Digital Egypt Pioneers Initiative (DEPI)

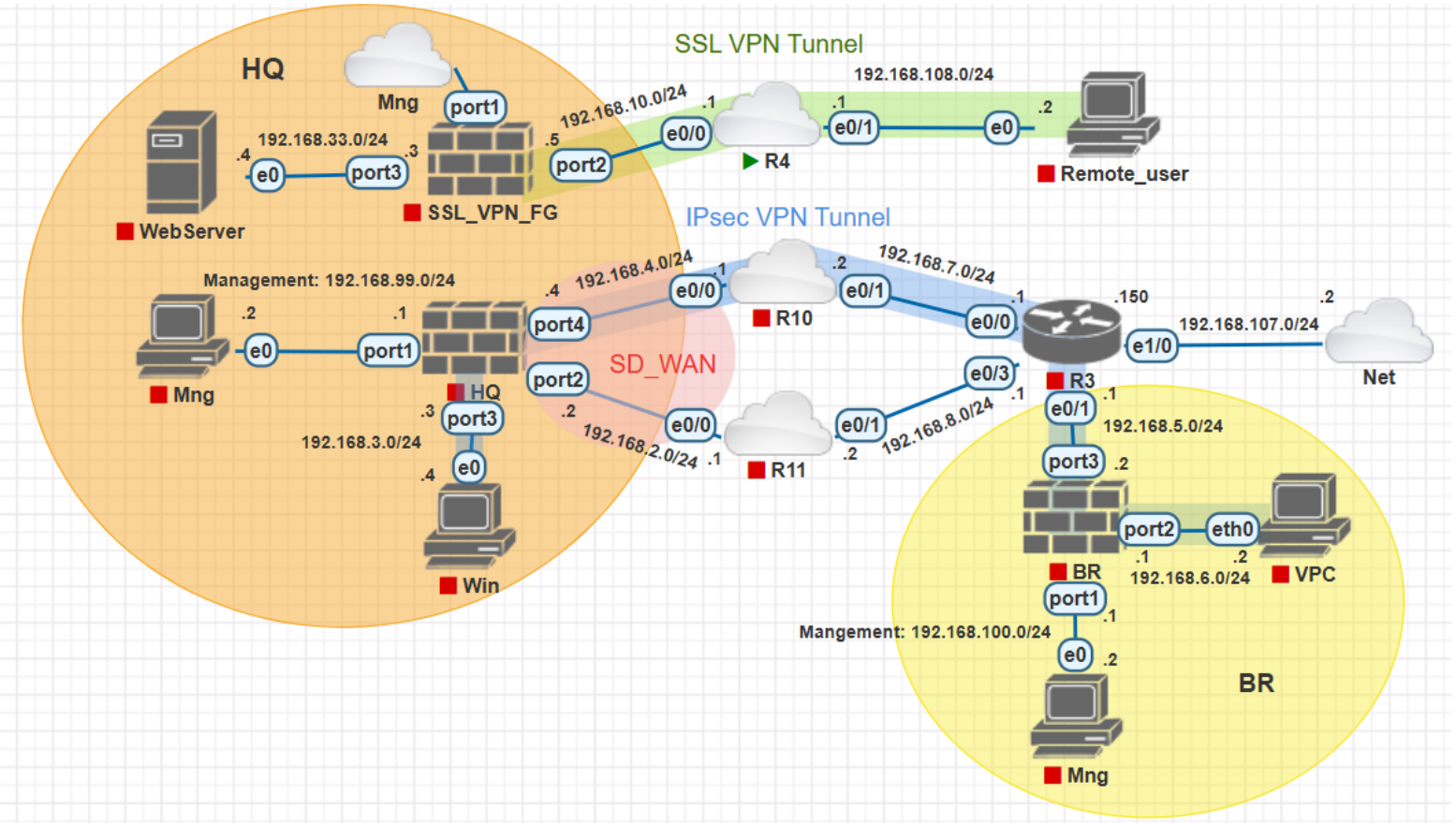
Final Project

Implementing VPN Solutions with FortiGate

Team Members

1-Mohamed Osman ebn Afan Mohamed
2-Nada Ibrahim Mohamed Shehata
3-Mohamed Tarek Mohamed
4-Mayar Mahmoud Ibrahim
5-Lobna Khaled Korani

Topology Diagram



project Phases :

1- Routers Configuration

2- Interfaces, Static Routes & Policies

3- VPN Concepts and Configuration

4- SSL_VPN Configuration

5- IPSEC VPN Configuration

6- VPN With SD_WAN

1- Routers Configuration

R3

```
Router#show running-config
Building configuration...
Current configuration : 1514 bytes
 Last configuration change at 02:00:01 UTC Tue Mar 25 2025
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router
boot-start-marker
boot-end-marker
no aaa new-model
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip cef
no ipv6 cef
multilink bundle-name authenticate
redundancy
interface Ethernet0/0
 ip address 192.168.7.1 255.255.255.0
 ip ospf 1 area 0
interface Ethernet0/1
 ip address 192.168.5.1 255.255.255.0
 ip ospf 1 area 0
interface Ethernet0/2
 no ip address
 ip ospf 1 area 0
 shutdown
interface Ethernet0/3
 ip address 192.168.8.1 255.255.255.0
 ip ospf 1 area 0
interface Ethernet1/0
```

```
 ip address 192.168.107.150 255.255.255.0
interface Ethernet1/1
 no ip address
 shutdown
interface Ethernet1/2
 no ip address
 shutdown
interface Ethernet1/3
 no ip address
 shutdown
router ospf 1
 network 192.168.5.0 0.0.0.255 area 0
 network 192.168.7.0 0.0.0.255 area 0
 network 192.168.8.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.107.2
ip route 192.168.3.0 255.255.255.0 192.168.7.2
ip route 192.168.3.0 255.255.255.0 192.168.8.2
ip route 192.168.6.0 255.255.255.0 192.168.5.2
control-plane
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input none
end
```

R4

```
Router#show running-config
Building configuration...
Current configuration : 947 bytes
last configuration change at 02:05:05 UTC Tue Mar 25 2025
version 15.4
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
no service password-encryption
hostname Router
!boot-start-marker
boot-end-marker
no aaa new-model
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip cef
no ipv6 cef
multilink bundle-name authenticated
redundancy
interface Ethernet0/0
 ip address 192.168.10.1 255.255.255.0
interface Ethernet0/1
 ip address 192.168.108.1 255.255.255.0
interface Ethernet0/2
 no ip address
 shutdown
interface Ethernet0/3
 no ip address
 shutdown
ip forward-protocol nd
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.10.5
control-plane
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input none
end
```

R10

```
Router#show running-config
Building configuration...
Current configuration : 1147 bytes
 Last configuration change at 02:08:41 UTC Tue Mar 25 2025
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router
boot-start-marker
boot-end-marker
no aaa new-model
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip cef
no ipv6 cef
multilink bundle-name authenticated
redundancy
interface Ethernet0/0
 ip address 192.168.4.1 255.255.255.0
interface Ethernet0/1
 ip address 192.168.7.2 255.255.255.0
 ip ospf 1 area 0
interface Ethernet0/2
 no ip address
 shutdown
interface Ethernet0/3
 no ip address
 shutdown
router ospf 1
 network 192.168.4.0 0.0.0.255 area 0
 network 192.168.7.0 0.0.0.255 area 0
ip forward-protocol nd
```

no ip http server

no ip http secure-server

ip route 0.0.0.0 0.0.0.0 192.168.7.1

ip route 192.168.3.0 255.255.255.0 192.168.4.4

ip route 192.168.6.0 255.255.255.0 192.168.7.1

control-plane

line con 0

 logging synchronous

line aux 0

line vty 0 4

 login

 transport input none

end

R11

Router#show running-config

Building configuration...

Current configuration : 1085 bytes

version 15.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

hostname Router

boot-start-marker

boot-end-marker

no aaa new-model

mmi polling-interval 60

no mmi auto-configure

no mmi pvc

mmi snmp-timeout 180

ip cef

no ipv6 cef

multilink bundle-name authenticated

redundancy

interface Ethernet0/0

 ip address 192.168.2.1 255.255.255.0

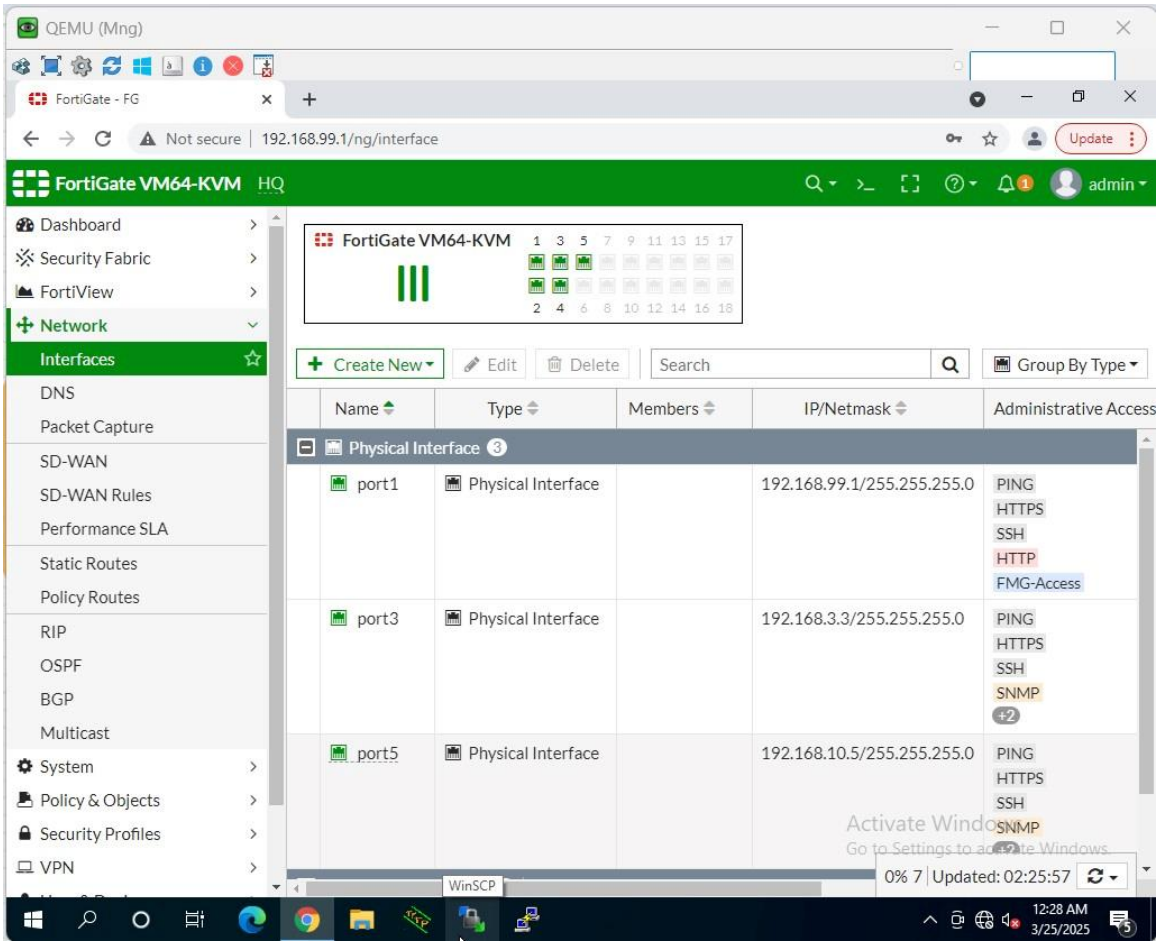
interface Ethernet0/1

```
 ip address 192.168.8.2 255.255.255.0
 ip ospf 1 area 0
interface Ethernet0/2
 no ip address
 shutdown
interface Ethernet0/3
 no ip address
 shutdown
router ospf 1
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.8.0 0.0.0.255 area 0
ip forward-protocol nd
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.8.1
ip route 192.168.3.0 255.255.255.0 192.168.2.2
ip route 192.168.6.0 255.255.255.0 192.168.8.1
control-plane
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
 transport input none
end
```

2-Interfaces, Static Routes & Policies

HQ FortiGate

HQ FortiGate Interfaces

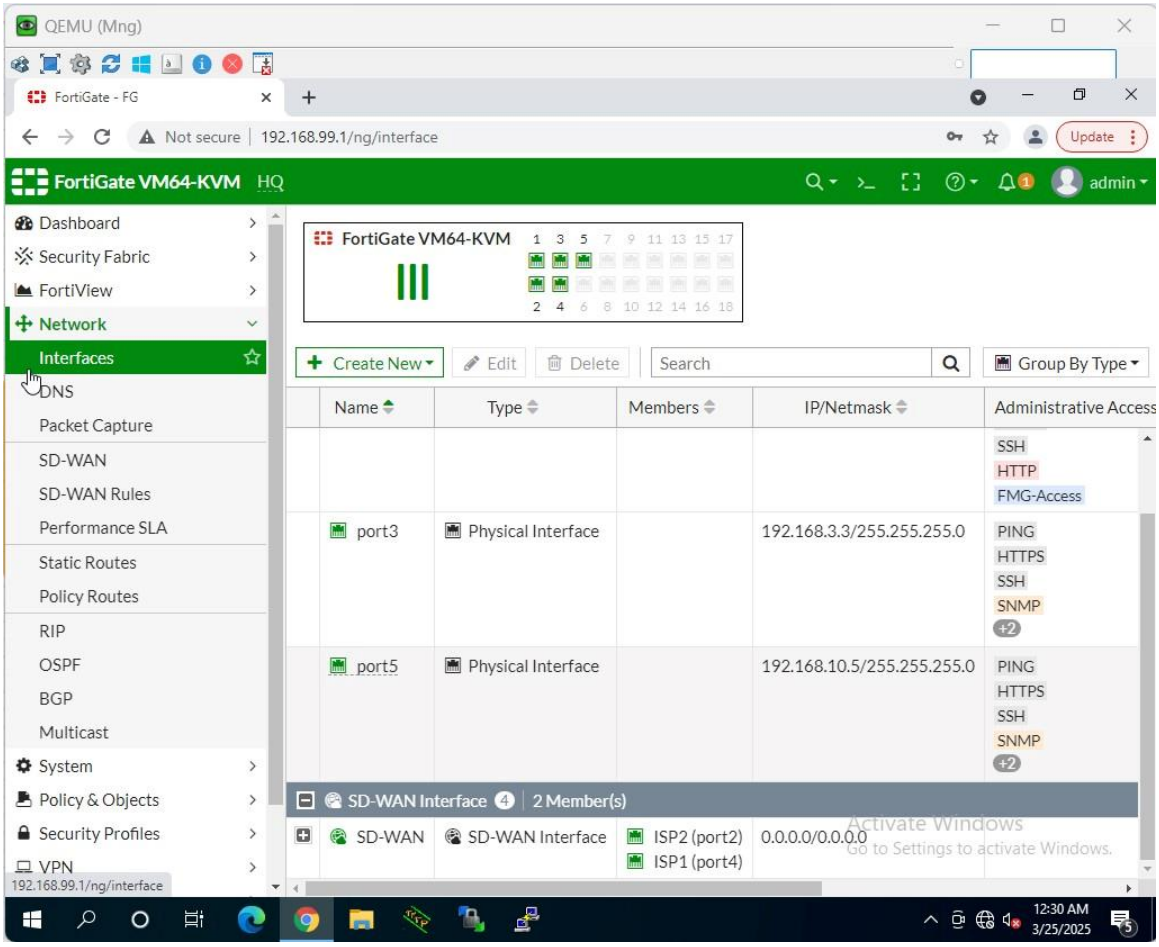


This photo displays the **Network Interfaces** page of a FortiGate VM64-KVM firewall. Here, we can see the list of physical interfaces configured on the firewall, along with their respective IP addresses, subnet masks, and administrative access settings.

- **Interfaces:**
  - **port1**: Assigned the IP **192.168.99.1/24**, allowing administrative access via **PING, HTTPS, SSH, HTTP, and FMG-Access**.
  - **port3**: Assigned the IP **192.168.3.3/24**, allowing **PING, HTTPS, SSH, and SNMP**.
  - **port5**: Assigned the IP **192.168.10.5/24**, allowing **PING, HTTPS, SSH, and SNMP**.

- **Administrative Access:** Defines the services that can be accessed through each interface, such as SSH for remote CLI access and HTTPS for web-based GUI management.

This configuration is essential for managing network access and securing remote administration.



This photo illustrates the **SD-WAN Interface** configuration on the FortiGate firewall. SD-WAN (Software-Defined Wide Area Network) helps in optimizing traffic distribution across multiple WAN connections.

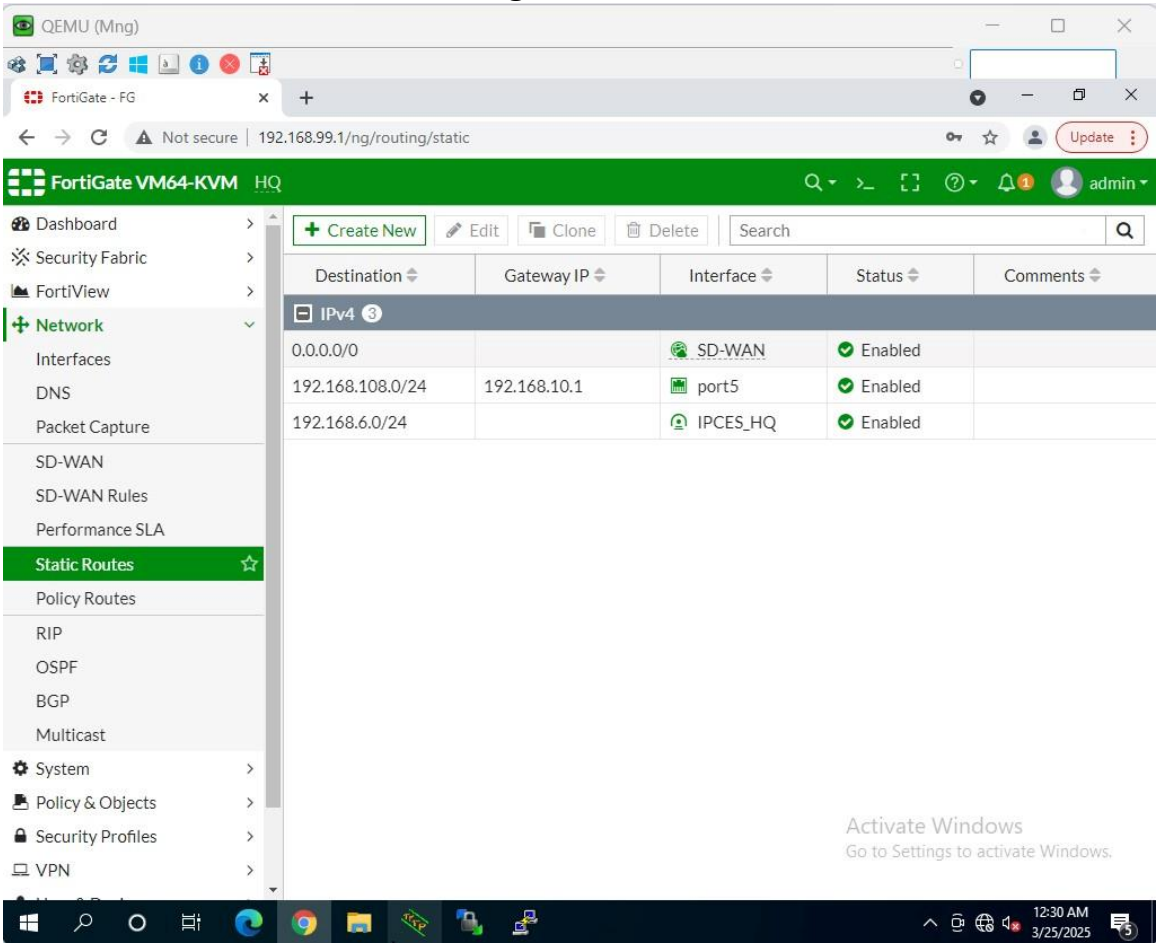
- **Physical Interfaces in SD-WAN:**
  - **ISP1 (port4)**
  - **ISP2 (port2)**

These interfaces are grouped into an SD-WAN interface, which ensures better load balancing and redundancy.

- **Benefits of SD-WAN:**
  - **Intelligent Traffic Routing**: Routes traffic based on link quality (latency, jitter, packet loss).
  - **Cost Efficiency**: Allows the use of multiple ISPs without relying on expensive MPLS links.
  - **Failover Support**: If one WAN link fails, traffic is seamlessly shifted to the available link.

This setup enhances performance for cloud applications and provides resilience in case of network failures.

HQ FortiGate Static Routes Configuration



This screenshot shows the **Static Routes** configuration in the FortiGate firewall. Static routes are essential for defining how traffic should be forwarded across the network.

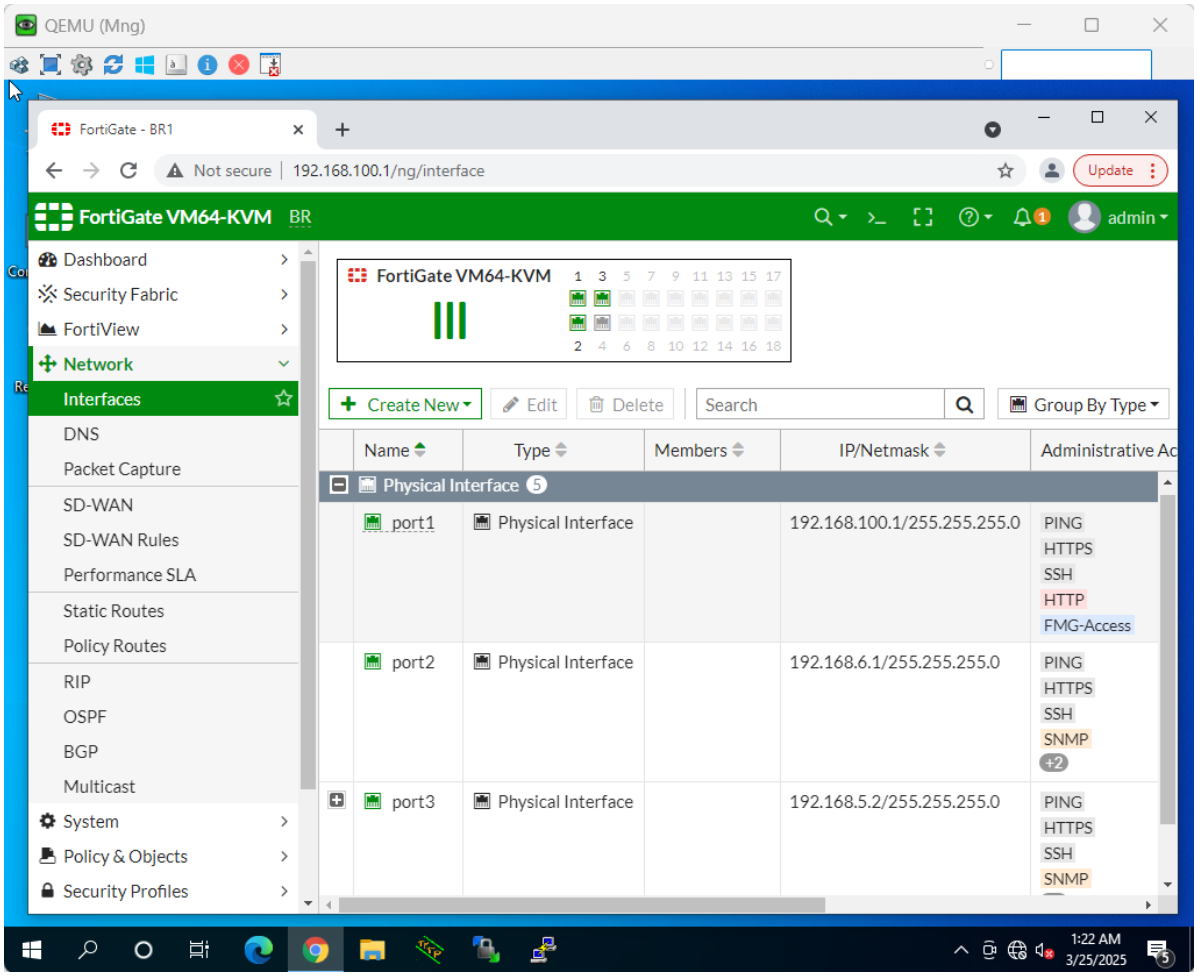
- **Configured Static Routes:**
  1. **0.0.0.0/0 -> SD-WAN** (Default Route)
     - Directs all external traffic through the SD-WAN interface.
  2. **192.168.10.0/24 -> 192.168.10.1 (port5)**
     - Routes traffic for the **192.168.10.0** subnet via port5.
  3. **192.168.6.0/24 -> IPCES_HQ**
     - Defines a static route for internal communication with another network.

- **Why Static Routes?**
  - Ensures controlled traffic forwarding.
  - Helps in defining custom routing when dynamic routing protocols are not in use.
  - Provides a fallback mechanism in case of SD-WAN link failures.

Proper static route configuration is crucial for seamless internal and external connectivity.

BR FortiGate

BR FortiGate Interfaces

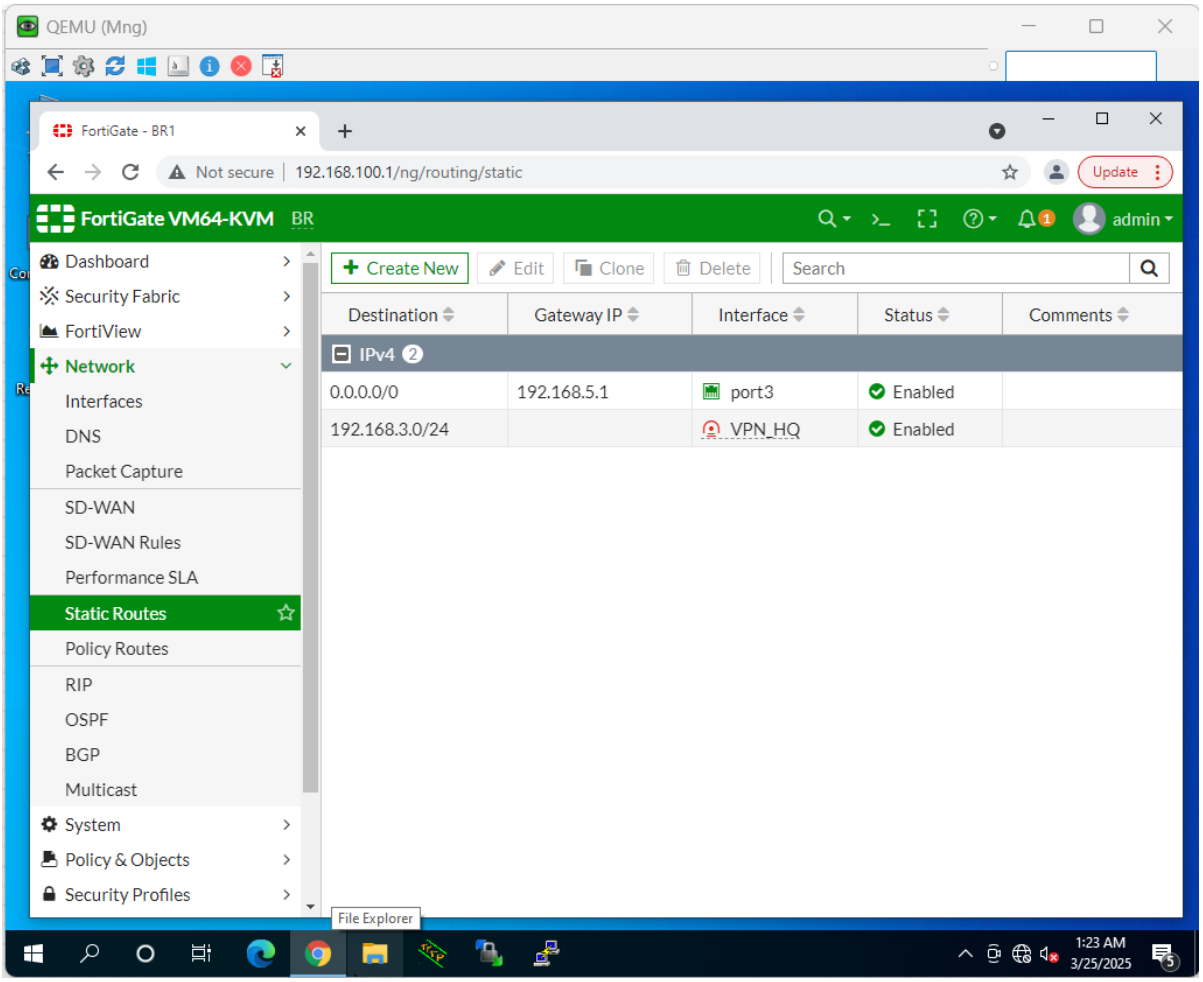


Description:

The first image displays the network interfaces configuration page of a FortiGate firewall. This section allows administrators to manage physical and virtual network interfaces, configure IP addresses, and set up administrative access protocols.

Key Details:

- The firewall is managed via the web interface at 192.168.100.1.
- There are three physical interfaces:
- Port1: Assigned IP 192.168.100.1/24, allows PING, HTTPS, SSH, HTTP, and FMG-Access.
- Port2: Assigned IP 192.168.6.1/24, allows PING, HTTPS, SSH, and SNMP.
- Port3: Assigned IP 192.168.5.2/24, allows PING, HTTPS, SSH, and SNMP.
- Administrative access permissions define how each port can be accessed for remote management.



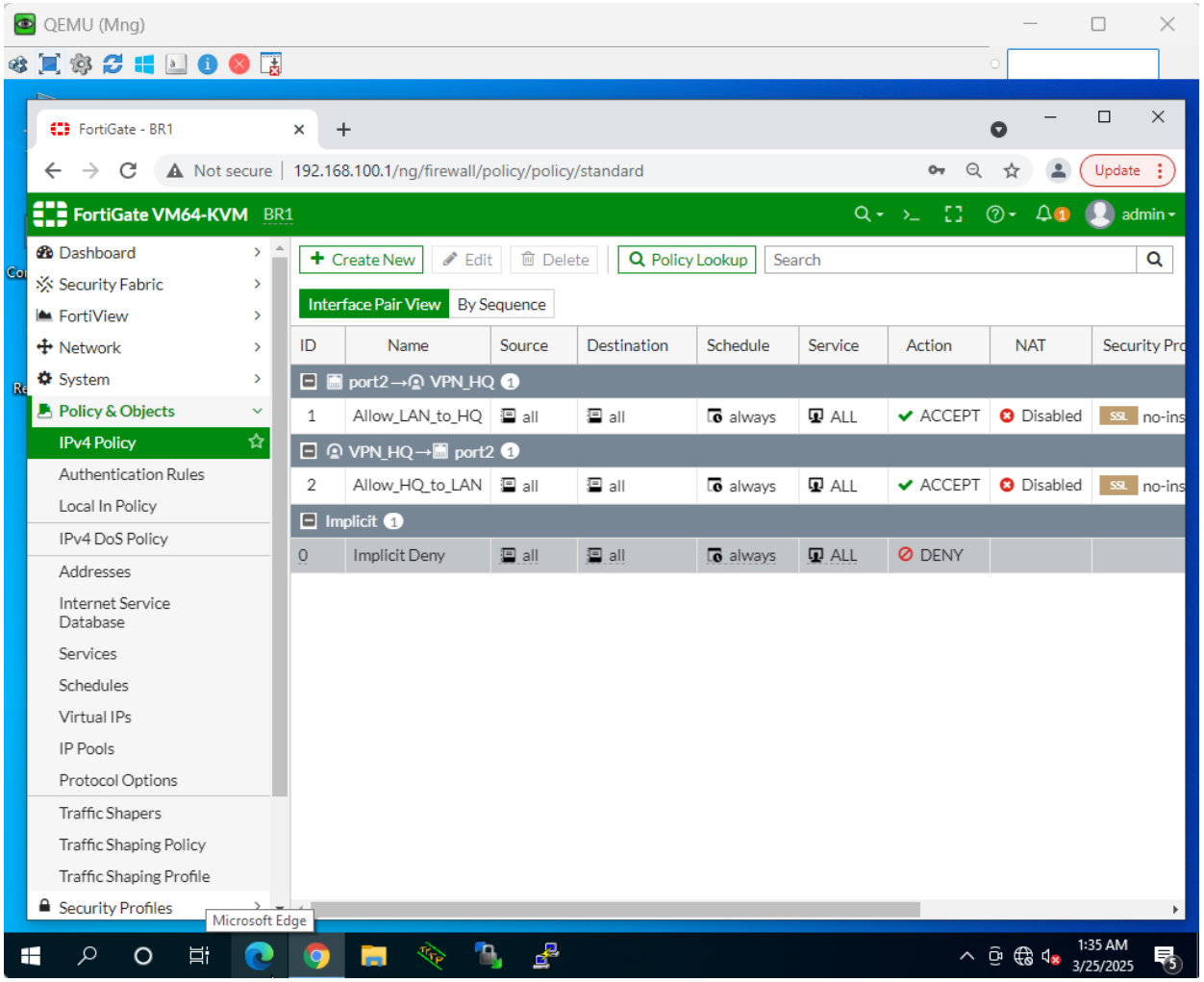
BR FortiGate Static Routes

Description:

The second image shows the static routing table, which defines how traffic is forwarded between different network segments.

Key Details:

- The firewall routes traffic through:
- Default Route (0.0.0.0/0) via 192.168.5.1 using port3, ensuring internet connectivity.
- Route for 192.168.3.0/24 through a VPN interface named VPN_HQ, used for secure remote connectivity.
- Both routes are enabled, ensuring proper traffic flow between LAN, WAN, and VPN-connected networks.



BR FortiGate Policies

Description:

The third image displays firewall policies that define rules for traffic filtering and security enforcement.

Key Details:

- The firewall policies are configured under IPv4 Policy.
- Two rules are explicitly set:

1. Allow LAN to HQ VPN: Traffic from port2 to VPN_HQ is allowed (ACCEPT).
2. Allow HQ VPN to LAN: Traffic from VPN_HQ to port2 is allowed (ACCEPT).

- The Implicit Deny Rule at the bottom ensures any traffic not explicitly allowed is blocked.
- NAT is disabled for the allowed policies, meaning original IP addresses are preserved.
- SSL inspection is set to no-inspection, allowing encrypted traffic to pass through without deep packet inspection.

2-VPN Concepts and Configuration

1. VPN Concepts

VPN (Virtual Private Network) secures data transmission over public networks.

Types:

Site-to-Site VPN – Connects networks securely.

Remote Access VPN – Allows users to connect remotely.

SSL VPN – Uses SSL encryption for web-based access.

IPsec VPN – Encrypts data at the network layer.

---

2. FortiGate VPN Configuration Examples

A. Site-to-Site IPsec VPN

Create Phase 1:

Go to **VPN > IPsec Wizard** → Select **Site to Site**.

Set **Remote Gateway, Pre-Shared Key, IKEv2, AES-256, SHA256**.

Create Phase 2:

Define **Local & Remote Subnet**, enable **PFS**.\

Firewall Policy:

Allow traffic from **VPN Tunnel to LAN**.

Static Route:

Route traffic through **VPN Tunnel**.

Test:

Check **VPN Monitor**, run **ping tests**.

B. SSL VPN

Enable SSL VPN:

VPN > SSL-VPN Settings → Enable on **WAN**.

User Authentication:

Create **SSL_VPN_Users** group

Firewall Policy:

Allow traffic from **ssl.root to LAN**.

Test:

Connect via **FortiClient VPN** and verify access

3-SSL_VPN Configuration

SSL VPN (Secure Sockets Layer Virtual Private Network) allows users to securely access an organization's internal network over the internet using encryption. Unlike traditional VPNs, SSL VPNs operate through a web browser or dedicated VPN client, making remote access more flexible and user-friendly.

Steps to Configure SSL VPN on FortiGate (GUI)

1. Create a User Group in User & Device > User Groups
2. Configure the SSL VPN portal
3. Enable SSL VPN in VPN > SSL-VPN Settings.
4. Configure Firewall Policy in Policy & Objects > IPv4 Policy.

SSL VPN User Configuration

1. Steps Taken

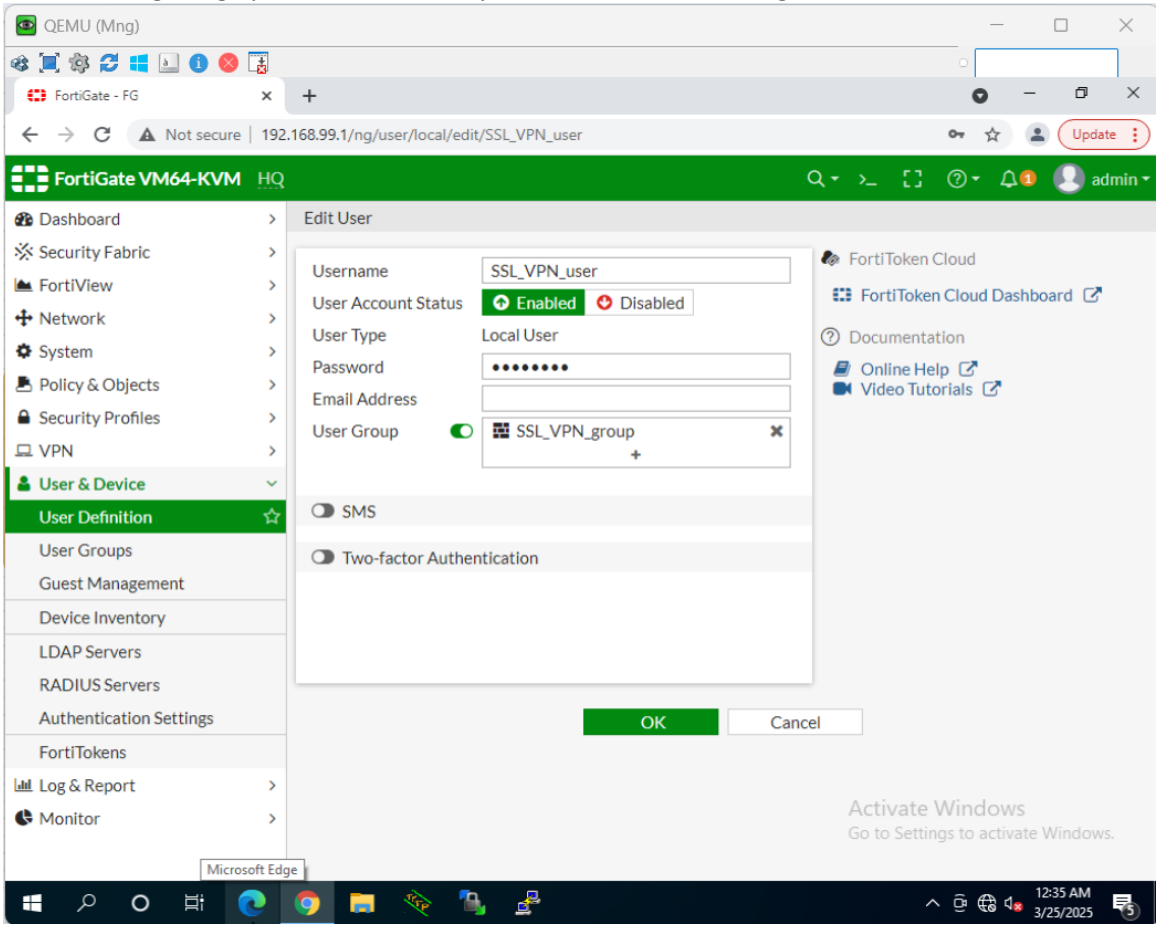
The following steps were taken to configure the SSL VPN user:
1. Logged into the FortiGate web interface as an administrator.
2. Navigated to 'User & Device' -> 'User Definition'.
3. Created a new local user with the username 'SSL_VPN_user'.
4. Enabled the user account.
5. Assigned the user to the 'SSL_VPN_group'.
6. Configured authentication settings, including optional two-factor authentication.

2. Explanation of the Configuration

The configuration screen in the image below shows the following details:

• **Username**: The user account created for SSL VPN access is named 'SSL_VPN_user'.
• **User Account Status**: The account is enabled, allowing it to be used for authentication.
• **User Type**: The user is categorized as a 'Local User', meaning credentials are stored within the firewall.
• **Password**: A secure password is set for the user (hidden in the interface).
• **User Group**: The user is assigned to the 'SSL_VPN_group', which dictates their access permissions.
• **Two-Factor Authentication**: This option is available for enhanced security but is not enabled in the current setup.

The following image provides a visual representation of the configured SSL VPN user:



By following the above steps, an SSL VPN user has been successfully created on the FortiGate firewall. This setup enhances network security by ensuring that only authorized users can access the internal network remotely. Further enhancements can include enabling two-factor authentication to add an extra layer of security.

SSL VPN Portal Configuration

1. Steps Taken

The following steps were taken to configure the SSL VPN portal:

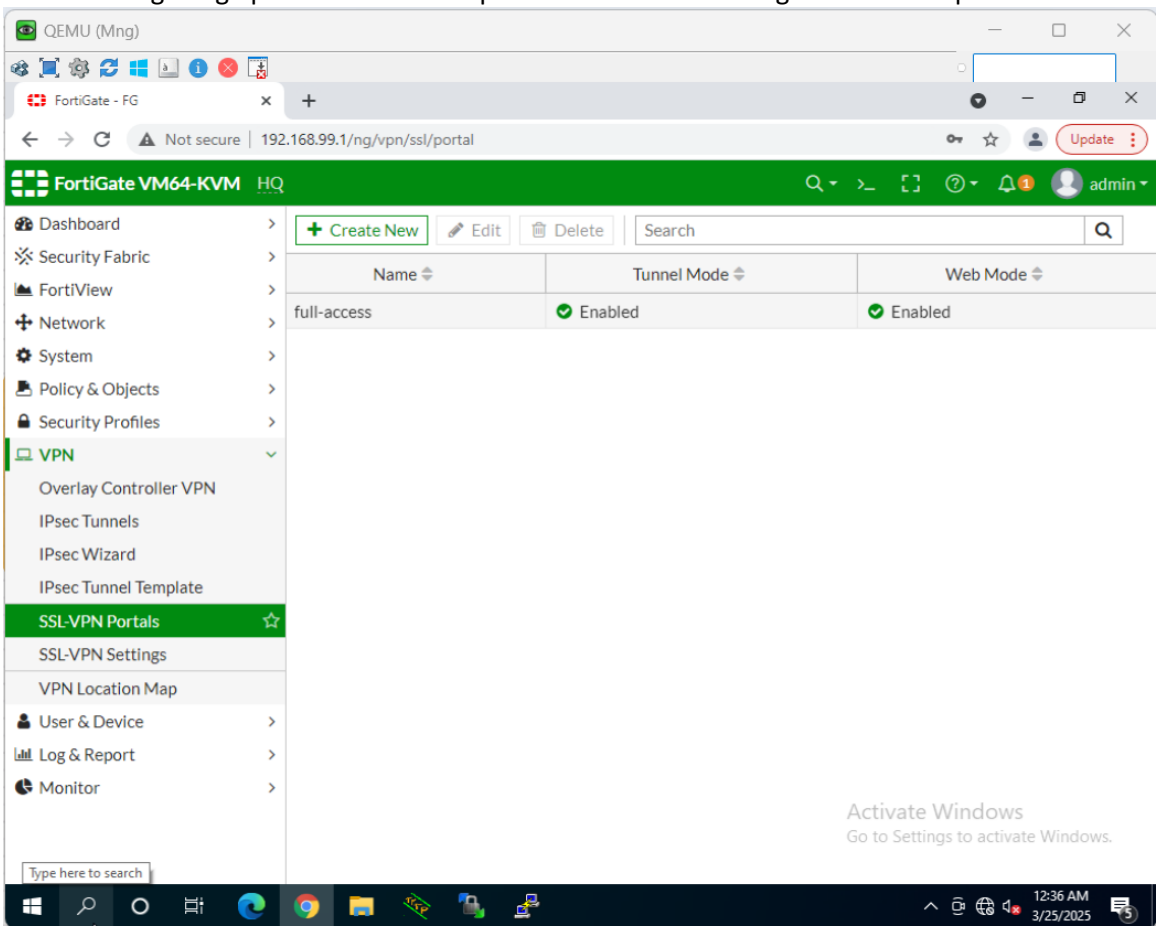
1. Logged into the FortiGate web interface as an administrator.
2. Navigated to 'VPN' -> 'SSL-VPN Portals'.
3. Verified the existence of the 'full-access' portal, which provides complete SSL VPN access.
4. Ensured that both Tunnel Mode and Web Mode were enabled for this portal.
5. Confirmed that the portal is ready for assignment to users or groups.

2. Explanation of the Configuration

The configuration screen in the image below shows the following details:

• **Portal Name**: 'full-access' – This portal provides unrestricted access to users.
• **Tunnel Mode**: Enabled – Allows users to establish a full tunnel VPN connection.
• **Web Mode**: Enabled – Allows users to access internal resources through a web-based VPN portal.
• **Portal Management**: New portals can be created, edited, or deleted based on security needs.

The following image provides a visual representation of the configured SSL VPN portal:



By following the above steps, an SSL VPN portal has been successfully verified on the FortiGate firewall. This setup allows users to securely connect to internal resources through Tunnel Mode or Web Mode. Further enhancements can include creating custom portals with restricted access based on user roles.

SSL VPN Settings Configuration

1. Steps Taken

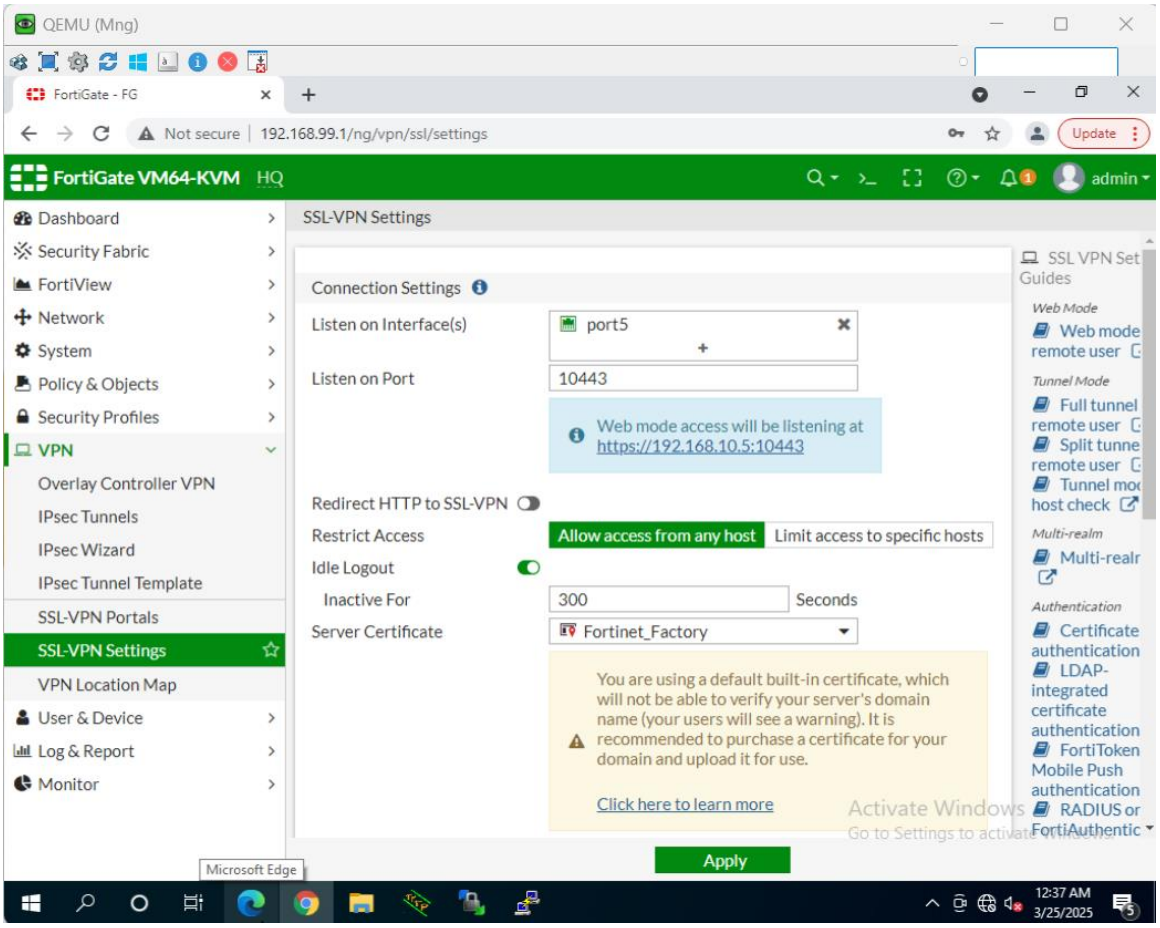
The following steps were taken to configure SSL VPN settings on the FortiGate firewall:

1. Logged into the FortiGate web interface as an administrator.
2. Navigated to 'VPN' -> 'SSL-VPN Settings'.
3. Configured the address range for tunnel mode clients.
4. Defined DNS servers for resolving domain names within the VPN.
5. Mapped user groups to the appropriate SSL VPN portal.

2. SSL VPN Connection Settings

The second image below displays the general SSL VPN connection settings:

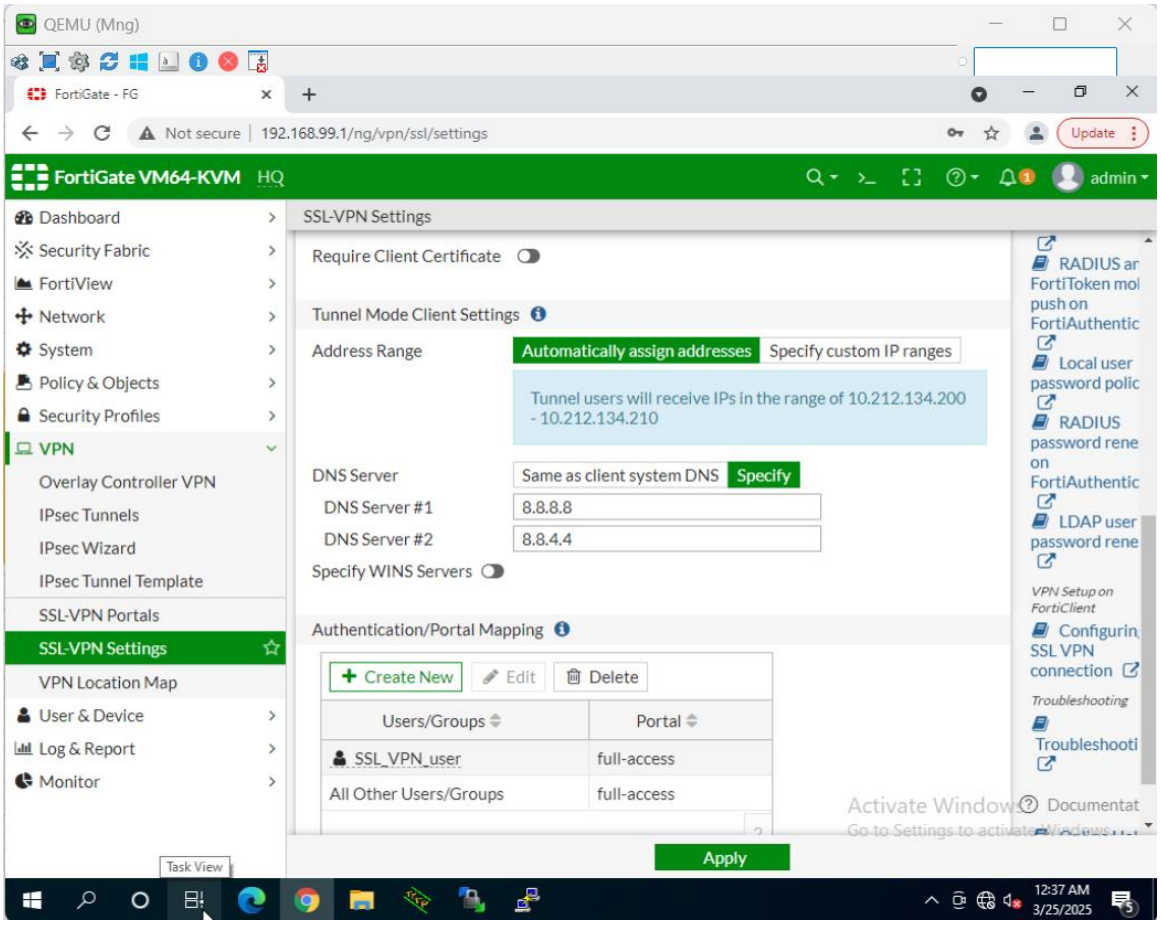
• **Listening Interface**: Configured to listen on 'port5'.
• **Listening Port**: Set to 10443 for secure VPN connections.
• **Access Control**: Allows access from any host.
• **Idle Logout**: Users are logged out after 300 seconds of inactivity.
• **SSL Certificate**: The default built-in certificate is used, but a custom certificate is recommended for enhanced security.



3. SSL VPN Client Settings

The first image below shows the client-side SSL VPN settings:

• **Address Range**: Tunnel users receive IPs in the range of 10.212.134.200 - 10.212.134.210.
• **DNS Server**: Configured with Google DNS (8.8.8.8 and 8.8.4.4) for name resolution.
• **User Mapping**: The user 'SSL_VPN_user' is assigned to the 'full-access' SSL VPN portal.



SSL VPN

Policy Configuration Details

Policy Name

- Allow_SSL_VPN
  - This name is assigned to the policy to easily identify its purpose.

Incoming Interface

- SSL-VPN tunnel interface (ssl.root)
  - This interface is used as the entry point for SSL VPN traffic.

Outgoing Interface

- Port3
  - This is the internal network interface where traffic from the VPN users will be forwarded.

Source

- SSLVPN_TUNNEL_ADDR1
- SSL_VPN_group
  - These sources define the remote VPN users and the IP address pool assigned to them.

Destination

- LOCAL_subnet
  - This specifies the internal network that remote users are allowed to access.

Schedule

- Always
  - The policy is active at all times, allowing SSL VPN users to connect whenever needed.

Service

- ALL
  - This policy allows all types of network traffic from VPN users to the internal network.

Action

• ACCEPT
- The firewall will permit traffic that matches this policy.

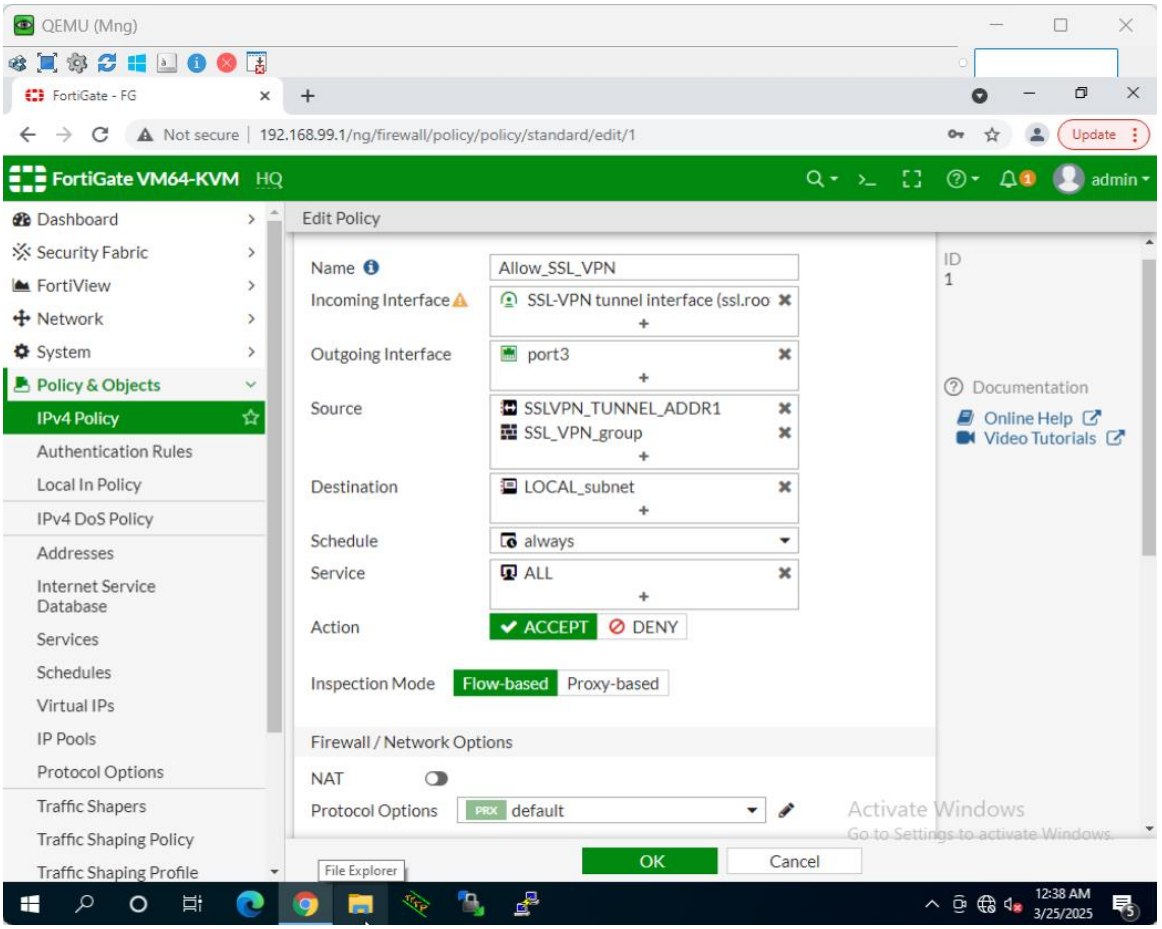
Inspection Mode

• Flow-based
- This mode is used for traffic inspection, optimizing performance and security.

Firewall / Network Options

• NAT: Disabled
- NAT (Network Address Translation) is turned off to allow end-to-end visibility of the VPN traffic.
• Protocol Options: Default
- The default protocol settings are applied to this policy.

This policy is configured to ensure secure remote access to the internal network via SSL VPN while maintaining flexibility and security. By allowing authenticated VPN users to connect to internal resources through a designated interface, organizations can enhance remote work capabilities securely.



4-IPSEC VPN Configuration and policies

We classify it into

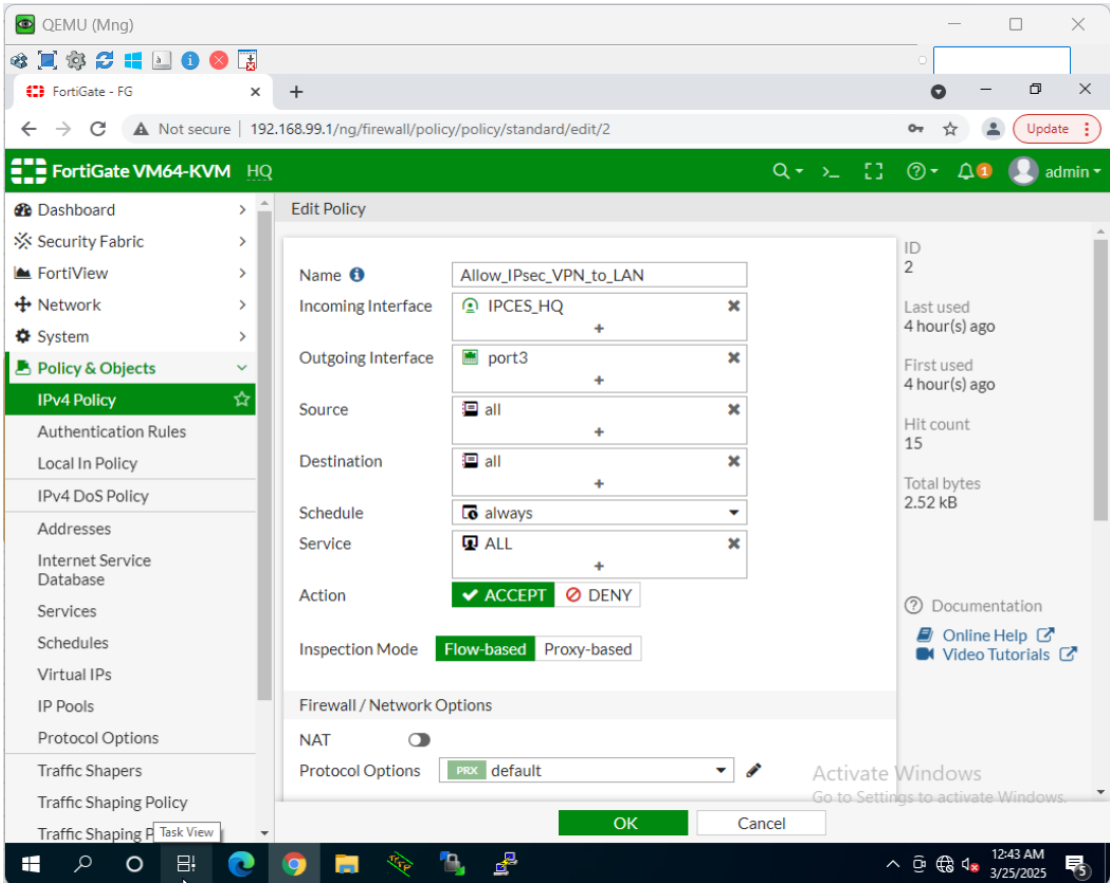
*HQ_Fortigate

*BR_Fortigate

HQ

(1) Ipsec_vpn policy

A- Allow IPsec_VPN to LAN



1. Name:

Allow_IPsec_VPN_to_LAN → This policy name indicates that it allows traffic from the **IPSec VPN** to the local network (LAN).

2. Incoming Interface:

IPCSEC_HQ → This is the interface receiving traffic from the **IPSec VPN**.

3. Outgoing Interface:

port3 → The traffic will be forwarded to this interface after passing through the VPN.

4. Source:

all → This means the policy is not restricted to a specific source; any device using the VPN is allowed.

5. Destination:

all → Any destination within the local network is allowed.

6. Schedule:

always → The policy is active at all times without any time restrictions.

7. Service:

ALL → This means all services and protocols are permitted without filtering.

8. Action:

ACCEPT ✅ → This allows traffic to pass according to this policy.

9. Inspection Mode:

Flow-based → Traffic is inspected based on data flow, which is more efficient than **Proxy-based** inspection.

10. Firewall / Network Options:

NAT: Disabled, meaning IP addresses will not be translated.

Protocol Options: Default.

11. Additional Information:

Last used **4 hours ago**.

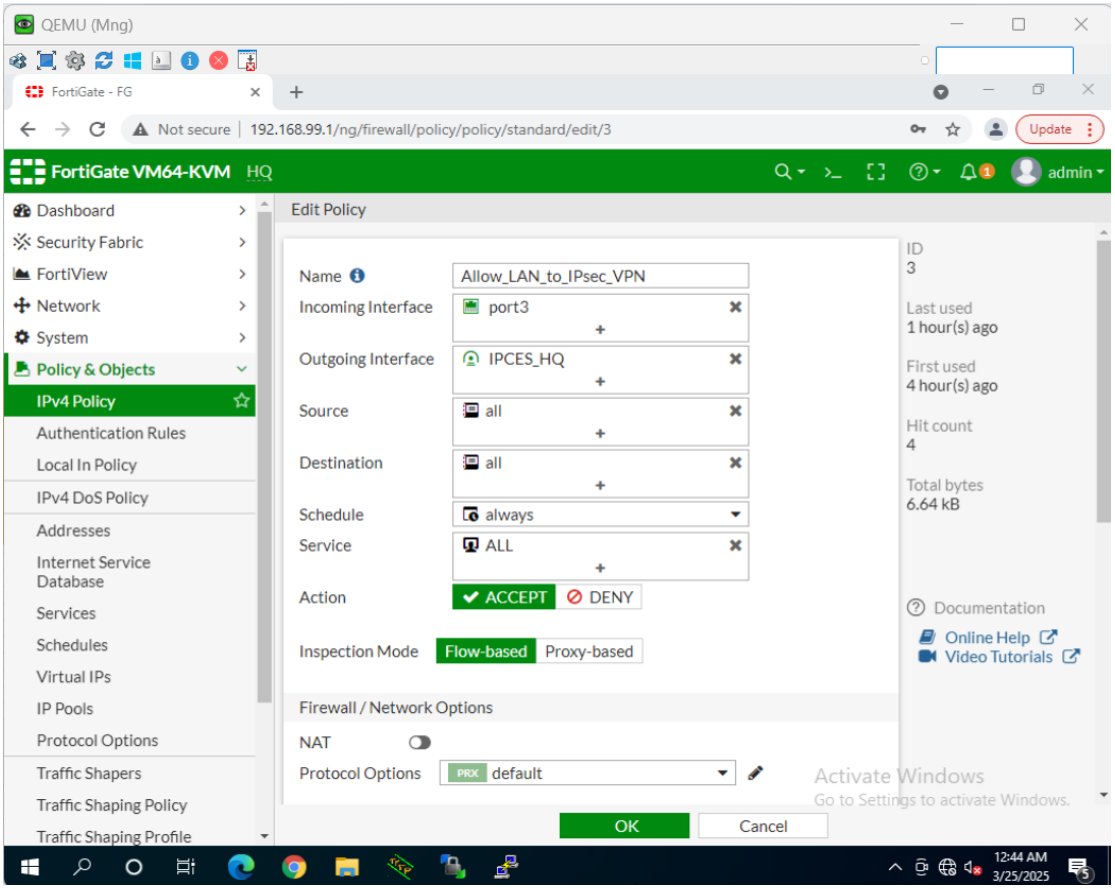
Hit count: 15, meaning the policy has been applied 15 times.

Total data passed: 2.52 KB.

Conclusion:

This policy is configured to allow traffic coming through **IPSec VPN** to the local network **without restrictions on source, destination, or service**.

B- Allow LAN to IPsec_VPN



This image shows the FortiGate firewall management interface, specifically within the Firewall Policy settings for an IPSec VPN connection.

Policy Details:
1. Policy Name: Allow_LAN_to_IPsec_VPN
2. Incoming Interface: port3
3. Outgoing Interface: IPCES_HQ (the VPN interface)
4. Source: all (all devices)
5. Destination: all (all destinations)
6. Schedule: always (always active)
7. Service: ALL (all services)
8. Action: ACCEPT (allow traffic)
9. Inspection Mode: Flow-based (packet flow inspection)
10. Firewall/Network Options:
   - NAT is disabled.
   - Default protocol options.

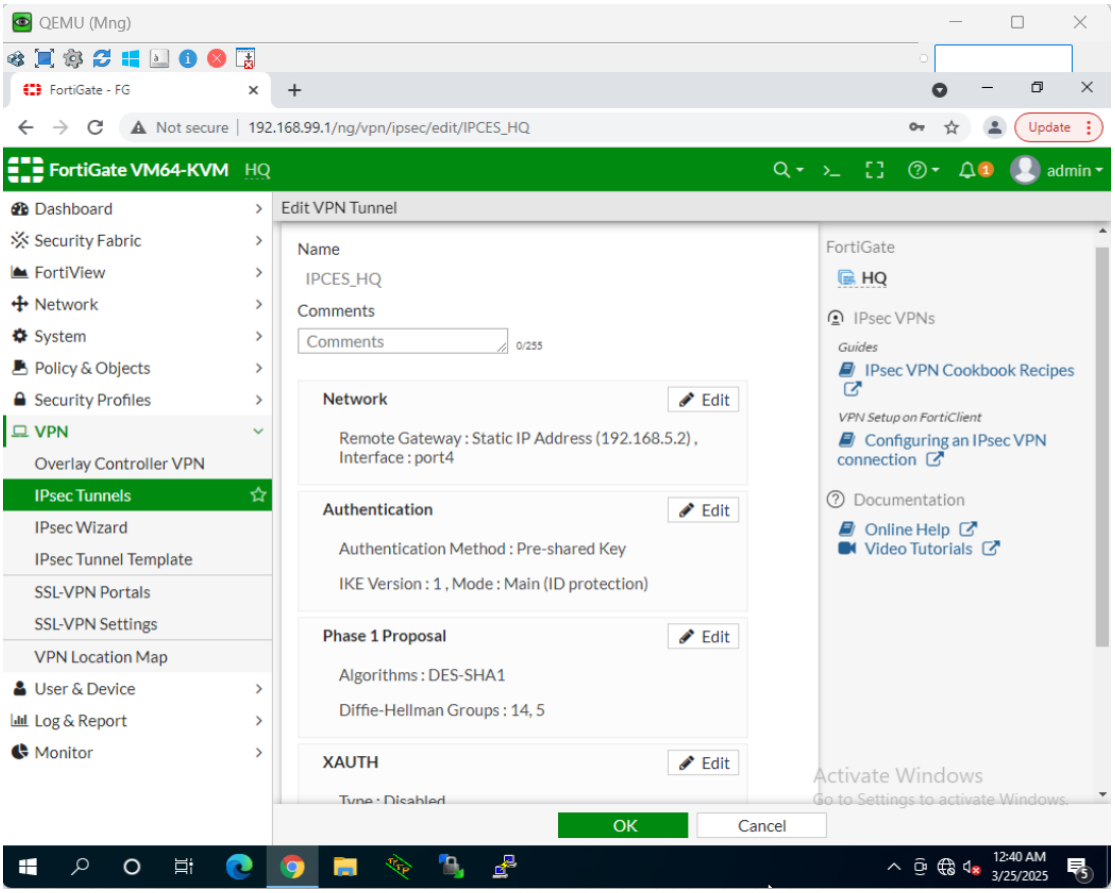
Explanation of the Policy:

This policy allows all traffic from devices in the LAN (port3) to reach the remote VPN network IPCES_HQ without restrictions. This means that any device within the local network can communicate with the remote network through the IPSec VPN tunnel.

Additional Interface Options:

- OK button: Saves changes.

- Cancel button: Discards changes.
- Documentation section: Provides links to Online Help and Video Tutorials for further guidance.



This image shows the IPSec VPN Tunnel Configuration screen in FortiGate, where a VPN tunnel named IPCES_HQ is being configured.

Key Configuration Details:
1. Tunnel Name: IPCES_HQ
2. Network:
  - Remote Gateway: Static IP address 192.168.5.2 (VPN peer's public IP)
  - Interface: port4 (interface handling the VPN connection)

3. Authentication:
  - Authentication Method: Pre-shared Key (PSK)
  - IKE Version: 1, Mode: Main (ID protection enabled)

4. Phase 1 Proposal:
  - Encryption & Hashing Algorithms: DES-SHA1
  - Diffie-Hellman Groups: 14, 5 (used for key exchange)

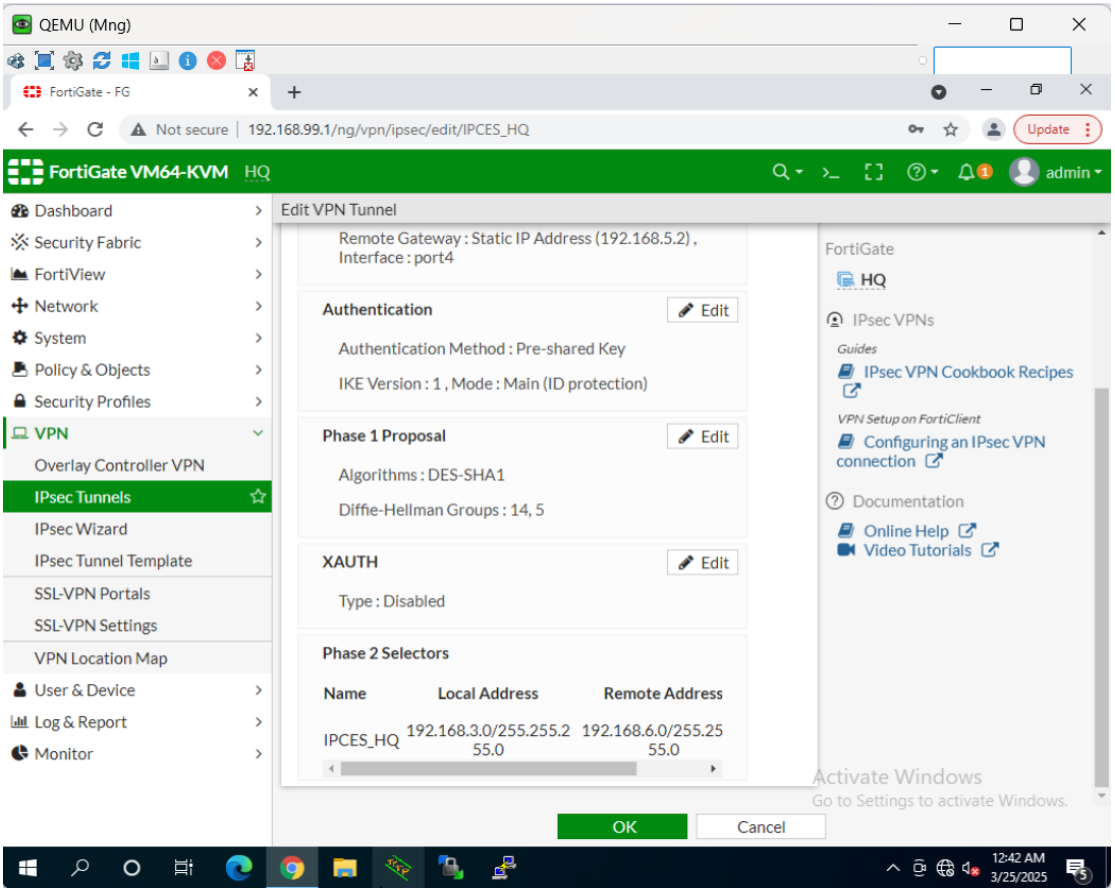
5. XAUTH (Extended Authentication): Disabled.

Explanation:
- This setup defines an IPSec VPN tunnel connecting the local FortiGate firewall to a remote site at 192.168.5.2.
- The pre-shared key authentication method is used to establish a secure connection.
- Phase 1 Proposal defines the cryptographic settings used to negotiate and establish the VPN tunnel.
- IKEv1 in Main Mode provides better security by protecting identity information during key exchange.

Available Actions:
- OK: Saves the configuration.
- Cancel: Discards changes.

- Edit Buttons: Allow modification of settings.

Additional Resources:
On the right, there are links to:
- IPSec VPN Cookbook Recipes for setup guidance.
- VPN Setup on FortiClient for configuring client-side VPN.
- Online Help & Video Tutorials for troubleshooting and learning.



FortiGate IPsec VPN Tunnel Configuration Overview

This screenshot shows the configuration of an IPsec VPN tunnel on a FortiGate firewall. Below are the key details:

General Configuration
- Remote Gateway: A static IP address (192.168.5.2) is assigned to the remote site.
- Interface: The tunnel is established on port4.

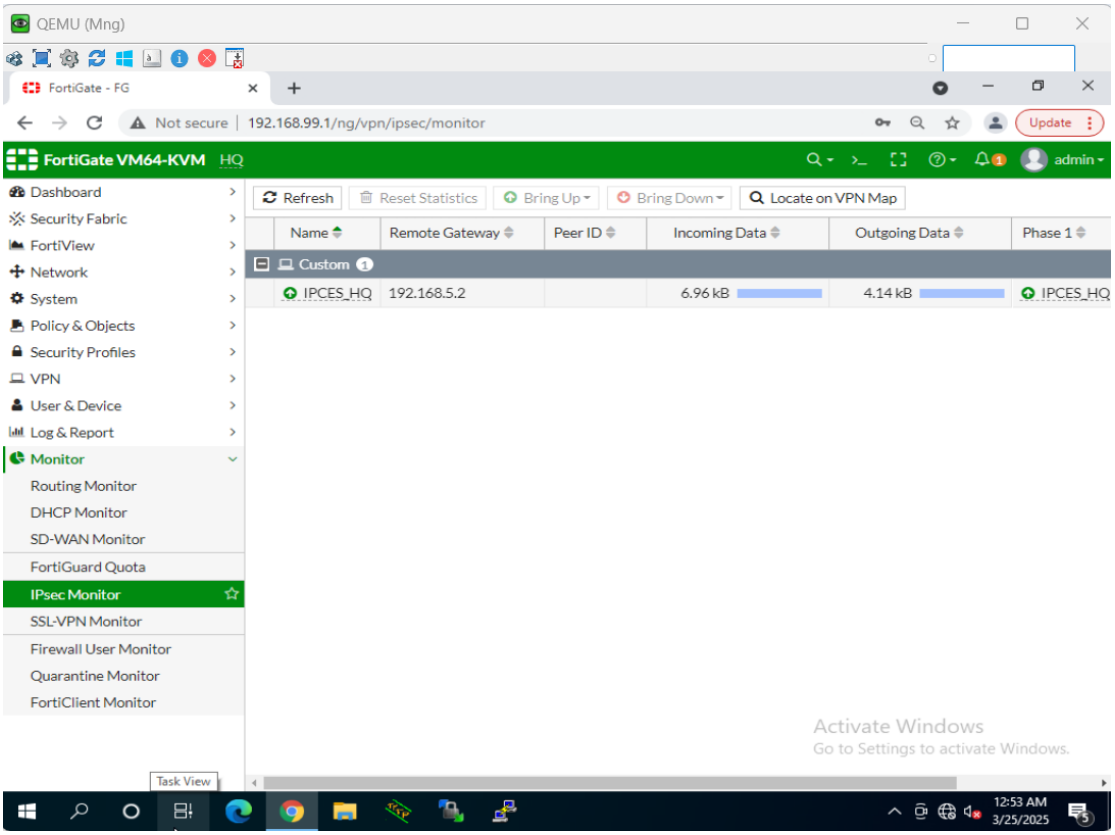
Authentication
- Authentication Method: Pre-shared Key (PSK) is used for secure authentication.
- IKE Version: Version 1.
- Mode: Main Mode with ID protection.

Phase 1 Proposal
- Algorithms: DES-SHA1 (Data Encryption Standard with SHA-1 hashing).
- Diffie-Hellman Groups: 14, 5 (These groups define the cryptographic strength of the key exchange).

XAUTH (Extended Authentication)
- Type: Disabled (No additional user authentication is required).

Phase 2 Selectors
- Local Address: 192.168.3.0/255.255.255.0 (The subnet on the local network).
- Remote Address: 192.168.6.0/255.255.255.0 (The subnet of the remote network).

The settings ensure a secure Site-to-Site IPsec VPN tunnel between the two networks.



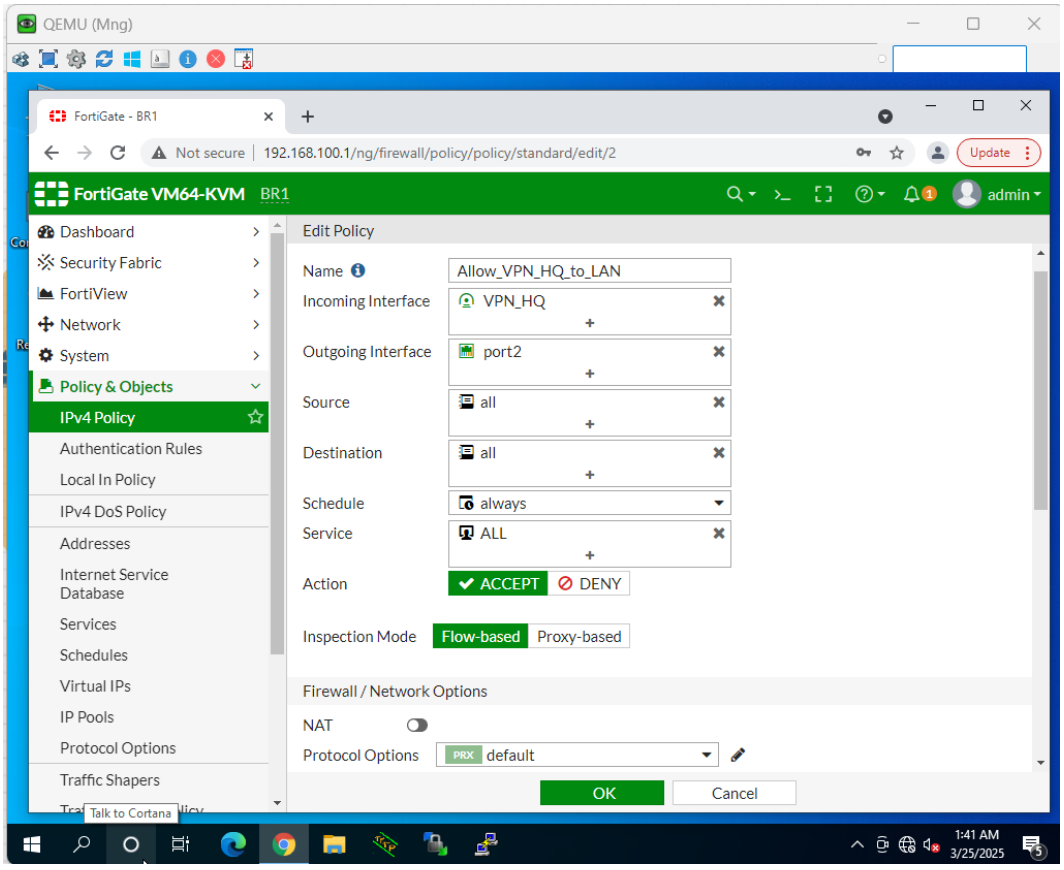
This image displays the IPSec Monitor section in the FortiGate firewall interface, showing the status of an active IPSec VPN connection.

Details from the IPSec Monitor:
1. VPN Name: IPCES_HQ
2. Remote Gateway: 192.168.5.2 (the IP address of the remote VPN endpoint)
3. Incoming Data: 6.96 kB (data received over the VPN tunnel)
4. Outgoing Data: 4.14 kB (data sent through the VPN tunnel)
5. Status: ✅ The green icon next to IPCES_HQ indicates that the VPN tunnel is up and running.

Available Actions:
- Refresh: Updates the status of the VPN tunnel.
- Reset Statistics: Clears the traffic data counters.
- Bring Up: Manually establishes the VPN tunnel if it's down.
- Bring Down: Disconnects the VPN tunnel.
- **Locate on VPN Map

*BR_Fortigate

This figure below demonstrates the configuration interface used to define this policy.



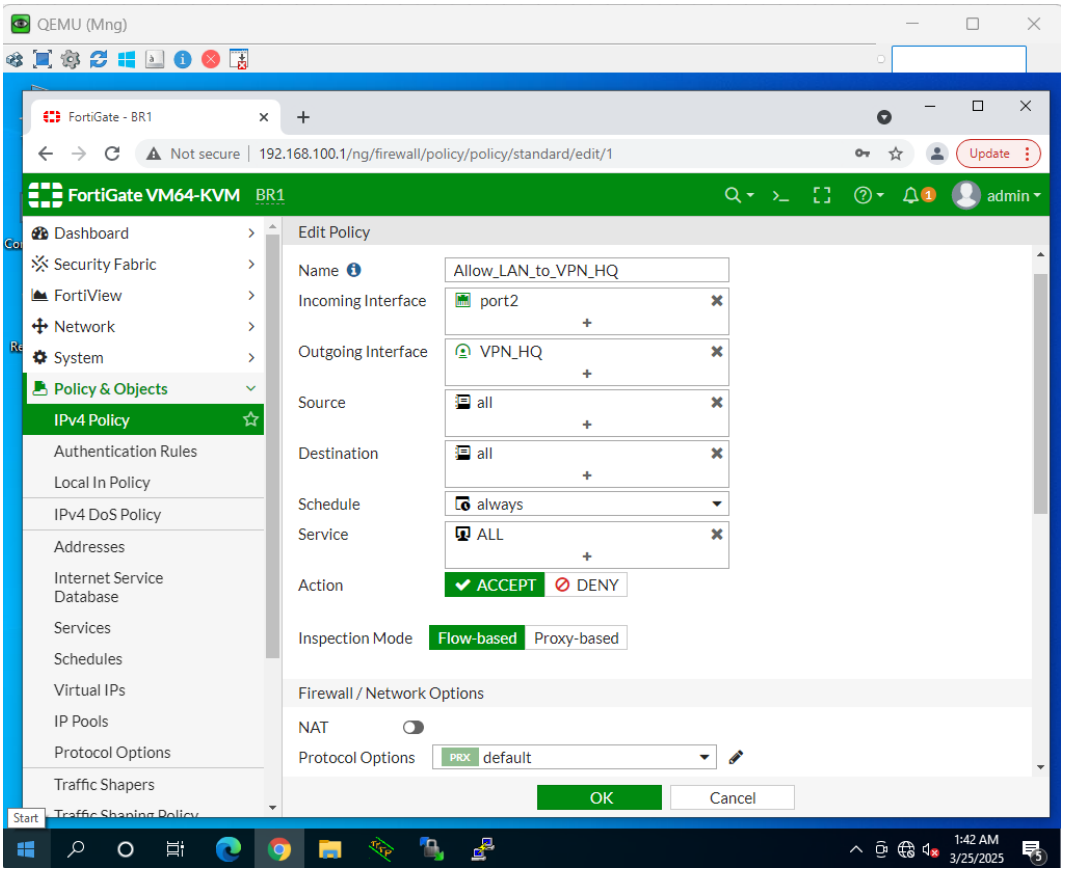
Policy Configuration

- • Name: Allow_VPN_HQ_to_LAN — This is the name assigned to the firewall policy. It clearly indicates that the policy allows traffic from the VPN connection at headquarters to access the internal LAN.
- • Incoming Interface: VPN_HQ — This specifies the interface from which the incoming traffic is expected, in this case, a VPN tunnel from HQ.
- • Outgoing Interface: port2 — The outgoing interface through which traffic will be forwarded to the LAN.
- • Source: all — This means any source IP address coming through the VPN_HQ interface is allowed.
- • Destination: all — All destination IPs are allowed, meaning the VPN client can access any IP within the LAN.
- • Schedule: always — The policy is active at all times.
- • Service: ALL — All services and protocols are allowed, such as HTTP, HTTPS, FTP, etc.
- • Action: ACCEPT — This allows the defined traffic through the firewall.
- • Inspection Mode: Flow-based — Enables scanning based on sessions and real-time traffic inspection for better performance.

Firewall / Network Options

- • NAT: Disabled — NAT is turned off, meaning the source IP address will not be modified when forwarding the traffic.
- • Protocol Options: default — Uses the default settings for protocol handling.

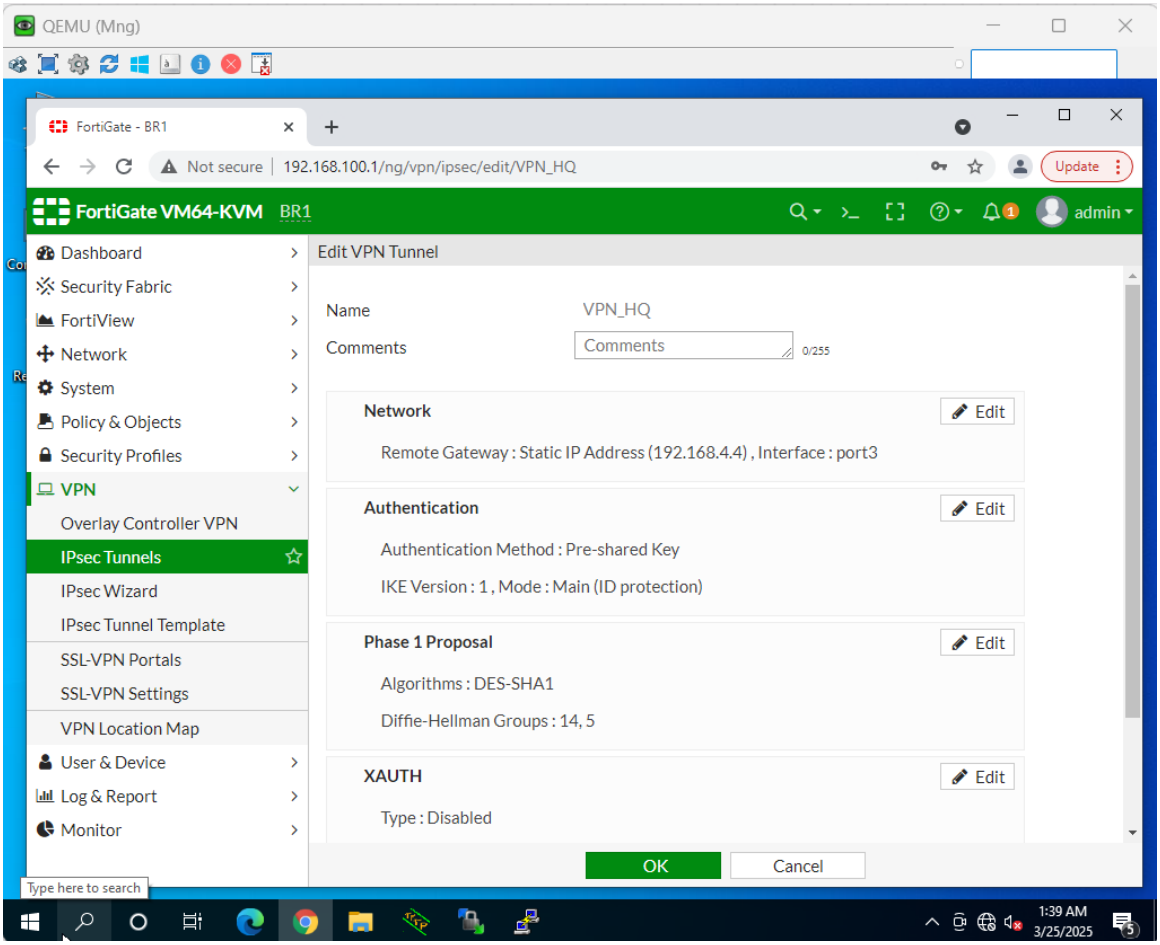
This configuration ensures that users connected via VPN from the headquarters are granted full access to the internal network through port2 interface without restrictions on time, services, or IP addresses.
This is useful for administrative tasks, remote support, and internal resource access.



Allow_LAN_to_VPN_HQ' created on a FortiGate firewall system. This policy is designed to allow traffic from the internal LAN (connected via port2) to reach the VPN HQ interface.

Policy Configuration Details

- Name: Allow_LAN_to_VPN_HQ
- Incoming Interface: port2 (This is the internal LAN port on the branch office firewall.)
- Outgoing Interface: VPN_HQ (Represents the VPN tunnel interface towards the headquarter.)
- Source: all (The policy applies to all traffic coming from the LAN side.)
- Destination: all (The policy allows access to all destinations through the VPN.)
- Schedule: always (This rule is always active, with no time-based restrictions.)
- Service: ALL (All types of services/protocols are allowed, such as HTTP, HTTPS, DNS, etc.)
- Action: ACCEPT (Traffic matching this policy is allowed to pass.)
- Inspection Mode: Flow-based (The firewall uses flow-based inspection for faster performance.)
- NAT: Disabled (No Network Address Translation is applied, allowing original IPs to be preserved.)
- Protocol Options: default (The system uses default protocol handling settings.)

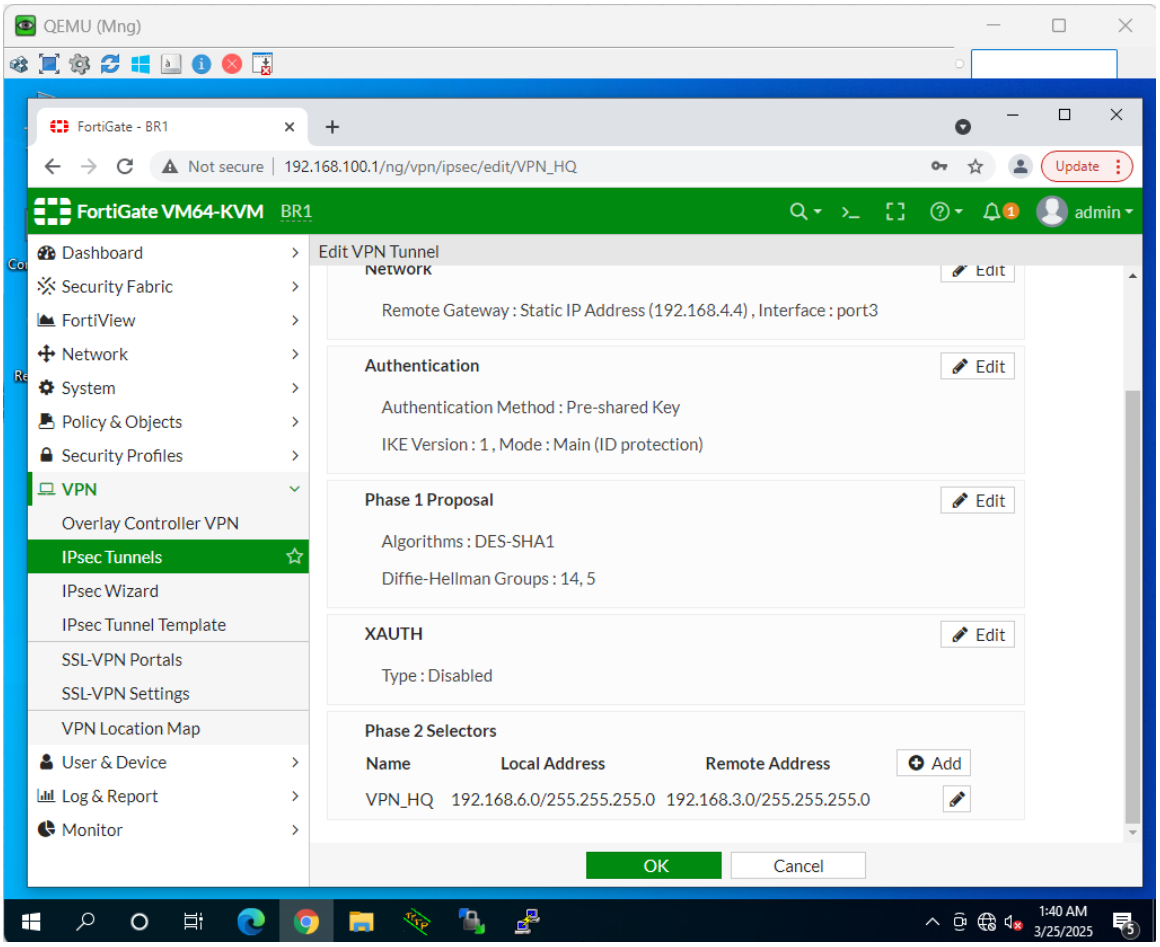


This photo serves as a technical report for the purpose of this configuration is to establish a secure site-to-site VPN tunnel named 'VPN_HQ' between branch offices. The settings were applied and tested within a virtual environment.

VPN Tunnel Configuration Overview
1. Network
Remote Gateway: The VPN tunnel connects to a static IP address 192.168.4.4.

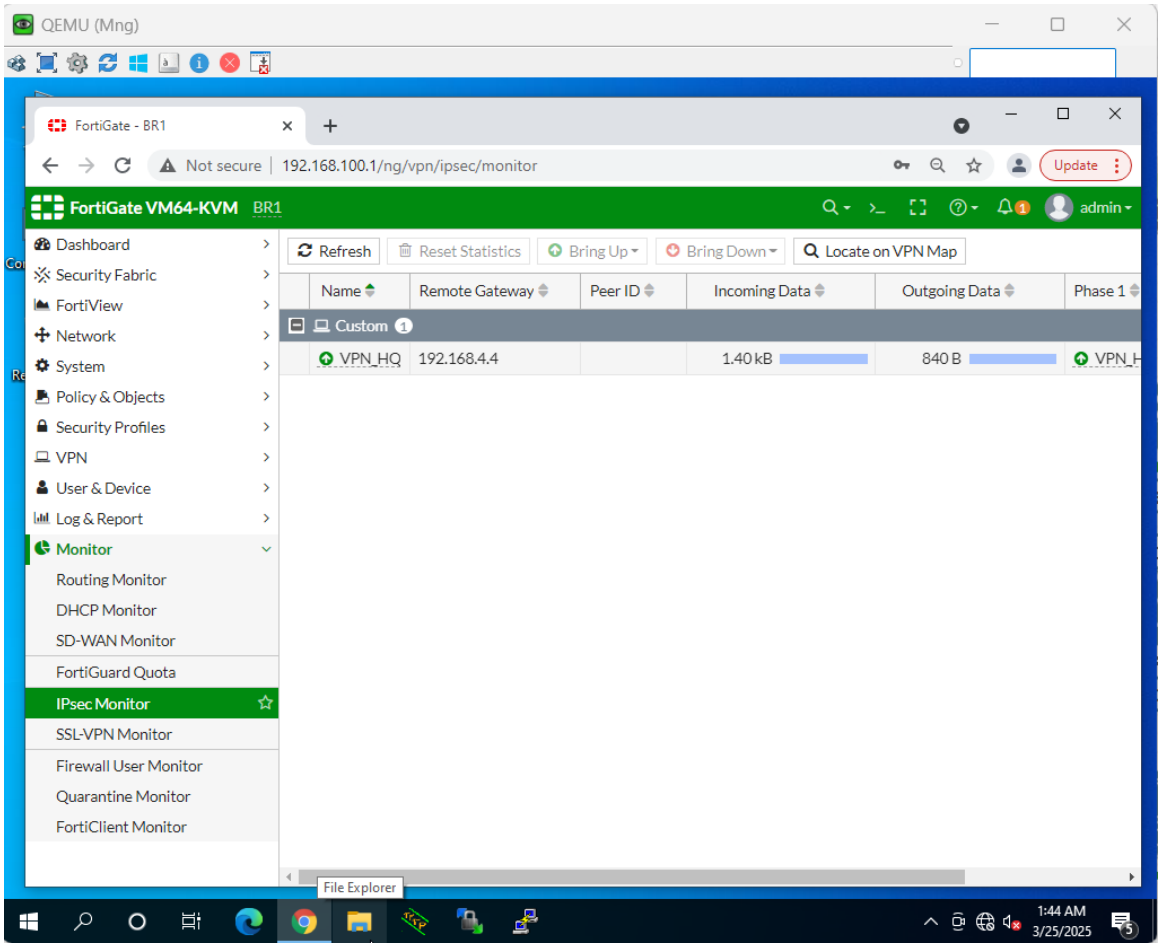
Interface: The local interface used for this VPN connection is port3.

2. Authentication
Authentication Method: The tunnel uses a pre-shared key for authentication.
IKE Version: The Internet Key Exchange version used is IKEv1.
Mode: Main mode is selected, which provides ID protection during negotiation.
Phase 1 Proposal
Algorithms: DES for encryption and SHA1 for hashing.
Diffie-Hellman Groups: Groups 14 and 5 are selected, which define the cryptographic strength during key exchange.
XAUTH
Type: Disabled. XAUTH is not enabled in this configuration, meaning no extended authentication is used for remote clients.



This Photo demonstrates how to configure an IPsec VPN Tunnel on a FortiGate Firewall (FortiGate VM64-KVM) to securely connect two networks over the internet using encryption and authentication methods. The configuration aims to create a Site-to-Site VPN between BR1 and HQ sites.

➤ Phase 2 Selectors
Name Local Address Remote Address
VPN_HQ 192.168.6.0/255.255.255.0 192.168.3.0/255.255.255.0
This defines the local and remote subnets that are allowed to communicate through the VPN.



Monitoring the IPsec VPN Tunnel

After configuring the VPN tunnel, it's essential to monitor the connection to verify that the tunnel is active and transferring data.

The screenshot below shows the IPSec Monitor screen from the FortiGate firewall interface, confirming that the VPN tunnel named VPN_HQ is up and running.

📄 Details from the Monitor:

Field Description

Name VPN_HQ – The name of the VPN tunnel configured.

Remote Gateway 192.168.4.4 – The IP address of the remote FortiGate (Headquarters).

Incoming Data 1.40 kB – This shows the amount of data received through the tunnel.

Outgoing Data 840 B – This indicates the amount of data sent from the branch.

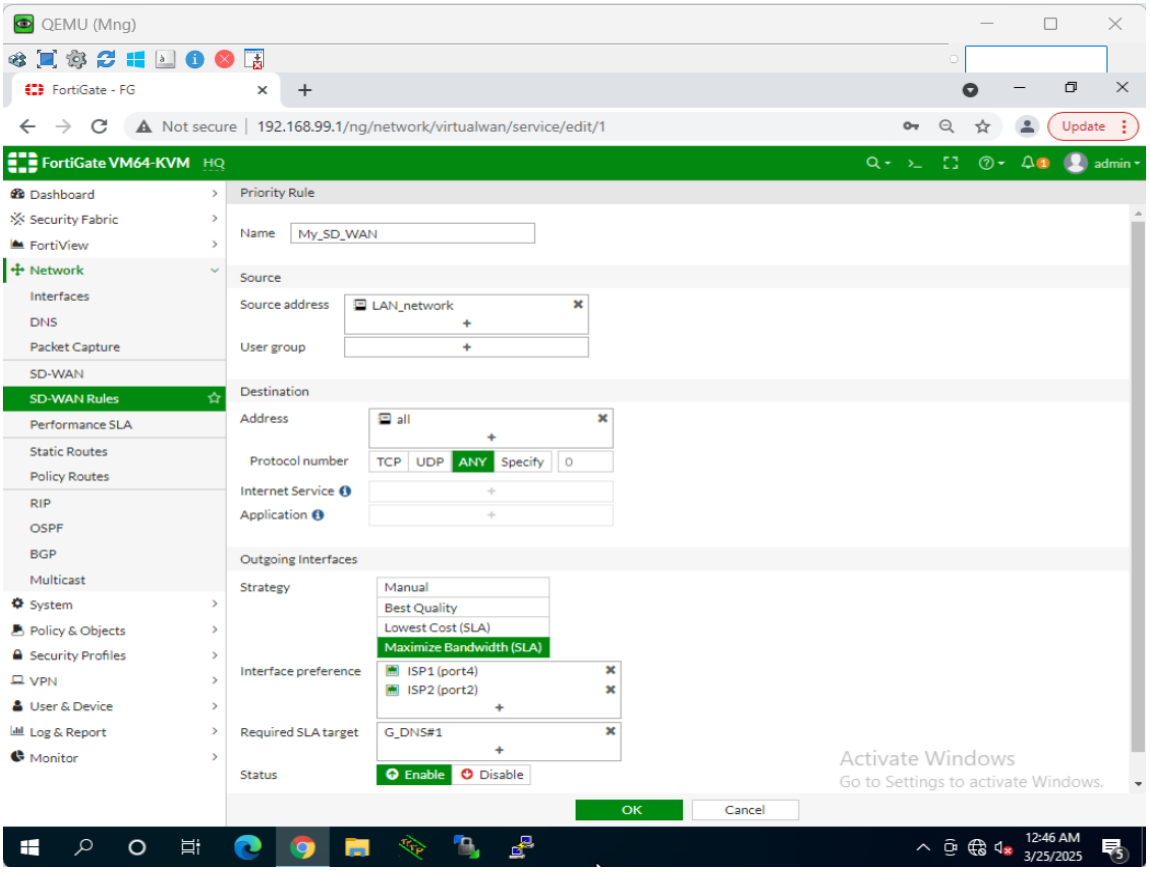
Status Icon ✅ The green icon shows that the VPN tunnel is active and healthy.

📌 Conclusion

The IPSec Monitor helps in verifying the real-time status of the VPN tunnel. It provides insight into data transfer and connection health, ensuring that the VPN is operational.

As shown, data is being exchanged, confirming successful deployment of the Site-to-Site VPN between BR1 and HQ.

5-VPN With SD_WAN



FortiGate SD-WAN Rule Configuration

Overview:

This document provides an analysis of the FortiGate SD-WAN rule configuration from the provided screenshot. The SD-WAN rule is configured to optimize traffic routing based on specific performance criteria.

Configuration Details:

Priority Rule Name:

The rule is named My_SD_WAN.

Source Settings:

Source Address: LAN_network

User Group: Not specified

Destination Settings:

Address: all (indicating that this rule applies to all destinations)

Protocol Number: ANY (applicable to all protocols including TCP and UDP)

Internet Service & Application: Not specified

Outgoing Interfaces:

Strategy: Maximize Bandwidth (SLA) (This means FortiGate will use all available interfaces to maximize bandwidth.

Interface Preference:

ISP1 (port4)

ISP2 (port2)

Required SLA Target: G_DNS#1

Status:

The rule is currently Enabled.

Analysis & Implications

SD-WAN Strategy:

The selected strategy, Maximize Bandwidth (SLA), ensures that both ISP1 and ISP2 links are used for load balancing, distributing traffic across multiple WAN links to optimize bandwidth usage.

Failover & Redundancy:

Since Maximize Bandwidth is selected, FortiGate dynamically switches between the interfaces based on the SLA target (G_DNS#1), ensuring consistent performance and automatic failover in case of link degradation.

Security & Optimization Considerations:

If security policies are not properly configured, some traffic may be routed inefficiently.

The ANY protocol setting allows all traffic types, which might require fine-tuning based on the organization's security policies.

Recommendations:

Define Internet Services or Applications:

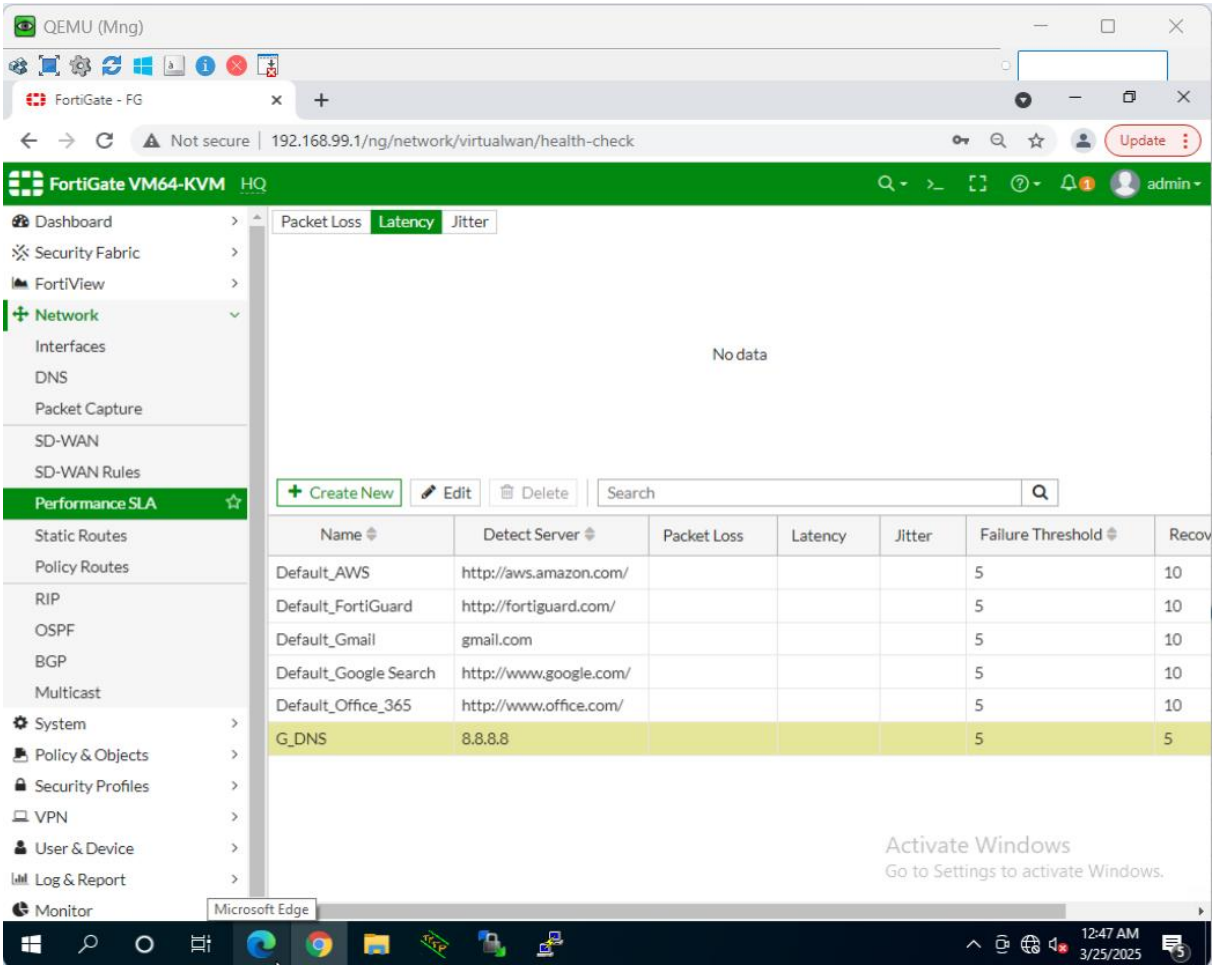
Specify particular applications or services to apply SD-WAN rules more effectively.

Monitor Performance Metrics:

Regularly check the SLA target (G_DNS#1) to ensure performance thresholds are met.

Conclusion:

This SD-WAN rule is optimized for bandwidth maximization by leveraging multiple ISP links dynamically. However, monitoring and fine-tuning should be performed to align with security and performance objectives.



FortiGate SD-WAN Performance SLA Configuration Documentation

1. Overview

This document analyzes the FortiGate SD-WAN Performance SLA configuration as shown in the provided image. The Performance SLA (Service Level Agreement) feature ensures optimal path selection based on network performance metrics such as latency, jitter, and packet loss.

2. Configuration Summary

The screenshot displays the Performance SLA section in the FortiGate GUI.

Multiple SLA targets have been configured for different online services, including AWS, FortiGuard, Gmail, Google Search, Office 365, and a custom-defined DNS check for 8.8.8.8.

3. Key Components

Detect Server: Defines the server to be used for health checks.

Packet Loss: The threshold percentage for packet loss before the path is considered unhealthy.

Latency: Measures the delay in milliseconds for the packet to reach the destination and return.

Jitter: Measures the variation in packet delay.

Failure Threshold: The number of failures required before the link is considered down.

Recovery Time: The duration before a failed link is re-evaluated for recovery.

4. Configured SLA Targets:

Name

Detect Server

Packet Loss
Latency
Jitter
Failure Threshold
Recovery Time
Default_AWS

http://aws.amazon.com/
5%
N/A
N/A
5
10
Default_FortiGuard
http://fortiguard.com/
5%
N/A
N/A
5
10
Default_Gmail
gmail.com
5%
N/A
N/A
5
10
Default_Google_Search
http://www.google.com/
5%
N/A
N/A
5
10
Default_Office_365
http://www.office.com/
5%
N/A
N/A
5
10
G_DNS
8.8.8.8
5%
N/A

N/A

5. Analysis and Recommendations

The configured SLA monitors key cloud services ensuring reliable SD-WAN path selection.

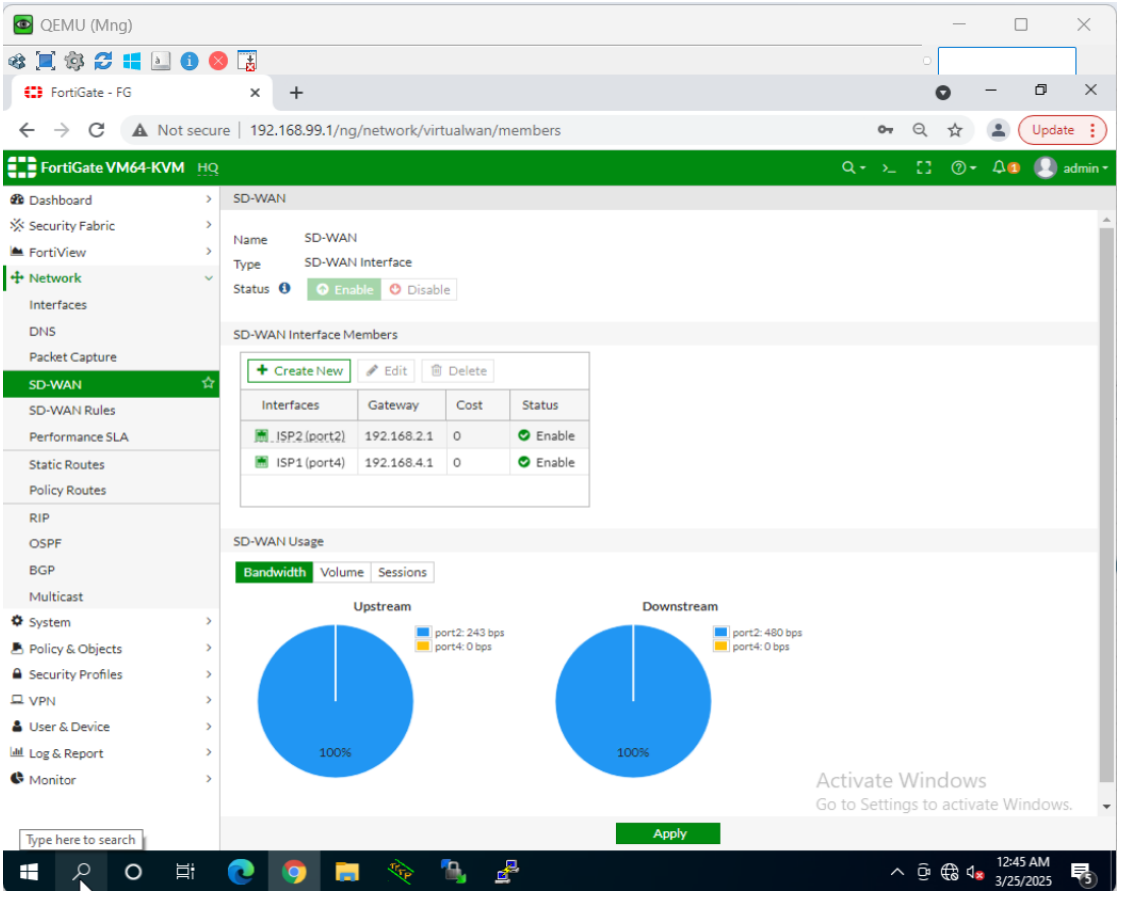
The failure threshold is set to 5, meaning five consecutive failures will mark the link as down.

Recovery times vary, with most services set to 10 seconds, while the DNS service (8.8.8.8) has a shorter recovery time of 5 seconds.

To optimize performance, consider adjusting thresholds based on real-time network conditions.

6. Conclusion

This Performance SLA setup ensures that FortiGate can intelligently select the best-performing path for critical cloud services based on network health metrics. Proper monitoring of these SLA parameters will improve network stability and efficiency.



Overview

This document provides an analysis of the SD-WAN interface configuration shown in the FortiGate VM64-KVM dashboard screenshot.

SD-WAN Interface Configuration

Interface Members

The FortiGate device has two WAN interfaces configured as SD-WAN members:

ISP2 (port2)

Gateway: 192.168.2.1

Cost: 0
Status: Enabled

ISP1 (port4)
Gateway: 192.168.4.1
Cost: 0
Status: Enabled
Current Traffic Statistics
The bandwidth usage shows the following real-time traffic patterns:

Upstream Traffic:
port2 (ISP2): 243 bps (bits per second)
port4 (ISP1): 0 bps (no current traffic)

Downstream Traffic:
port2 (ISP2): 480 bps
port4 (ISP1): 0 bps

Observations
Equal Cost Configuration: Both interfaces have a cost of 0, which means they are equally preferred in the SD-WAN path selection algorithm.

Active Traffic: Currently, all traffic is being routed through ISP2 (port2) as indicated by the bandwidth usage statistics.

ISP1 Not Utilized: ISP1 (port4) shows no current traffic flow, suggesting either:

No active sessions requiring bandwidth

SD-WAN rules are preferring ISP2

ISP1 may be a backup connection

Interface Naming: The interfaces follow a logical naming convention (ISP1, ISP2) which helps with administration.

Recommendations
Review SD-WAN Rules: Check the SD-WAN rules configuration to understand why ISP1 isn't being utilized.

Cost Adjustment: Consider adjusting the cost values if one connection should be preferred over the other.

Performance SLA: Configure Performance SLA measurements to enable dynamic path selection based on real-time performance metrics.

Load Balancing: If both connections should be active, implement load balancing rules to distribute traffic across both

ISPs.

Monitoring: Continue monitoring the bandwidth usage patterns to identify any anomalies or underutilized resources.

Navigation Path

The SD-WAN interface configuration can be found in the FortiGate dashboard under:

Dashboard > SD-WAN > SD-WAN Interface Members