spoke2
7 minutes ago	[green]	tunnel-up		IPsec connection status change	Spoke2
7 minutes ago	[green]	phase2-up		IPsec phase 2 status change	Spoke2
7 minutes ago	[green]	install_sa		install IPsec SA	Spoke2
7 minutes ago	[green]	negotiate	success	progress IPsec phase 2	Spoke2
9 minutes ago	[green]	negotiate	success	progress IPsec phase 1	Spoke2
9 minutes ago	[green]	negotiate	success	progress IPsec phase 1	Spoke2
9 minutes ago	[green]	negotiate	success	progress IPsec phase 1	Spoke2
9 minutes ago	[green]	negotiate	success	progress IPsec phase 1	Spoke2
21 hours ago	[green]	tunnel-stats		IPsec tunnel statistics	Spoke2
21 hours ago	[green]	tunnel-stats		IPsec tunnel statistics	Spoke2
21 hours ago	[green]	tunnel-stats		IPsec tunnel statistics	Spoke2
22 hours ago	[green]	tunnel-stats		IPsec tunnel statistics	Spoke2
22 hours ago	[green]	tunnel-stats		IPsec tunnel statistics	Spoke2
22 hours ago	[green]	tunnel-stats		IPsec tunnel statistics	Spoke2
22 hours ago	[green]	tunnel-stats		IPsec tunnel statistics	Spoke2
22 hours ago	[green]	negotiate	success	negotiate IPsec phase 2	Spoke2

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.

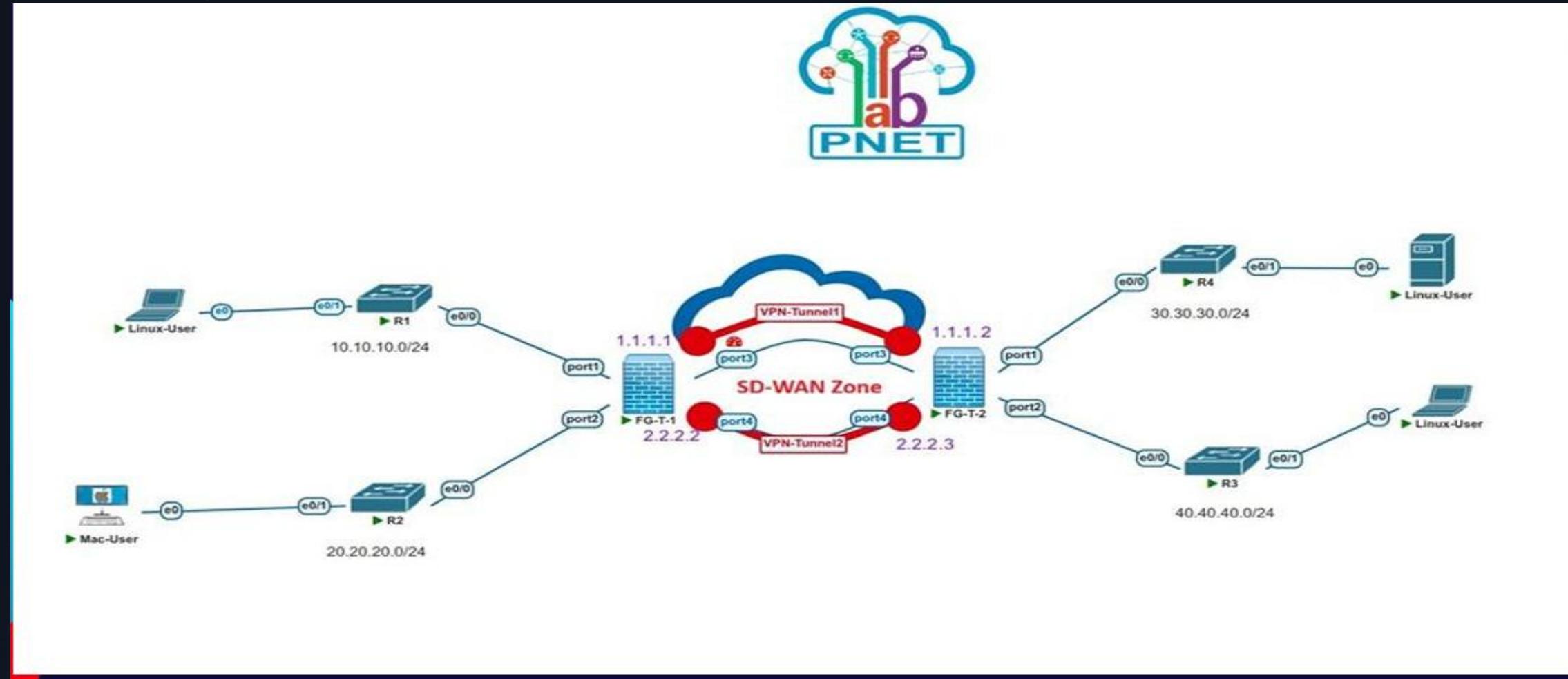
FortiGate VPN with SD-WAN Integration

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

The screenshot shows the FortiGate management interface for SD-WAN configuration. The left sidebar navigation bar includes options like Hub, Dashboard, Network (Interfaces, DNS, Packet Capture), SD-WAN (selected), Static Routes, Policy Routes, RIP, OSPF, BGP, Routing Objects, Multicast, Policy & Objects, Security Profiles, VPN, User & Authentication, System (with a red notification dot), Security Fabric, and Log & Report.

The main content area displays two donut charts: one for Download traffic split between port5 (green) and port6 (orange), and another for Upload traffic split between port5 (green) and port6 (orange). Both charts show a total value of 2.

Below the charts is a table titled "SD-WAN Zones" with columns: Interfaces, Gateway, Cost, Download, and Upload. It lists a single zone named "SDWAN_Zone" which contains two members: "Hub_WAN2 (port5)" and "Hub_WAN3 (port6)". The table also includes performance metrics for each member: download speeds of 2.10 kbps and 1.97 kbps, and upload speeds of 1.52 kbps and 1.83 kbps respectively.

	Interfaces	Gateway	Cost	Download	Upload
virtual-wan-link					
SDWAN_Zone					
Hub_WAN2 (port5)	192.168.244.2	0	2.10 kbps	1.52 kbps	
Hub_WAN3 (port6)	192.168.244.2	0	1.97 kbps	1.83 kbps	

SD-WAN Zones and members

SD-WAN Configuration on FortiGate

The screenshot shows the FortiGate SD-WAN Priority Rule configuration interface. A priority rule named "Instagram" is being edited. The rule has the following settings:

- Source:** Source address is set to "Hub_local_subnet_1".
- User group:** User group is set to "+".
- Destination:** Address is set to "+".
- Internet Service:** Internet service is set to "+".
- Application:** Application is set to "Instagram".

The rule has an ID of 1, was last used 14 minutes ago, and has a hit count of 0. There are links for "API Preview" and "Edit in CLI". Below the main form, there is a section for "Outgoing Interfaces" with three options: "Manual", "Best Quality" (selected), and "Lowest Cost (SLA)".

Instagram

SD-WAN Rules

The screenshot shows the FortiGate SD-WAN Priority Rule configuration interface. A priority rule named "Youtube" is being edited. The rule has the following settings:

- Source:** Source address is set to "Hub_local_subnet_1".
- User group:** User group is set to "+".
- Destination:** Address is set to "+".
- Internet Service:** Internet service is set to "+".
- Application:** Application is set to "YouTube".

The rule has an ID of 1, was last used 14 minutes ago, and has a hit count of 0. There are links for "API Preview" and "Edit in CLI". Below the main form, there is a section for "Outgoing Interfaces" with three options: "Manual", "Best Quality" (selected), and "Lowest Cost (SLA)".

Youtube

SD-WAN Configuration on FortiGate

Edit Policy

Name: Internet_out

Incoming Interface: Hub_LAN (port2)

Outgoing Interface: SDWAN_Zone

Source: Hub_local_subnet_1

Destination: all

Schedule: always

Service: ALL

Action: ✓ ACCEPT (selected) ✎ DENY

Inspection Mode: Flow-based (selected) Proxy-based

Firewall / Network Options

NAT:

IP Pool Configuration: Use Outgoing Interface Address Use Dynamic IP Pool

Preserve Source Port:

Passive Health Check:

Protocol Options: PROT default

Statistics (since last reset)

ID	9
Last used	1 second(s) ago
First used	16 minute(s) ago
Active sessions	8
Hit count	216
Total bytes	391.21 kB
Current bandwidth	0 bps

Clear Counters

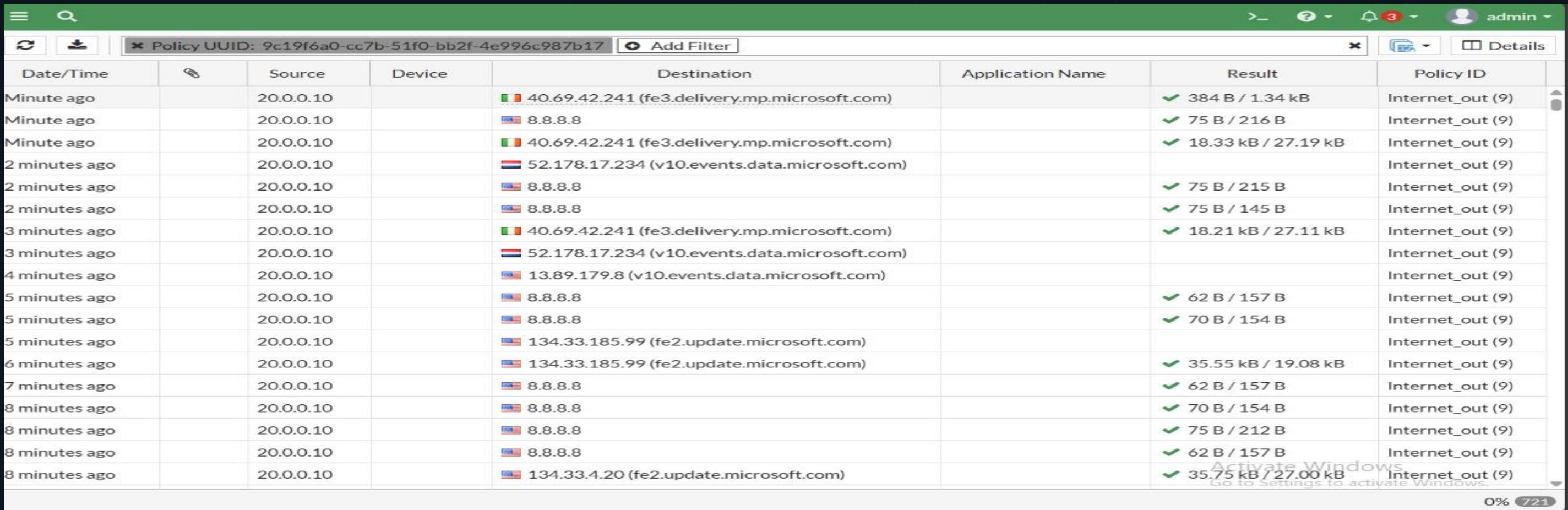
Last 7 Days Bytes ▾

Activate Windows
Go to Settings to activate Windows.

OK Cancel

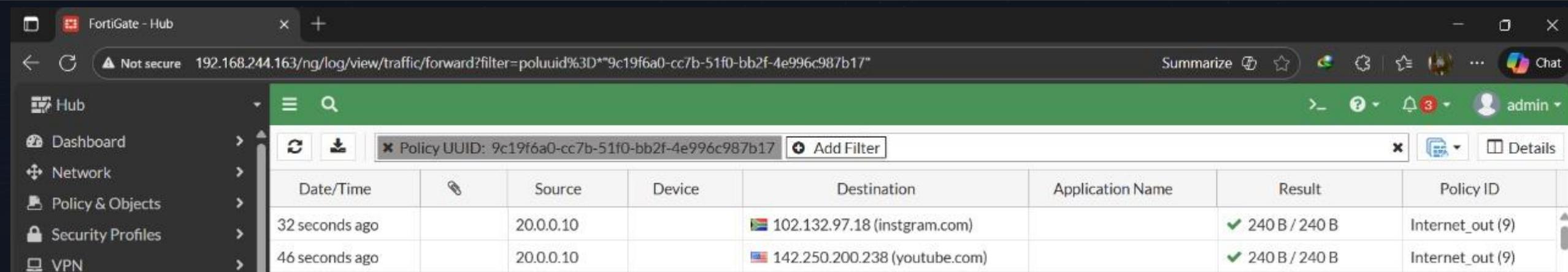
SD-WAN Policy

SD-WAN Configuration on FortiGate



A screenshot of a FortiGate SD-WAN traffic log table. The table has columns for Date/Time, Source, Device, Destination, Application Name, Result, and Policy ID. The table shows numerous entries over the last 8 minutes, primarily from source 20.0.0.10 to various Microsoft delivery and update servers. Most entries show successful results (green checkmarks) and are categorized under the policy Internet_out (9). A watermark for "Activate Windows" is visible across the table.

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)



A screenshot of a FortiGate SD-WAN traffic log table. The table has columns for Date/Time, Source, Device, Destination, Application Name, Result, and Policy ID. The table shows two entries: one from 32 seconds ago to 102.132.97.18 (instagram.com) and another from 46 seconds ago to 142.250.200.238 (youtube.com), both resulting in 240 B / 240 B and categorized under the policy Internet_out (9).

Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
32 seconds ago	20.0.0.10		102.132.97.18 (instagram.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

Made with  GAMMA



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

