

# Implementing VPN Solutions with FortiGate



رواد مسار الرقمية

Fortinet Cybersecurity Engineer

# Project by:

Mohamed Ahmed Mohamed Haridy

shahd yesen salah abdelmoamen

Jana Hany Salah Eldin

Nada Ahmed Abo-Bakr Abdelnaser

Shams Ibrahim Ali Mohamed

Merna medhat hamdy rabia

Supervised by: Eng. Alhussieny Mohamed Ali

Presented to: Dr.Hussien Harb

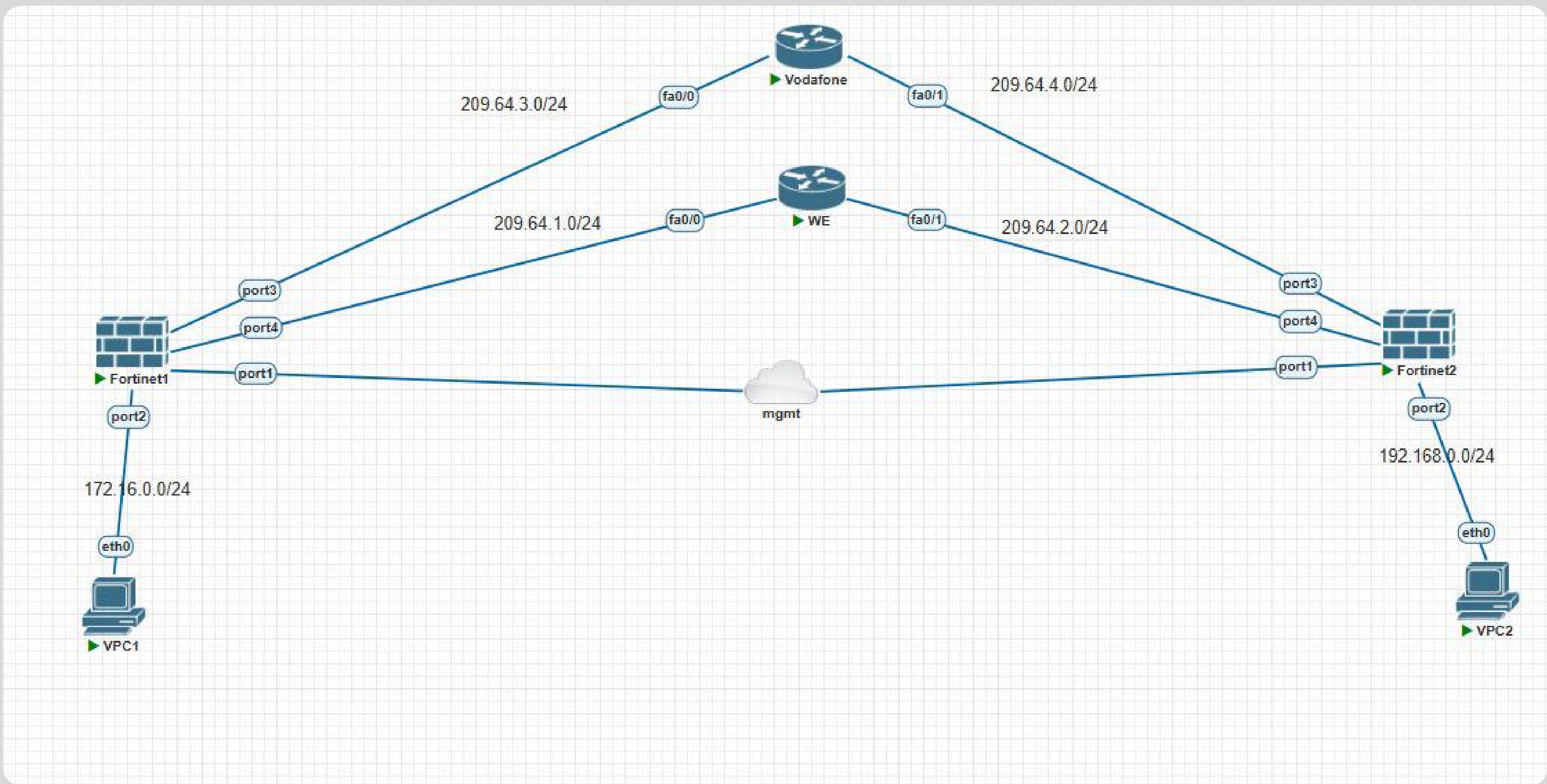
# INTRODUCTION

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

The screenshot shows the FortiGate Management interface under the 'Network' section, specifically the 'Interfaces' tab. The left sidebar lists various network-related configurations. The main pane displays a table of interfaces with the following columns: Name, Type, Members, IP/Netmask, Administrative Access, DHCP Clients, DHCP Ranges, and Ref. The table includes sections for '802.3ad Aggregate', 'Physical Interface', 'SD-WAN Zone', and 'Tunnel Interface'. The 'Physical Interface' section contains four entries: port1, port2, port3, and port4. The 'SD-WAN Zone' section contains two entries: virtual-wan-link and vpn-zone. The 'Tunnel Interface' section contains one entry: Tunnel 1.

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
802.3ad Aggregate 1	802.3ad Aggregate			PING Security Fabric Connection		10.255.1.2-10.255.1.254	2
Physical Interface 6							
port1	Physical Interface		192.168.126.250/255.255.255.0	PING HTTPS SSH HTTP			4
port2	Physical Interface		172.16.0.1/255.255.255.0	PING HTTPS SSH	1	172.16.0.2-172.16.0.254	3
port3	Physical Interface		209.64.3.2/255.255.255.0	PING HTTPS SSH			3
port4	Physical Interface		209.64.1.2/255.255.255.0	PING HTTPS SSH			3
SD-WAN Zone 2							
virtual-wan-link	SD-WAN Zone		0.0.0.0/0.0.0.0				
vpn-zone	SD-WAN Zone	vpn_tunnel_3 vpn_tunnel_4	0.0.0.0/0.0.0.0				
Tunnel Interface 1							

- 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

IP/Netmask: 172.16.0.1/255.255.255.0

Create address object matching subnet:

Secondary IP address:

Administrative Access

IPv4	<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> PING	<input type="checkbox"/> FMG-Access
	<input checked="" type="checkbox"/> SSH	<input type="checkbox"/> SNMP	<input type="checkbox"/> FTM
	<input type="checkbox"/> RADIUS Accounting	<input type="checkbox"/> Security Fabric Connection <span style="color: blue;">(i)</span>	<input type="checkbox"/> Speed Test

Receive LLDP (i): Use VDOM Setting  Enable  Disable

Transmit LLDP (i): Use VDOM Setting  Enable  Disable

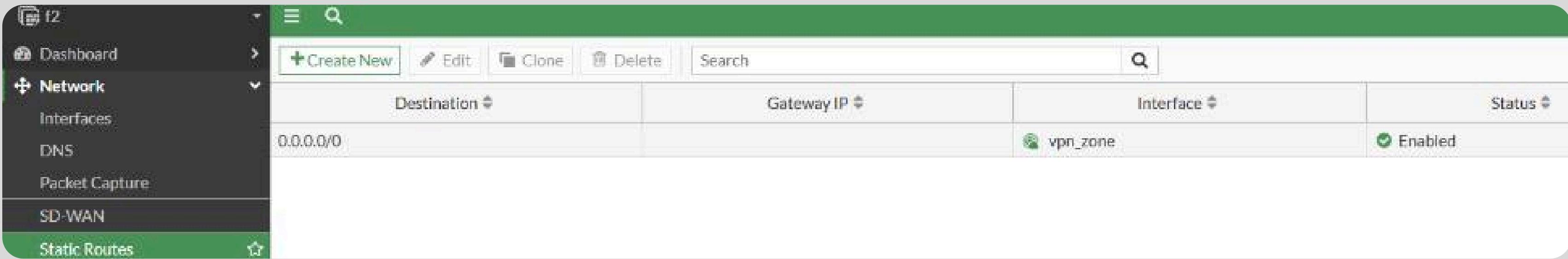
DHCP Server

DHCP status: Enabled Disabled

Address range: 172.16.0.2-172.16.0.254

+

# STATIC ROUTE CONFIGURATION OVERVIEW



The screenshot shows a network management interface with a green header bar. The left sidebar includes options like Dashboard, Network (with sub-options Interfaces, DNS, and Packet Capture), SD-WAN, and Static Routes, with Static Routes being the active tab. The main area displays a table with columns: Destination, Gateway IP, Interface, and Status. A single row is visible, showing a Destination of 0.0.0.0/0, a Gateway IP of vpn\_zone, an Interface of vpn\_zone, and a Status of Enabled.

Destination	Gateway IP	Interface	Status
0.0.0.0/0	vpn_zone	vpn_zone	Enabled

- 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)

WE

```
*Mar 1 00:00:00.155: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router>
Router>
Router>
Router>en
Router#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

  172.16.0.0/24 is subnetted, 1 subnets
S    172.16.0.0 [1/0] via 209.64.1.2
  10.0.0.0/24 is subnetted, 1 subnets
S    10.0.0.0 [1/0] via 209.64.2.2
C    209.64.1.0/24 is directly connected, FastEthernet0/0
C    209.64.2.0/24 is directly connected, FastEthernet0/1
Router#
```

Vodafone

```
Router>
Router>
Router>
Router>en
Router#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

  172.16.0.0/24 is subnetted, 1 subnets
S    172.16.0.0 [1/0] via 209.64.3.2
C    209.64.4.0/24 is directly connected, FastEthernet0/1
  10.0.0.0/24 is subnetted, 1 subnets
S    10.0.0.0 [1/0] via 209.64.4.2
C    209.64.3.0/24 is directly connected, FastEthernet0/0
Router#
```

# SSL VPN

steps for ssl vpn :

## 1- create a user

The screenshot shows the FortiGate management interface for creating a new user. The left sidebar menu is visible, showing various system settings like Dashboard, Network, Policy & Objects, Security Profiles, and User & Authentication. Under User & Authentication, 'User Definition' is selected. The main window title is 'Edit User'. The configuration fields are as follows:

- Username: fortinet
- User Account Status: Enabled (selected)
- User Type: Local User
- Password: (redacted)
- User Group: vpn\_ssl\_group (selected)
- Two-factor Authentication: Off (unchecked)

At the bottom are 'OK' and 'Cancel' buttons.

## 2- add user to a group

The screenshot shows the FortiManager interface for managing User Groups. The left sidebar navigation includes Dashboard, Network, Policy & Objects, Security Profiles, VPN, User & Authentication (selected), User Definition, and User Groups. The main content area displays a table of User Groups with columns for Group Name, Group Type, and Members.

Group Name	Group Type	Members
Guest-group	Firewall	guest
SSO_Guest_Users	Fortinet Single Sign-On (FSSO)	
vpn_ssl_group	Firewall	fortinet

### 3- CONFIGURE SSL PORTAL

Name

Limit Users to One SSL-VPN Connection at a Time

Tunnel Mode

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

Enabled Based on Policy Destination  
Only client traffic in which the destination matches the destination of the configured fi the SSL-VPN tunnel.

Enabled for Trusted Destinations  
Only client traffic which does not match explicitly trusted destinations will be directed

Source IP Pools

Tunnel Mode Client Options

### ENABLE WEB MODE & TUNNEL MODE

Name	Tunnel Mode	Web Mode
full-access	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled

# 4- configure ssl settings

The screenshot shows the 'SSL-VPN Settings' configuration page. On the left sidebar, 'SSL-VPN Settings' is highlighted with a green bar. The main panel displays the following configuration:

- Connection Settings**:
  - Enable SSL-VPN:
  - Listen on Interface(s): port1
  - Listen on Port: 10443
  - A tooltip indicates: "Web mode access will be listening at <https://192.168.126.250:10443>".
- Server Certificate**: Fortinet\_Factory
- A note states: "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." with a "Create Certificate" button.
- Redirect HTTP to SSL-VPN**:
- Restrict Access**: Allow access from any host
- Idle Logout**:
- Inactive For**: 300 Seconds

# 5- configure ssl\_vpn policy

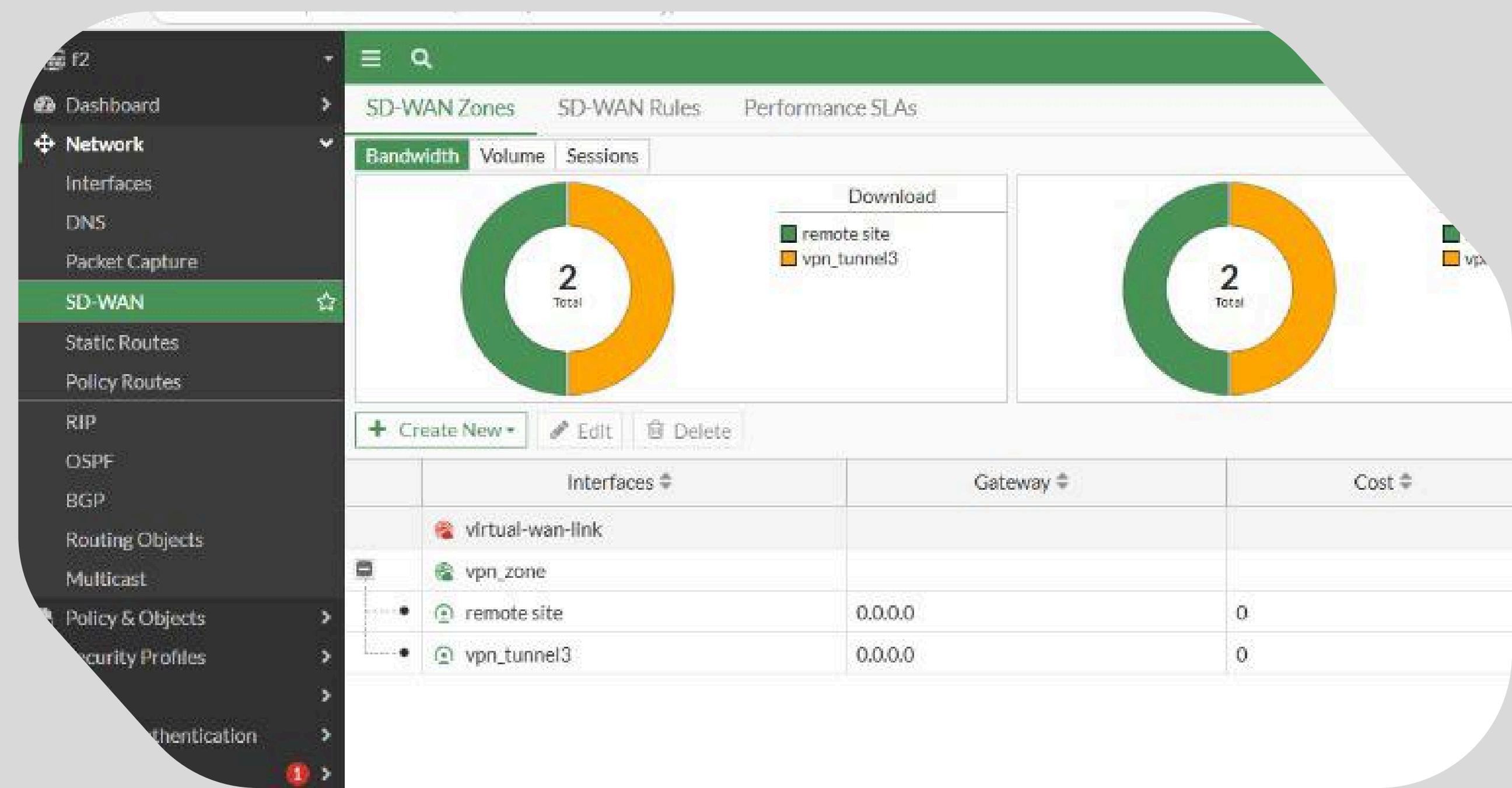
SSL-VPN tunnel interface (ssl.root)	port1	vpn_ssl_group	all	always	ALL	ACCE
		fortinet				

# 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

The image displays two side-by-side screenshots of a network configuration interface, likely from a Juniper SD-WAN controller. Both screens show the configuration of IPsec tunnels for establishing a VPN connection between a local site and a remote site.

**Left Screenshot (Device f2):**

- Name:** remote site
- Comments:** VPN: remote site (Created by VPN wizard for SD-WAN) 51/255
- Network:** Remote Gateway: Static IP Address (209.64.1.2), Local Gateway: 209.64.2.2, Interface: port4
- Authentication:** Authentication Method: Pre-shared Key, IKE Version: 1, Mode: Main (ID protection)
- Phase 1 Proposal:** Algorithms: DES-MD5, DES-SHA1, Diffie-Hellman Groups: 14, 5
- XAUTH:** Type: Disabled
- Phase 2 Selectors:** Name: remote site, Local Address: 10.0.0.0/255.255.255.0, Remote Address: 172.16.0.0/255.255.255.0

**Right Screenshot (Device f1):**

- Name:** vpn\_tunnel\_4
- Comments:** VPN: vpn\_tunnel\_4 (Created by VPN wizard for SD-WAN) 52/255
- Network:** Remote Gateway: Static IP Address (209.64.2.2), Local Gateway: 209.64.1.2, Interface: port4
- Authentication:** Authentication Method: Pre-shared Key, IKE Version: 1, Mode: Main (ID protection)
- Phase 1 Proposal:** Algorithms: DES-MD5, DES-SHA1, Diffie-Hellman Groups: 14, 5
- XAUTH:** Type: Disabled
- Phase 2 Selectors:** Name: vpn\_tunnel\_4, Local Address: 172.16.0.0/255.255.255.50, Remote Address: 10.0.0.0/255.255.255.0

# ESTABLISHING THE SECOND TUNNEL ON F1 AND F2

The image displays two side-by-side screenshots of a network configuration interface, likely from a Juniper SD-WAN controller. Both screens show the 'Edit VPN Tunnel' configuration page for two different devices, f2 and f1.

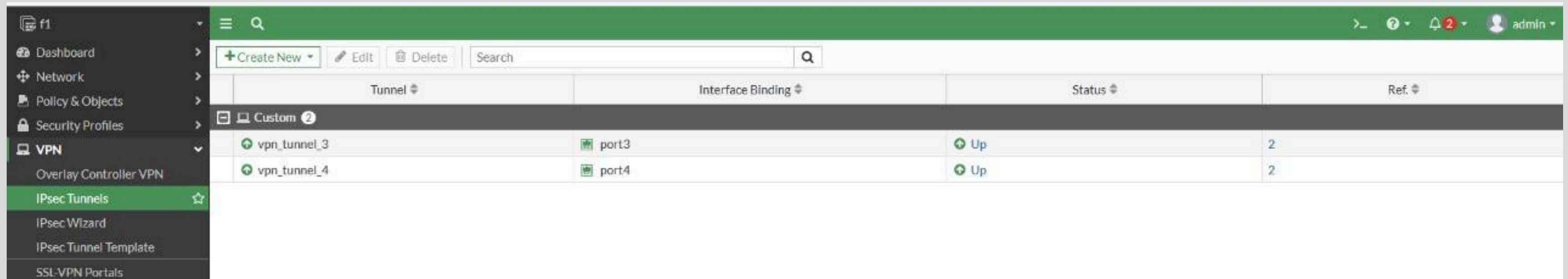
**Left Screenshot (Device f2):**

- Name:** vpn\_tunnel3
- Comments:** VPN:vpn\_tunnel3 (Created by VPN wizard for SD-WAN)
- Network:** Remote Gateway: Static IP Address (209.64.3.2), Local Gateway: 209.64.4.2, Interface: port3
- Authentication:** Authentication Method: Pre-shared Key, IKE Version: 1, Mode: Main (ID protection)
- Phase 1 Proposal:** Algorithms: DES-MD5, DES-SHA1, Diffie-Hellman Groups: 14, 5
- XAUTH:** Type: Disabled
- Phase 2 Selectors:** Name: vpn\_tunnel3, Local Address: 10.0.0.0/255.255.255.0, Remote Address: 172.16.0.0/255.255.255.255, Distance: 5.0

**Right Screenshot (Device f1):**

- Name:** vpn\_tunnel\_3
- Comments:** VPN:vpn\_tunnel\_3 (Created by VPN wizard for SD-WAN)
- Network:** Remote Gateway: Static IP Address (209.64.4.2), Local Gateway: 209.64.3.2, Interface: port3
- Authentication:** Authentication Method: Pre-shared Key, IKE Version: 1, Mode: Main (ID protection)
- Phase 1 Proposal:** Algorithms: DES-MD5, DES-SHA1, Diffie-Hellman Groups: 14, 5
- XAUTH:** Type: Disabled
- Phase 2 Selectors:** Name: vpn\_tunnel\_3, Local Address: 172.16.0.0/255.255.255.255, Remote Address: 10.0.0.0/255.255.255.0, Distance: 5.0

# CHECKING THE STATUS OF THE TUNNELS

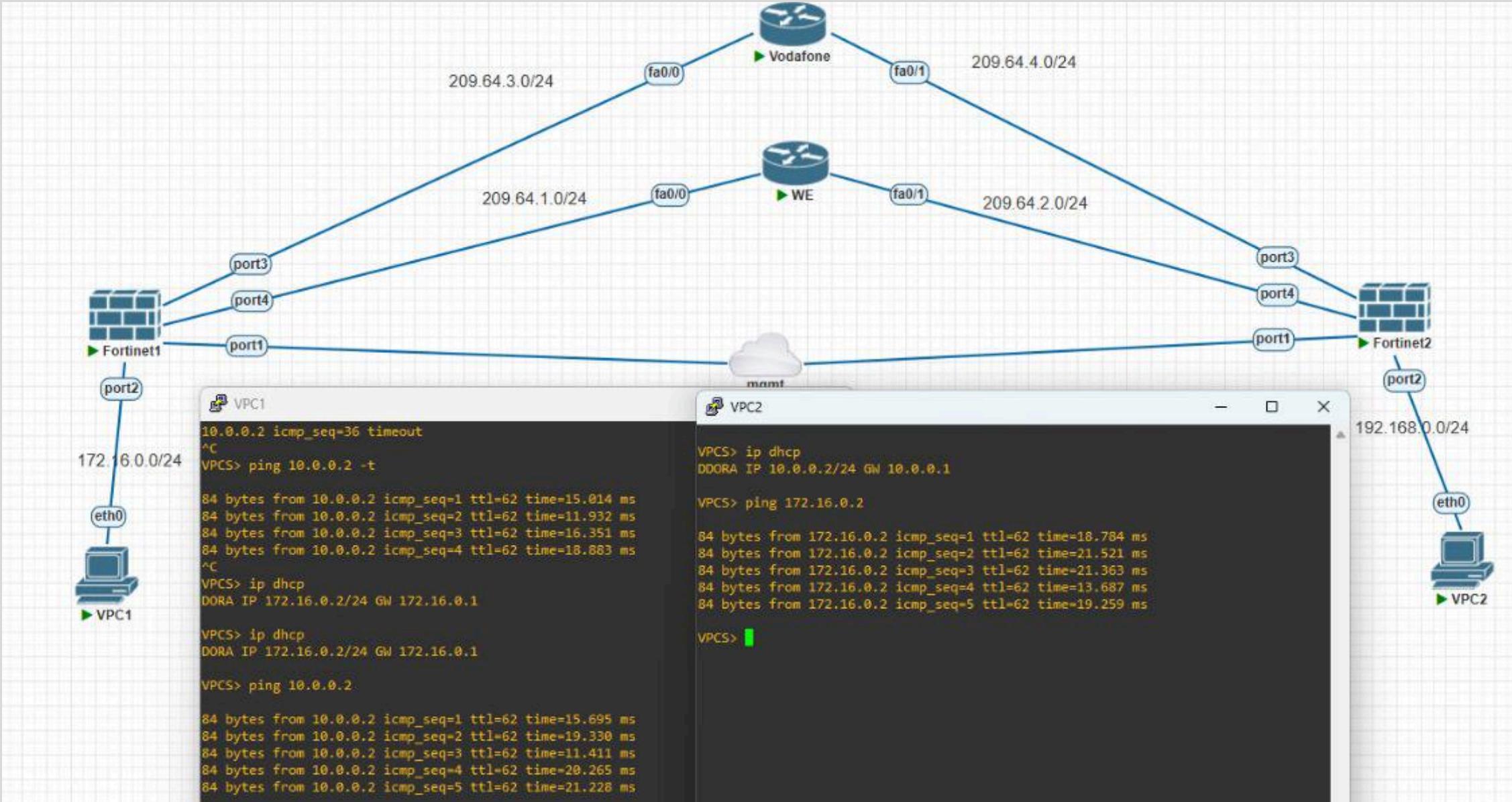


The screenshot shows the FortiGate management interface for checking tunnel status. The left sidebar menu is visible with options like Dashboard, Network, Policy & Objects, Security Profiles, VPN (selected), Overlay Controller VPN, IPsec Tunnels (selected), IPsec Wizard, IPsec Tunnel Template, and SSL-VPN Portals. The main content area displays a table titled 'IPsec Tunnels' with columns: Tunnel, Interface Binding, Status, and Ref. Two tunnels are listed: 'vpn\_tunnel\_3' and 'vpn\_tunnel\_4'. Both tunnels are bound to 'port3' and 'port4' respectively. Their status is 'Up', indicated by green icons. The 'Ref.' column shows the value '2' for both tunnels.

Tunnel	Interface Binding	Status	Ref.
vpn_tunnel_3	port3	Up	2
vpn_tunnel_4	port4	Up	2

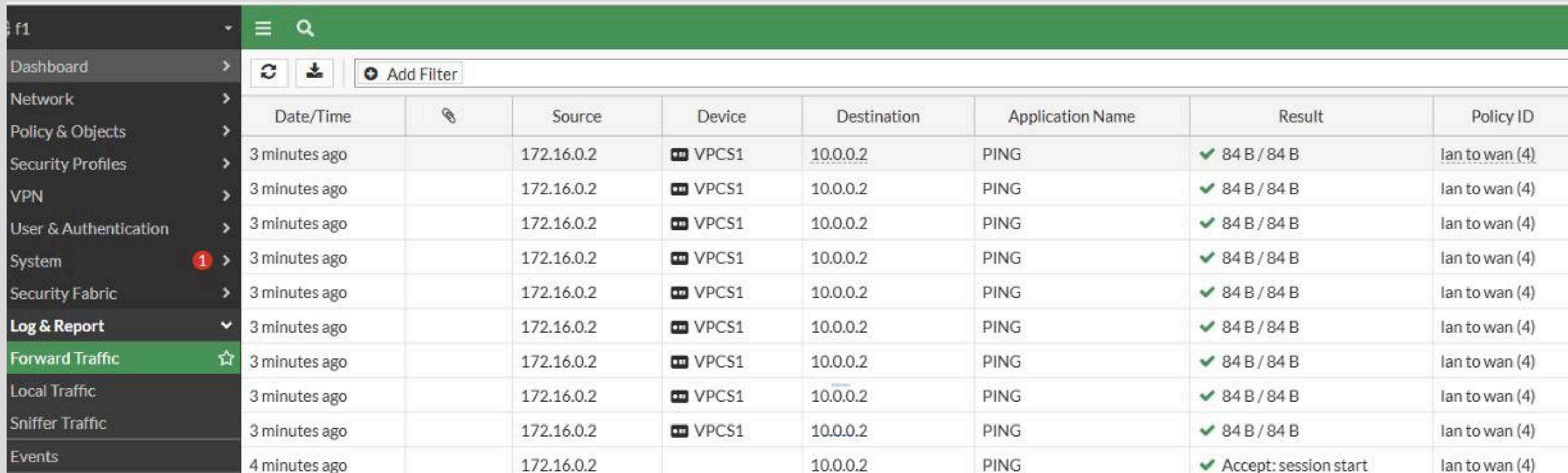
- On each FortiGate, the UP status indicates that:
- The remote peer is reachable.
- Both firewalls agree on all security parameters (encryption, authentication, DH group, etc.).
- The tunnel interface is active and ready to pass traffic.
- Routing and firewall policies are correctly configured to allow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



The screenshot shows a network monitoring interface with a green header bar. The left sidebar contains navigation links: Dashboard, Network, Policy & Objects, Security Profiles, VPN, User & Authentication, System (with a red notification badge), Security Fabric, Log & Report (selected), Forward Traffic (highlighted in green), Local Traffic, Sniffer Traffic, and Events. The main area displays a table of traffic logs. The columns are: Date/Time, Source, Device, Destination, Application Name, Result, and Policy ID. The table shows eight rows of data, all with a timestamp of '3 minutes ago' and a source of '172.16.0.2'. The device column shows 'VPCS1' with a small icon. The destination is '10.0.0.2'. The application name is 'PING'. The result column shows a green checkmark followed by '84 B / 84 B'. The policy ID column shows 'lan to wan (4)' for all rows except the last one, which shows 'Accept: session start'.

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)
4 minutes ago	172.16.0.2		10.0.0.2	PING	✓ Accept: session start	lan to wan (4)

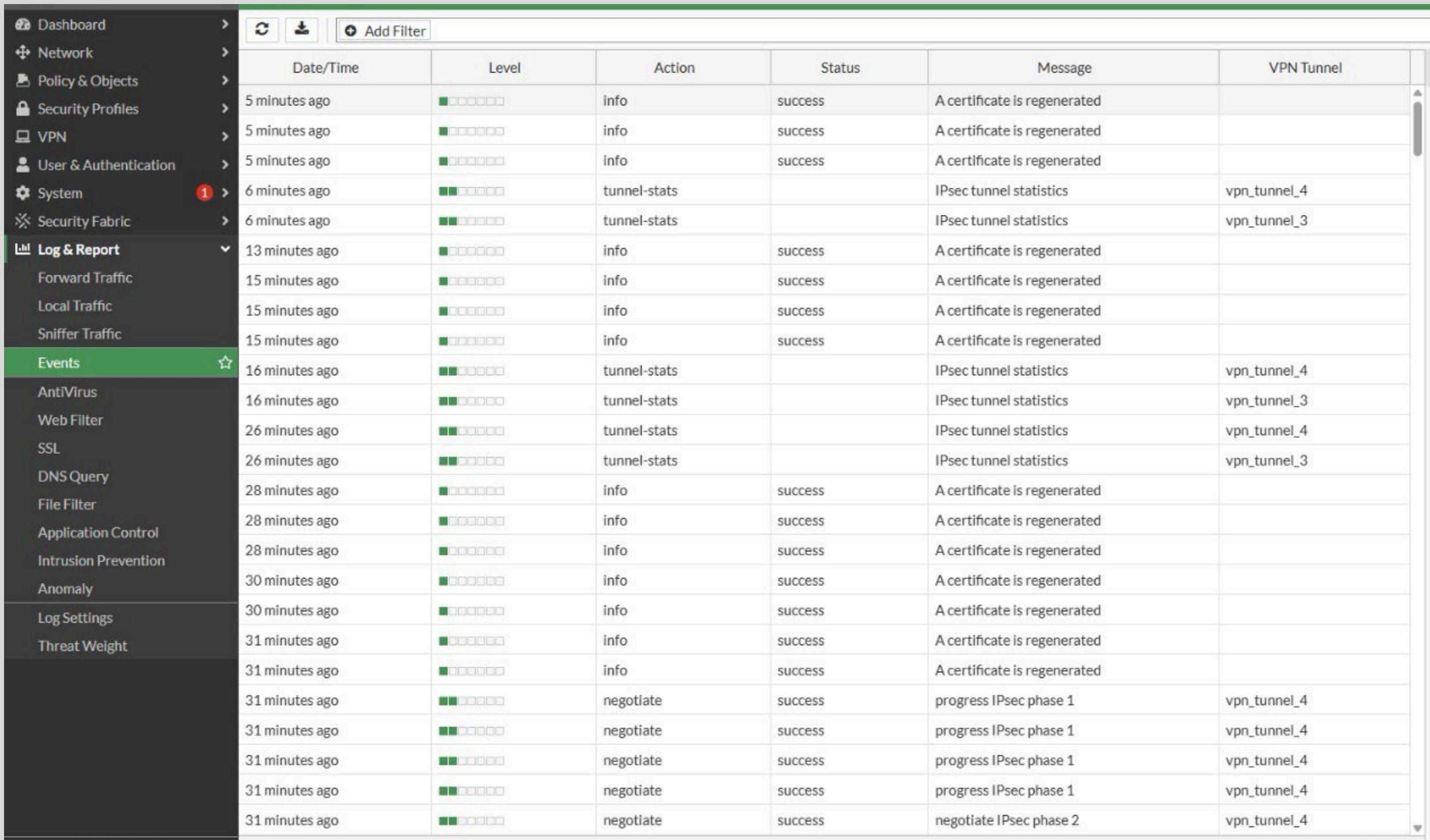
The log confirms successful bidirectional traffic between both sites.

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



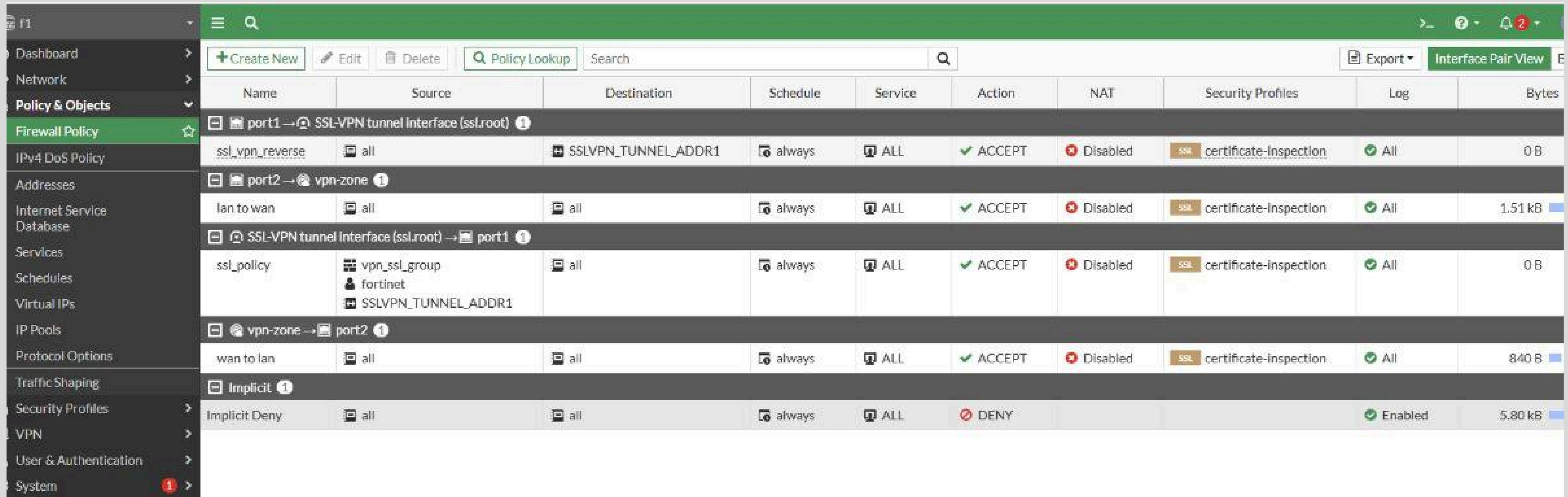
The screenshot shows the FortiGate event log interface. The left sidebar lists various monitoring categories like Dashboard, Network, Policy & Objects, Security Profiles, VPN, User & Authentication, System, Security Fabric, and Log & Report. Under Log & Report, there are sections for Forward Traffic, Local Traffic, Sniffer Traffic, and Events. The Events section is selected and highlighted in green. The main area displays a table of events with columns: Date/Time, Level, Action, Status, Message, and VPN Tunnel. The table contains numerous entries, mostly from the last 30 minutes, related to IPsec tunnel statistics and certificate regeneration, with some entries indicating successful negotiations and others showing progress.

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



The screenshot shows the Firewall Policy Overview page for Firewall 1. The left sidebar contains navigation links for Dashboard, Network, Policy & Objects (selected), Firewall Policy (selected), IPv4 DoS Policy, Addresses, Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, Protocol Options, Traffic Shaping, Security Profiles, VPN, User & Authentication, and System. The main content area displays a table of firewall policies.

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
port1 → SSL-VPN tunnel Interface (ssl.root) ①									
ssl vpn_reverse	all	SSLVPN_TUNNEL_ADDR1	always	ALL	✓ ACCEPT	Disabled	certificate-inspection	All	0 B
port2 → vpn-zone ①									
Ian to wan	all	all	always	ALL	✓ ACCEPT	Disabled	certificate-inspection	All	1.51 kB
SSL-VPN tunnel Interface (ssl.root) → port1 ①									
ssl_policy	vpn_ssl_group fortinet SSLVPN_TUNNEL_ADDR1	all	always	ALL	✓ ACCEPT	Disabled	certificate-inspection	All	0 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			Enabled	5.80 kB

# Firewall 2:

The screenshot shows a firewall configuration interface with a navigation menu on the left and a main table view on the right.

**Navigation Menu:**

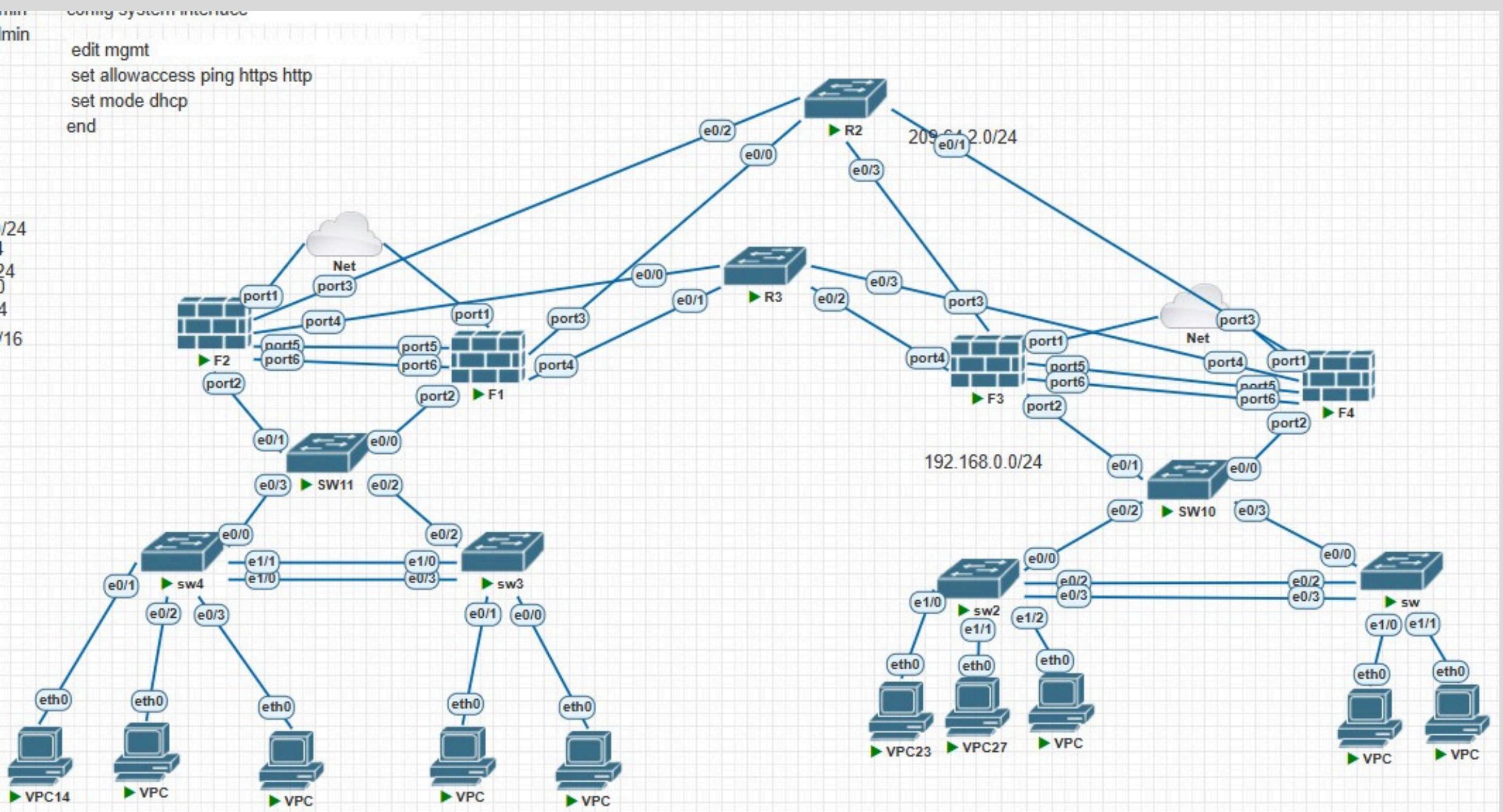
- Dashboard
- Network
- Policy & Objects**
  - Firewall Policy** (selected)
  - IPv4 DoS Policy
  - Addresses
  - Internet Service Database
  - Services
  - Schedules
  - Virtual IPs

**Main View:**

The main view displays three policy entries in a table:

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
port2 → vpn_zone 1	lan to wan	all	all	always	ALL	✓ ACCEPT	✗ Disabled	ssl certificate-inspection	All 168 B
vpn_zone → port2 1	wan to lan	all	all	always	ALL	✓ ACCEPT	✗ Disabled	ssl certificate-inspection	All 840 B
Implicit 1	Implicit Deny	all	all	always	ALL	✗ DENY			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
!
```

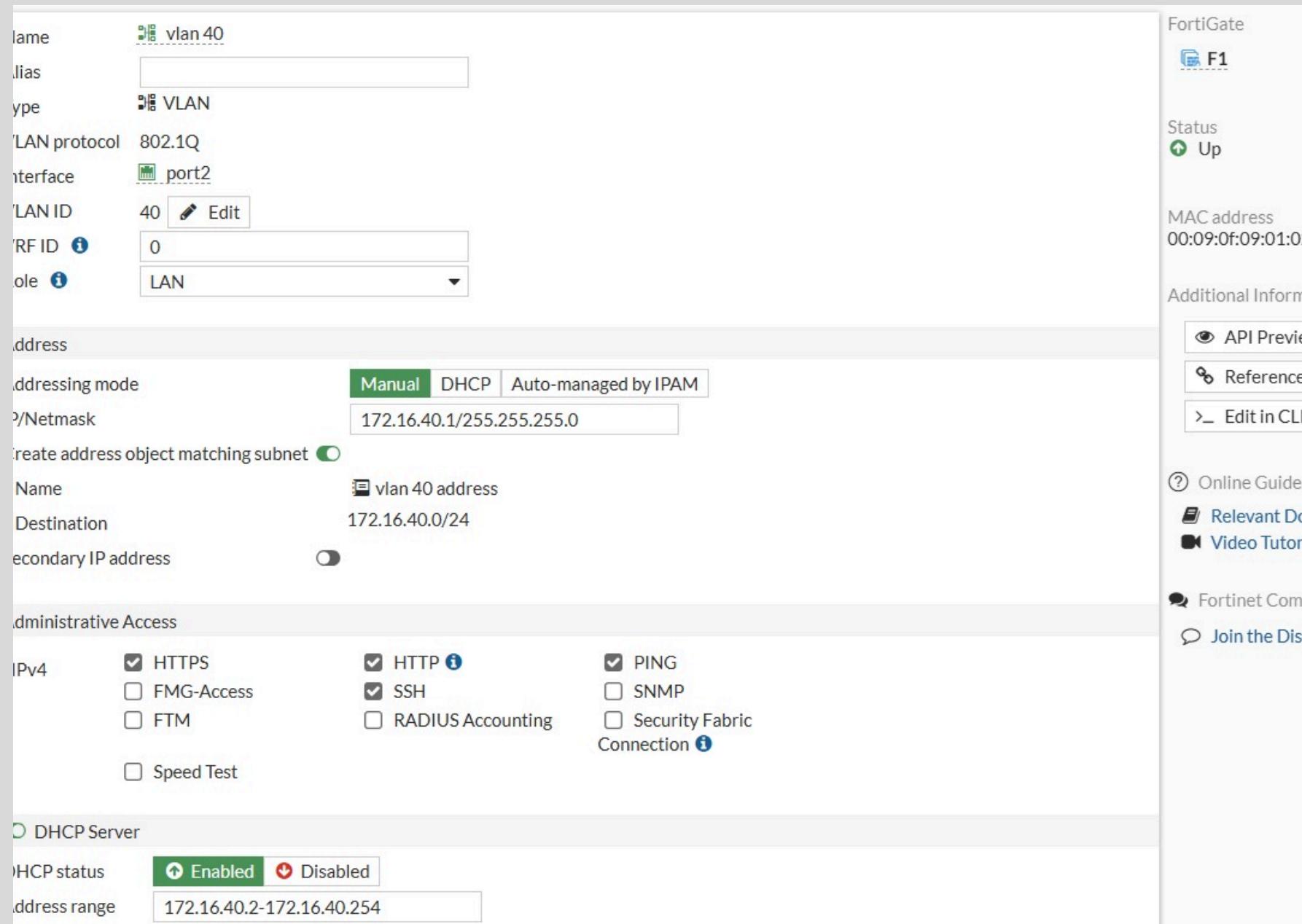
```
!
!
interface Port-channel1
switchport trunk allowed vlan 10,20,30,40,50,60
switchport trunk encapsulation dot1q
switchport trunk native vlan 100
switchport mode trunk
switchport nonegotiate
!
interface Ethernet0/0
```

# Add Vlans on both Fortigate :

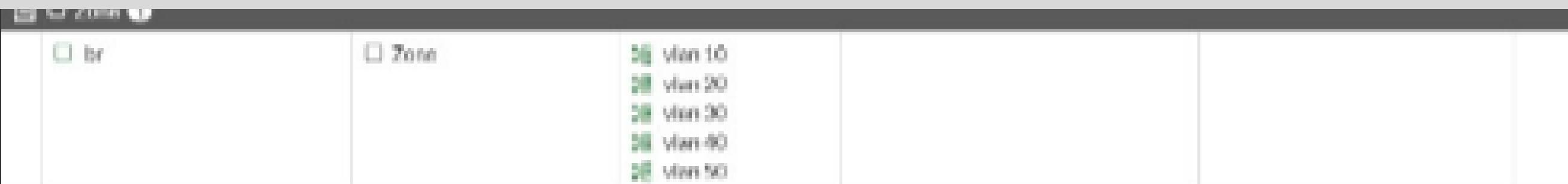
	port2	Physical Interface	0.0.0.0/0.0.0	PING HTTPS SSH			13
•	vlan 10	VLAN	192.168.10.1/255.255.255.0	PING HTTPS SSH	1	192.168.10.2-192.168.10.254	3
•	vlan 20	VLAN	192.168.20.1/255.255.255.0	PING HTTPS SSH	1	192.168.20.2-192.168.20.254	3
•	vlan 30	VLAN	192.168.30.1/255.255.255.0	PING HTTPS SSH		192.168.30.2-192.168.30.254	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 SSH		192.168.50.2-192.168.50.254	3

	port2	Physical Interface	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 SSH		172.16.50.2-172.16.50.254	3

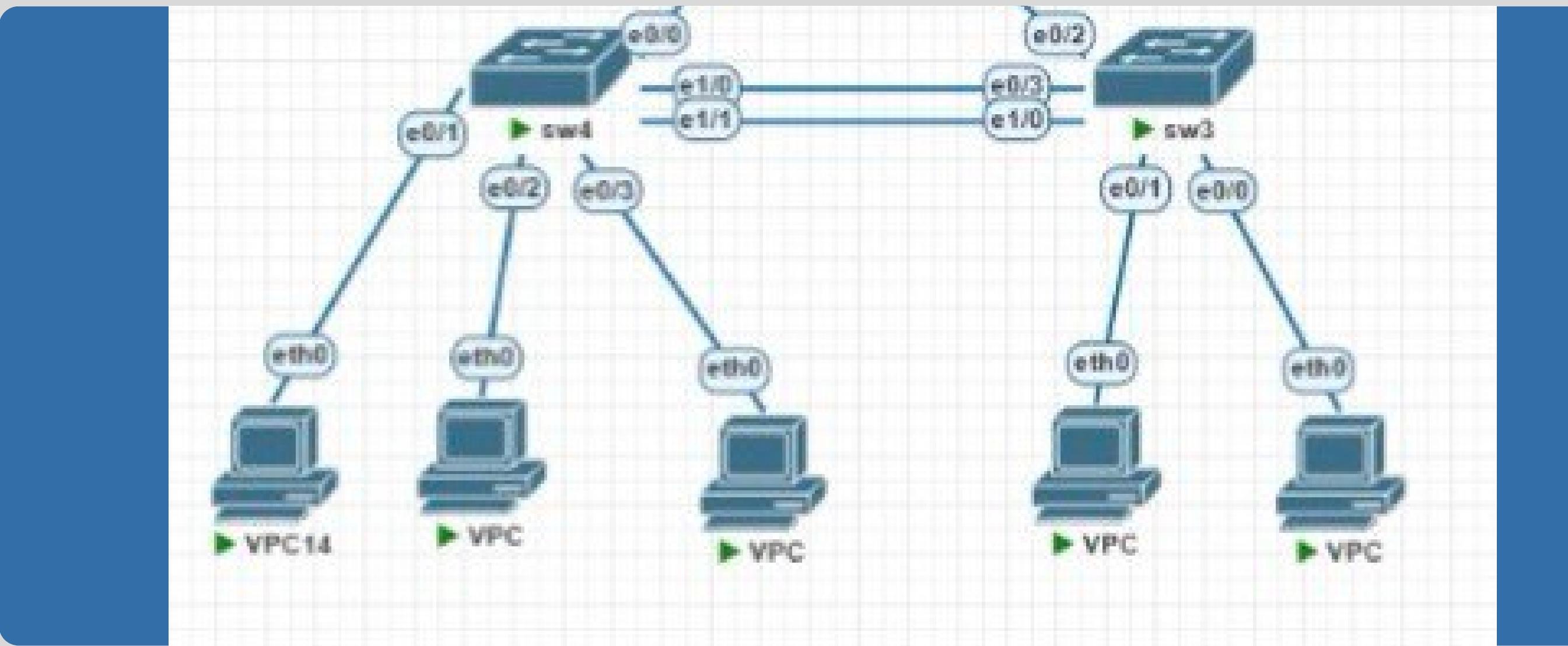
# Enable Dhcp & creating vlans :



# 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 :

HA: Primary

**High Availability**

Mode: Active-Passive

Device priority: 200

**Cluster Settings**

Group name: br

Password: \*\*\*\*\* [Change](#)

Session pickup:

Monitor Interfaces: port1, port2, port3, port4

Heartbeat interfaces: port5, port6

**Heartbeat Interface Priority**

port5: 50

port6: 50

Management Interface Reservation

Unicast Heartbeat

**Additional Information**

[API Preview](#)

[Edit in CLI](#)

**High Availability**

[Identifying the HA Cluster and Cluster Units](#)

[FGSP \(Session-Sync\) Peer Setup](#)

[Troubleshoot an HA Formation](#)

[Check HA Sync Status](#)

**Cluster Setup**

[HA Active-Passive Cluster Setup](#)

[HA Active-Active Cluster Setup](#)

[HA Virtual Cluster Setup](#)

**Documentation**

[Online Help](#)

[Video Tutorials](#)

Status	Priority	Hostname	Serial No.	Role	System Uptime	Sessions	Throughput
<span style="color: green;">✓</span> Synchronized	200	f4	FGVMEV-BZEEWI0B	Primary	9h 17m	27 <div style="width: 76.00%; background-color: #0070C0;"></div>	76.00 kbps
<span style="color: green;">✓</span> Synchronized	100	f3	FGVMEVUYD105_612	Secondary	9h 17m	1 <div style="width: 4.00%; background-color: #0070C0;"></div>	42.00 kbps

Status	Priority	Hostname	Serial No.	Role	System Uptime	Sessions	Throughput
<span style="color: green;">✓</span> Synchronized	200	F1	FGVMEVNTCORGLDBE	Primary	1h 23m	14 <div style="width: 39.00%; background-color: #0070C0;"></div>	39.00 kbps
<span style="color: green;">✓</span> Synchronized	100	f2	FGVMEV1A7X7BSU14	Secondary	1h 22m	0	38.00 kbps

# Add Firewall Policies

## Firewall Policies Overview:

The screenshot shows a network configuration interface with a sidebar and a main content area. The sidebar contains navigation links for Dashboard, Network, Policy & Objects, Firewall Policy (selected), Local In Policy, IPv4 DoS Policy, Proxy Policy, Authentication Rules, Addresses, Internet Service, Database, Services, Schedules, Virtual IPs, and IP Pools. The main content area displays a table of Firewall Policies with the following columns: Name, From, To, Source, Destination, Schedule, Service, Action, NAT, Security Profiles, Log, and a blank column. The table lists ten policies, including 'lan\_vpn', 'wan\_vpn', 'ssl vpn access', 'mgmt to all', 'hr to hr', 'it to it', 'fin to fin', 'sales to sales', and 'Implicit Deny'. Most policies have 'ACCEPT' as the action and are set to 'Enabled'. The 'Implicit Deny' policy has 'DENY' as the action and is set to 'Disabled'.

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	
lan_vpn	port2	vpn---	f3 to f1_local	f3 to f1_remote	always	ALL	✓ ACCEPT	✗ Disabled	ssl certificate-inspection	All	
wan_vpn	vpn---	port2	f3 to f1_remote	f3 to f1_local	always	ALL	✓ ACCEPT	✗ Disabled	ssl certificate-inspection	All	
ssl vpn access	SSL-VPN tunnel interface (ssl.root)	port1	ssl_group SSLVPN_TUNNEL_ADDR1	all	always	ALL	✓ ACCEPT	✓ Enabled	AV default WEB default ssl certificate-inspection	All	
mgmt to all	port2	vpn---	vlan 10 address	f3 to f1_remote	always	ALL	✓ ACCEPT	✗ Disabled	ssl certificate-inspection	All	
hr to hr	port2	vpn---	vlan 20 address	f3 to f1_local_subnet_2	always	ALL	✓ ACCEPT	✗ Disabled	ssl certificate-inspection	All	
it to it	port2	vpn---	vlan 30 address	f3 to f1_remote_subnet_3	always	ALL	✓ ACCEPT	✗ Disabled	ssl certificate-inspection	All	
fin to fin	port2	vpn---	vlan 40 address	f3 to f1_remote_subnet_4	always	ALL	✓ ACCEPT	✗ Disabled	ssl certificate-inspection	All	
sales to sales	port2	vpn---	vlan 50 address	f3 to f1_remote_subnet_5	always	ALL	✓ ACCEPT	✗ Disabled	ssl certificate-inspection	All	
Implicit Deny	any	any	all	all	always	ALL	✗ DENY			✗ Disabled	

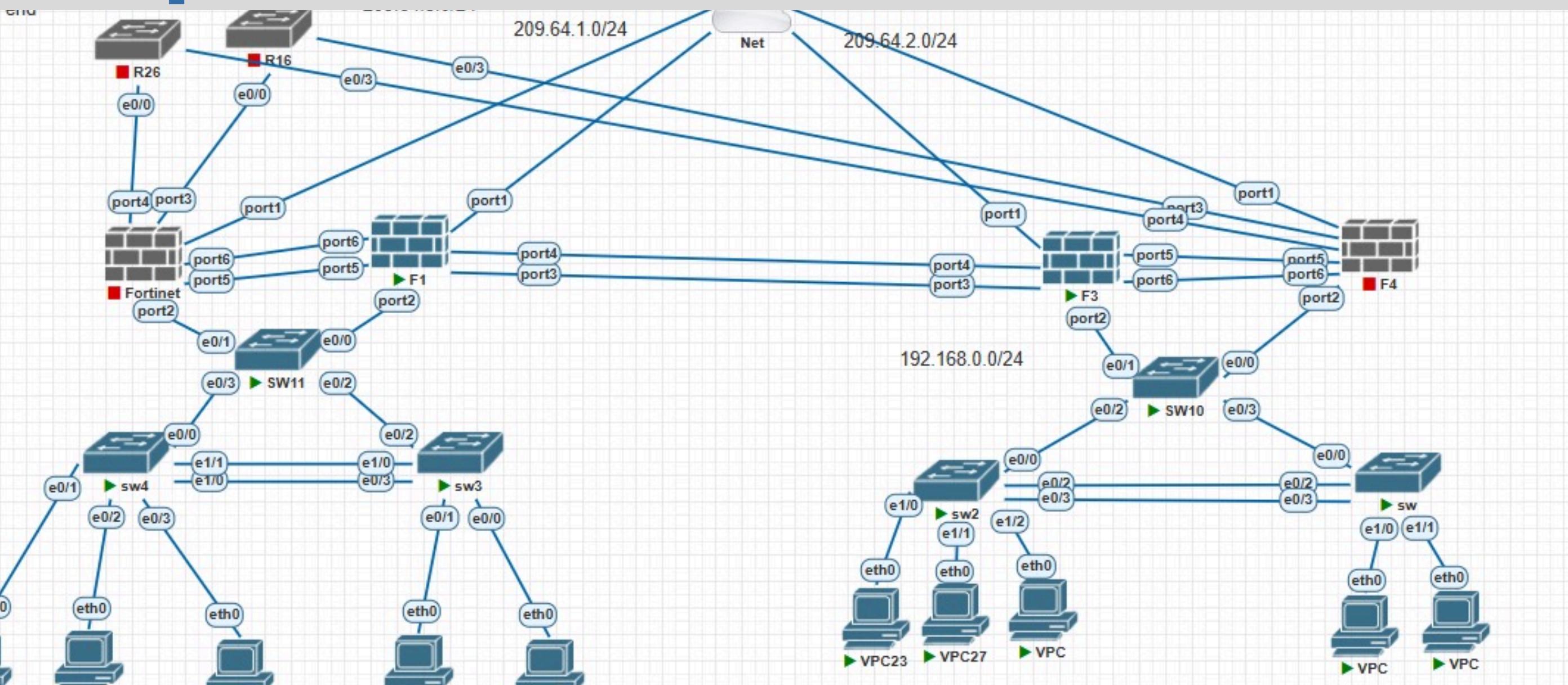
# **ssl VPN & IPsec VPN & SD-WAn:**

**same like new Topology**

**BUT .....**

**there is a problem ?**

# Update :



Networks are

209.64.3.0/24 & 209.64.1.0/24

only

F3			
Dashboard			
Network			
Policy & Objects			
Security Profiles			
VPN			
Overlay Controller VPN			
<a href="#">+ Create New</a> <a href="#">Edit</a> <a href="#">Delete</a> <input type="text"/> Search			
Tunnel			
Interface Binding			
Status			
<b>Custom ②</b>			
vpn	port4	Up	2
vpn_tunnel_3	port3	Up	2

**Thank you**