رواد مصر الرقمية

Project Documentation

Implementing VPN Solutions with FortiGate

Prepared By

Name	ID	Contact
Mohab Nasser Abdelkader	21040461	mohabnasserr@gmail.com
Ahmed Khaled Mohamed	21053590	pmqz8899@gmail.com
Amr Khaled Ahmed	21030745	amr171516@gmail.com
Youssef Mohamed Youssef	21053592	youssefmy825@gmail.com

2025 - Round 3 Graduation Project
Version 3.0

1. Project Description

This project focuses on designing and implementing secure Virtual Private Network (VPN) solutions using FortiGate firewalls to support both remote user connectivity and inter-site secure communication. The work includes three main components:

1. SSL VPN for Remote Access

A secure SSL VPN was configured to enable remote users to safely connect to the internal network through encrypted HTTPS tunnels.
Key configurations included:

- **User authentication and access control**
- **Custom IP pools for VPN clients**
- **Security policies to regulate and monitor traffic**
  Connectivity was verified using FortiClient in both web mode and tunnel mode, ensuring reliable and secure remote access.

1.2. IPsec Site-to-Site VPN

A Site-to-Site IPsec tunnel was established between two FortiGate devices to securely connect separate LAN networks over the internet.
The configuration involved:

- **Phase 1 and Phase 2 parameters**
- **Static routing**
- **Firewall policies**
  This setup ensures fully encrypted, seamless communication between both sites.

1.3. SD-WAN Implementation

SD-WAN was implemented to optimize network performance across multiple internet links.
The solution provides:

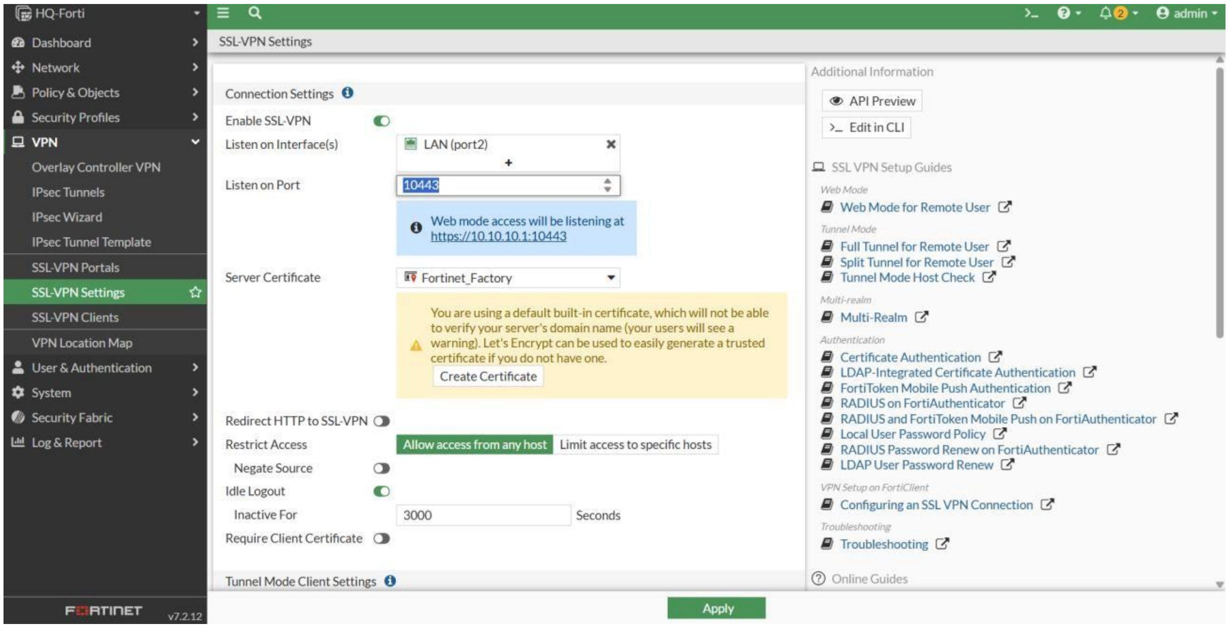
- **Intelligent traffic distribution**
- **Application-aware routing (e.g., VoIP, video, web)**
- **Automatic failover and load balancing**
- **Real-time link performance monitoring**
  This ensures high availability, improved efficiency, and enhanced reliability for critical applications.

2. SSL VPN Configuration Documentation

2.1 HQ FortiGate SSL VPN Configuration

Step 1: SSL VPN Settings
Navigate: **VPN → SSL-VPN Settings Configuration**

- Listen on Interface: port2 (LAN)
- Listen on Port: 10443 (HTTPS)
- Server Certificate: Fortinet_Factory
- Idle Timeout: 3000 seconds
- Tunnel Mode IP Pools: SSLVPN_TUNNEL_ADDR1 (10.212.134.200 - 10.212.134.210)
- IPv6 Pools: SSLVPN_TUNNEL_IPv6_ADDR1 (fdff:ffff::/120)
- Default Portal: full-access



SSL-VPN Settings

Connection Settings

Enable SSL-VPN: enabled

Listen on Interface(s): LAN (port2)

Listen on Port: 10443

Web mode access will be listening at https://10.10.10.1:10443

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.

Redirect HTTP to SSL-VPN: disabled

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

Negate Source: disabled

Idle Logout: enabled

Inactive For: 3000 Seconds

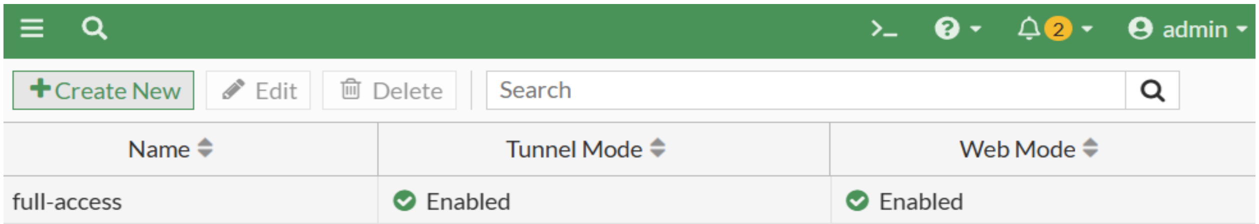
Require Client Certificate: disabled

Tunnel Mode Client Settings

Portal Settings (full-access):

- Tunnel Mode: Enabled
- IPv6 Tunnel Mode: Enabled
- Web Mode: Enabled

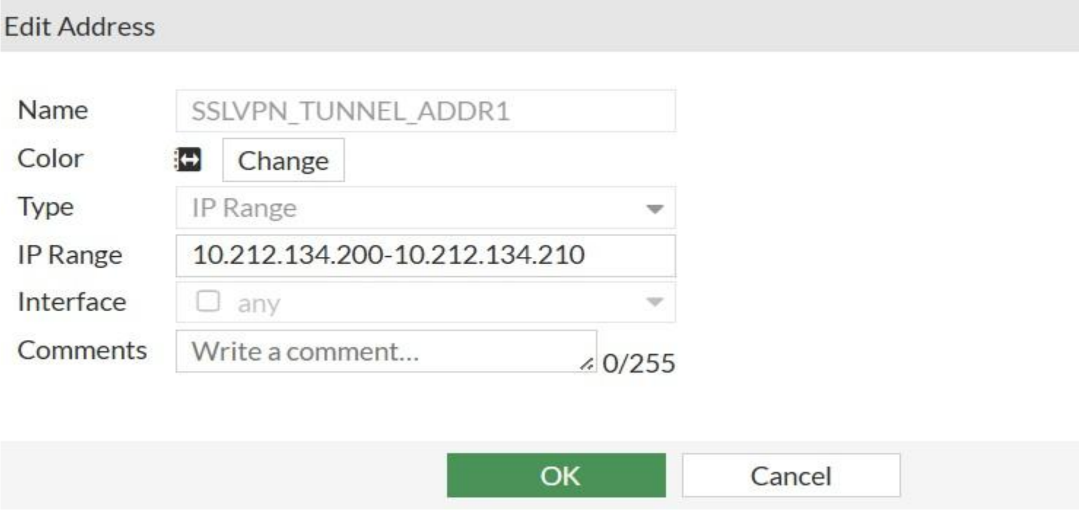
- IP Pools: SSLVPN_TUNNEL_ADDR1



Name	Tunnel Mode	Web Mode
full-access	✓ Enabled	✓ Enabled

Step 2: Create IP Pool for SSL VPN Users

- Name: SSLVPN_TUNNEL_ADDR1
- Type: IP Range
- Start IP: 10.212.134.200
- End IP: 10.212.134.210


Edit Address

Name	SSLVPN_TUNNEL_ADDR1
Color	Change
Type	IP Range
IP Range	10.212.134.200-10.212.134.210
Interface	□ any
Comments	Write a comment... 0/255

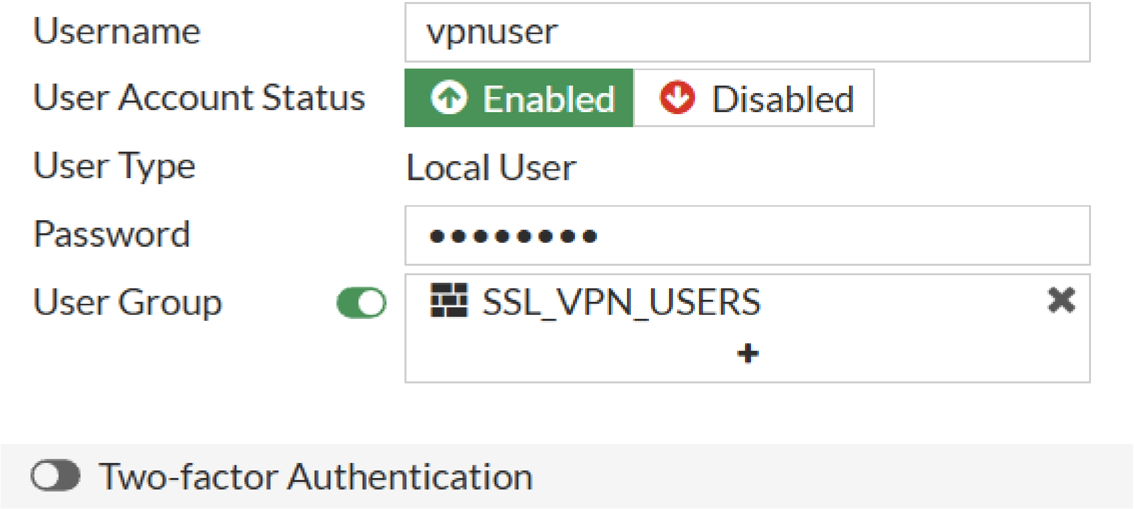
Step 3: Create User Account

- Username: vpnuser
- Type: Local User
- Password: (Set secure password)

Step 4: Create User Group

- Name: SSL_VPN_USERS
- Type: Firewall

- Status: Enabled



Username: vpnuser

User Account Status: [✓ Enabled] Disabled

User Type: Local User

Password: •••••••••

User Group ● SSL_VPN_USERS

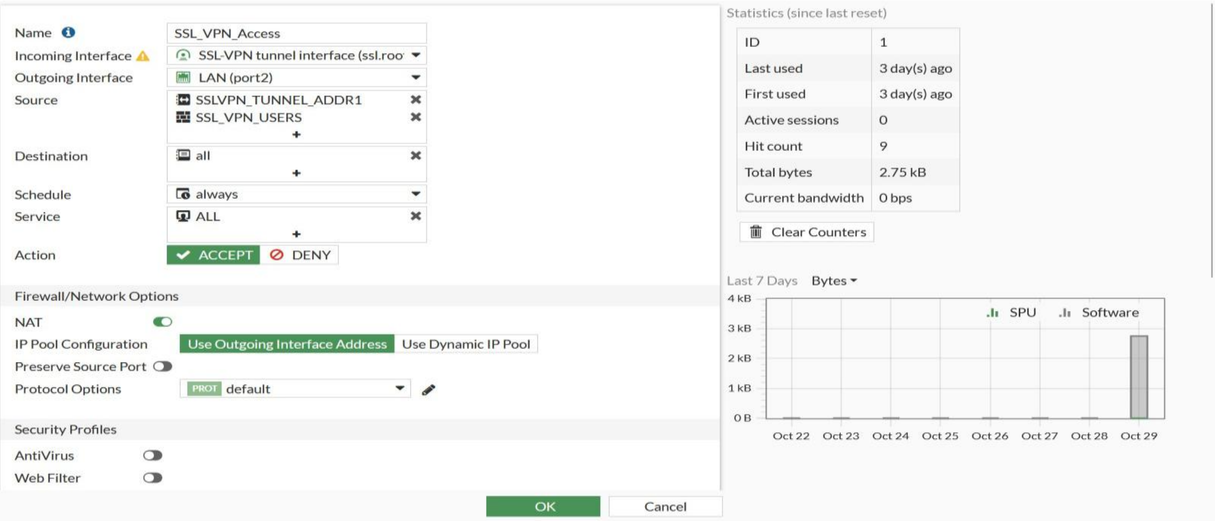
○ Two-factor Authentication

- Members: vpnuser

Step 5: Firewall Policy Configuration

- Name: SSL_VPN_Access
- Incoming Interface: SSL VPN tunnel interface (ssl.root)
- Outgoing Interface: LAN (port2)
- Source: SSLVPN_TUNNEL_ADDR1
- Destination: All
- Schedule: Always
- Service: All
- Action: ACCEPT

- NAT: Enabled (Use Outgoing Interface Address)



Name: SSL_VPN_Access
Incoming Interface: SSL-VPN tunnel interface (ssl.roo
Outgoing Interface: LAN (port2)
Source: SSLVPN_TUNNEL_ADDR1, SSL_VPN_USERS
Destination: all
Schedule: always
Service: ALL
Action: ✓ ACCEPT | DENY

Firewall/Network Options
NAT: ●
IP Pool Configuration: Use Outgoing Interface Address | Use Dynamic IP Pool
Preserve Source Port: ○
Protocol Options: PROT default

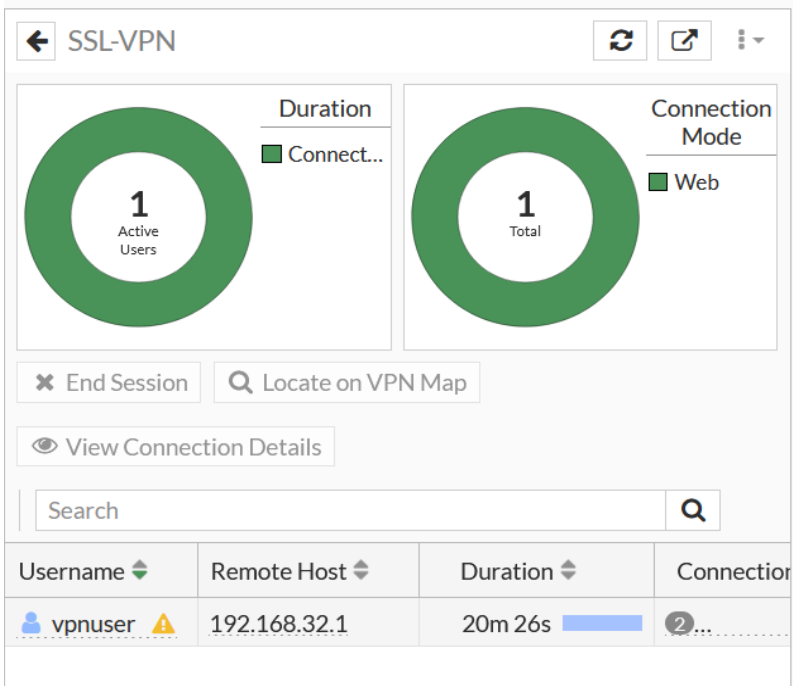
Security Profiles
AntiVirus: ○
Web Filter: ○

Statistics (since last reset)

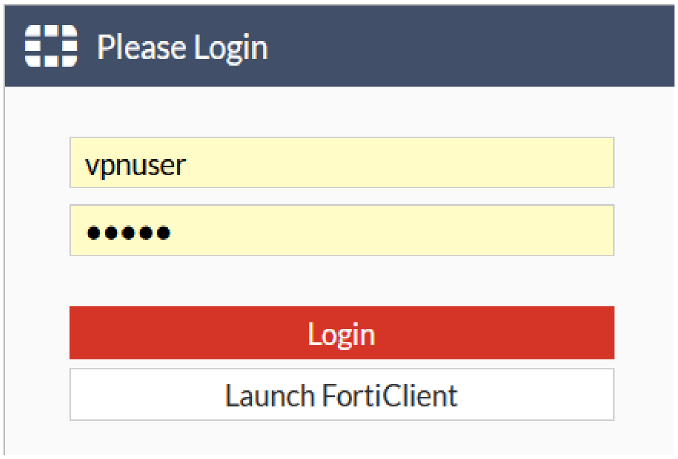
ID	1
Last used	3 day(s) ago
First used	3 day(s) ago
Active sessions	0
Hit count	9
Total bytes	2.75 kB
Current bandwidth	0 bps

Step 6: Web-Based Mode Testing

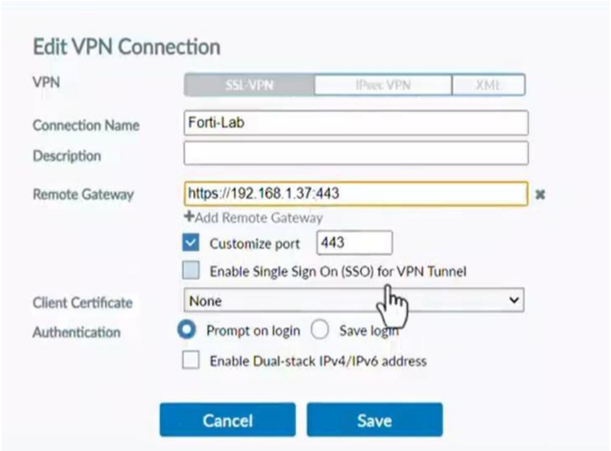
- SSL VPN portal accessible at https://192.168.32.135:10443
- FortiClient launch and download options available
- Verify login as vpnuser and check active connections on FortiGate Dashboard → Network



Username	Remote Host	Duration	Connectior
vpnuser	192.168.32.1	20m 26s	2...



vpnuser
●●●●●



Edit VPN Connection

VPN: SSL-VPN | IPsec VPN | XML
Connection Name: Forti-Lab
Description:
Remote Gateway: https://192.168.1.37:443
+Add Remote Gateway
☑ Customize port 443
□ Enable Single Sign On (SSO) for VPN Tunnel
Client Certificate: None
Authentication: ● Prompt on login ○ Save login
□ Enable Dual-stack IPv4/IPv6 address

Step 7: Tunnel Mode Testing

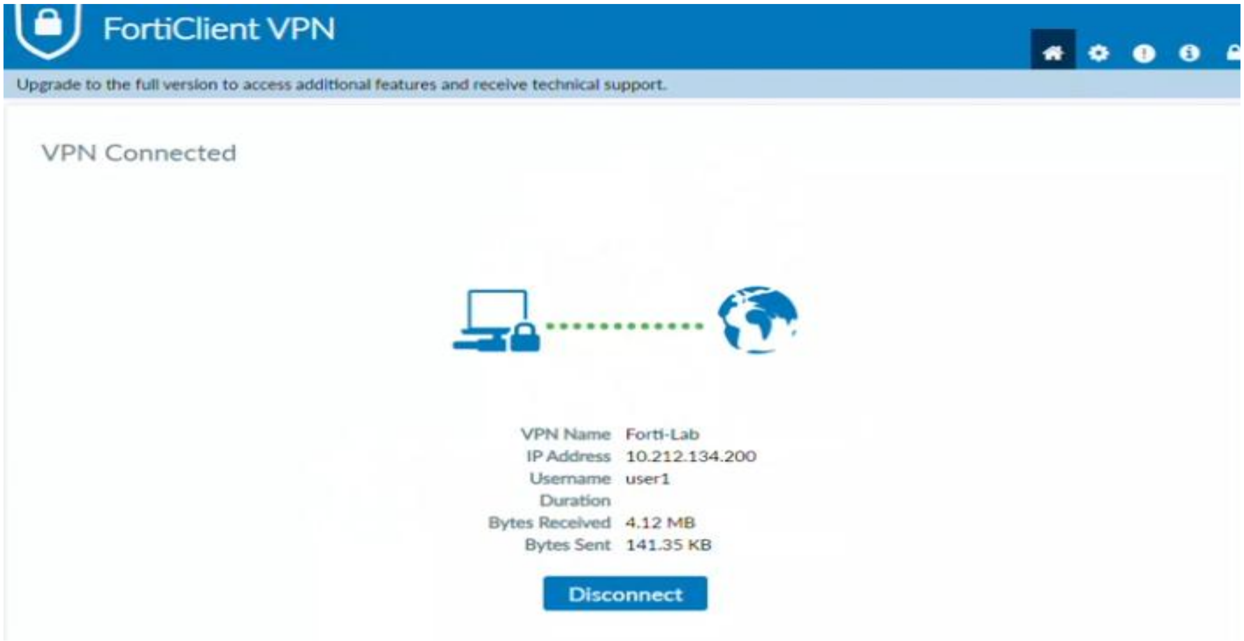
- VPN Name: <Specify>
- Connection Type: SSL-VPN
- Remote Gateway: https://<IP>:10443
- Port: 10443
- Authentication: Username/Password
- Dual-stack IPv4/IPv6: Enabled

Step 8: Connection and Monitoring

In this step, after establishing the connection using **tunnel mode**, I selected **Forti-Lab** and tested the setup using the **VPN user** I had previously created.

As shown in the image, the monitoring interface displays several key details for each connected user:

1. **Username** – identifies the authenticated VPN user.
2. **IP Address** – shows the assigned IP for the VPN session.
3. **Connection Duration** – indicates how long the user has been connected.
4. **Bytes Sent and Received** – displays the amount of data transmitted during



FortiClient VPN

Upgrade to the full version to access additional features and receive technical support.

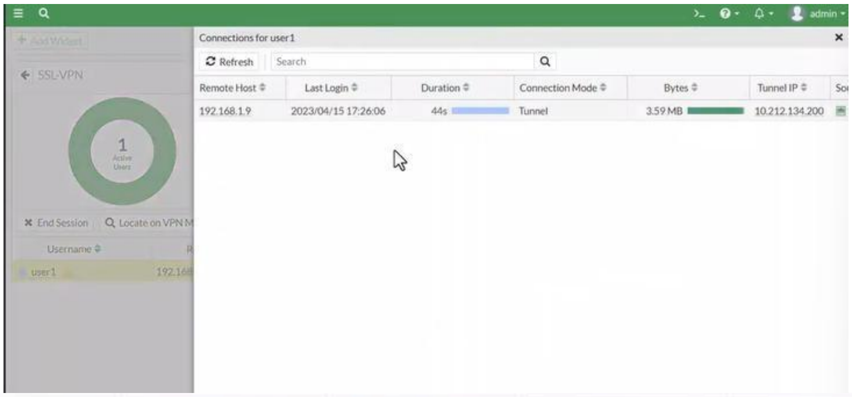
VPN Connected

VPN Name Forti-Lab
IP Address 10.212.134.200
Username user1
Duration
Bytes Received 4.12 MB
Bytes Sent 141.35 KB

Step 9: Monitoring & Active Connections:

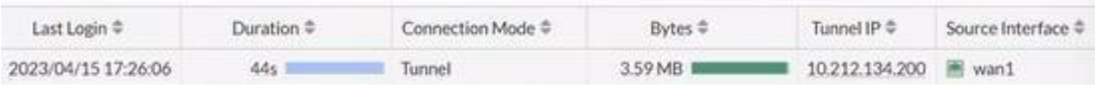
Dash Board Shows :

- Displays: Username, IP, Connection Duration, Bytes Sent/Received
- Active Users: 1
- Connection Mode: Web
- Username: vpnuser
- Remote Host: 192.168.1.9
- Tunnel Ip: 10.212.134.200
- Duration: 44s
- Source interface: Wan1
- Tunnel IP: Assigned from SSLVPN_TUNNEL_ADDR1 pool



Connections for user1

Remote Host	Last Login	Duration	Connection Mode	Bytes	Tunnel IP	So
192.168.1.9	2023/04/15 17:26:06	44s	Tunnel	3.59 MB	10.212.134.200	



Last Login	Duration	Connection Mode	Bytes	Tunnel IP	Source Interface
2023/04/15 17:26:06	44s	Tunnel	3.59 MB	10.212.134.200	wan1

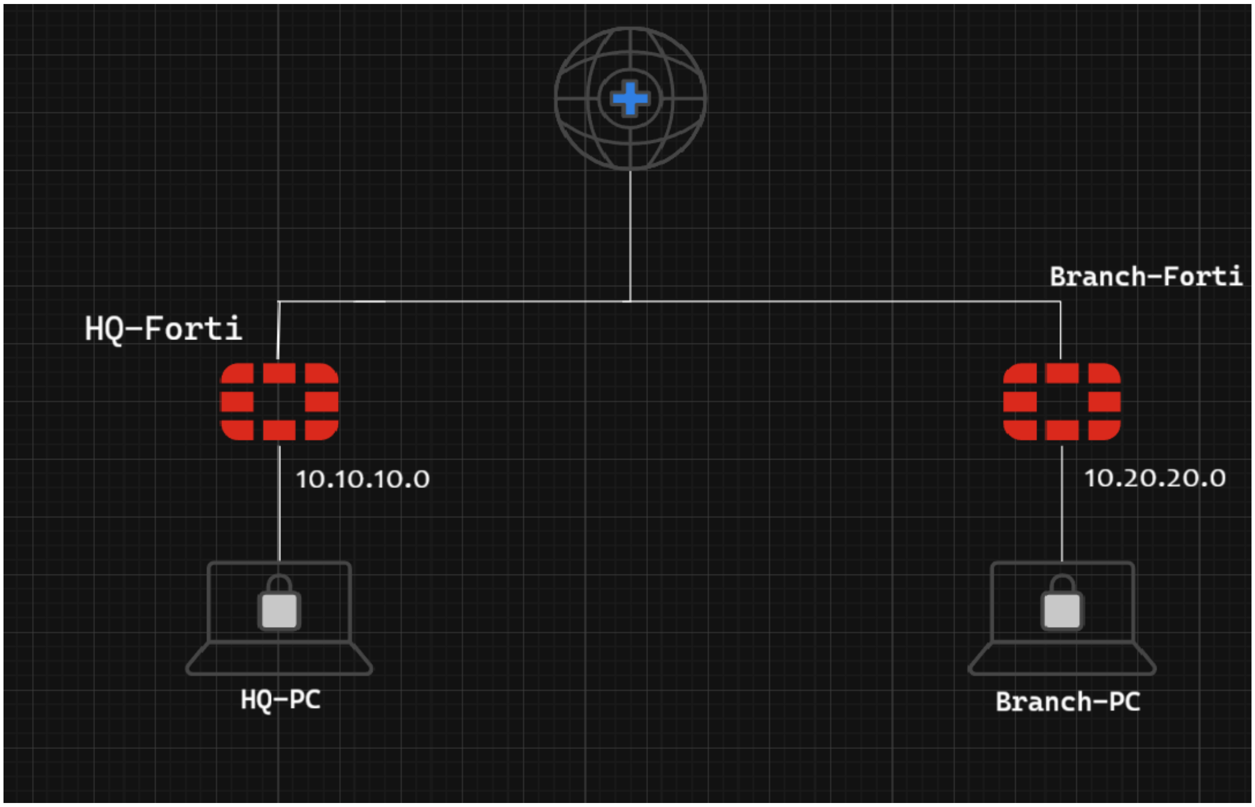
3. IPsec VPN Configuration Documentation

3.1 Objective

Establish a secure IPsec VPN tunnel between two FortiGate devices for encrypted communication between remote networks.

3.2 Network Topology

Site A LAN (10.10.10.0/24) --- FortiGate A ---- Internet ---- FortiGate B --- Site B LAN (10.20.20.0/24)

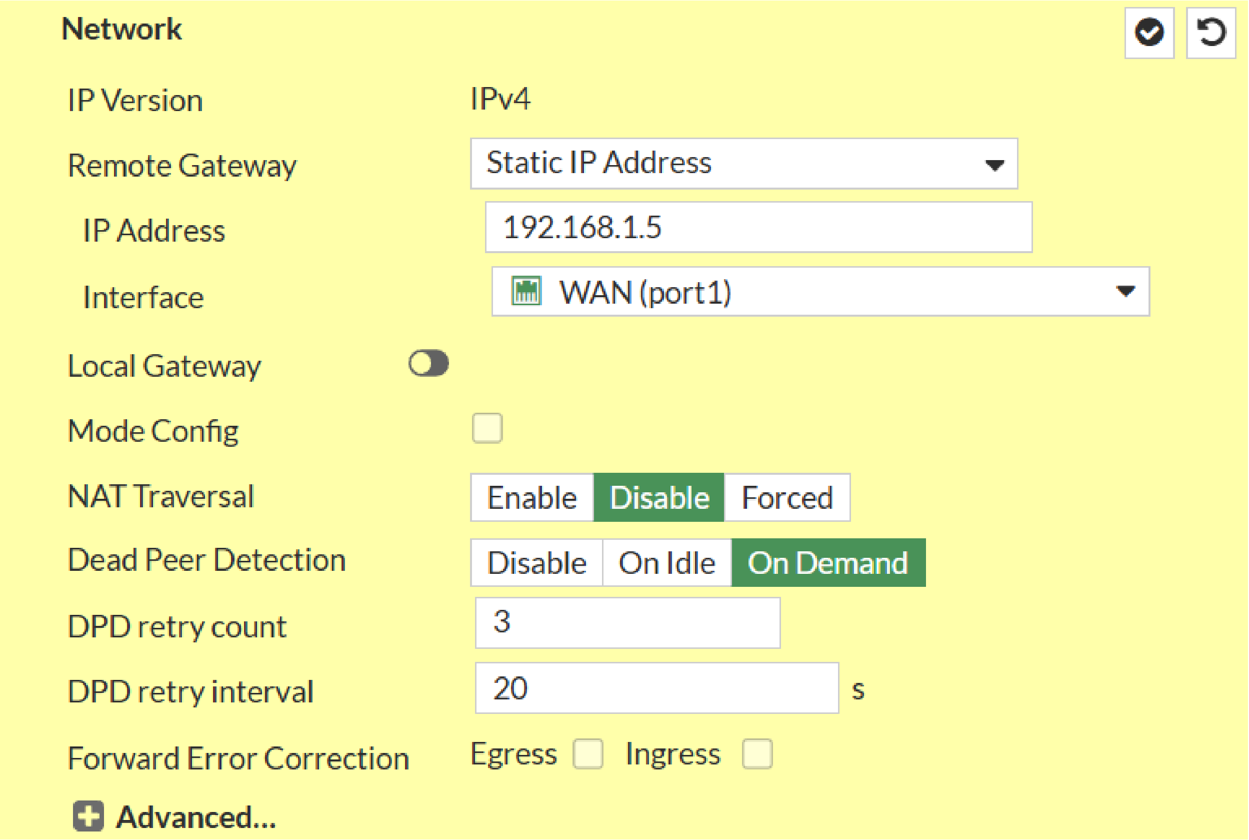


- Two FortiGate firewalls were used to connect two different LAN networks through the internet using an IPsec VPN tunnel.
- Each FortiGate represents a branch office / Headquarter office.

3.3 HQ FortiGate Configuration

Step 1: Phase 1 Configuration

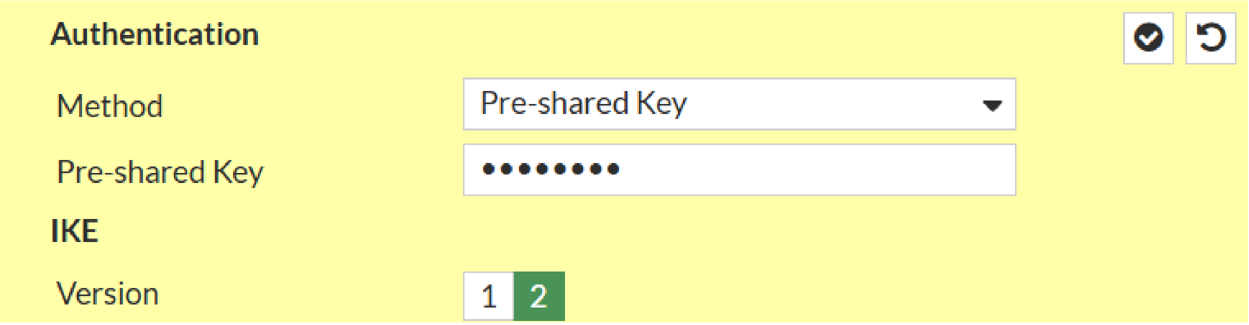
- VPN → IPsec Tunnels → Create New → Custom
- Name: HQ-to-Branch
- Remote Gateway: 192.168.1.5
- Interface: WAN (port1)
- Authentication Method: Pre-shared Key
- IKE Version: IKEv2
- Encryption: DES
- Authentication: SHA384
- DH Group: 14,5
- Key Lifetime: 86400



Network

IP Version	IPv4
Remote Gateway	Static IP Address
IP Address	192.168.1.5
Interface	WAN (port1)
Local Gateway	○
Mode Config	□
NAT Traversal	Enable [✓ Disable] Forced
Dead Peer Detection	Disable On Idle [✓ On Demand]
DPD retry count	3
DPD retry interval	20 s
Forward Error Correction	Egress □ Ingress □

Advanced...



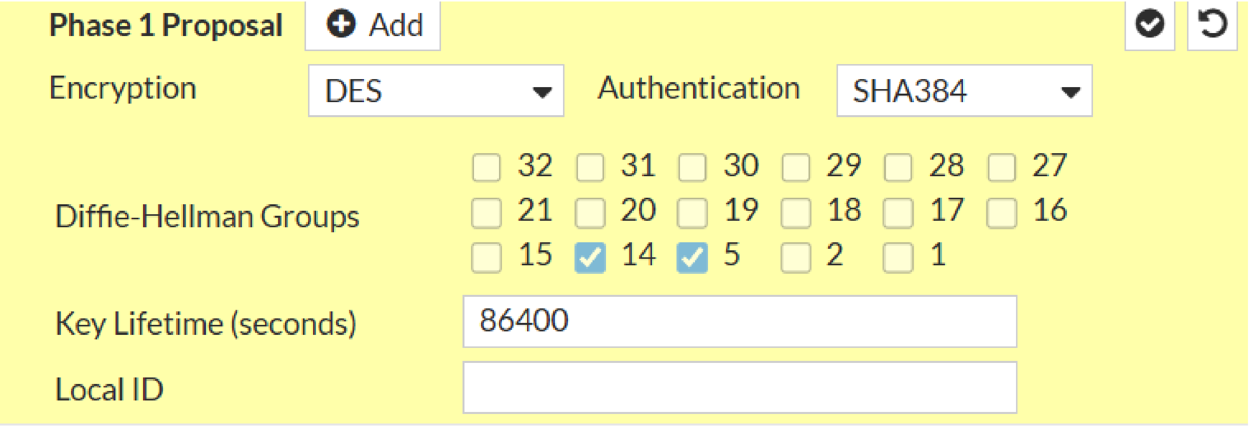
Authentication

Method: Pre-shared Key

Pre-shared Key: •••••••••

IKE

Version: 1 [✓ 2]



Phase 1 Proposal Add

Encryption: DES   Authentication: SHA384

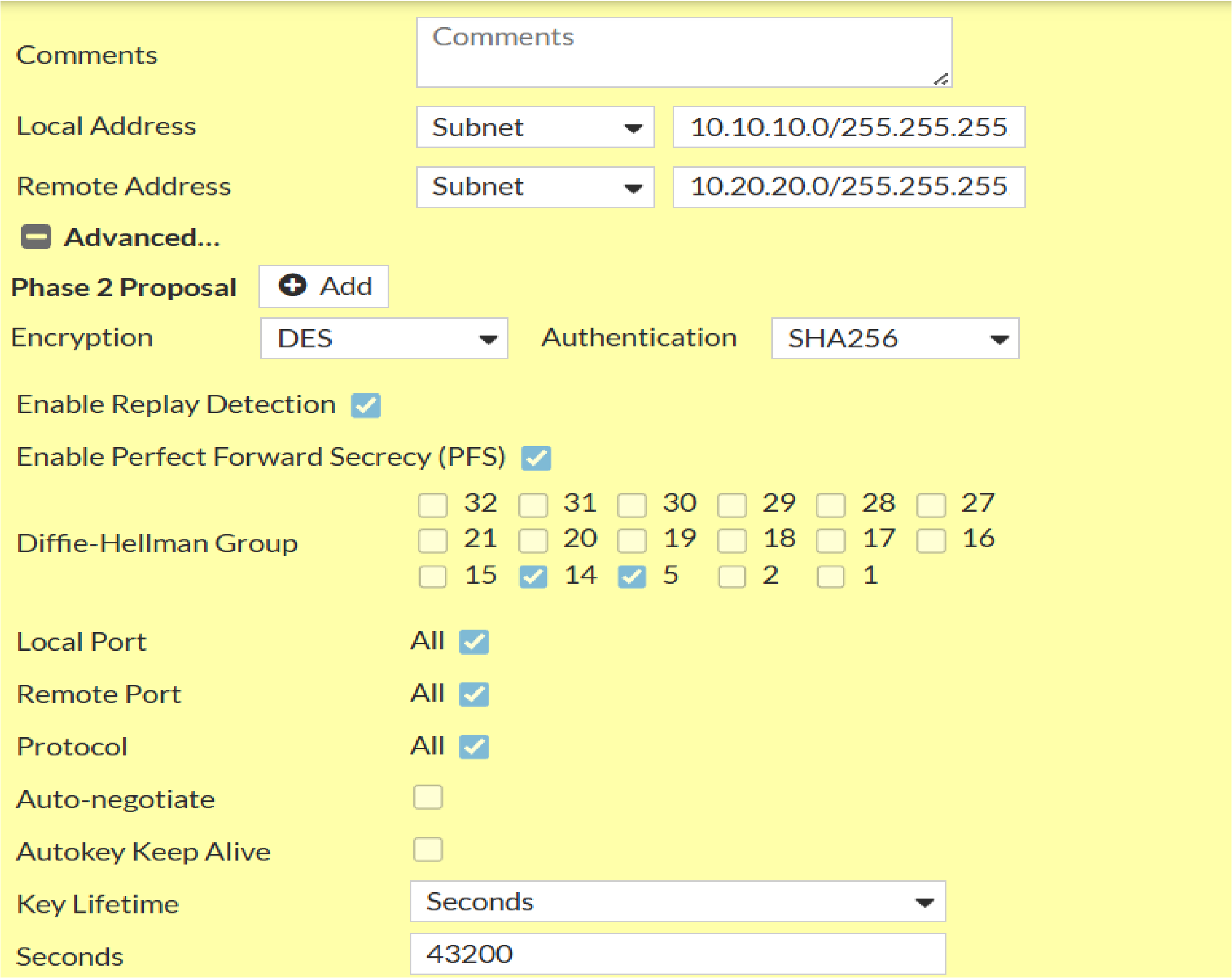
Diffie-Hellman Groups:
☐ 32 ☐ 31 ☐ 30 ☐ 29 ☐ 28 ☐ 27
☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16
☐ 15 ☑ 14 ☑ 5 ☐ 2 ☐ 1

Key Lifetime (seconds): 86400

Local ID:

Step 2: Phase 2 Configuration

- **Local Subnet:** 10.10.10.0/255.255.255.0
- **Remote Subnet:** 10.20.20.0/255.255.255.0
- **Encryption:** DES
- **Authentication:** SHA256
- **Enable Replay Detection**



Comments	Comments	
Local Address	Subnet	10.10.10.0/255.255.255
Remote Address	Subnet	10.20.20.0/255.255.255

Advanced...

Phase 2 Proposal

Encryption	DES	Authentication	SHA256

Enable Replay Detection ☑

Enable Perfect Forward Secrecy (PFS) ☑

Diffie-Hellman Group

□ 32	□ 31	□ 30	□ 29	□ 28	□ 27
□ 21	□ 20	□ 19	□ 18	□ 17	□ 16
□ 15	☑ 14	☑ 5	□ 2	□ 1	

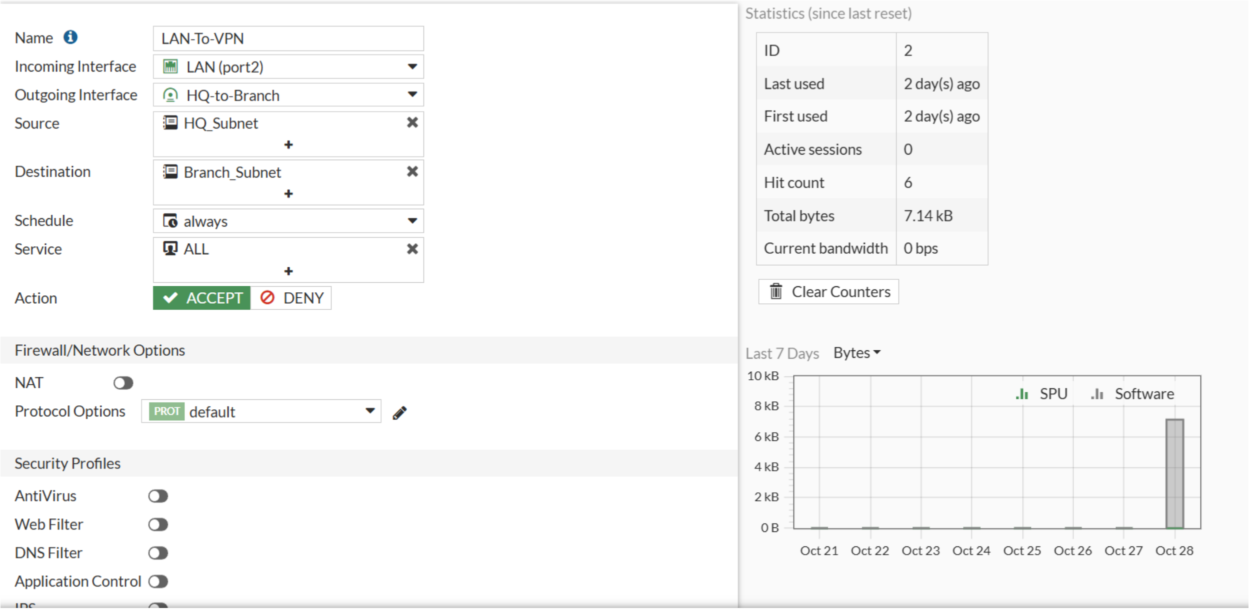
Local Port	All ☑
Remote Port	All ☑
Protocol	All ☑
Auto-negotiate	□
Autokey Keep Alive	□
Key Lifetime	Seconds
Seconds	43200

Step 3: Firewall Policies

- Create policies to allow traffic from LAN → VPN and VPN → LAN on both FortiGates.

1- LAN-To-VPN

- ○ **Incoming Interface:** LAN (port2)
- ○ **Outgoing Interface:** HQ-to-Branch
- ○ **Action:** Accept
- ○ **NAT:** Disabled
- ○ **Source :** HQ Subnet (10.10.10.0/24)
- ○ **Destination :** HQ Subnet (10.20.20.0/24)



Name	LAN-To-VPN
Incoming Interface	LAN (port2)
Outgoing Interface	HQ-to-Branch
Source	HQ_Subnet
Destination	Branch_Subnet
Schedule	always
Service	ALL
Action	✓ ACCEPT ⊘ DENY

Firewall/Network Options

NAT ○

Protocol Options PROT default

Security Profiles

AntiVirus ○

Web Filter ○

DNS Filter ○

Application Control ○

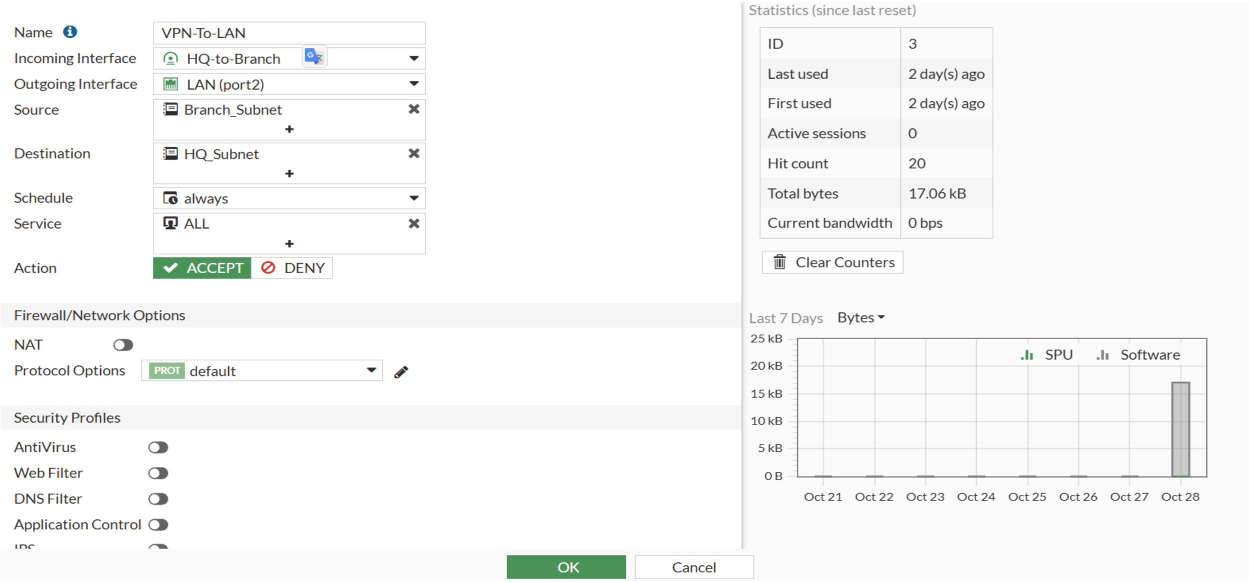
Statistics (since last reset)

ID	2
Last used	2 day(s) ago
First used	2 day(s) ago
Active sessions	0
Hit count	6
Total bytes	7.14 kB
Current bandwidth	0 bps

Clear Counters

VPN-to-LAN

- **Incoming Interface:** HQ-to-Branch
- **Outgoing Interface:** LAN (port2)
- **Action:** Accept
- **NAT:** Disabled
- **Source :** Branch Subnet (10.20.20.0/24)
- **Destination :** HQ Subnet (10.10.10.0/24)



Name	VPN-To-LAN
Incoming Interface	HQ-to-Branch
Outgoing Interface	LAN (port2)
Source	Branch_Subnet
Destination	HQ_Subnet
Schedule	always
Service	ALL
Action	✓ ACCEPT ⊘ DENY

Firewall/Network Options

NAT ○

Protocol Options PROT default

Security Profiles

AntiVirus ○

Web Filter ○

DNS Filter ○

Application Control ○

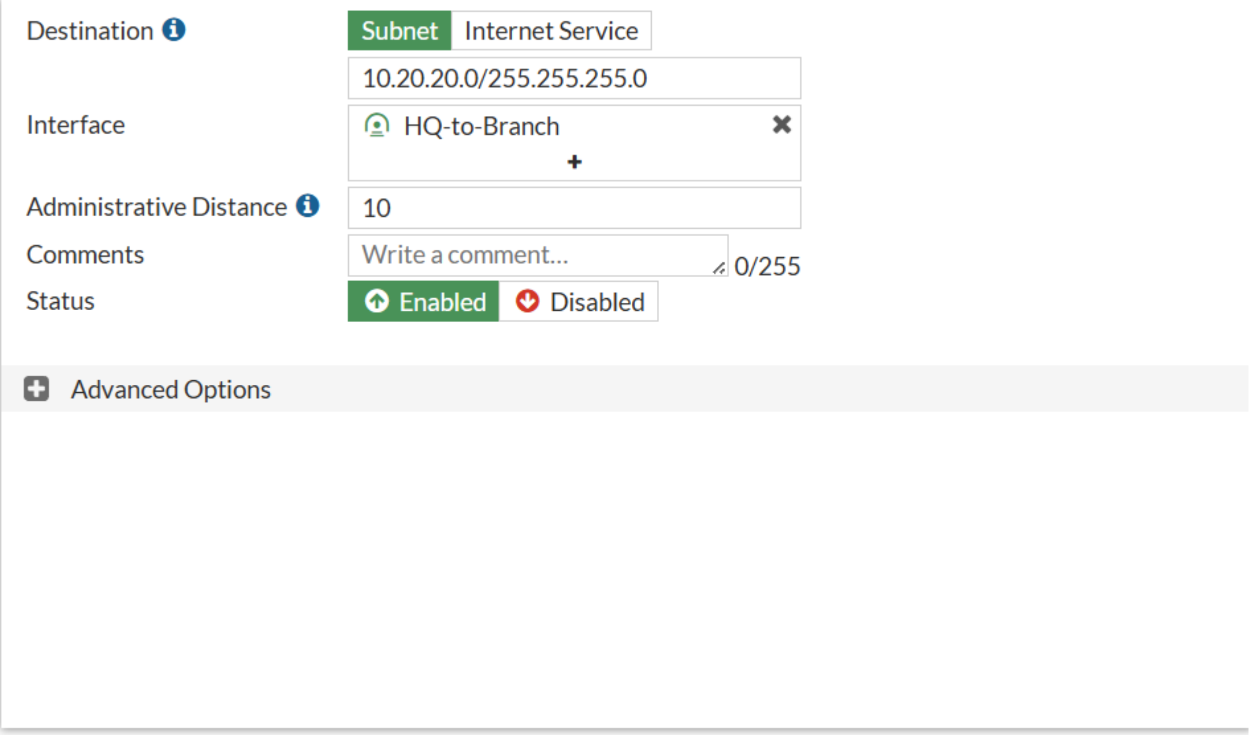
Statistics (since last reset)

ID	3
Last used	2 day(s) ago
First used	2 day(s) ago
Active sessions	0
Hit count	20
Total bytes	17.06 kB
Current bandwidth	0 bps

Clear Counters

Step 4: Static Routes

- Add static routes to reach the remote subnet through the VPN tunnel.\
- Destination : Subnet (10.20.20.0 / 255.255.255.0)
- Interface : HQ-to-Branch



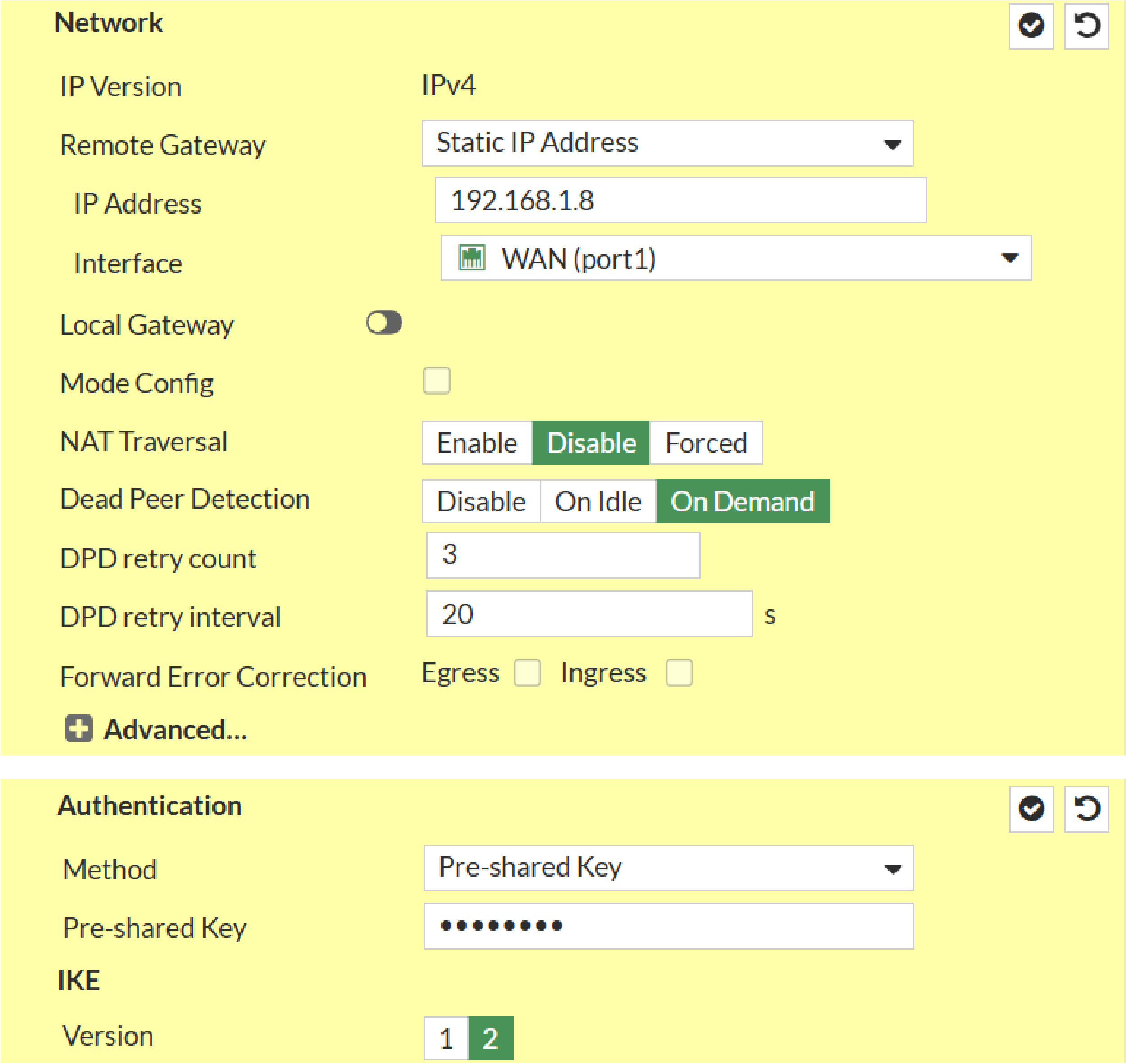
Destination ℹ [✓ Subnet] Internet Service
10.20.20.0/255.255.255.0
Interface HQ-to-Branch
Administrative Distance ℹ 10
Comments Write a comment... 0/255
Status [✓ Enabled] Disabled

3.4 Branch FortiGate Configuration

Step 1: Phase 1 Configuration

- **Go to VPN → IPsec Tunnels → Create New → Custom.**
- **Name: Branch-to-HQ**
- **Remote Gateway: Static IP Address (192.168.1.8) *(HQ WAN IP)***
- **Interface: WAN (port1)**
- **Authentication Method: Pre-shared Key**
- **IKE Version: IKEv2**

- **Encryption: DES**
- **Authentication: SHA384**
- **DH Group: 14,5**
- **Key Lifetime: 86400**



Network

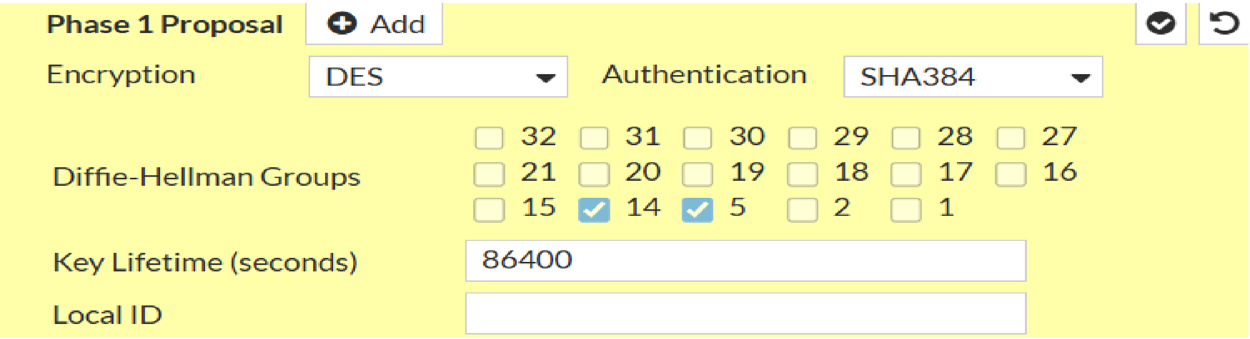
IP Version	IPv4
Remote Gateway	Static IP Address
IP Address	192.168.1.8
Interface	WAN (port1)
Local Gateway	○
Mode Config	□
NAT Traversal	Enable [✓ Disable] Forced
Dead Peer Detection	Disable On Idle [✓ On Demand]
DPD retry count	3
DPD retry interval	20 s
Forward Error Correction	Egress □ Ingress □

Authentication

Method	Pre-shared Key
Pre-shared Key	••••••••

IKE

Version	1 [✓ 2]



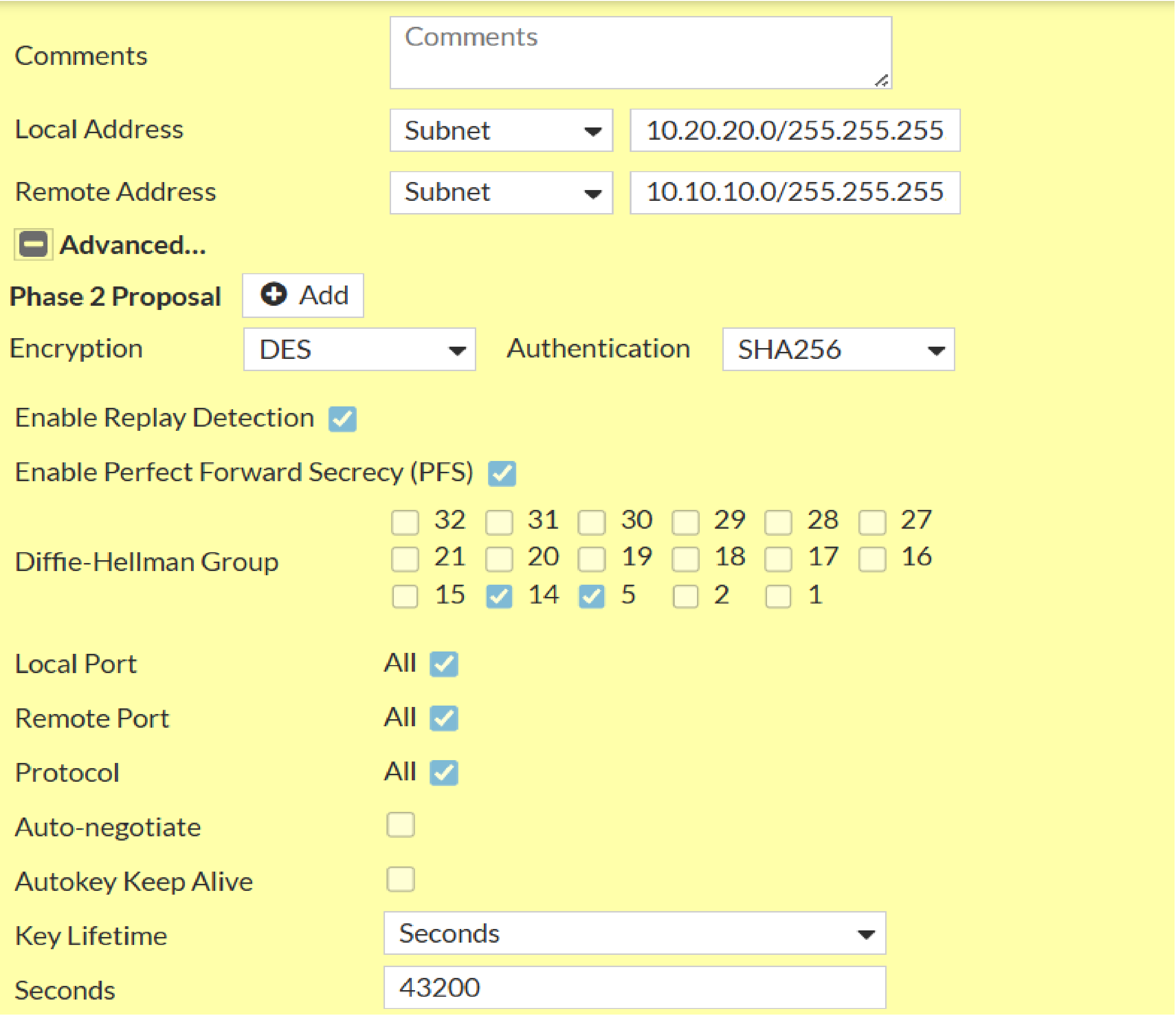
Phase 1 Proposal

Encryption: DES — Authentication: SHA384

Diffie-Hellman Groups:
□ 32 □ 31 □ 30 □ 29 □ 28 □ 27
□ 21 □ 20 □ 19 □ 18 □ 17 □ 16
□ 15 ☑ 14 ☑ 5 □ 2 □ 1

Key Lifetime (seconds): 86400

Local ID:



Comments: Comments

Local Address: Subnet — 10.20.20.0/255.255.255

Remote Address: Subnet — 10.10.10.0/255.255.255

Advanced...

Phase 2 Proposal

Encryption: DES — Authentication: SHA256

Enable Replay Detection ☑

Enable Perfect Forward Secrecy (PFS) ☑

Diffie-Hellman Group:
□ 32 □ 31 □ 30 □ 29 □ 28 □ 27
□ 21 □ 20 □ 19 □ 18 □ 17 □ 16
□ 15 ☑ 14 ☑ 5 □ 2 □ 1

Local Port: All ☑

Remote Port: All ☑

Protocol: All ☑

Auto-negotiate: □

Autokey Keep Alive: □

Key Lifetime: Seconds

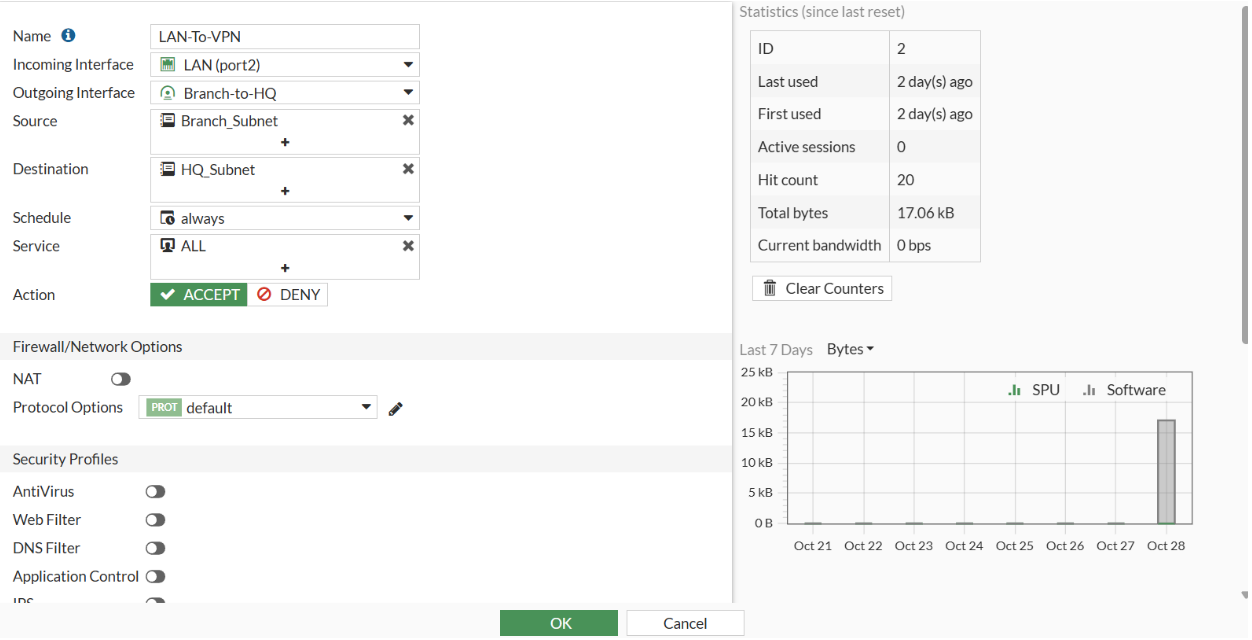
Seconds: 43200

Note :
Make sure the Pre-shared Key matches exactly with the one configured on HQ.

3.5 : Firewall Policies

1- LAN-To-VPN

- **Incoming Interface: LAN (port2)**
- **Outgoing Interface: Branch-to-HQ**
- **Action: Accept**
- **NAT: Disabled**
- **Source: Branch Subnet (10.20.20.0/24)**
- **Destination: HQ Subnet (10.10.10.0/24)**



Name	LAN-To-VPN
Incoming Interface	LAN (port2)
Outgoing Interface	Branch-to-HQ
Source	Branch_Subnet
Destination	HQ_Subnet
Schedule	always
Service	ALL
Action	✓ ACCEPT ⊘ DENY

Firewall/Network Options

NAT ○

Protocol Options PROT default

Security Profiles

AntiVirus ○

Web Filter ○

DNS Filter ○

Application Control ○

IPS ○

OK Cancel

Statistics (since last reset)

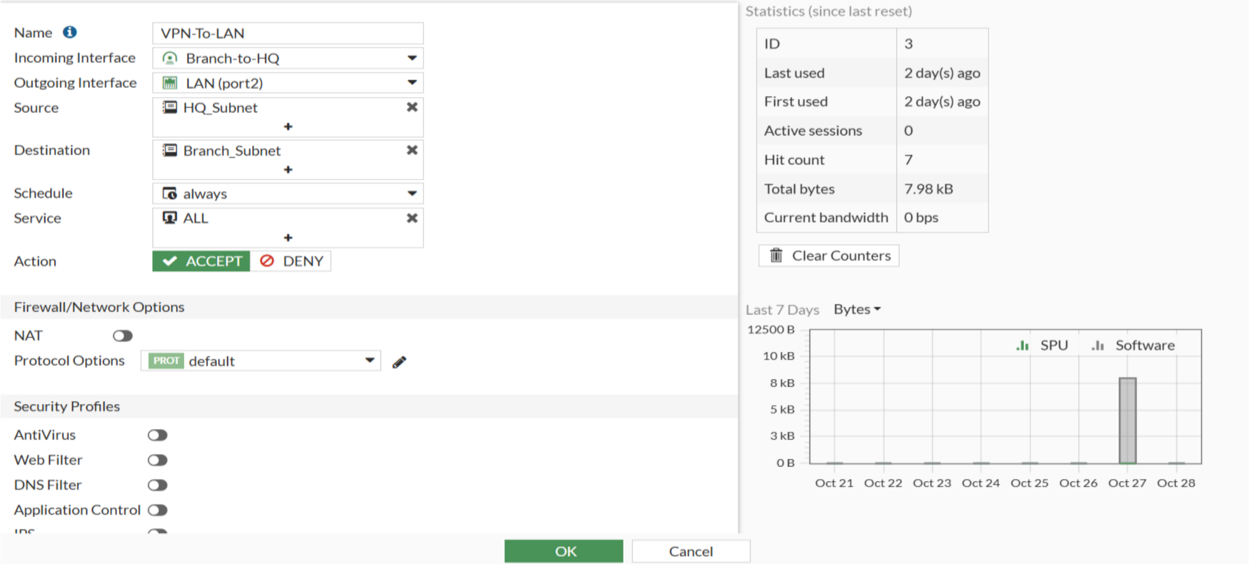
ID	2
Last used	2 day(s) ago
First used	2 day(s) ago
Active sessions	0
Hit count	20
Total bytes	17.06 kB
Current bandwidth	0 bps

Clear Counters

Last 7 Days Bytes

2- VPN-To-LAN

- **Incoming Interface: Branch-to-HQ**
- **Outgoing Interface: LAN (port2)**
- **Action: Accept**
- **NAT: Disabled**
- **Source: HQ Subnet (10.10.10.0/24)**
- **Destination: Branch Subnet (10.20.20.0/24)**



Name	VPN-To-LAN
Incoming Interface	Branch-to-HQ
Outgoing Interface	LAN (port2)
Source	HQ_Subnet
Destination	Branch_Subnet
Schedule	always
Service	ALL
Action	✓ ACCEPT ⊘ DENY

Firewall/Network Options

NAT	○
Protocol Options	PROT default

Security Profiles

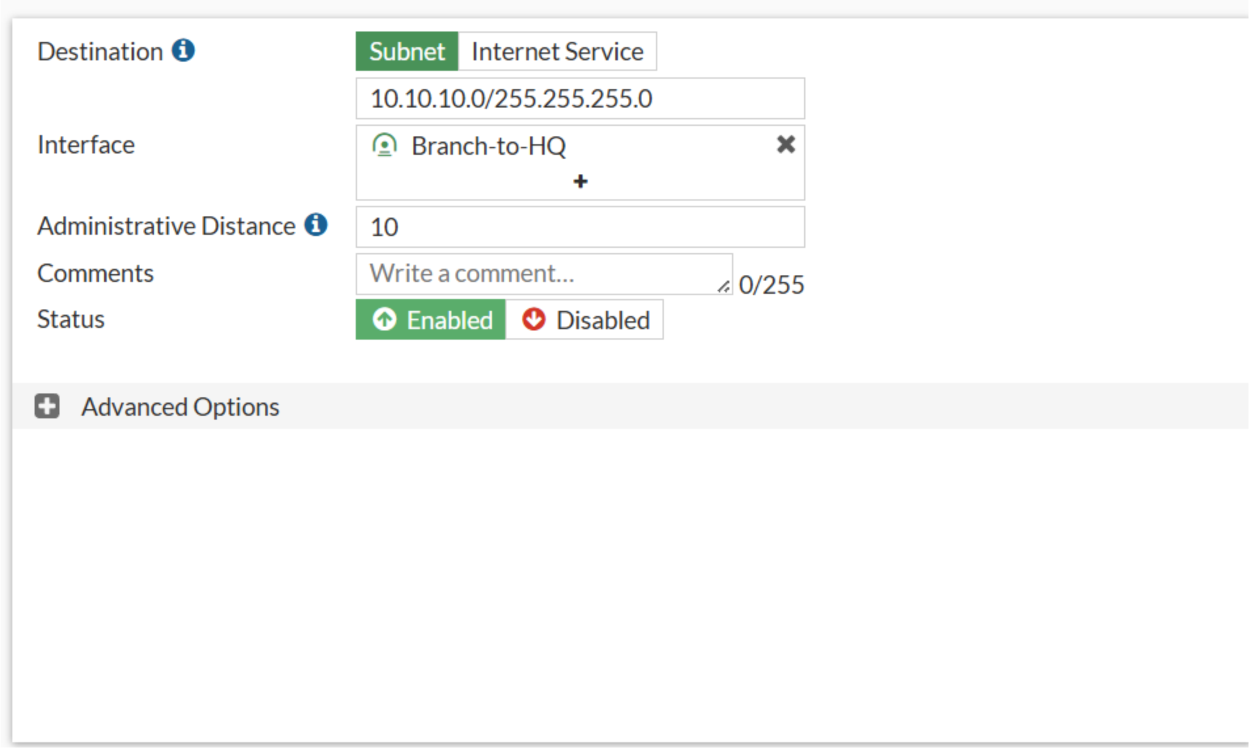
AntiVirus	○
Web Filter	○
DNS Filter	○
Application Control	○
IPS	○

Statistics (since last reset)

ID	3
Last used	2 day(s) ago
First used	2 day(s) ago
Active sessions	0
Hit count	7
Total bytes	7.98 kB
Current bandwidth	0 bps

Step 4: Static Routes

- **Destination: 10.10.10.0 / 255.255.255.0**
- **Interface: Branch-to-HQ**



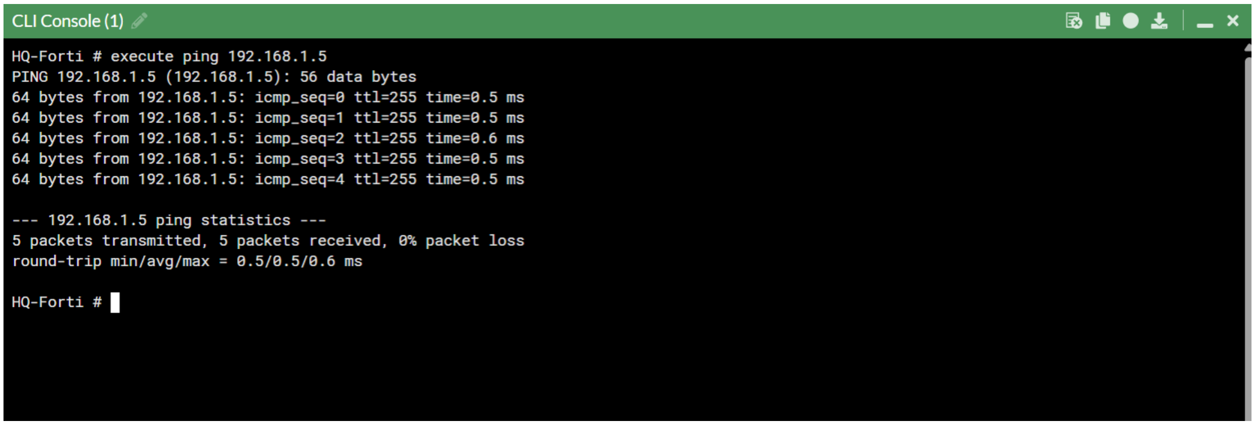
Destination	Subnet Internet Service 10.10.10.0/255.255.255.0
Interface	Branch-to-HQ
Administrative Distance	10
Comments	Write a comment... 0/255
Status	Enabled Disabled

3.6. Connectivity Test Results

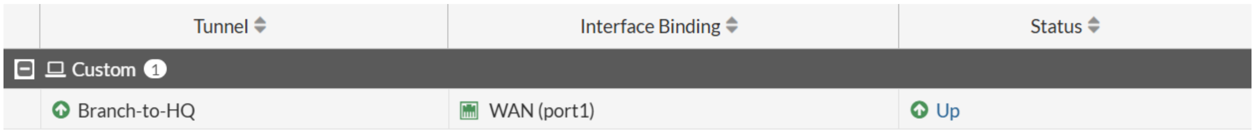
Test 1: Ping Test Between Branches

- **From: HQ Forti 192.168.1.8**
- **To: Branch Forti 192.168.1.5**

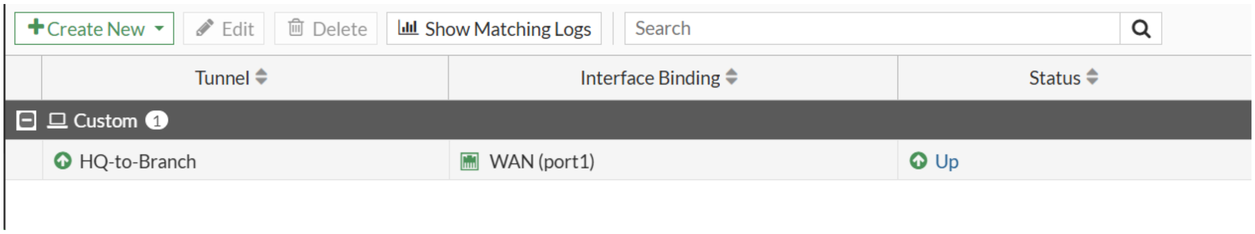
Result: Successful ping replies received, indicating that both LAN networks are reachable through the IPsec VPN tunnel.



```
HQ-Forti # execute ping 192.168.1.5
PING 192.168.1.5 (192.168.1.5): 56 data bytes
64 bytes from 192.168.1.5: icmp_seq=0 ttl=255 time=0.5 ms
64 bytes from 192.168.1.5: icmp_seq=1 ttl=255 time=0.5 ms
64 bytes from 192.168.1.5: icmp_seq=2 ttl=255 time=0.6 ms
64 bytes from 192.168.1.5: icmp_seq=3 ttl=255 time=0.5 ms
64 bytes from 192.168.1.5: icmp_seq=4 ttl=255 time=0.5 ms

--- 192.168.1.5 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.5/0.5/0.6 ms

HQ-Forti #
```



Tunnel	Interface Binding	Status
⊟ Custom 1		
Branch-to-HQ	WAN (port1)	Up

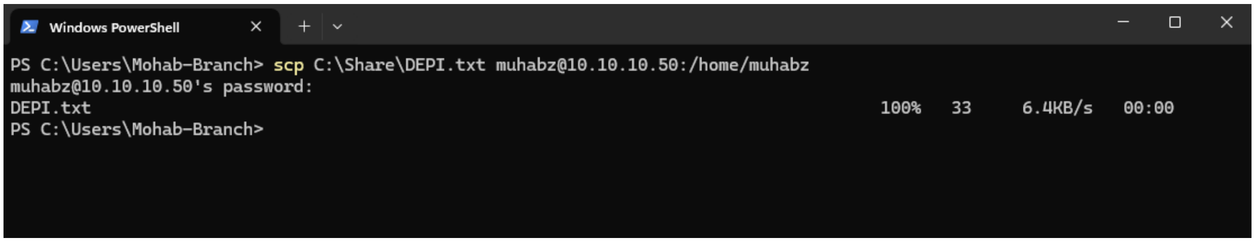


Tunnel	Interface Binding	Status
⊟ Custom 1		
HQ-to-Branch	WAN (port1)	Up

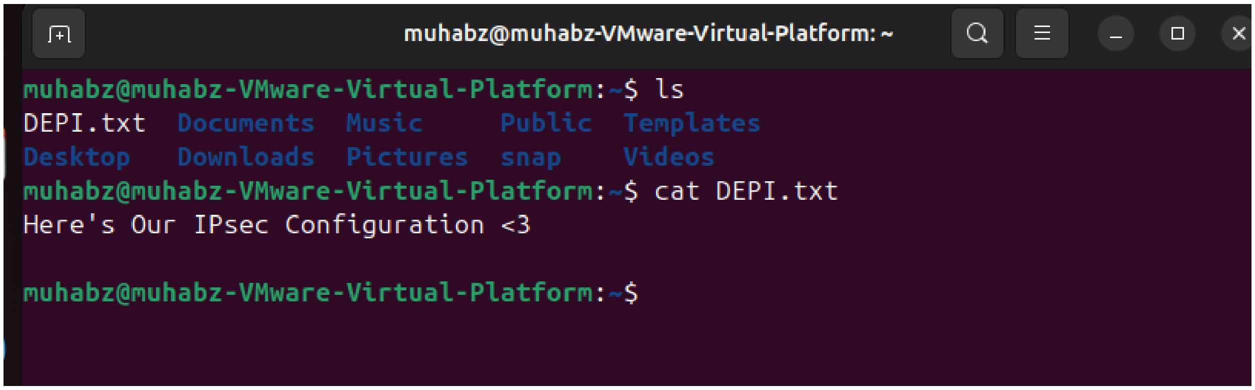
Test 2: File Transfer Test (SCP Protocol)

- **Objective: Verify real data transfer through the IPsec tunnel.**
- **Setup:**
  - **A Windows machine connected to HQ LAN (10.10.10.50).**
    (From DHCP Of LAN)
  - **A Kali Linux machine connected to Branch LAN (10.20.20.50).**
    (From DHCP Of LAN)

- **Method:**
  - From the Windows PC, access the Kali shared folder using SSH protocol (\\10.20.20.50\share).
  - Attempt to copy a test file (e.g., test.txt) between both devices.
- **Command:**
  - From Windows PC Open The PowerShell and Type :
  - scp C:\Share\DEPI.txt muhabz@10.10.10.50:/home/muhabz
- **Result:**
  File transfer completed successfully with stable throughput and no packet loss.
  This confirms that the IPsec tunnel securely transmits not only ICMP packets but also application-layer data traffic.



```
PS C:\Users\Mohab-Branch> scp C:\Share\DEPI.txt muhabz@10.10.10.50:/home/muhabz
muhabz@10.10.10.50's password:
DEPI.txt                                                                100%   33     6.4KB/s   00:00
PS C:\Users\Mohab-Branch>
```



```
muhabz@muhabz-VMware-Virtual-Platform:~$ ls
DEPI.txt  Documents  Music     Public  Templates
Desktop   Downloads  Pictures  snap    Videos
muhabz@muhabz-VMware-Virtual-Platform:~$ cat DEPI.txt
Here's Our IPsec Configuration <3

muhabz@muhabz-VMware-Virtual-Platform:~$
```

6. Conclusion

The IPsec VPN tunnel between the HQ FortiGate and the Branch FortiGate was successfully established and tested.
Connectivity between the two LANs was confirmed through ICMP ping tests and SSH file transfer verification.
This demonstrates that encrypted communication and secure data exchange between both networks are fully operational.
The configuration followed standard security best practices, ensuring data integrity and confidentiality across the VPN connection.

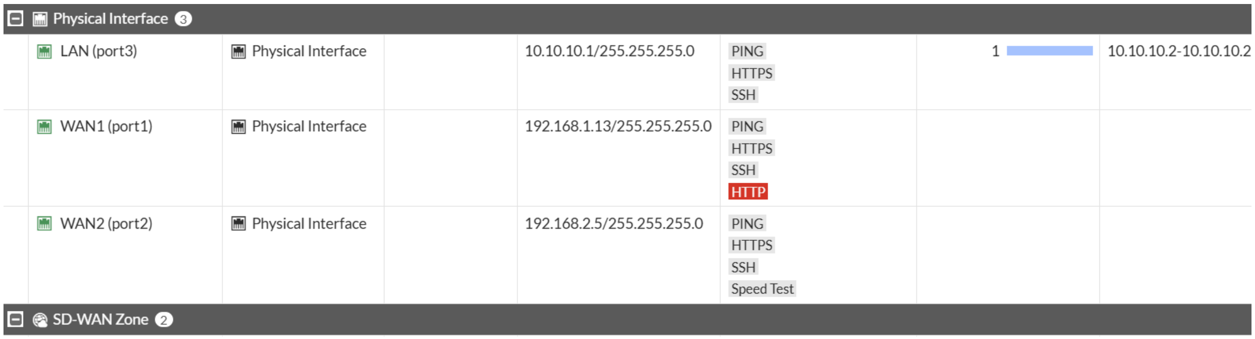
4. SD-WAN Implementation Documentation

Purpose:

- Combine multiple internet links for smart traffic distribution
- Application-aware routing (VoIP, Video, Web)
- Automatic failover and load balancing
- Real-time performance monitoring

Environment:

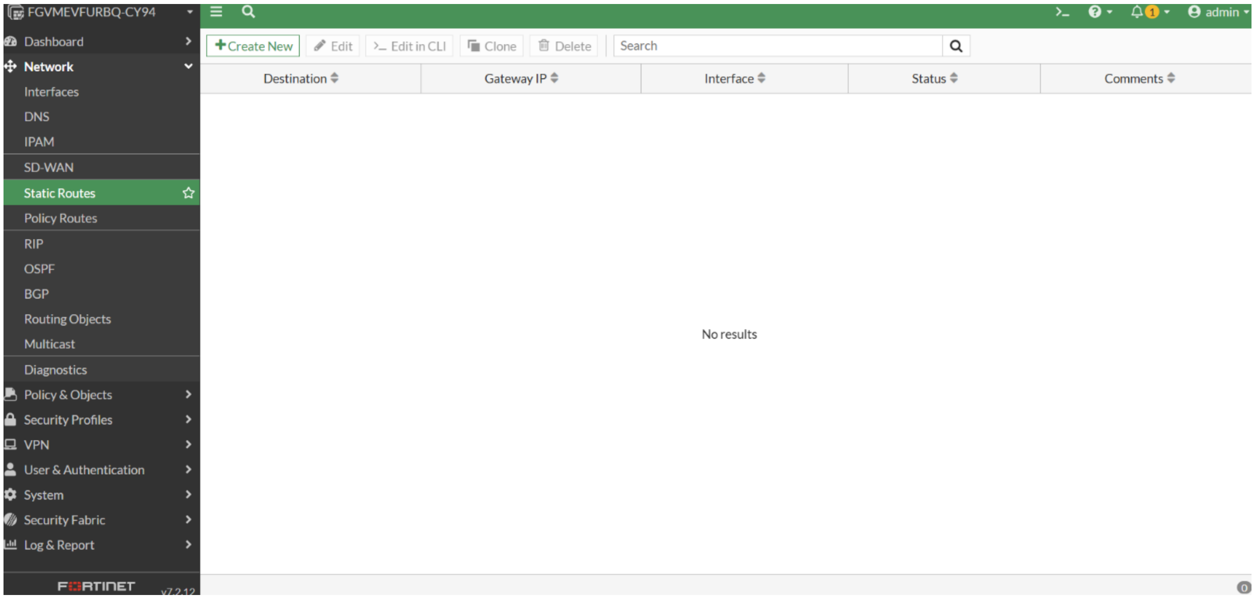
- 2 WAN links
- LAN: 10.10.10.0/24
- Device: FortiGate Firewall



⊟ Physical Interface 3						
LAN (port3)	Physical Interface		10.10.10.1/255.255.255.0	PING HTTPS SSH	1	10.10.10.2-10.10.10.2
WAN1 (port1)	Physical Interface		192.168.1.13/255.255.255.0	PING HTTPS SSH HTTP		
WAN2 (port2)	Physical Interface		192.168.2.5/255.255.255.0	PING HTTPS SSH Speed Test		
⊟ SD-WAN Zone 2						

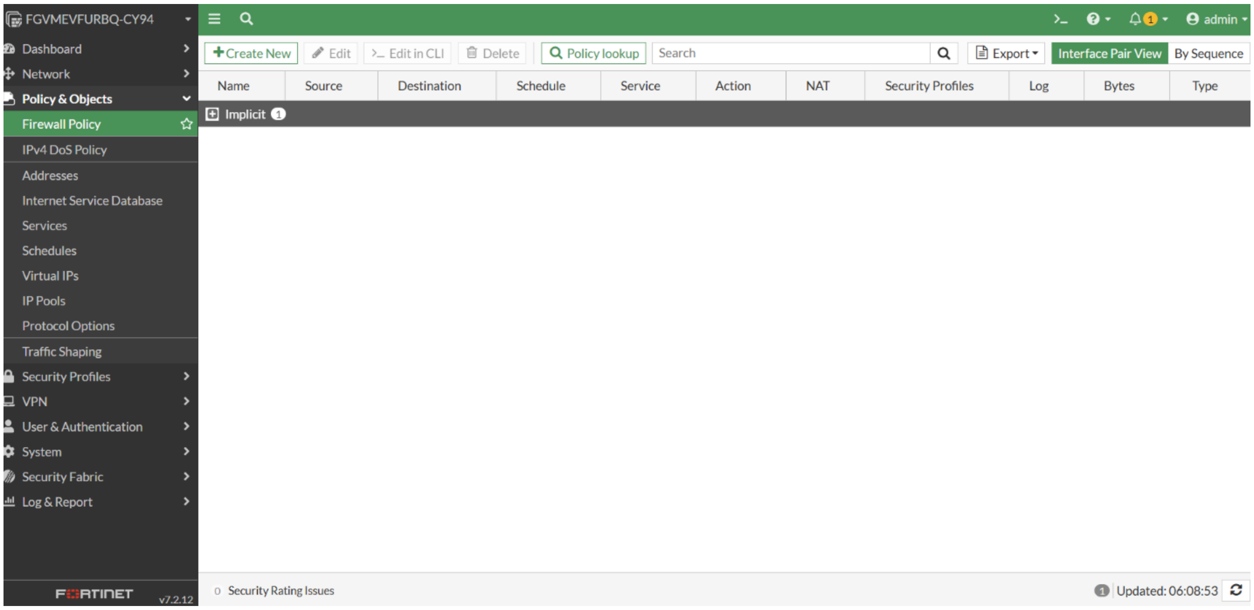
Implementation Steps:

- **4.1 : Verify Initial Configuration**
- Checked Firewall Policies: No policies are active.
- Checked Routing: No static routes or default routes exist.
- **Purpose:** Ensure a clean environment before enabling SD-WAN.



Destination	Gateway IP	Interface	Status	Comments

No results



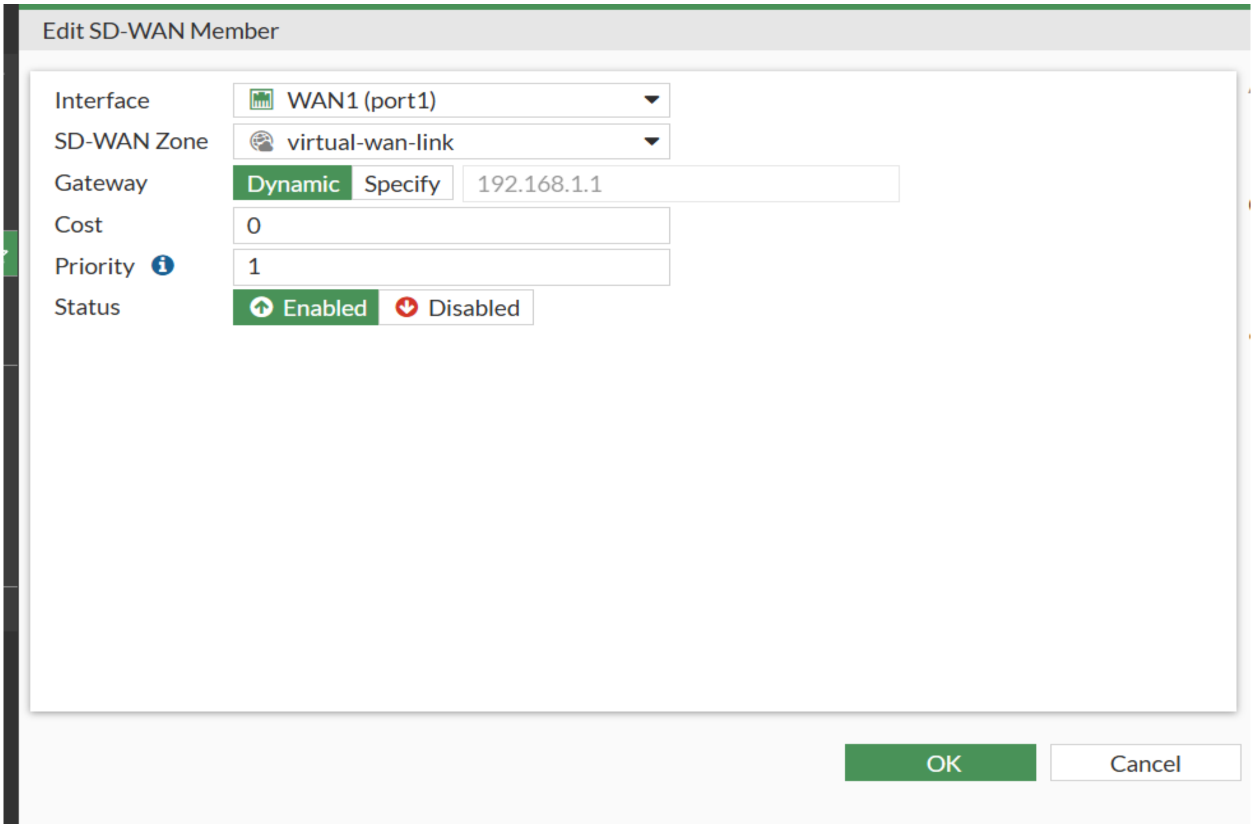
Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes	Type
Implicit 1										

0 Security Rating Issues

1 Updated: 06:08:53

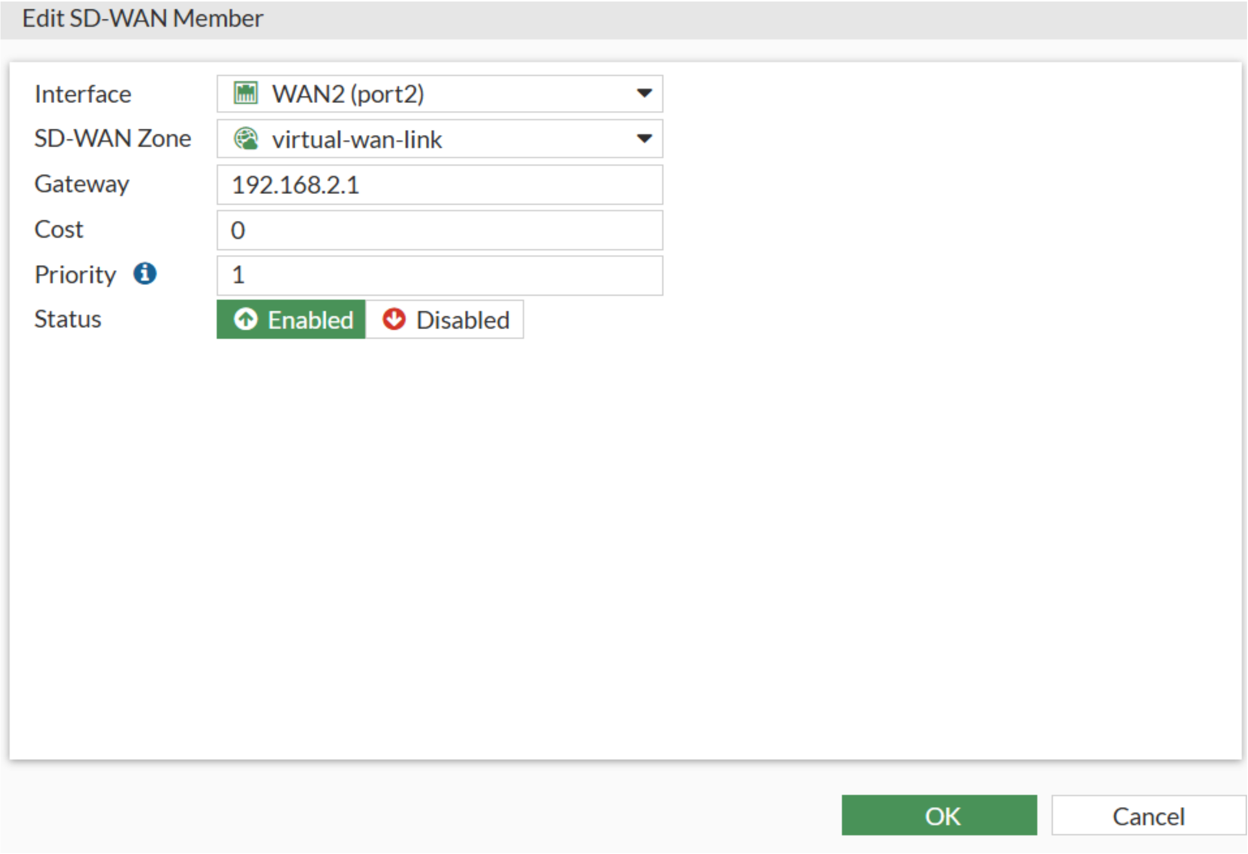
4.2 : Add Internet Links as SD-WAN Members

- Each WAN link is added as a **Member** inside SD-WAN:
  - WAN1 → Member 1
  - WAN2 → Member 2
- **Purpose:** Integrate all WAN links under a single SD-WAN zone for centralized management.



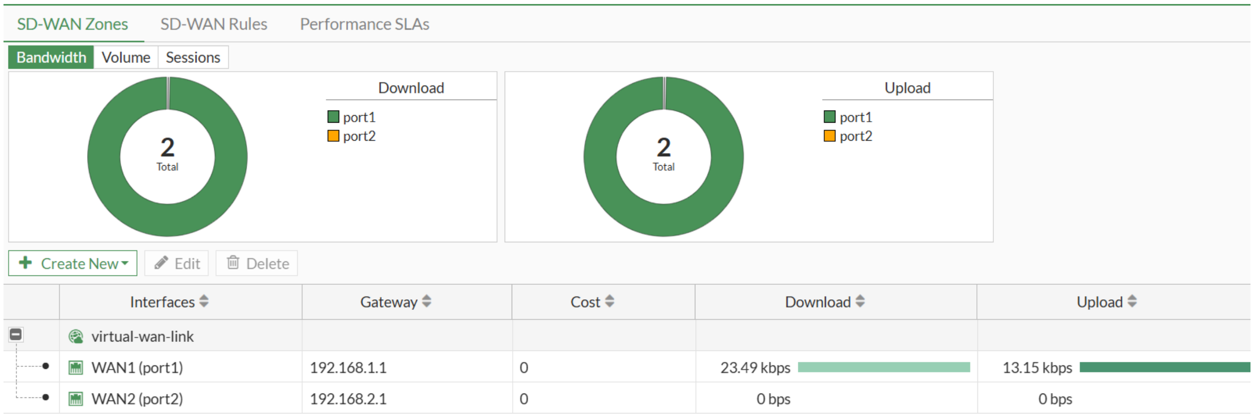
Edit SD-WAN Member

Interface	WAN1 (port1)
SD-WAN Zone	virtual-wan-link
Gateway	[✓ Dynamic] Specify 192.168.1.1
Cost	0
Priority	1
Status	[✓ Enabled] Disabled



Edit SD-WAN Member

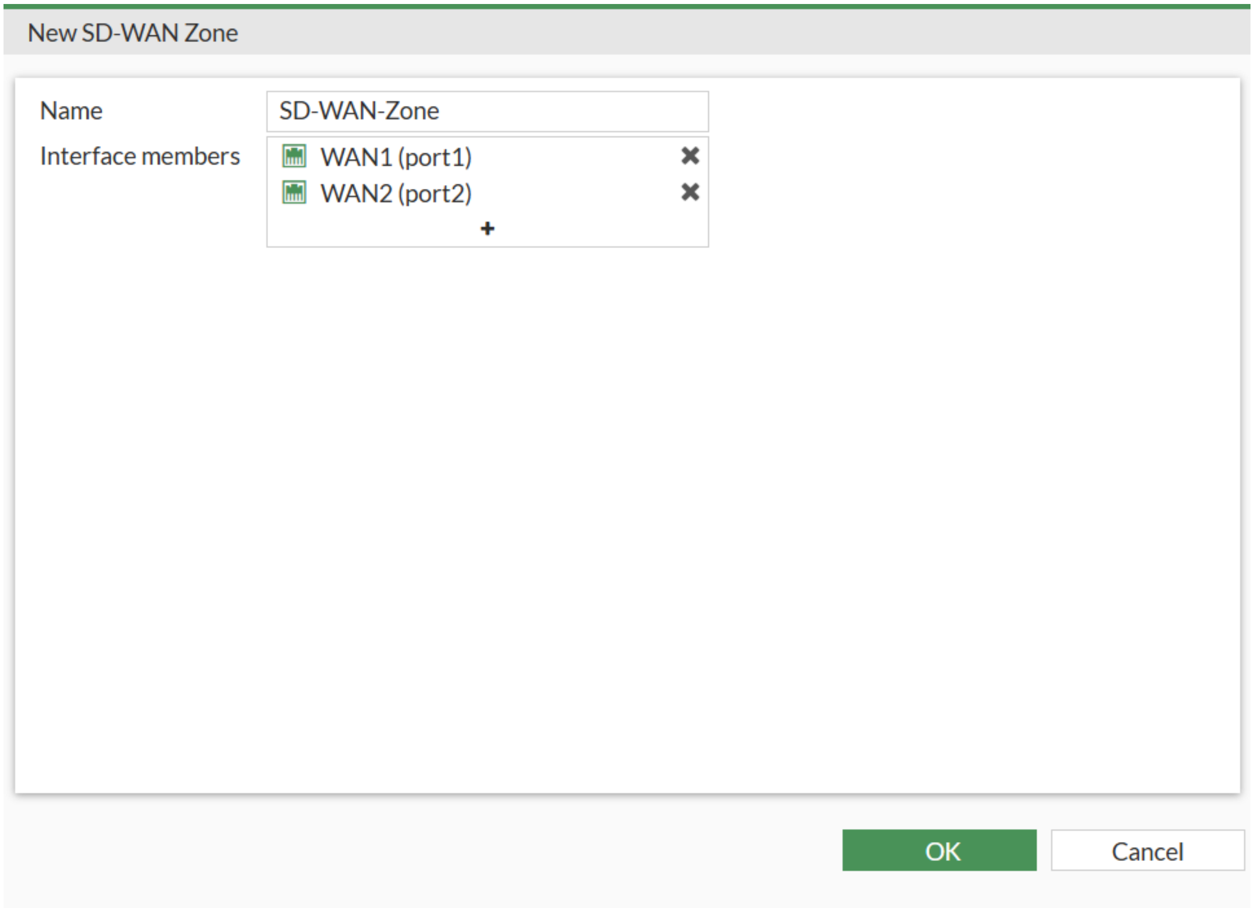
Interface	WAN2 (port2)
SD-WAN Zone	virtual-wan-link
Gateway	192.168.2.1
Cost	0
Priority	1
Status	[✓ Enabled] Disabled



	Interfaces	Gateway	Cost	Download	Upload
⊟	virtual-wan-link				
	WAN1 (port1)	192.168.1.1	0	23.49 kbps	13.15 kbps
	WAN2 (port2)	192.168.2.1	0	0 bps	0 bps

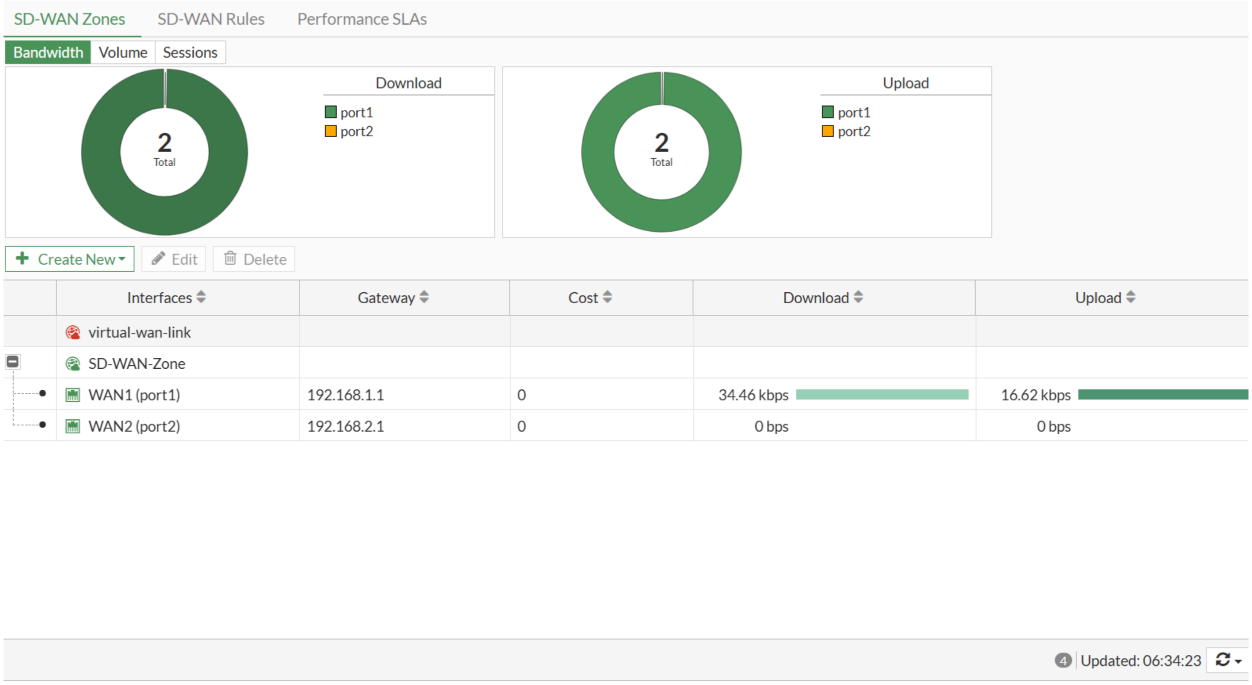
4.3: Create SD-WAN Zone

- Created a **SD-WAN Zone** named SD-WAN-Zone.
- Added all WAN members (WAN1, WAN2) into this zone.


New SD-WAN Zone

Name: SD-WAN-Zone

Interface members: WAN1 (port1), WAN2 (port2)

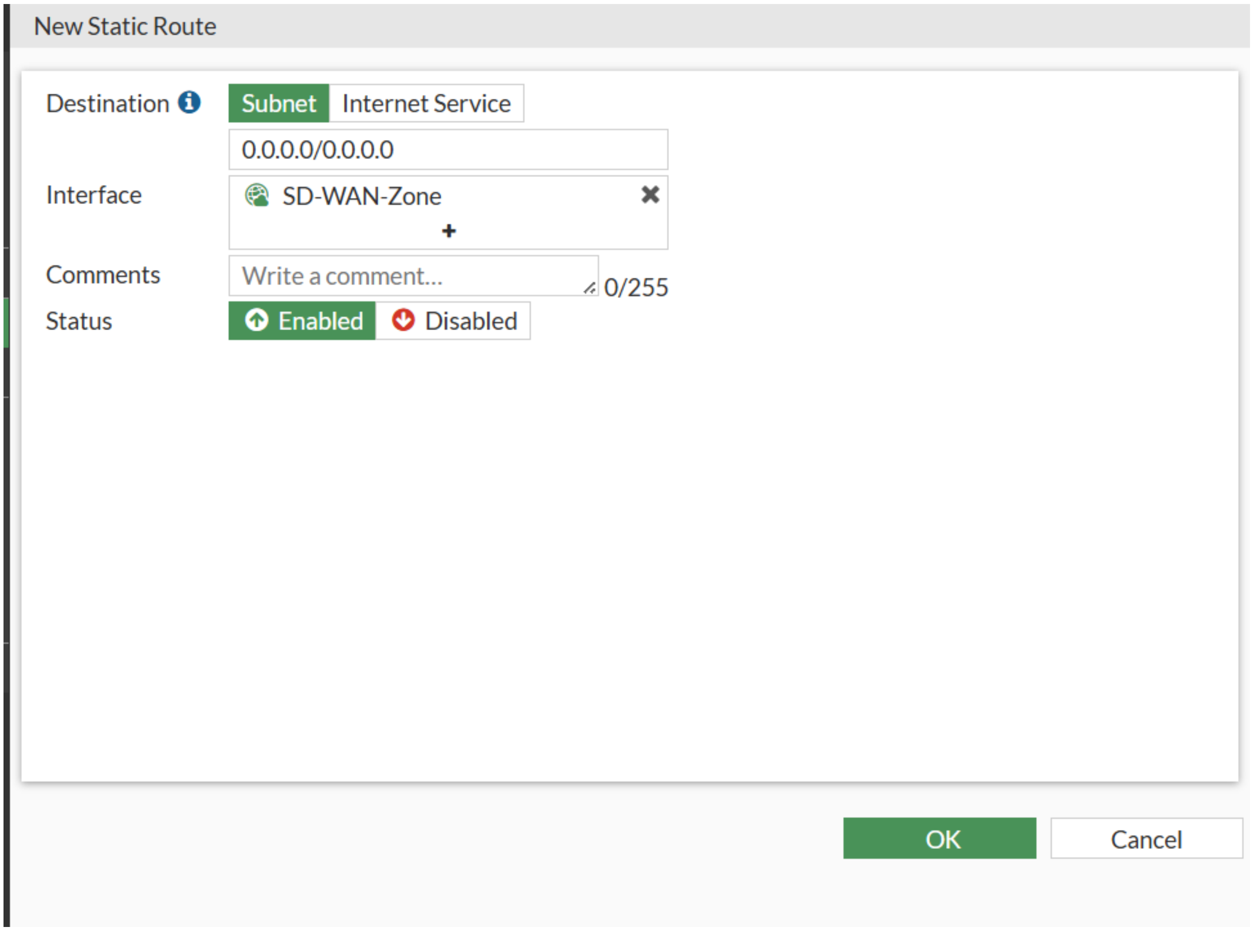


Interfaces	Gateway	Cost	Download	Upload
virtual-wan-link				
SD-WAN-Zone				
WAN1 (port1)	192.168.1.1	0	34.46 kbps	16.62 kbps
WAN2 (port2)	192.168.2.1	0	0 bps	0 bps

Updated: 06:34:23

4.4 : Configure Default Static Route

- **Static Route Configuration:**
  - **Destination:** 0.0.0.0/0
  - **Interface:** SD-WAN-Zone
- **Purpose:** Direct all outbound traffic through the SD-WAN zone instead of individual WAN interfaces.



New Static Route

Destination: Subnet
0.0.0.0/0.0.0.0

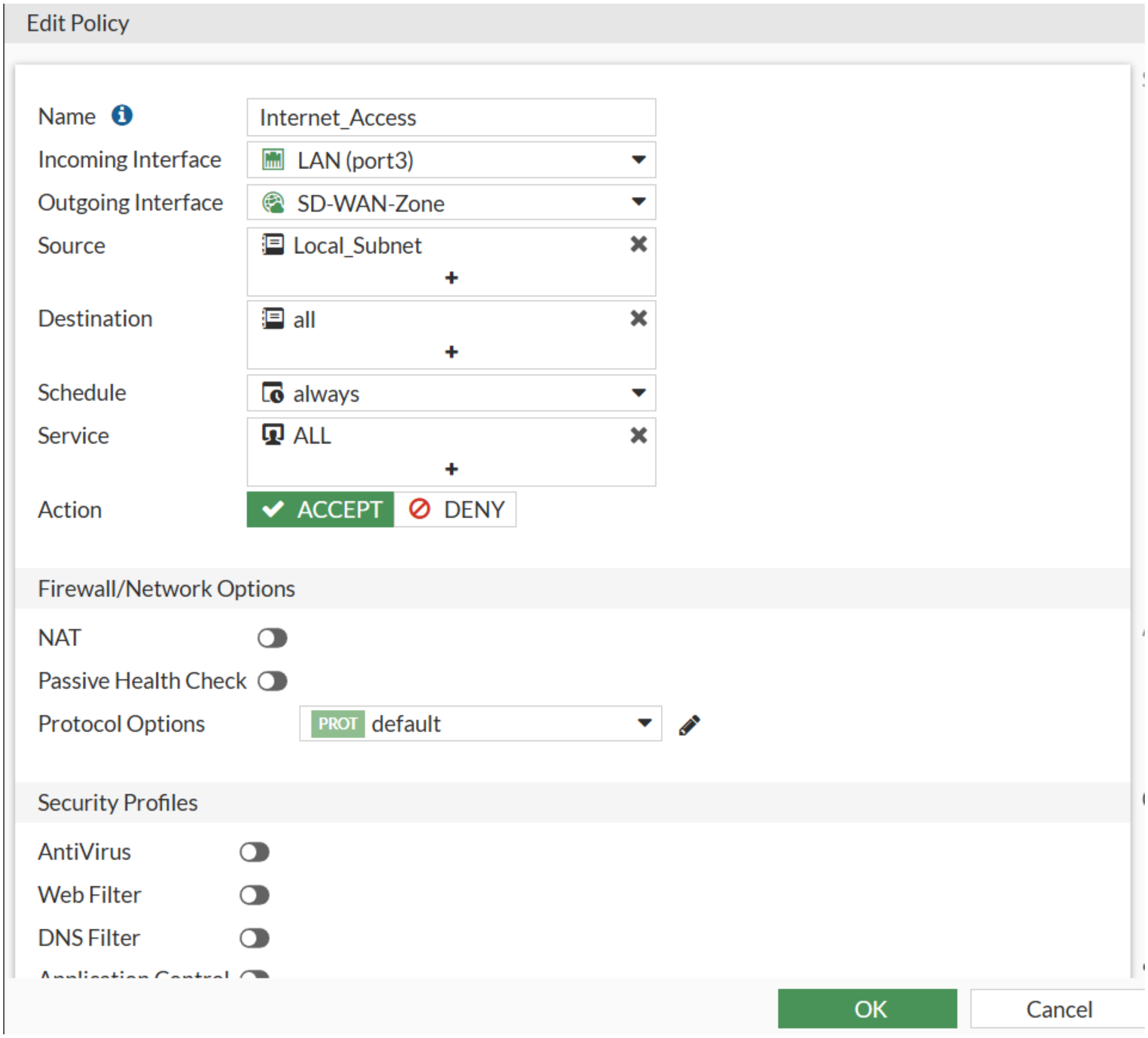
Interface: SD-WAN-Zone

Comments: Write a comment... 0/255

Status: Enabled

4.5 : Configure Firewall Policy

- Created a firewall policy named Internet Access:
    - **Incoming Interface:** LAN
    - **Outgoing Interface:** SD-WAN-Zone
    - **Source:** Local Subnet 10.10.10.0/24
    - **Destination:** All
    - **Schedule:** All
    - **Service:** All
- **Purpose:** Ensure internal traffic exits to the internet via the SD-WAN zone.



Edit Policy

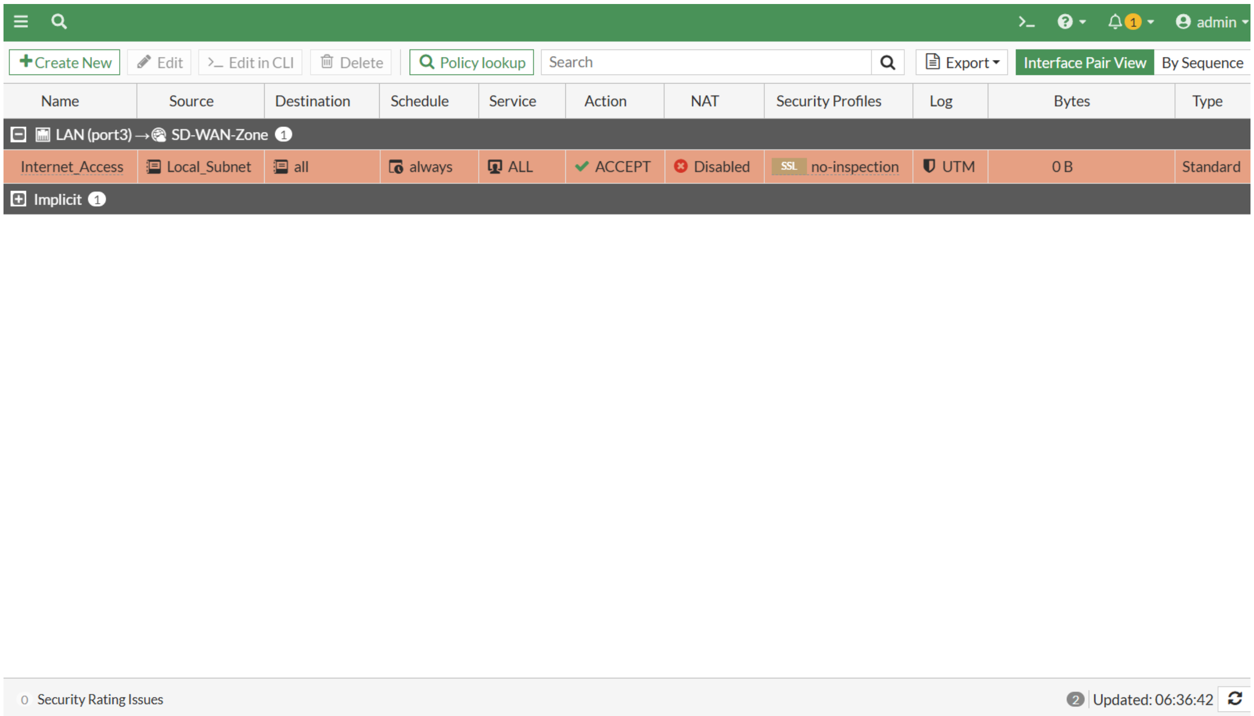
Name	Internet_Access
Incoming Interface	LAN (port3)
Outgoing Interface	SD-WAN-Zone
Source	Local_Subnet
Destination	all
Schedule	always
Service	ALL
Action	✓ ACCEPT ⊘ DENY

Firewall/Network Options

NAT	○
Passive Health Check	○
Protocol Options	PROT default

Security Profiles

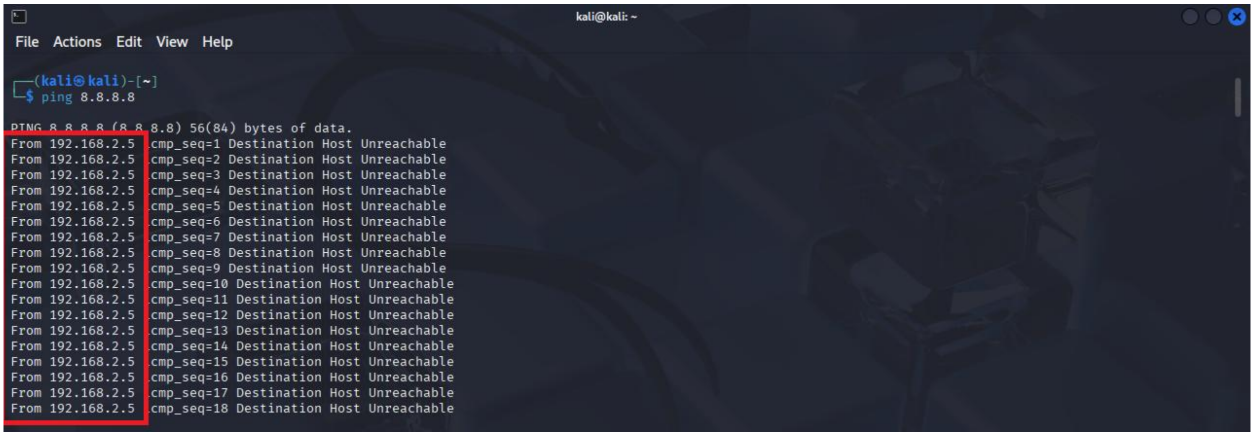
AntiVirus	○
Web Filter	○
DNS Filter	○
Application Control	○



Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes	Type
LAN (port3) → SD-WAN-Zone 1										
Internet_Access	Local_Subnet	all	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	UTM	0 B	Standard
Implicit 1										

0 Security Rating Issues

Updated: 06:36:42

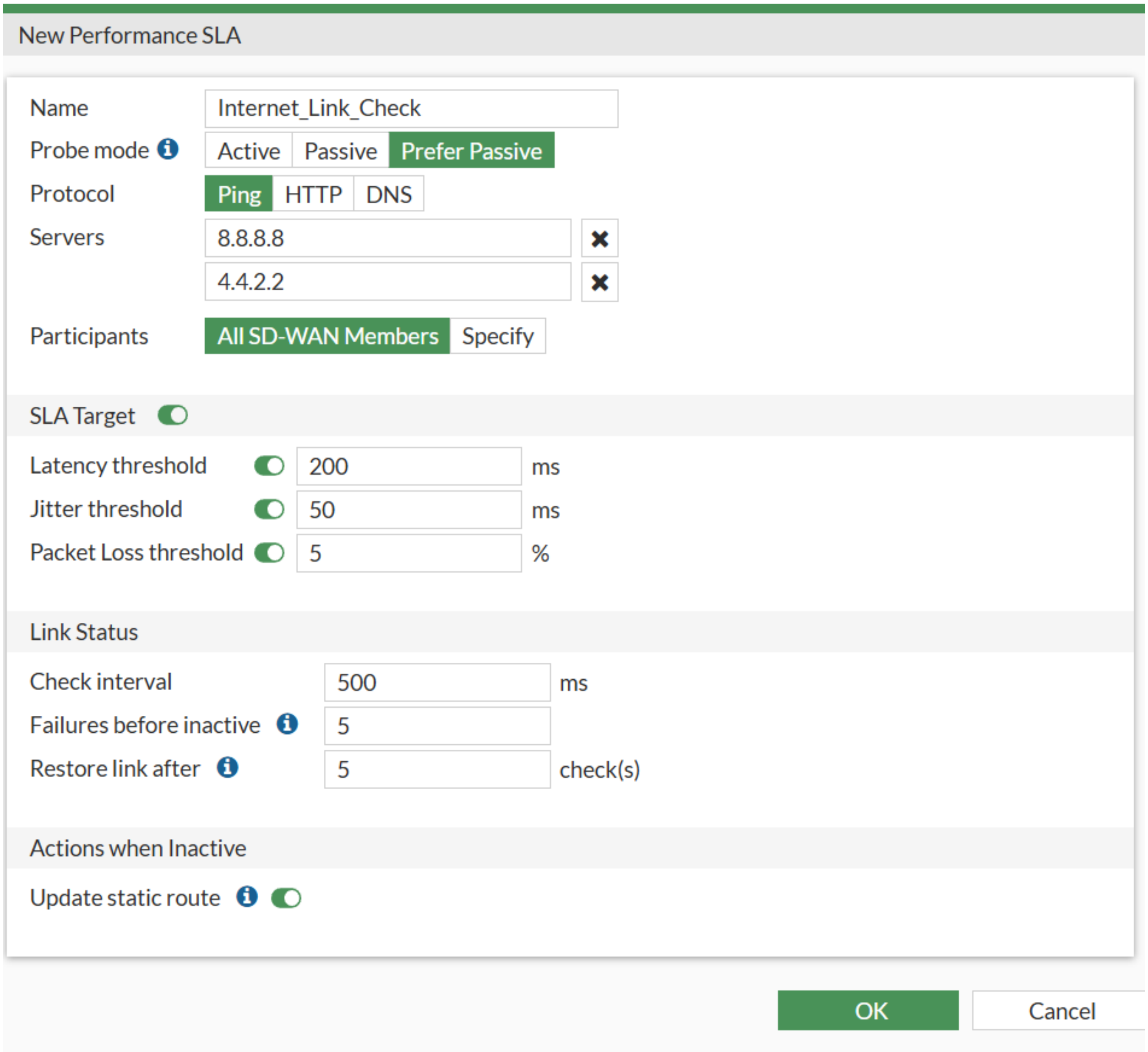


```
┌──(kali㉿kali)-[~]
└─$ ping 8.8.8.8

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 192.168.2.5 cmp_seq=1 Destination Host Unreachable
From 192.168.2.5 cmp_seq=2 Destination Host Unreachable
From 192.168.2.5 cmp_seq=3 Destination Host Unreachable
From 192.168.2.5 cmp_seq=4 Destination Host Unreachable
From 192.168.2.5 cmp_seq=5 Destination Host Unreachable
From 192.168.2.5 cmp_seq=6 Destination Host Unreachable
From 192.168.2.5 cmp_seq=7 Destination Host Unreachable
From 192.168.2.5 cmp_seq=8 Destination Host Unreachable
From 192.168.2.5 cmp_seq=9 Destination Host Unreachable
From 192.168.2.5 cmp_seq=10 Destination Host Unreachable
From 192.168.2.5 cmp_seq=11 Destination Host Unreachable
From 192.168.2.5 cmp_seq=12 Destination Host Unreachable
From 192.168.2.5 cmp_seq=13 Destination Host Unreachable
From 192.168.2.5 cmp_seq=14 Destination Host Unreachable
From 192.168.2.5 cmp_seq=15 Destination Host Unreachable
From 192.168.2.5 cmp_seq=16 Destination Host Unreachable
From 192.168.2.5 cmp_seq=17 Destination Host Unreachable
From 192.168.2.5 cmp_seq=18 Destination Host Unreachable
```

4.6 : Configure Performance SLA

- **Name:** Internet_Link_Check
- **Probe Mode:** Prefer Passive
- **Protocol:** Ping
- **Servers:** 8.8.8.8, 4.4.2.2
- **Participated Members:** All SD-WAN Members

- **SLA Targets:**
  - Latency: 200ms
  - Jitter: 50ms
  - Packet Loss: 5%
- **Purpose:** Monitor link quality and enable intelligent routing decisions based on performance.



New Performance SLA

Name	Internet_Link_Check	
Probe mode	Active Passive [✓ Prefer Passive]	
Protocol	[✓ Ping] HTTP DNS	
Servers	8.8.8.8 4.4.2.2	
Participants	[✓ All SD-WAN Members] Specify	

SLA Target ●

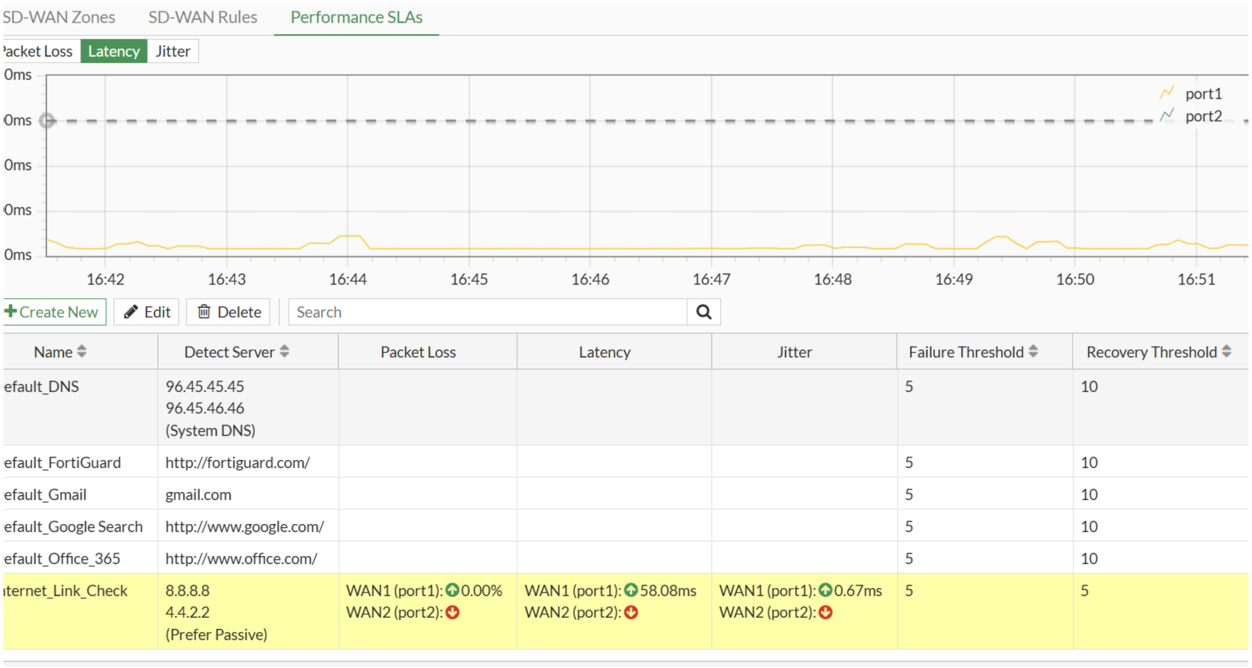
Latency threshold ●	200	ms
Jitter threshold ●	50	ms
Packet Loss threshold ●	5	%

Link Status

Check interval	500	ms
Failures before inactive	5	
Restore link after	5	check(s)

Actions when Inactive

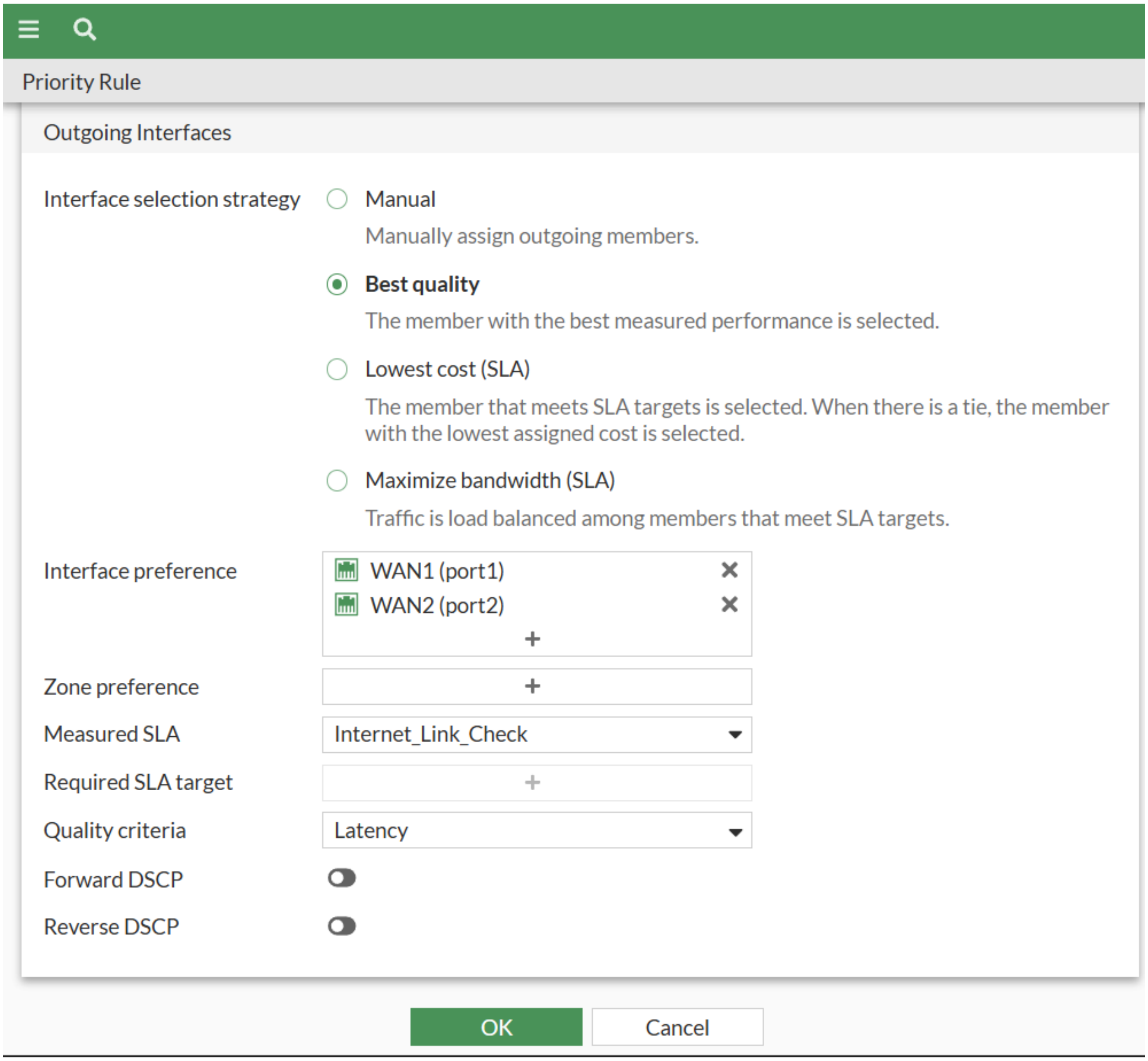
Update static route ●



Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
efault_DNS	96.45.45.45 96.45.46.46 (System DNS)				5	10
efault_FortiGuard	http://fortiguard.com/				5	10
efault_Gmail	gmail.com				5	10
efault_Google Search	http://www.google.com/				5	10
efault_Office_365	http://www.office.com/				5	10
iternet_Link_Check	8.8.8.8 4.4.2.2 (Prefer Passive)	WAN1 (port1): ⬆0.00% WAN2 (port2): ⬇	WAN1 (port1): ⬆58.08ms WAN2 (port2): ⬇	WAN1 (port1): ⬆0.67ms WAN2 (port2): ⬇	5	5

4.7 : Create SD-WAN Rules

- Example rules implemented:
  - Traffic from subnet 10.10.10.0/24 to **YouTube** → routed via **WAN1**
  - Traffic from subnet 10.10.10.0/24 for **VoIP calls** → routed via the **best performing link** automatically
- **Purpose:** Direct traffic efficiently based on application type and link quality.



Priority Rule

Outgoing Interfaces

Interface selection strategy

○ Manual
Manually assign outgoing members.

● **Best quality**
The member with the best measured performance is selected.

○ Lowest cost (SLA)
The member that meets SLA targets is selected. When there is a tie, the member with the lowest assigned cost is selected.

○ Maximize bandwidth (SLA)
Traffic is load balanced among members that meet SLA targets.

Interface preference: WAN1 (port1) ✕, WAN2 (port2) ✕, +

Zone preference: +

Measured SLA: Internet_Link_Check

Required SLA target: +

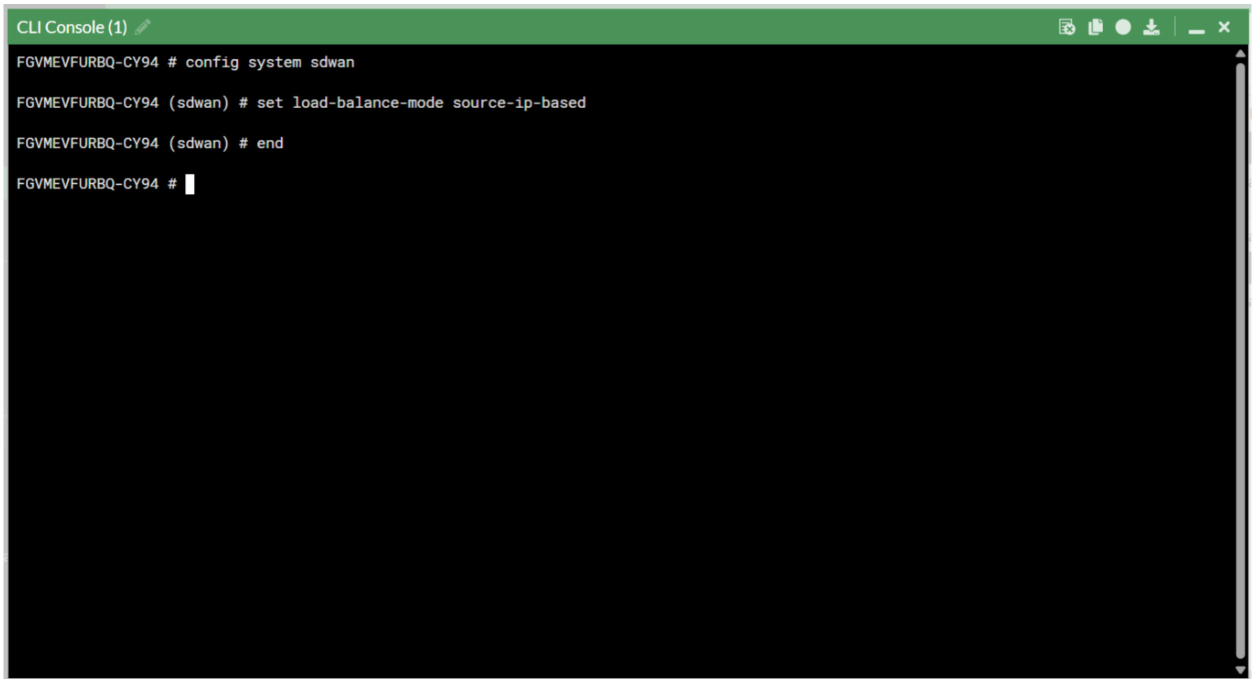
Quality criteria: Latency

Forward DSCP

Reverse DSCP

4.8 : Load Balancing Configuration

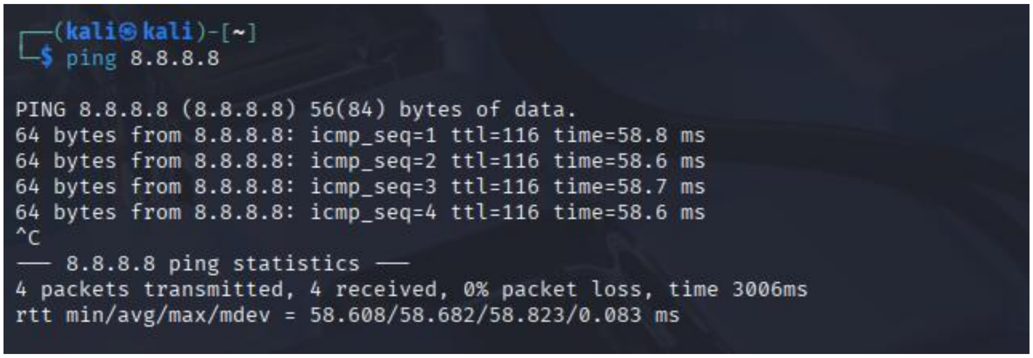
- **Mode:** Source-IP based
- **Purpose:** Distribute traffic across WAN links evenly while keeping sessions consistent per source IP.
- Configured in GUI (or optionally CLI for mode selection).



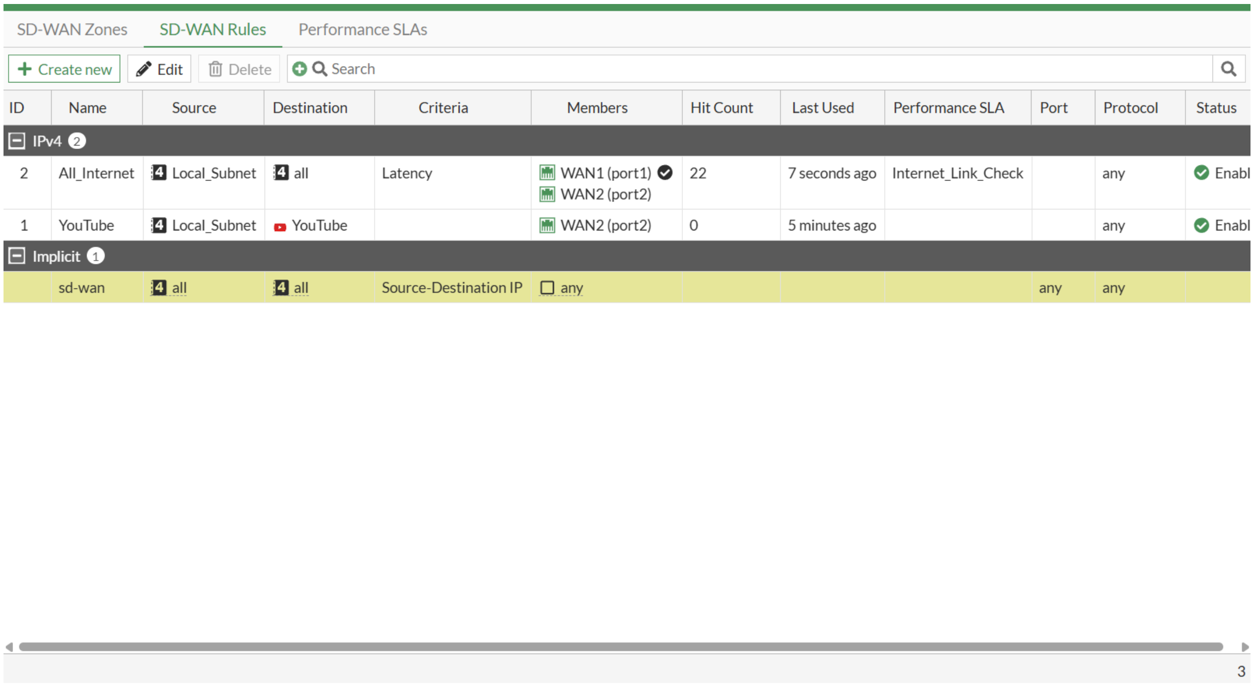
```
FGVMEVFURBQ-CY94 # config system sdwan

FGVMEVFURBQ-CY94 (sdwan) # set load-balance-mode source-ip-based

FGVMEVFURBQ-CY94 (sdwan) # end

FGVMEVFURBQ-CY94 #
```

4.9 Testing & Monitoring

- Observed SD-WAN member status:
  - WAN1: Up
  - WAN2: Down
- Tested traffic routing for YouTube and VoIP services to verify SLA rules and best-quality routing.
- Verified failover functionality by simulating WAN link failure.
- Monitored latency, jitter, and packet loss via SD-WAN Monitor dashboard.



```
┌──(kali㉿kali)-[~]
└─$ ping 8.8.8.8

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=58.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=58.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=58.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=58.6 ms
^C
—— 8.8.8.8 ping statistics ——
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 58.608/58.682/58.823/0.083 ms
```



ID	Name	Source	Destination	Criteria	Members	Hit Count	Last Used	Performance SLA	Port	Protocol	Status
IPv4 2											
2	All_Internet	Local_Subnet	all	Latency	WAN1 (port1) ✓ WAN2 (port2)	22	7 seconds ago	Internet_Link_Check		any	✓ Enabl
1	YouTube	Local_Subnet	YouTube		WAN2 (port2)	0	5 minutes ago			any	✓ Enabl
Implicit 1											
	sd-wan	all	all	Source-Destination IP	□ any				any	any	

Conclusion

The SD-WAN implementation provides:

- Intelligent routing and application-aware traffic steering.
- Automatic failover for uninterrupted connectivity.
- Efficient utilization of all WAN links with load balancing.
- Real-time performance monitoring for proactive network management.

Conclusion

In conclusion, this project successfully demonstrated the design and implementation of secure and efficient VPN solutions using FortiGate technologies. By combining **SSL VPN**, **IPsec Site-to-Site VPN**, and **SD-WAN**, the network achieved enhanced security, optimized performance, and reliable connectivity for both remote users and interconnected sites.

These configurations ensure encrypted communication, seamless user access, and intelligent traffic management, making the network more resilient and ready for real-world operational needs. The project highlights the importance of modern security practices and provides a solid foundation for future scalability and advanced network enhancements.