Implementing VPN Solutions with FortiGate

رواد مصر الرقمية

Fortinet Cybersecurity Engineer

Project by:

Mohamed Ahmed Mohamed Haridy
shahd yesen salah abdelmoamen
Jana Hany Salah Eldin
Nada Ahmed Abo-Bakr Abdelnaser
Shams Ibrahem Ali Mohamed
Merna medhat hamdy rabia

Supervised by: Eng. Alhussieny Mohamed Ali

Presented to: Dr.Hussien Harb

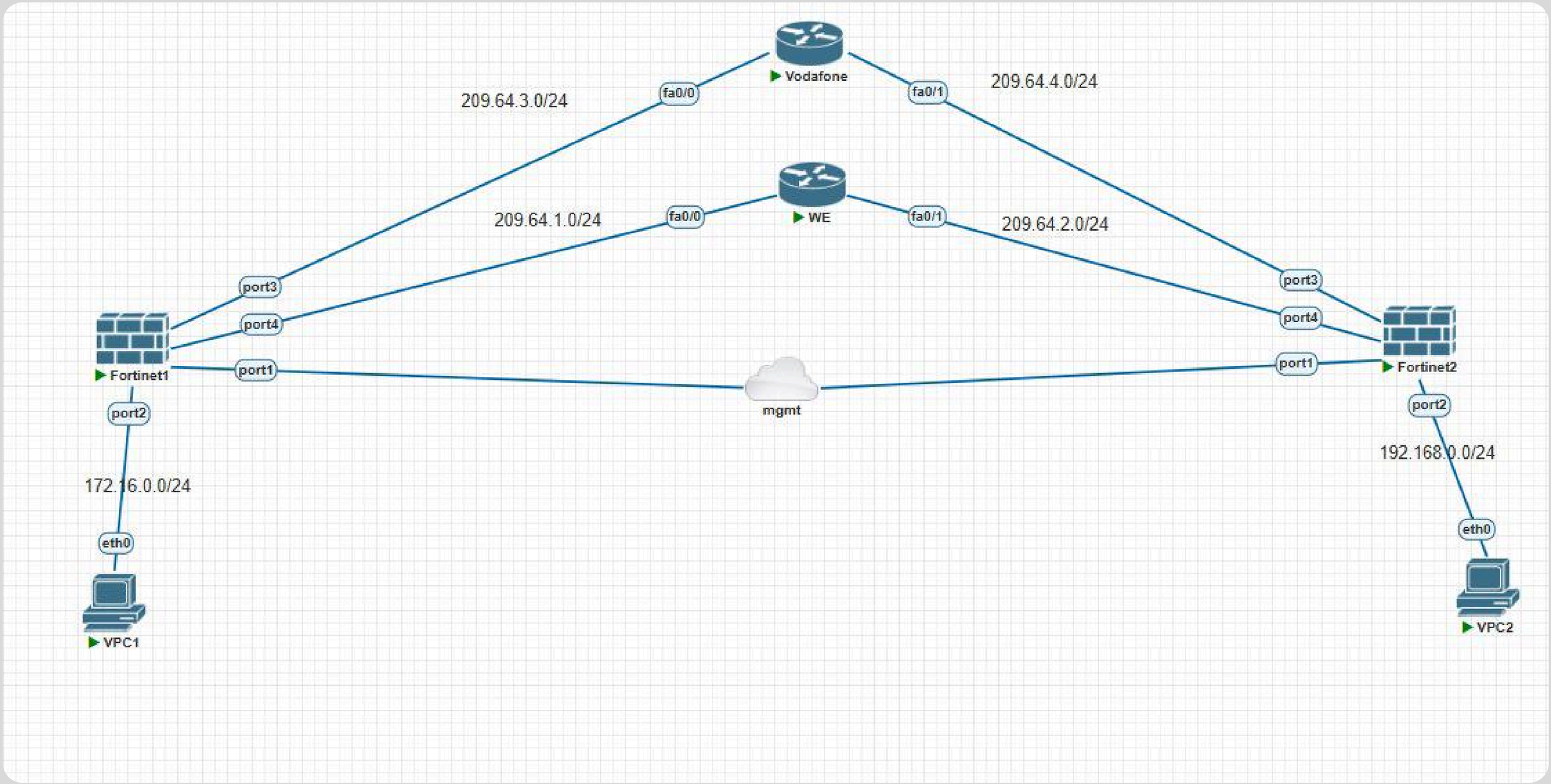
INTRODUCTION

In modern enterprise networks, secure communication between geographically separated sites is essential. An IPsec tunnel provides a reliable and encrypted method to interconnect two remote locations over the public internet as if they were part of the same private network. By establishing an IPsec tunnel between Headquarter and Branch Office, organizations ensure that sensitive data—such as business applications, voice traffic, and internal services—travels safely and remains protected from unauthorized access.

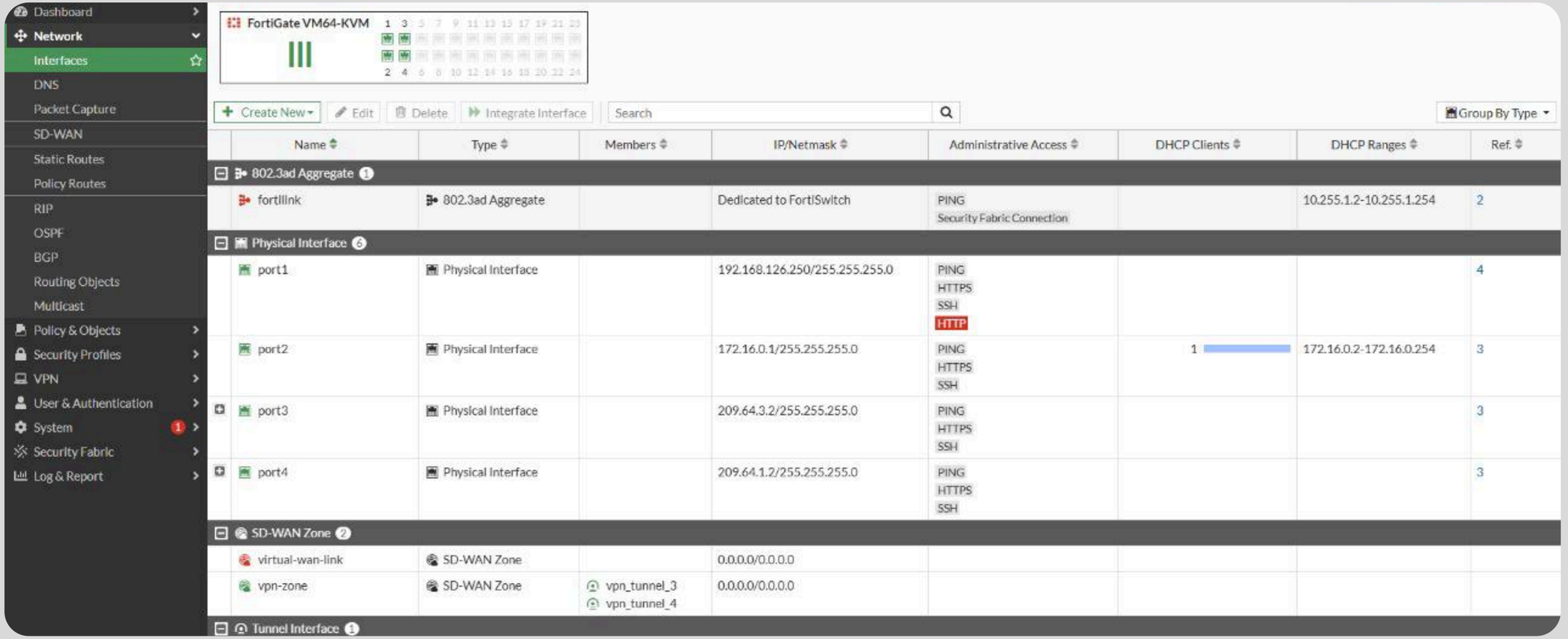
This solution delivers confidentiality, data integrity, and strong authentication, creating a virtual private pathway that allows seamless communication between internal subnets. IPsec tunnels are widely used because they are cost-effective, scalable, and supported by most modern firewalls and routers.

Implementing an IPsec tunnel between two sites enhances the overall network architecture by enabling secure resource sharing, centralized management, and continuous business operations across distributed locations.

SITE TO SITE SECURE NETWORK TOPOLOGY

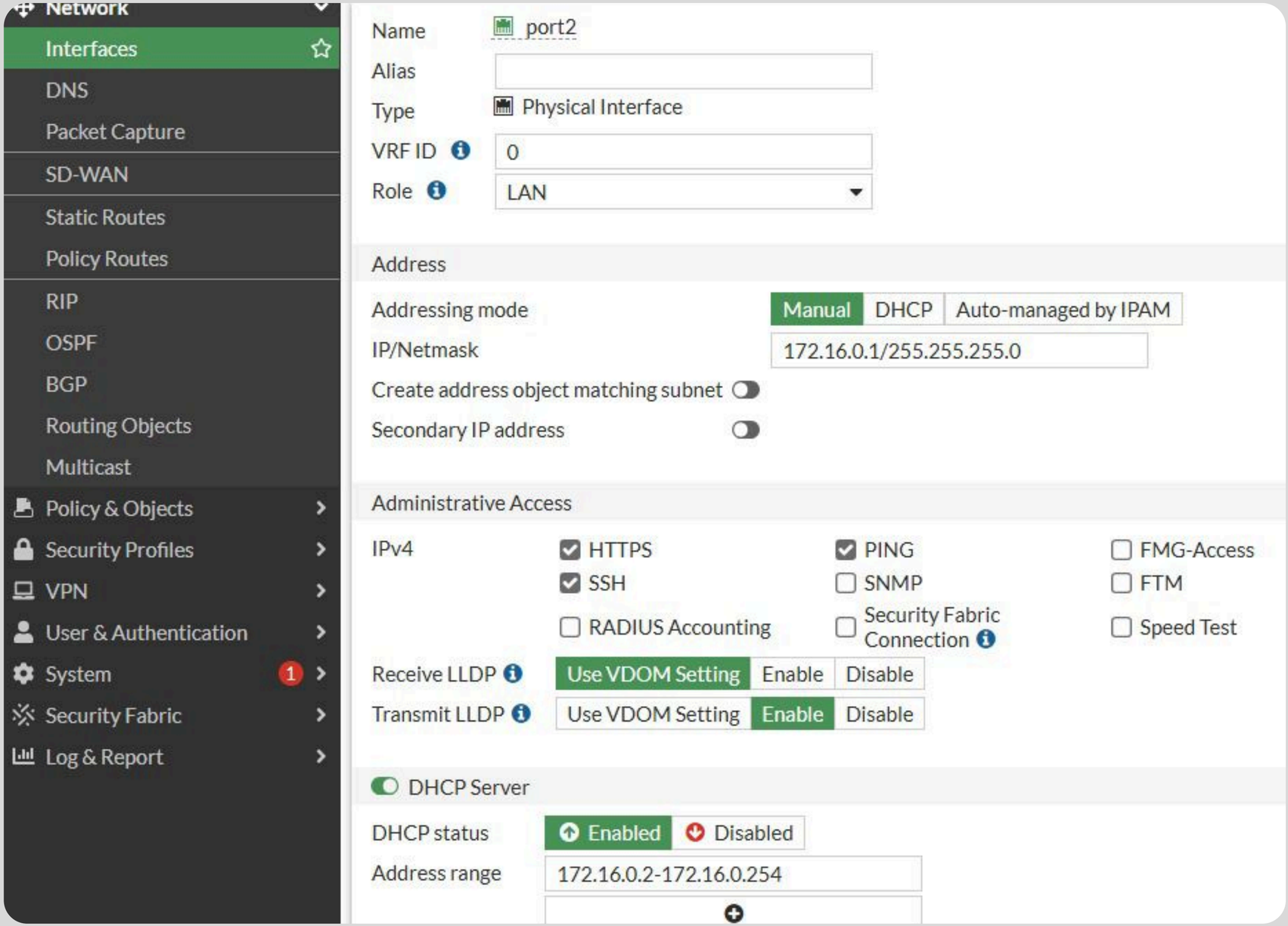


FortiGate Interface Summary

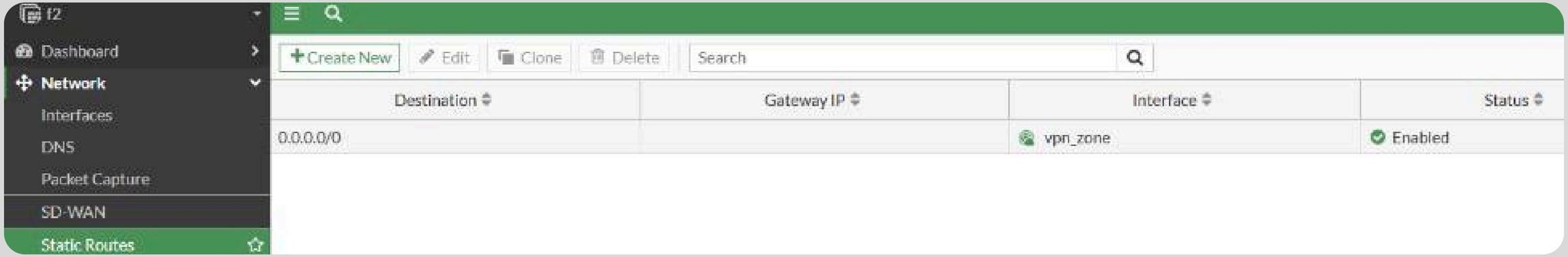


- Interfaces list with IP assignments and access permissions.
  - Physical ports + SD-WAN zone + VPN tunnels.
  - Admin services enabled: Ping / HTTPS / SSH.

ENABLE DHCP

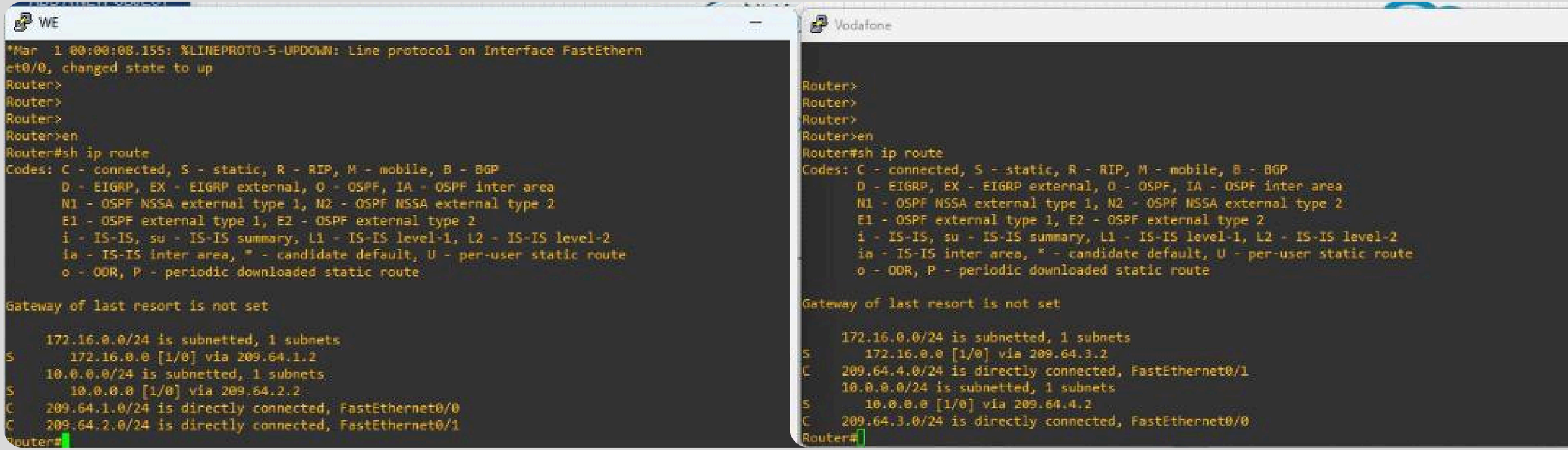

Network
Interfaces
DNS
Packet Capture
SD-WAN
Static Routes
Policy Routes
RIP
OSPF
BGP
Routing Objects
Multicast
Policy & Objects
Security Profiles
VPN
User & Authentication
System
1
Security Fabric
Log & Report
Name
port2
Alias
Type
Physical Interface
VRF ID
0
Role
LAN
Address
Addressing mode
Manual
DHCP
Auto-managed by IPAM
IP/Netmask
172.16.0.1/255.255.255.0
Create address object matching subnet
Secondary IP address
Administrative Access
IPv4
HTTPS
PING
FMG-Access
SSH
SNMP
FTM
RADIUS Accounting
Security Fabric Connection
Speed Test
Receive LLDP
Use VDOM Setting
Enable
Disable
Transmit LLDP
Use VDOM Setting
Enable
Disable
DHCP Server
DHCP status
Enabled
Disabled
Address range
172.16.0.2-172.16.0.254

STATIC ROUTE CONFIGURATION OVERVIEW



- Security Assurance: This guarantees that data destined for the remote network is encrypted and secured through the IPsec tunnel.
- Key Result: We gain full control over outbound routing, ensuring all remote traffic follows the mandated secure path.

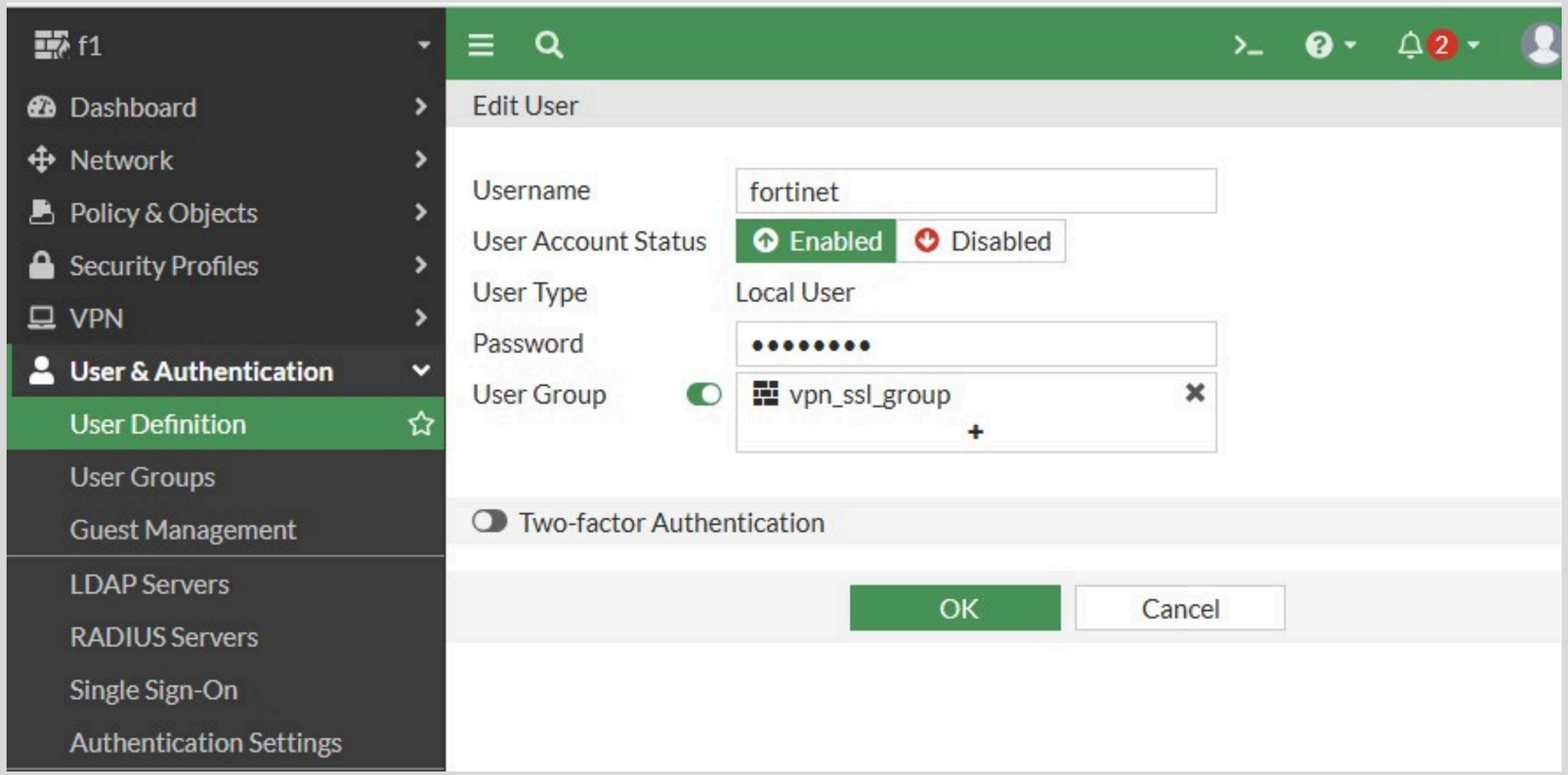
ISP ROUTERS STATIC ROUTING (VODAFONE & WE)



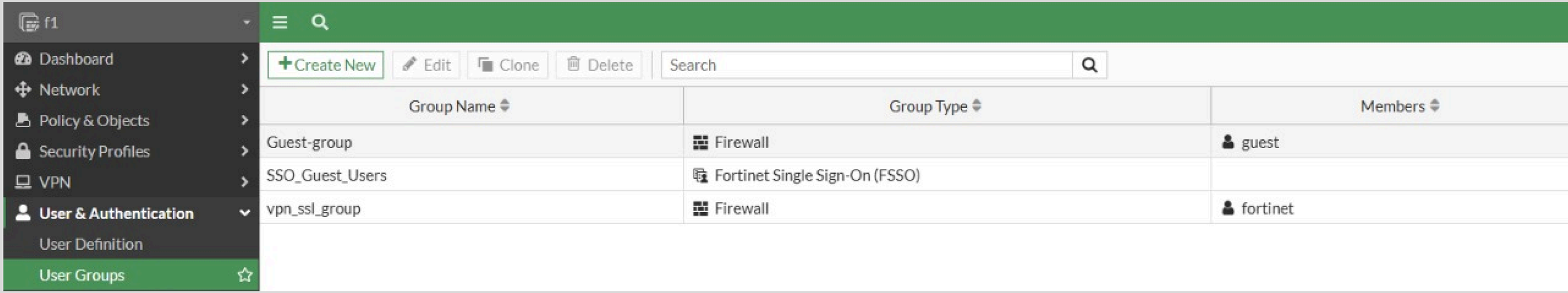
SSL VPN

steps for ssl vpn :

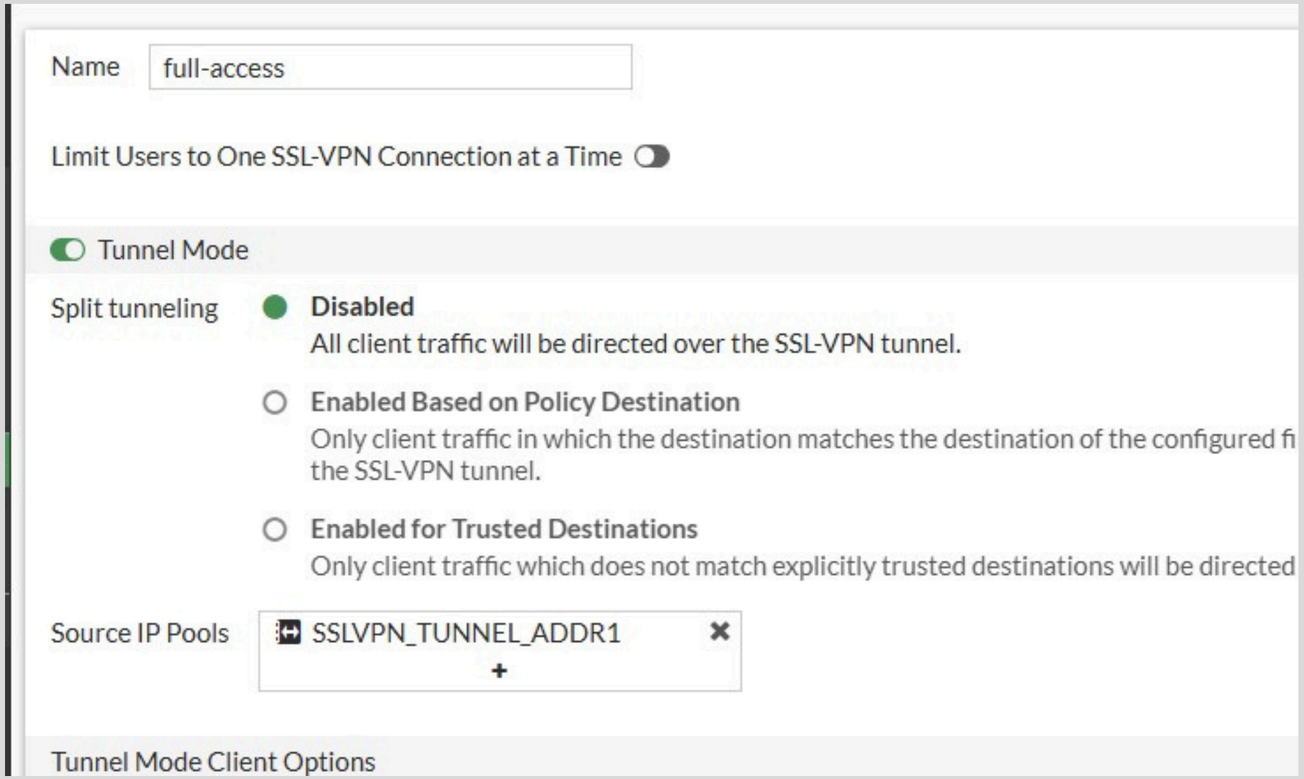
1- create a user



2- add user to a group



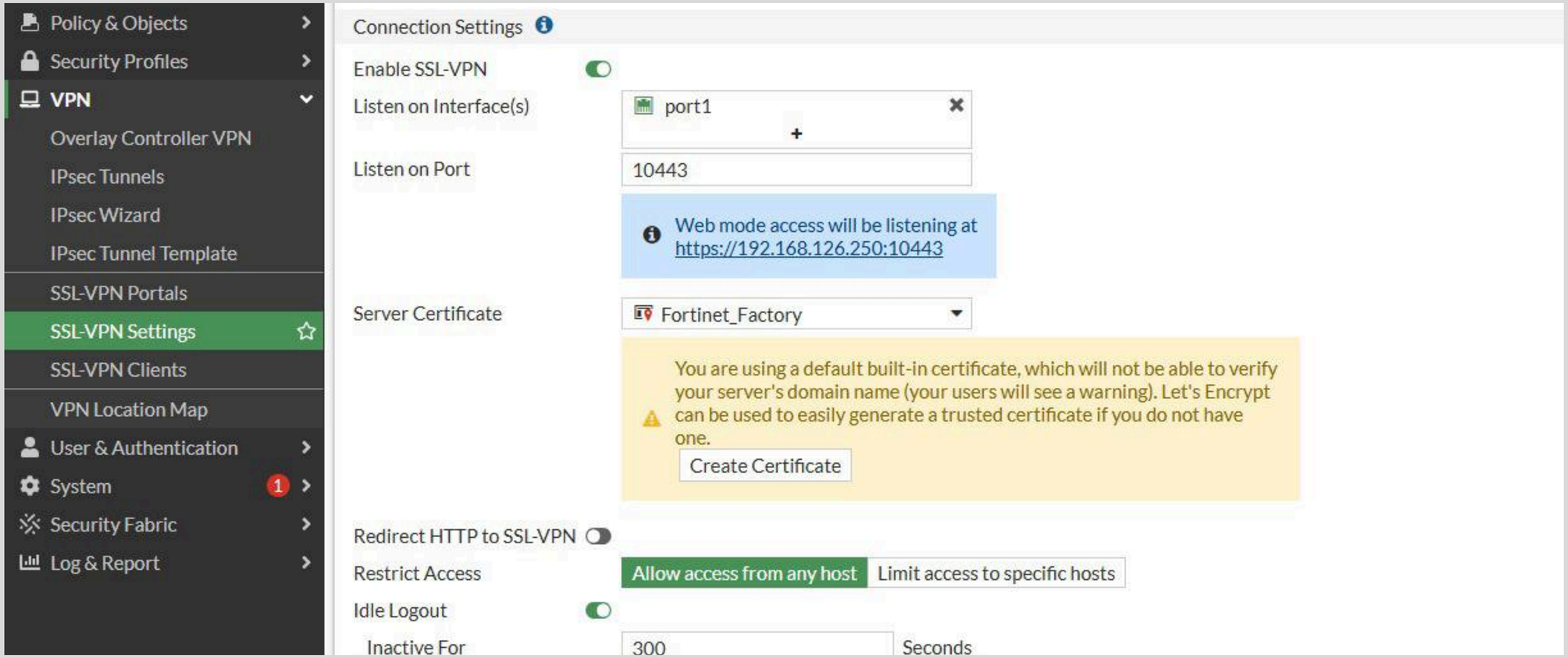
3- CONFIGURE SSL PORTAL



ENABLE WEB MODE &TUNNEL MODE

Name	Tunnel Mode	Web Mode
full-access	Enabled	Enabled

4- configure ssl settings



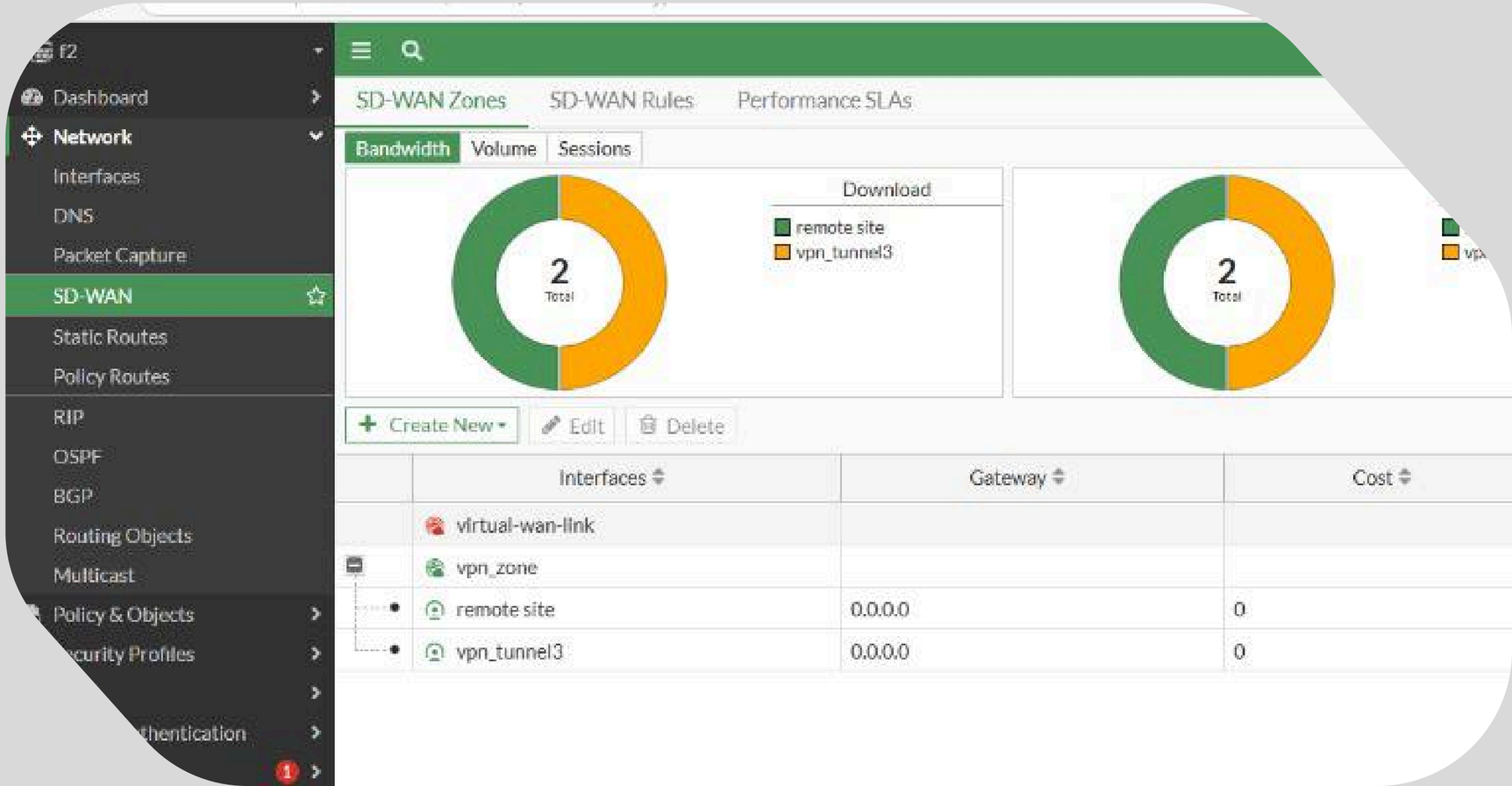
5- configure ssl_vpn policy

SD-WAN over IPSec

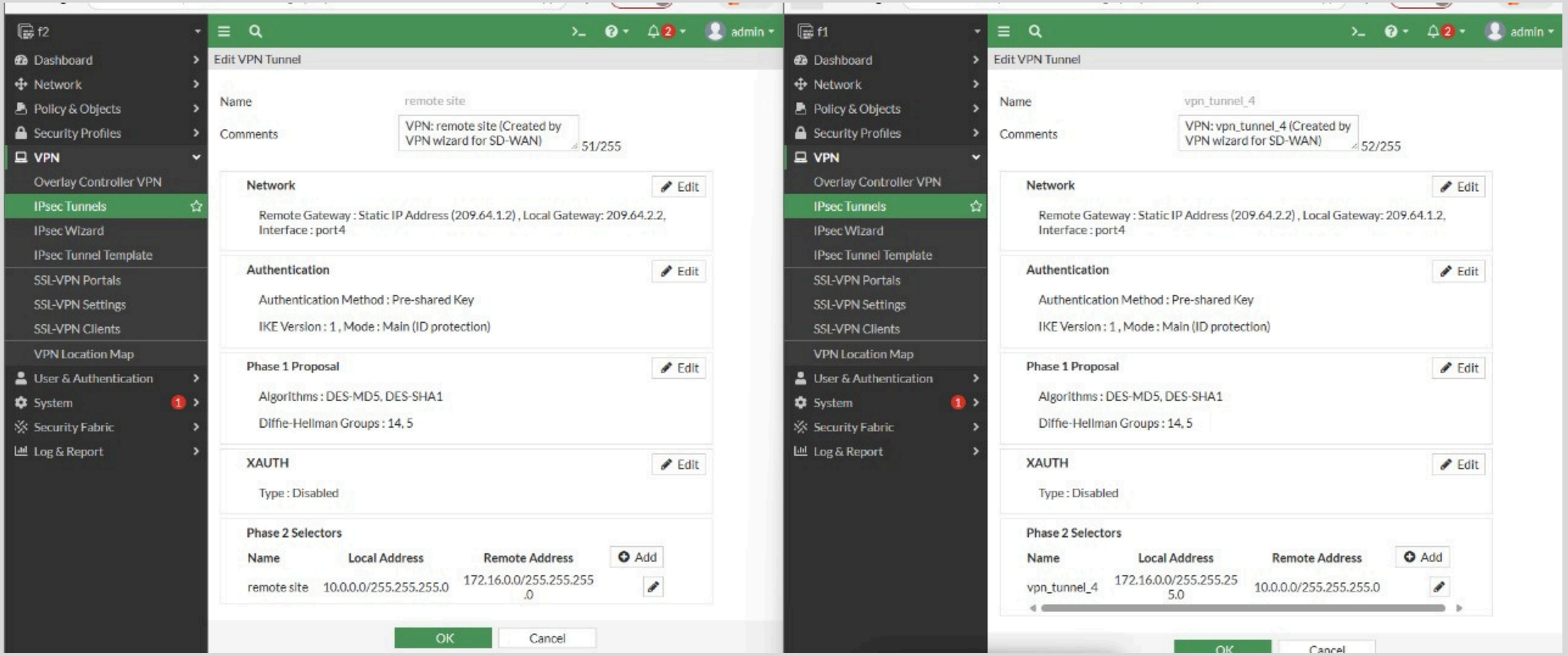
Purpose: Combine multiple internet links for smart traffic distribution, load balancing, and automatic failover.

Benefits of VPN + SD-WAN

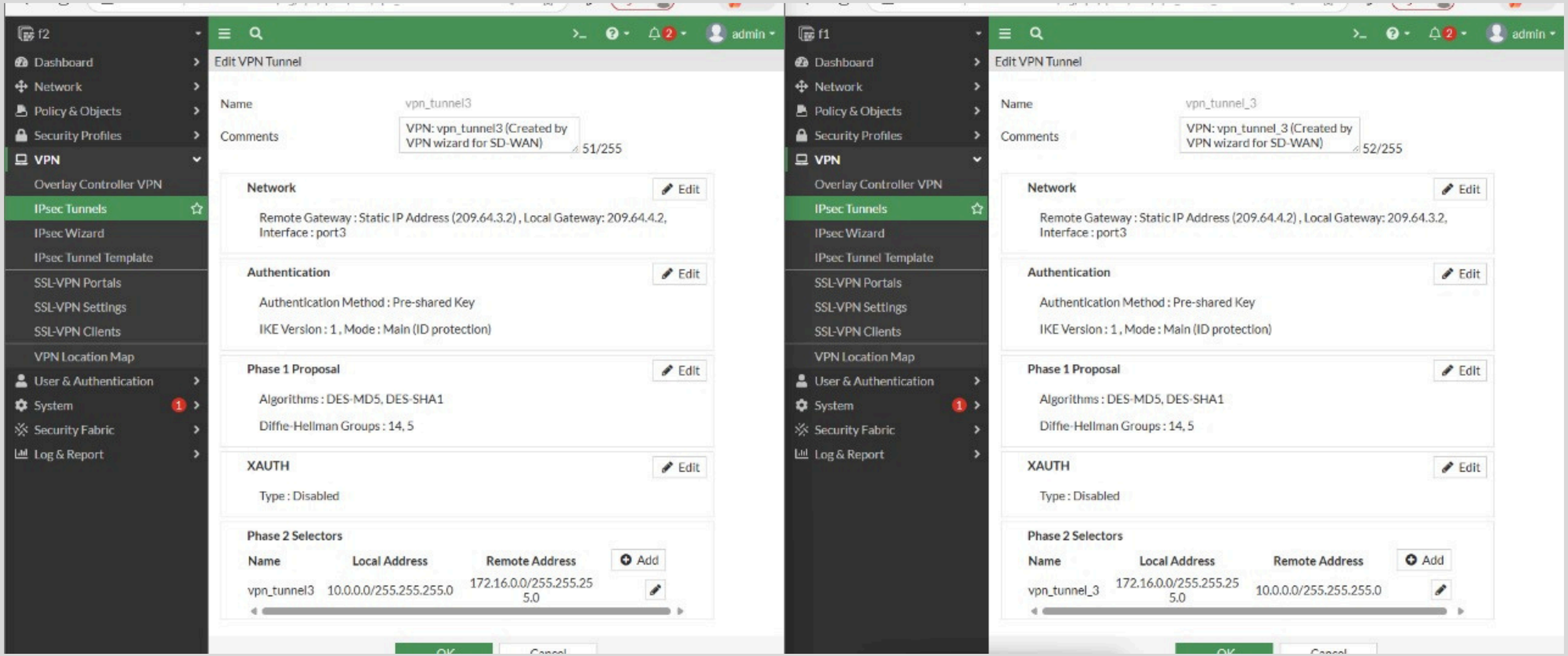
- Secure communication between remote networks and users.
- Optimized internet and application performance.
- High availability and automatic failover.
- Centralized monitoring and proactive network management.



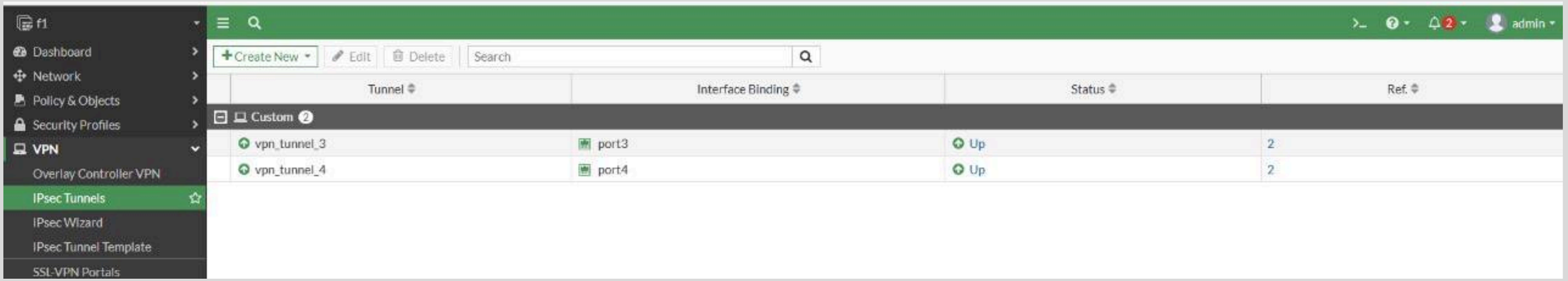
ESTABLISHING THE FIRST TUNNEL ON F1 AND F2



ESTABLISHING THE SECOND TUNNEL ON F1 AND F2

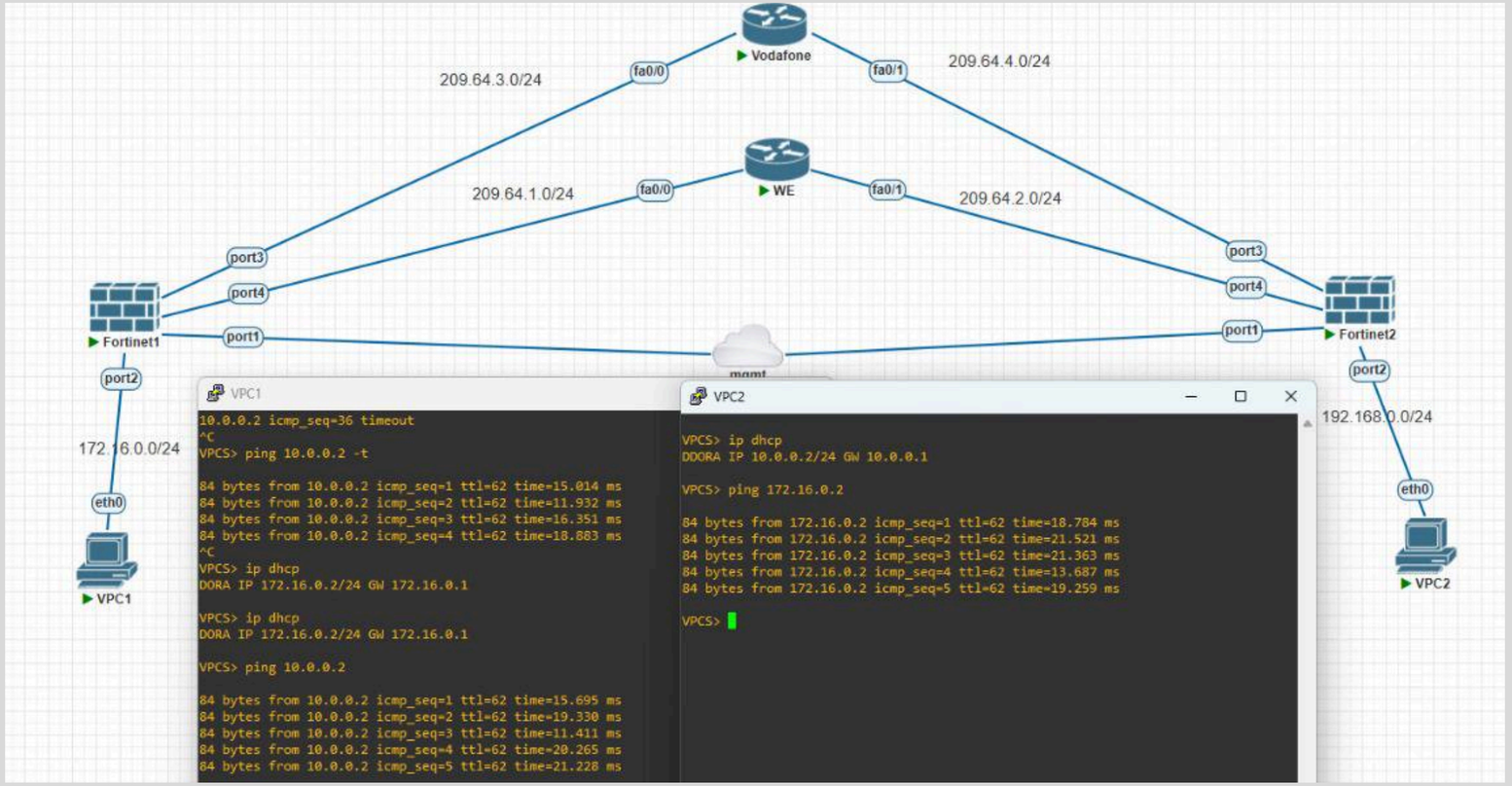


CHECKING THE STATUS OF THE TUNNELS



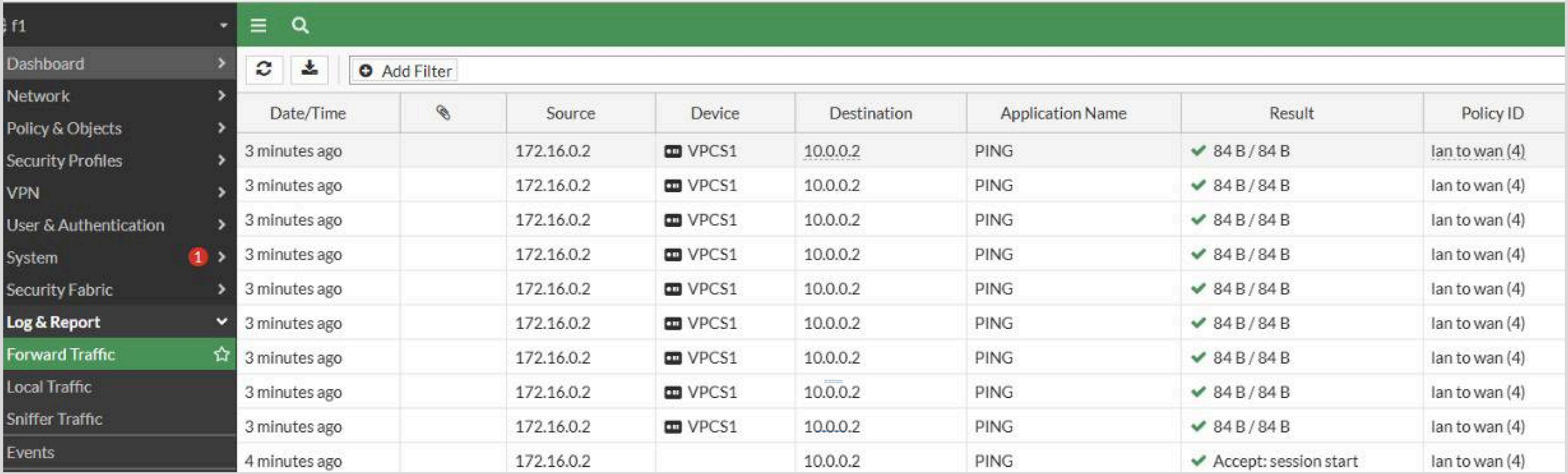
- On each FortiGate, the UP status indicates that:
- The remote peer is reachable.
- Both firewalls agree on all security parameters (encryption, authentication, DH group, etc.).
- The tunnel interface is active and ready to pass traffic.
- Routing and firewall policies are correctly configured to allow inter-site communication.

End-to-End VPN Connectivity Verification



- The topology shows two FortiGate firewalls connected via dual ISP paths (Vodafone & WE).
- IPsec VPN successfully established, allowing communication between 172.16.0.0/24 and 10.0.0.0/24 networks.
- Ping tests from both VPC sides confirm stable bidirectional reachability through the VPN tunnel.
- Latency values indicate active encrypted traffic flow routed across the VPN links.

Traffic Validation & Tunnel Reachability



Date/Time		Source	Device	Destination	Application Name	Result	Policy ID
3 minutes ago		172.16.0.2	VPCS1	10.0.0.2	PING	84 B / 84 B	lan to wan (4)
3 minutes ago		172.16.0.2	VPCS1	10.0.0.2	PING	84 B / 84 B	lan to wan (4)
3 minutes ago		172.16.0.2	VPCS1	10.0.0.2	PING	84 B / 84 B	lan to wan (4)
3 minutes ago		172.16.0.2	VPCS1	10.0.0.2	PING	84 B / 84 B	lan to wan (4)
3 minutes ago		172.16.0.2	VPCS1	10.0.0.2	PING	84 B / 84 B	lan to wan (4)
3 minutes ago		172.16.0.2	VPCS1	10.0.0.2	PING	84 B / 84 B	lan to wan (4)
3 minutes ago		172.16.0.2	VPCS1	10.0.0.2	PING	84 B / 84 B	lan to wan (4)
3 minutes ago		172.16.0.2	VPCS1	10.0.0.2	PING	84 B / 84 B	lan to wan (4)
3 minutes ago		172.16.0.2	VPCS1	10.0.0.2	PING	84 B / 84 B	lan to wan (4)
4 minutes ago		172.16.0.2		10.0.0.2	PING	Accept: session start	lan to wan (4)

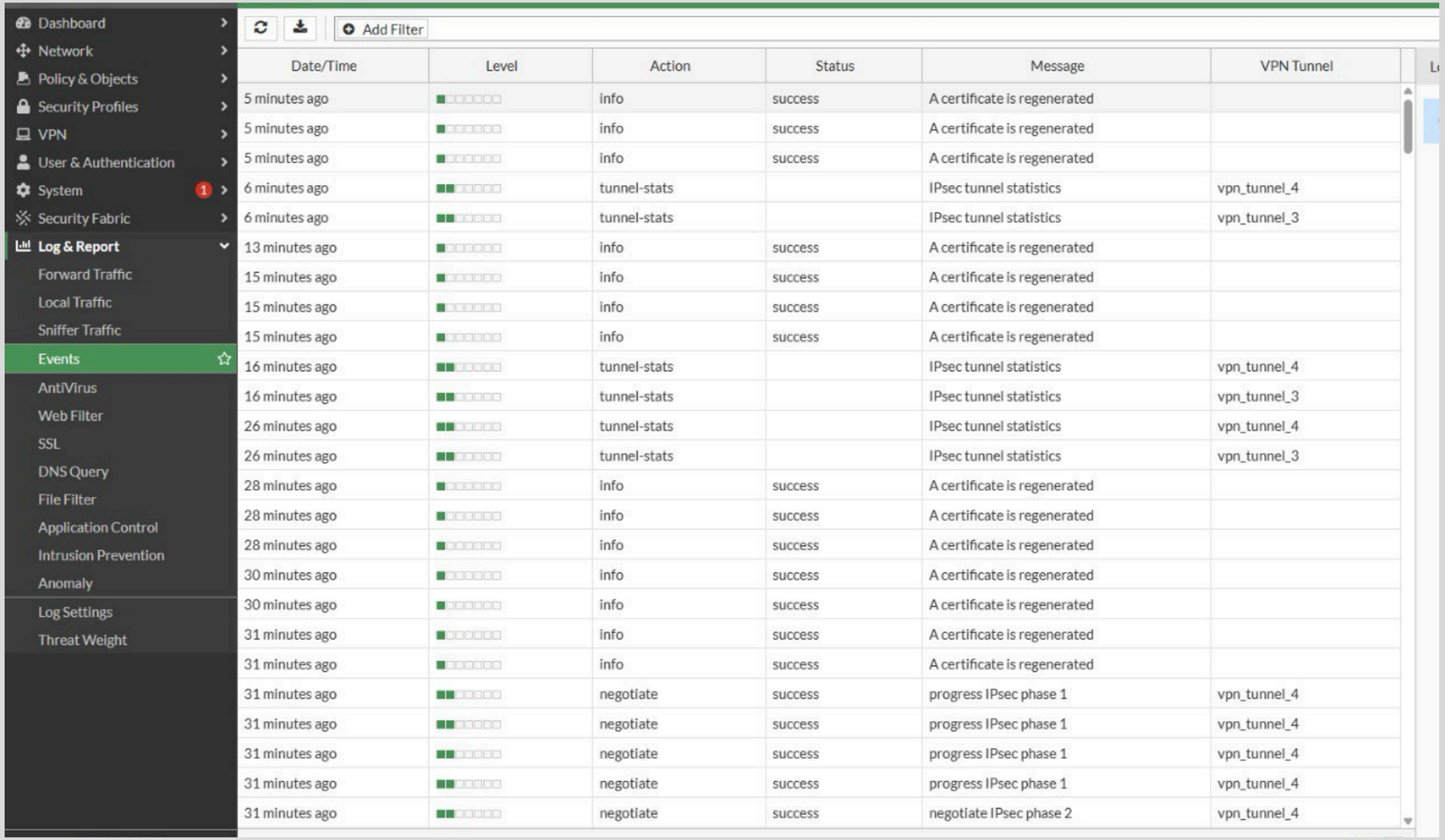
The log confirms successful bidirectional traffic between both sites.

ICMP sessions were allowed through the configured policies, with full visibility over source, destination, and application status.

Key Result

- PING requests successfully passed over the VPN path
- Policies enforced correctly: LAN → WAN and WAN → LAN
- No drops, blocks, or inspection failures recorded

MONITORING THE EVENTS ON FORTIGATE

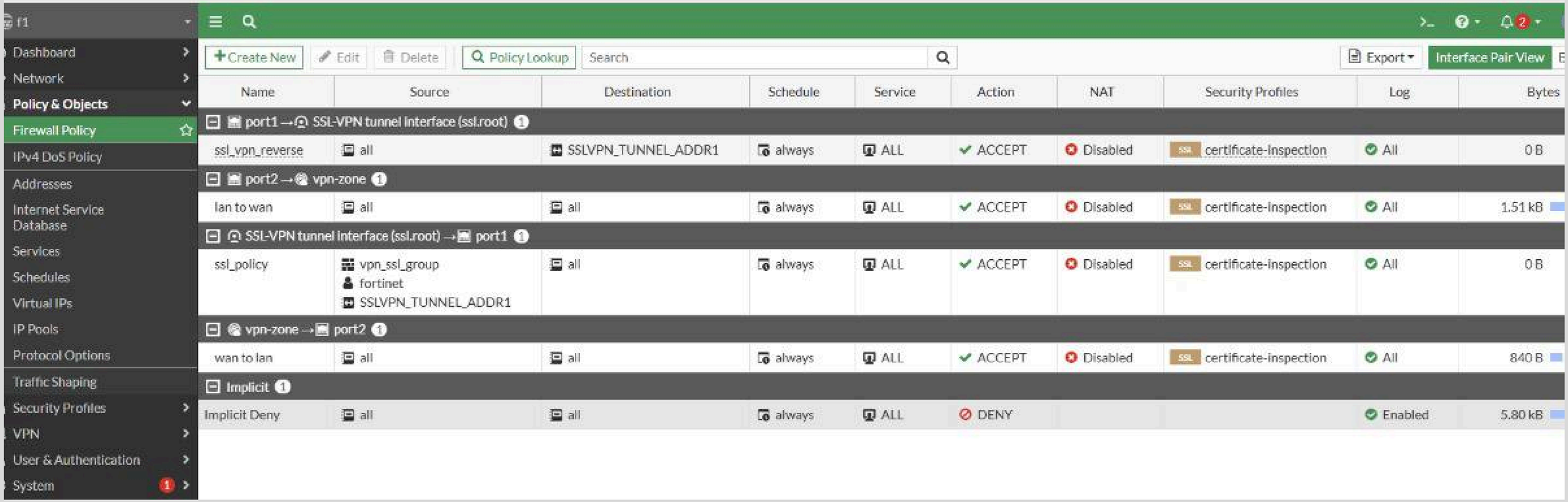


Date/Time	Level	Action	Status	Message	VPN Tunnel
5 minutes ago		info	success	A certificate is regenerated	
5 minutes ago		info	success	A certificate is regenerated	
5 minutes ago		info	success	A certificate is regenerated	
6 minutes ago		tunnel-stats		IPsec tunnel statistics	vpn_tunnel_4
6 minutes ago		tunnel-stats		IPsec tunnel statistics	vpn_tunnel_3
13 minutes ago		info	success	A certificate is regenerated	
15 minutes ago		info	success	A certificate is regenerated	
15 minutes ago		info	success	A certificate is regenerated	
15 minutes ago		info	success	A certificate is regenerated	
16 minutes ago		tunnel-stats		IPsec tunnel statistics	vpn_tunnel_4
16 minutes ago		tunnel-stats		IPsec tunnel statistics	vpn_tunnel_3
26 minutes ago		tunnel-stats		IPsec tunnel statistics	vpn_tunnel_4
26 minutes ago		tunnel-stats		IPsec tunnel statistics	vpn_tunnel_3
28 minutes ago		info	success	A certificate is regenerated	
28 minutes ago		info	success	A certificate is regenerated	
28 minutes ago		info	success	A certificate is regenerated	
30 minutes ago		info	success	A certificate is regenerated	
30 minutes ago		info	success	A certificate is regenerated	
31 minutes ago		info	success	A certificate is regenerated	
31 minutes ago		info	success	A certificate is regenerated	
31 minutes ago		negotiate	success	progress IPsec phase 1	vpn_tunnel_4
31 minutes ago		negotiate	success	progress IPsec phase 1	vpn_tunnel_4
31 minutes ago		negotiate	success	progress IPsec phase 1	vpn_tunnel_4
31 minutes ago		negotiate	success	progress IPsec phase 1	vpn_tunnel_4
31 minutes ago		negotiate	success	negotiate IPsec phase 2	vpn_tunnel_4

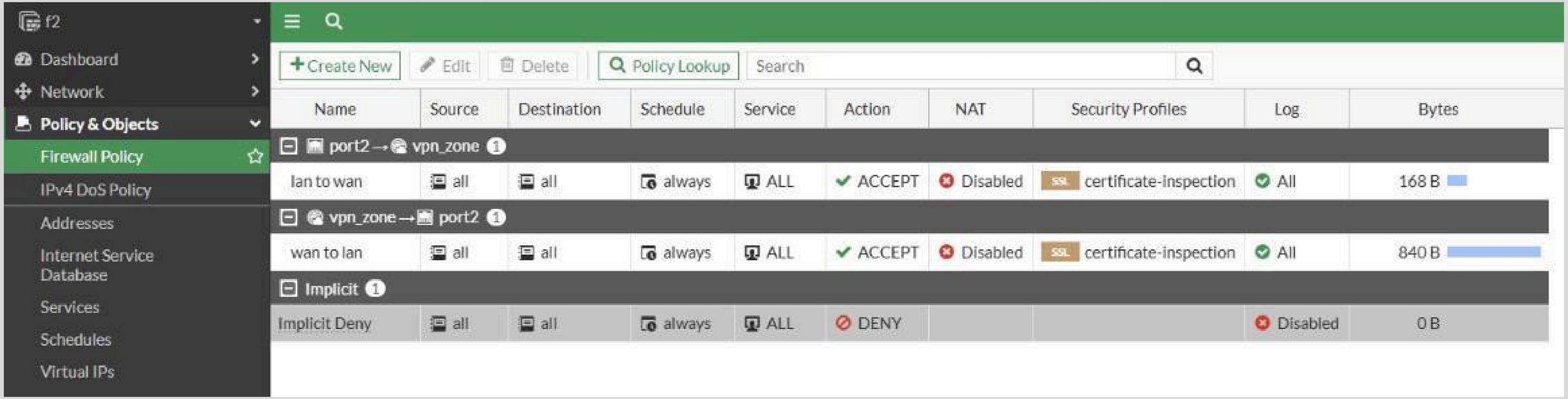
- Monitoring the IPsec tunnel UP status on each FortiGate device is essential to ensure stable and secure communication between the two sites. When the tunnel status shows UP, it confirms that both Phase 1 and Phase 2 negotiations have completed successfully, and that encrypted traffic can flow between the local and remote networks without interruption

Firewall Policy Overview

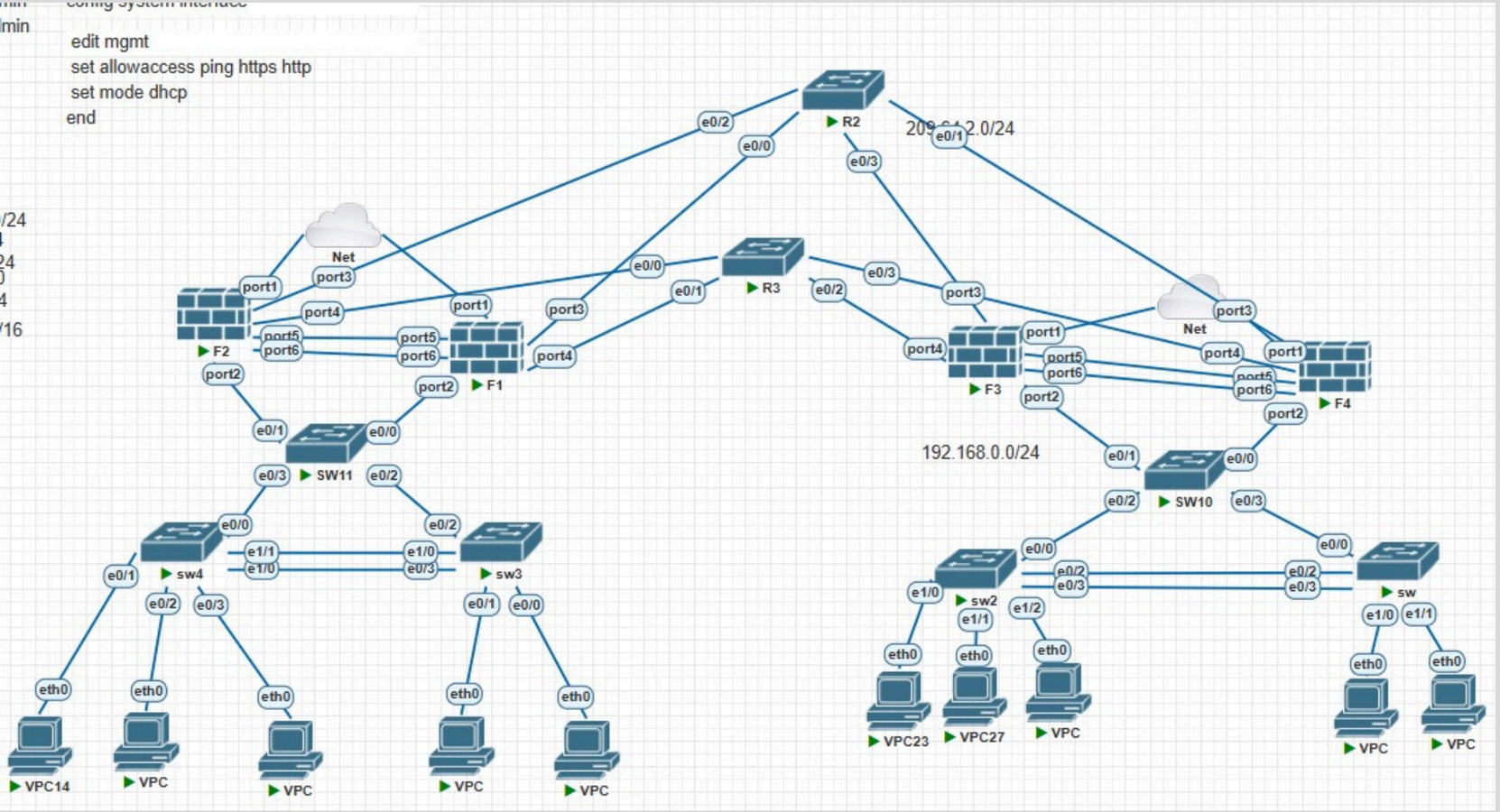
Firewall 1:



Firewall 2:


f2
Dashboard
Network
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
Create New
Edit
Delete
Policy Lookup
Search
Name
Source
Destination
Schedule
Service
Action
NAT
Security Profiles
Log
Bytes
port2 → vpn_zone 1
lan to wan
all
all
always
ALL
ACCEPT
Disabled
certificate-inspection
All
168 B
vpn_zone → port2 1
wan to lan
all
all
always
ALL
ACCEPT
Disabled
certificate-inspection
All
840 B
Implicit 1
Implicit Deny
all
all
always
ALL
DENY
Disabled
0 B

old Topology :



What Were Done

- Vlans
- Portchannel
- layer 2 security
- DHCP by FortiGate
- Vlan Routing by FortiGate
- HA
- SSL VPN
- IPSEC VPN
- SD-WAN
- policies

VLANS

in both HQ & BRANCH :

vlans	**name**	**ip / HQ**	**IP / BR**
vlan 10	**Management**	**172.16.10.0/24**	**192.168.10.0/24**
vlan 20	HR	**172.16.20.0/24**	**192.168.20.0/24**
vlan 30	IT	**172.16.30.0/24**	**192.168.30.0/24**
vlan 40	Finance	**172.16.40.0/24**	**192.168.40.0/24**
vlan 50	Sales	**172.16.50.0/24**	**192.168.50.0/24**
vlan 99	unused	**172.16.99.0/24**	**192.168.99.0/24**
vlan 100	Native	**172.16.100.0/24**	**192.168.10.0/24**

Define each port s vlan on sw :

Access :

```
!
interface Ethernet0/0
 switchport access vlan 20
 switchport mode access
 switchport port-security maximum 2
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0050.7966.6814
 switchport port-security mac-address sticky 0050.7966.682a
 switchport port-security
 duplex full
 spanning-tree portfast edge
 spanning-tree bpduguard enable
!
interface Ethernet0/1
 switchport access vlan 10
 switchport port-security maximum 2
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 duplex full
 spanning-tree portfast edge
 spanning-tree bpduguard enable
```

```
interface Ethernet0/1
 switchport access vlan 40
 switchport mode access
 switchport port-security maximum 5
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0050.7966.680b
 switchport port-security mac-address sticky 0050.7966.6819
 switchport port-security mac-address sticky 0050.7966.6842
 switchport port-security mac-address sticky ce8a.8e02.7601
 switchport port-security
 spanning-tree portfast edge
 spanning-tree bpduguard enable
!
interface Ethernet0/2
 switchport access vlan 50
 switchport mode access
 switchport port-security maximum 5
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0050.7966.680c
 switchport port-security mac-address sticky 0050.7966.6820
 switchport port-security mac-address sticky 0050.7966.683d
 switchport port-security mac-address sticky 6252.4ba0.dc13
 switchport port-security mac-address sticky 6694.1c9f.c875
 switchport port-security
 spanning-tree portfast edge
 spanning-tree bpduguard enable
!
interface Ethernet0/3
 switchport access vlan 30
 switchport mode access
```

Trunk:

```
!
interface Ethernet0/2
 switchport trunk allowed vlan 10,20,30,40,50,100
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 ip dhcp snooping trust
!
```

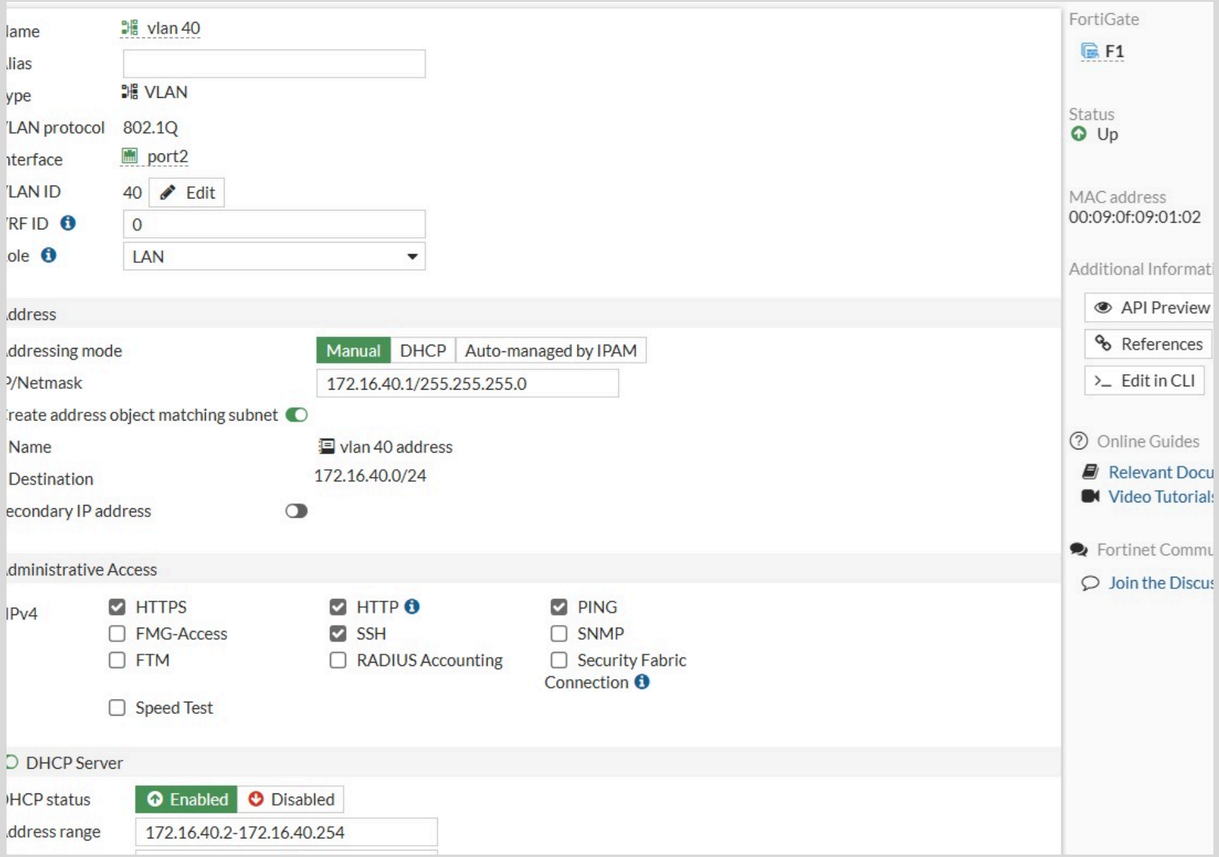
```
!
!
interface Port-channel1
 switchport trunk allowed vlan 10,20,30,40,50,60
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport mode trunk
 switchport nonegotiate
!
interface Ethernet0/0
```

Add Vlans on both Fortigate :

	port2	Physical Interface		0.0.0.0/0.0.0.0	PING HTTPS SSH		13
	vlan 10	VLAN		192.168.10.1/255.255.255.0	PING HTTPS SSH	1	192.168.10.2-192.168.10.254 3
	vlan 20	VLAN		192.168.20.1/255.255.255.0	PING HTTPS SSH	1	192.168.20.2-192.168.20.254 3
	vlan 30	VLAN		192.168.30.1/255.255.255.0	PING HTTPS SSH		192.168.30.2-192.168.30.254 3
	vlan 40	VLAN		192.168.40.2/255.255.255.0	PING HTTPS SSH		192.168.40.2-192.168.40.254 3
	vlan 50	VLAN		192.168.50.1/255.255.255.0	PING HTTPS		192.168.50.2-192.168.50.254 3

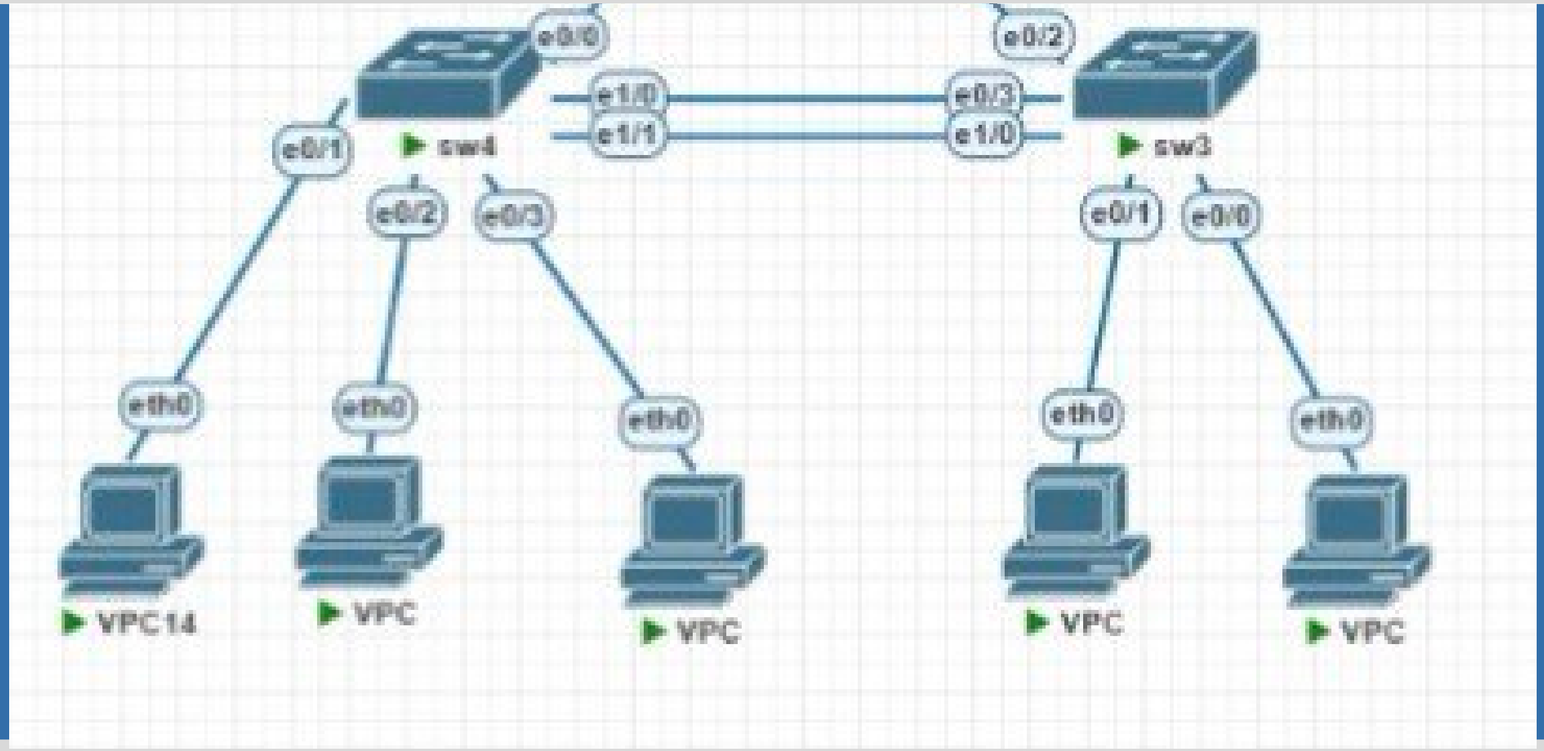
	port2	Physical Interface		0.0.0.0/0.0.0.0			13
	vlan 10	VLAN		172.16.10.1/255.255.255.0	PING HTTPS SSH	1	172.16.10.2-172.16.10.254 3
	vlan 20	VLAN		172.16.20.1/255.255.255.0	PING HTTPS SSH		172.16.20.2-172.16.20.254 3
	vlan 30	VLAN		172.16.30.1/255.255.255.0	PING HTTPS SSH	1	172.16.30.2-172.16.30.254 3
	vlan 40	VLAN		172.16.40.1/255.255.255.0	PING HTTPS SSH		172.16.40.2-172.16.40.254 3
	vlan 50	VLAN		172.16.50.1/255.255.255.0	PING HTTPS		172.16.50.2-172.16.50.254 3

Enable Dhcp & creating vlans :



Routing between Vlans :

ETHERCHANNEL IMPROVEMENT (BACKBONE)

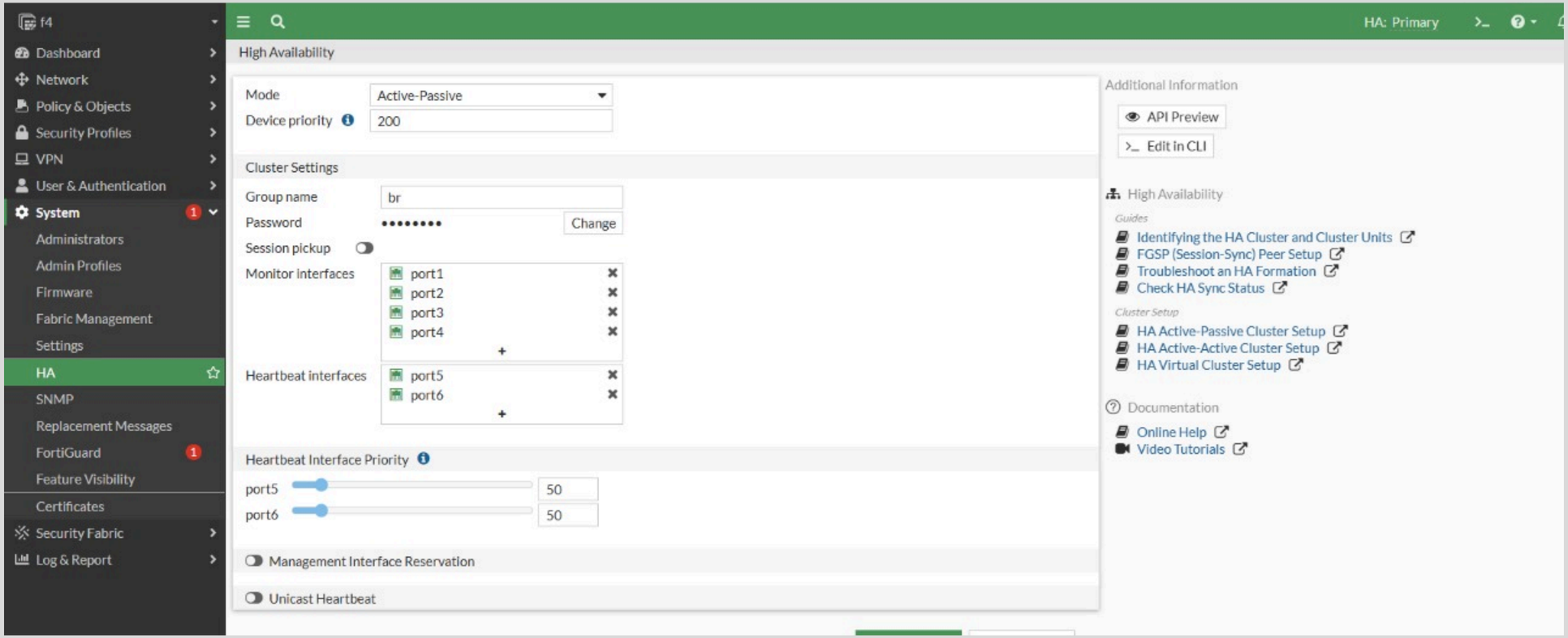


- All duplicated links merged into Port-Channel1.
- LACP used to form one logical trunk link.
- Eliminated STP blocking.
- Increased backbone bandwidth.
- High availability if one link fails.

Trunk Paths Mapping

```
!
!
interface Port-channel1
 switchport trunk allowed vlan 10,20,30,40,50,60
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
```

HA :

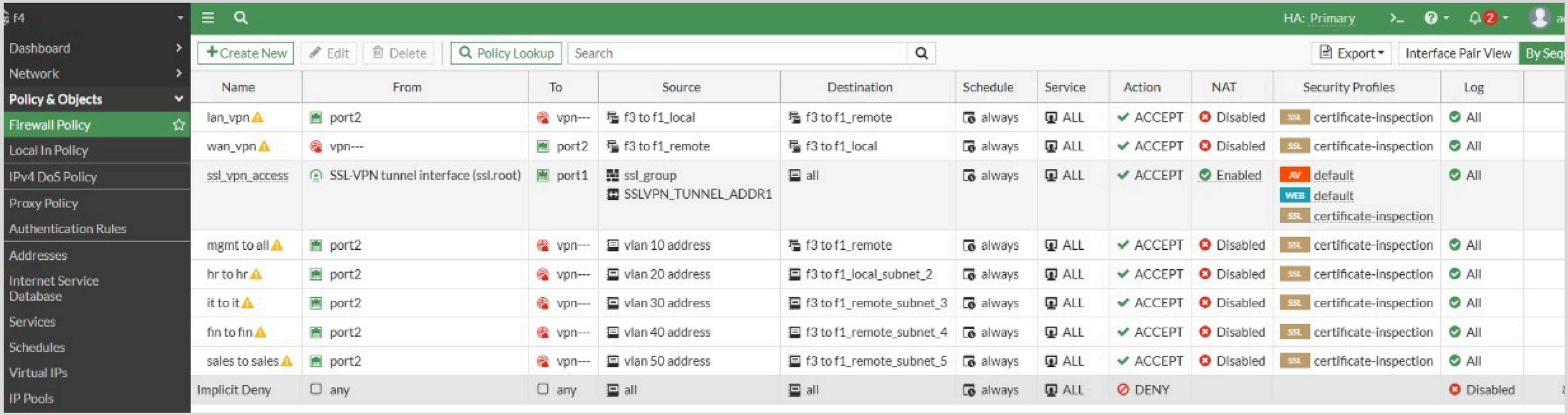


Status	Priority	Hostname	Serial No.	Role	System Uptime	Sessions	Throughput
Synchronized	200	f4	FGVMEV-BZZEEWI0B	Primary	9h 17m	27	76.00 kbps
Synchronized	100	f3	FGVMEVUYD10S_612	Secondary	9h 17m	1	42.00 kbps

Status	Priority	Hostname	Serial No.	Role	System Uptime	Sessions	Throughput
Synchronized	200	F1	FGVMEVNTCORGLDBE	Primary	1h 23m	14	39.00 kbps
Synchronized	100	f2	FGVMEV1A7X7BSU14	Secondary	1h 22m	0	38.00 kbps

Add Firewall Policies

Firewall Policies Overview:



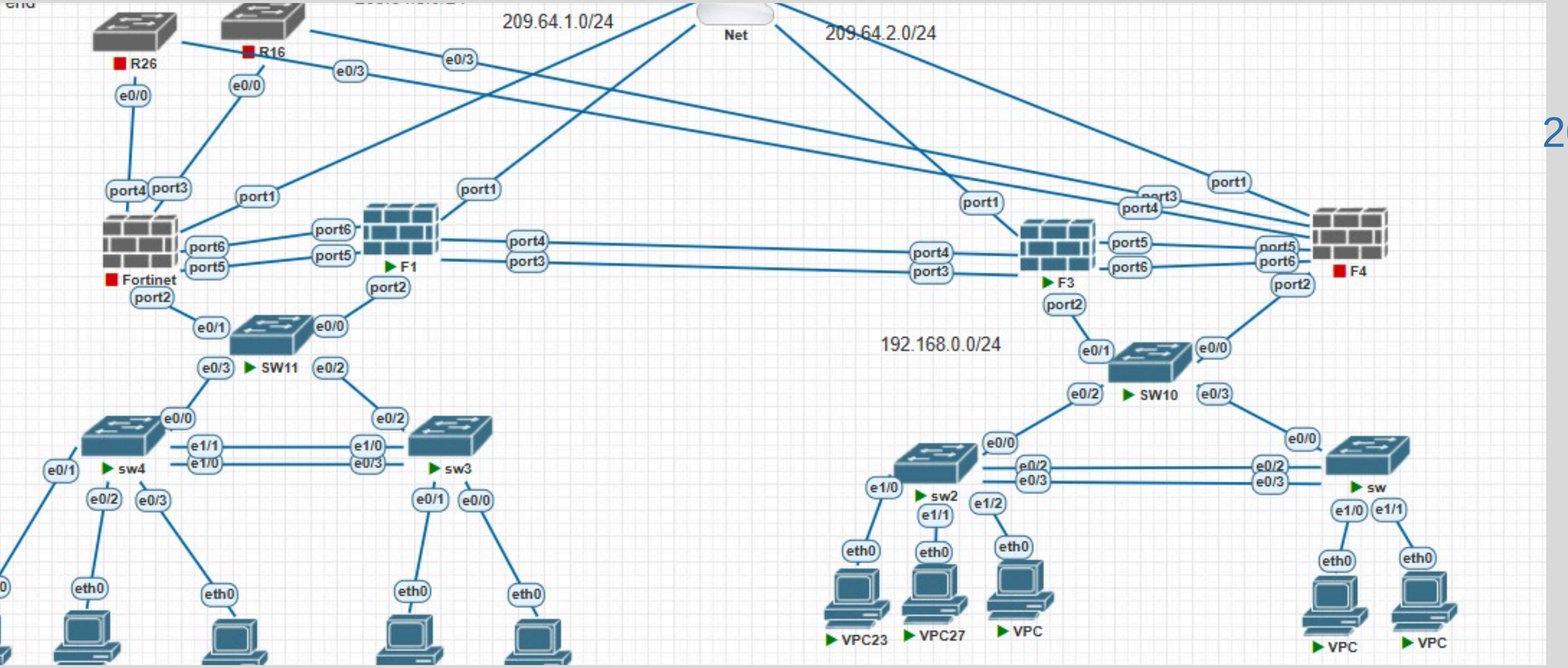
ssl VPN & IPsec VPN & SD-WAn:

same like new Topology

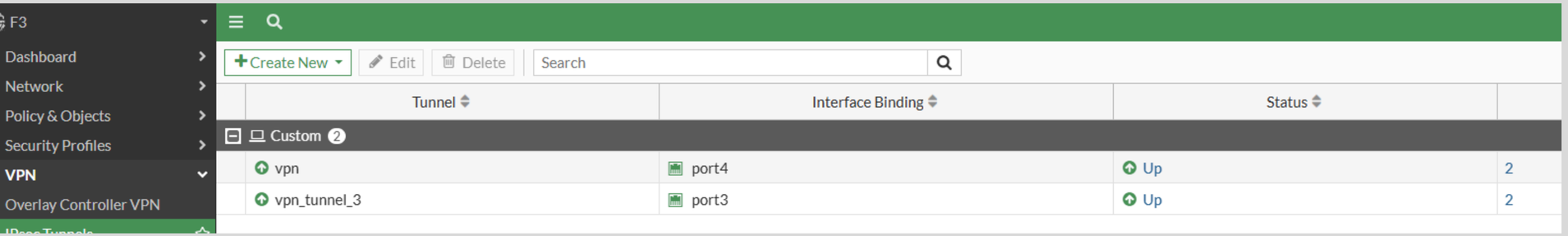
BUT .....

there is a problem ?

Update :



Networks are 209.64.3.0/24 & 209.64.1.0/24 only



Thank you