Digital Egypt Pioneers Initiative (DEPI)

Final Project: Implementing VPN Solutions with FortiGate

R3_DEPI3_CAI3_ISS8_S2 Fortinet Cybersecurity Engineer

Team Members:
Mohamed Hany Samir
Seif Goda Adel
Ahmed Mohamed Mostafa
Amr khaled Mohamed
Abdallah Ahmed Dighedy

Same style as HQ

7. IPsec VPN Configuration

- Phase 1
- Phase 2
- Policies
- Routing

8. SSL-VPN Configuration

- Portal
- Authentication
- IP pool
- Routing policies

9. SD-WAN Simulation (Static Failover)

- WAN1
- WAN2
- Failover logic

10. Conclusion

- What was achieved
- Key takeaways

1. Introduction

This project focuses on designing, configuring, and testing a complete multi-site enterprise network using FortiGate firewalls and Cisco routers within a simulated GNS3 environment. The primary objective is to implement secure inter-site communication between the Headquarters (HQ) and Branch Office (BR), provide secure remote access for external users via SSL-VPN, and simulate WAN redundancy through dual-ISP connectivity.

The project integrates several key technologies:

- **LAN segmentation** at HQ and Branch
- **IPsec Site-to-Site VPN** between HQ and BR
- **SSL-VPN remote access** for mobile/remote users
- **Static SD-WAN simulation** using dual WAN links (R3 and R4)
- **Routing using static routes**
- **Cisco router connectivity** to emulate WAN and ISP environments

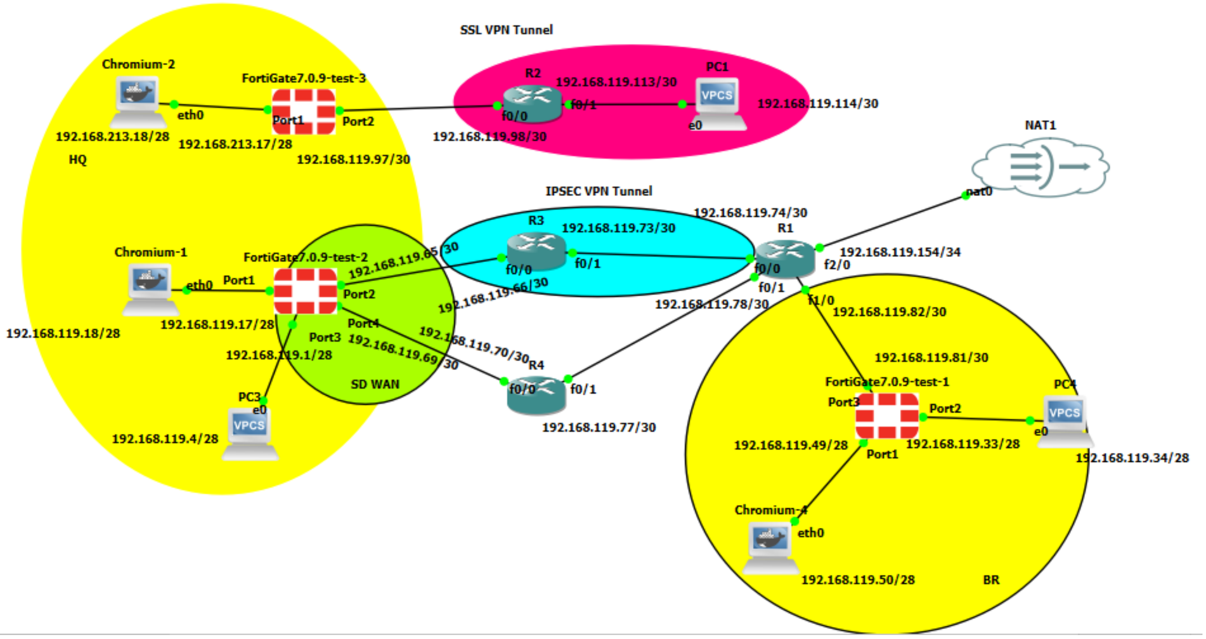
By the end of the project, the network must support:

- Secure and stable communication between HQ and BR networks
- Remote user VPN access with controlled permissions
- Redundant WAN paths with automatic failover
- Full routing and reachability across the topology

This report documents the complete network design, configuration steps, testing process, and final results.

2. Network Topology Overview

The project network topology simulates a realistic enterprise environment consisting of three main security domains: the Headquarters (HQ), the Branch Office (BR), and a remote user environment connected through SSL-VPN. The topology also includes multiple Cisco routers to represent WAN segments, ISP paths, and routing between security devices.



2.1 Headquarters (HQ)

The HQ site contains:

- A **FortiGate firewall (HQ-FG)** acting as the primary security gateway
- An internal **HQ LAN network (192.168.119.0/28)**
- Two WAN connections connected to:
  - **R1** (WAN1 – primary path)
  - **R2** (WAN2 – backup path)

The HQ FortiGate manages LAN user access, provides security policies, and forms one side of the site-to-site IPsec VPN tunnel with the Branch.

2.2 Branch Office (BR)

The BR site includes:

- A **FortiGate firewall (BR-FG)** for local security
- An internal **BR LAN network (192.168.119.32/28)**
- A WAN connection through **R1**, which links back to the HQ via routers R3 and R4

The BR FortiGate establishes the second side of the IPsec VPN tunnel and routes traffic back to HQ securely.

2.3 Remote User Environment (SSL-VPN)

To simulate remote-access VPN users, the topology includes:

- A **dedicated SSL-VPN FortiGate (SSL-FG)**
- A WAN connection through **R2**
- A Remote User PC connected behind R2

The SSL-FG provides secure user authentication, tunnel-mode VPN, and controlled access to HQ and BR resources.

2.4 WAN and ISP Simulation (Routers)

Several Cisco routers emulate Internet and WAN paths:

Router	Role
R3	Primary WAN path from HQ
R4	Secondary WAN path (failover)
R1	WAN router for BR site
R2	WAN router for remote user / SSL VPN
R1	Upstream ISP/NAT/Gateway device

2.5 IPsec VPN Tunnel

An IPsec Site-to-Site VPN tunnel is established between HQ-FG and BR-FG to provide encrypted, secure communication between both LANs. This tunnel ensures confidentiality and integrity of data traveling over the emulated WAN.

2.6 SD-WAN Failover Simulation

While not full SD-WAN, the project uses:

- **Dual static default routes**
- **Different priorities**
- **Primary route via R3**
- **Failover route via R4**

This simulates WAN redundancy: if R3 fails, the HQ-FG automatically shifts traffic to R4.

3. IP Addressing Scheme

A structured and consistent IP addressing plan was implemented to support inter-site communication, WAN routing, VPN connectivity, and remote user access. The addressing scheme uses multiple subnet sizes (/28 and /30) to separate management, LAN, and WAN segments. This ensures proper route segmentation, simplified troubleshooting, and secure traffic flow across all parts of the network.

3.1 Headquarters (HQ) Networks

Network Purpose	Subnet	Mask	Gateway	Device
HQ LAN	**192.168.119.0/28**	255.255.255.240	192.168.119.1	HQ-FG port3
HQ MGMT	**192.168.119.16/28**	255.255.255.240	—	HQ-FG port1 (192.168.119.17)
HQ WAN1 (to R3)	**192.168.119.64/30**	255.255.255.252	192.168.119.66	HQ-FG port2 (192.168.119.65)
HQ WAN2 (to R4)	**192.168.119.68/30**	255.255.255.252	192.168.119.70	HQ-FG port4 (192.168.119.69)

3.2 Branch Office (BR) Networks

Network Purpose	Subnet	Mask	Gateway	Device
BR LAN	**192.168.119.32/28**	255.255.255.240	192.168.119.33	BR-FG port2
BR MGMT	**192.168.119.48/28**	255.255.255.240	—	BR-FG port1 (192.168.119.49)
BR WAN (to R1)	**192.168.119.80/30**	255.255.255.252	192.168.119.82	BR-FG port3 (192.168.119.81)

3.3 SSL-VPN Gateway Network

Network Purpose	Subnet	Mask	Gateway	Device
SSL-FG MGMT	**192.168.119.16/28**	255.255.255.240	—	SSL-FG port1 (192.168.119.19)
SSL-FG WAN (to R2)	**192.168.119.96/30**	255.255.255.252	192.168.119.98	SSL-FG port2 (192.168.119.97)
SSL-VPN Client Pool	**(To be configured)**	—	—	Assigned during VPN

3.4 End Hosts

Location	IP	Mask	Gateway
HQ PC	**192.168.119.4**	255.255.255.240	192.168.119.1
BR PC	**192.168.119.34**	255.255.255.240	192.168.119.33
Remote User PC	**192.168.119.114** (behind R2)	255.255.255.252	192.168.119.113

3.5 WAN Routers

Router	FG Peer Network	Router IP	FortiGate IP
R3 → HQ WAN1	192.168.119.64/30	192.168.119.66	192.168.119.65
R4 → HQ WAN2	192.168.119.68/30	192.168.119.70	192.168.119.69
R1 → BR WAN	192.168.119.80/30	192.168.119.82	192.168.119.81
R2 → SSL-FG WAN	192.168.119.96/30	192.168.119.98	192.168.119.97

4. Device Roles

The network topology consists of multiple FortiGate firewalls, Cisco routers, and end-user hosts. Each device plays an essential role in providing security, routing, VPN connectivity, and WAN failover. This section describes the function of each device and how it contributes to the overall network design.

4.1 Headquarters FortiGate (HQ-FG)

The HQ FortiGate acts as the main security appliance for the Headquarters site. Its responsibilities include:

- Securing the **HQ LAN network (192.168.119.0/28)**
- Acting as the **HQ endpoint of the IPsec Site-to-Site VPN**
- Handling **traffic routing** toward the WAN routers R3 and R4
- Providing **dual-WAN default routes** for failover (simulated SD-WAN)
- Applying **firewall policies** between LAN, WAN, and VPN interfaces

Its two WAN interfaces (port2 and port4) connect to R3 and R4, allowing the firewall to switch between primary and secondary WAN links in case of failure.

4.2 Branch Office FortiGate (BR-FG)

The BR FortiGate provides security and routing for the branch office. Its key responsibilities are:

- Protecting the **BR LAN network (192.168.119.32/28)**
- Acting as the **Branch endpoint of the IPsec VPN tunnel** to HQ
- Routing traffic to the WAN router **R1**
- Enforcing firewall rules for local branch users

The BR-FG forms the second half of the IPsec VPN tunnel, enabling secure communication with the HQ network.

4.3 SSL-VPN FortiGate (SSL-FG)

The SSL-VPN FortiGate is designed specifically to serve **remote-access VPN users**. In this topology:

- It operates independently from HQ and BR firewalls

- It connects to the WAN via **R2**
- It provides **SSL-VPN portal and tunnel mode access**
- It authenticates remote users and assigns them IP addresses via a defined pool
- It enforces access control to HQ and BR resources

Remote users connect through this firewall to securely reach internal networks.

4.4 Cisco Routers (WAN/ISP Simulation)

Several Cisco routers simulate the wide-area network and ISP paths:

R1 — Branch WAN Router— ISP/NAT Router

- Connects BR-FG to the WAN
- Forwards traffic between BR and HQ
- Simulates the Internet environment
- Receives traffic from R3 and R4
- Acts as a (fake) upstream gateway for external pings and testing

```
!========================
! R1 CONFIG (CORE ROUTER)
!========================
hostname R1
no ip domain-lookup
ip cef

interface FastEthernet0/0
 description R1 <-> R3
 ip address 192.168.119.74 255.255.255.252
 ip ospf 1 area 0
 no shutdown
```

```
interface FastEthernet0/1

 description R1 <-> R4

 ip address 192.168.119.78 255.255.255.252

 ip ospf 1 area 0

 no shutdown


interface FastEthernet1/0

 description R1 <-> BR-FG port3

 ip address 192.168.119.82 255.255.255.252

 ip ospf 1 area 0

 no shutdown


interface FastEthernet1/1

 no ip address

 shutdown


interface FastEthernet2/0

 description R1 <-> INTERNET / CLOUD

 ip address 192.168.119.145 255.255.255.252

 no shutdown


router ospf 1

 router-id 3.3.3.3

 network 192.168.119.72 0.0.0.3 area 0

 network 192.168.119.76 0.0.0.3 area 0

 network 192.168.119.80 0.0.0.3 area 0
```

```
! Default route to "internet"

ip route 0.0.0.0 0.0.0.0 192.168.119.146


! HQ LAN (192.168.119.0/28) via R3 and R4

ip route 192.168.119.0 255.255.255.240 192.168.119.73

ip route 192.168.119.0 255.255.255.240 192.168.119.77


! BR LAN (192.168.119.32/28) via BR-FG

ip route 192.168.119.32 255.255.255.240 192.168.119.81


line con 0

 logging synchronous

line vty 0 4

 login

 transport input none

end
```

R2 — Remote User WAN Router

- Provides WAN connectivity to the SSL-VPN FortiGate
- Hosts the Remote User PC behind it

```
!========================

! R2 CONFIG

!========================

hostname R2

no ip domain-lookup

ip cef
```

```
interface FastEthernet0/0
 description R2 <-> SSL-FG port2
 ip address 192.168.119.98 255.255.255.252
 no shutdown

interface FastEthernet0/1
 description R2 <-> Remote_User
 ip address 192.168.119.113 255.255.255.252
 no shutdown

interface FastEthernet1/0
 no ip address
 shutdown
interface FastEthernet1/1
 no ip address
 shutdown
interface FastEthernet2/0
 no ip address
 shutdown

! Default route towards SSL VPN firewall
ip route 0.0.0.0 0.0.0.0 192.168.119.97

line con 0
 logging synchronous
```

```
line vty 0 4
 login
 transport input none
end
```

R3 — Primary HQ WAN Router

- Connects HQ-FG to the upstream network
- Serves as the **primary default route**
- Used during normal operations

```
!========================
! R3 CONFIG
!========================
hostname R3
no ip domain-lookup
ip cef

interface FastEthernet0/0
 description R3 <-> HQ-FG port2
 ip address 192.168.119.66 255.255.255.252
 ip ospf 1 area 0
 no shutdown

interface FastEthernet0/1
 description R3 <-> R1
 ip address 192.168.119.73 255.255.255.252
 ip ospf 1 area 0
 no shutdown
```

```
interface FastEthernet1/0
 no ip address
 shutdown
interface FastEthernet1/1
 no ip address
 shutdown
interface FastEthernet2/0
 no ip address
 shutdown

router ospf 1
 router-id 10.10.10.10
 network 192.168.119.64 0.0.0.3 area 0
 network 192.168.119.72 0.0.0.3 area 0

! Default route towards core (R1)
ip route 0.0.0.0 0.0.0.0 192.168.119.74

! Route to HQ LAN via HQ-FG WAN (port2)
ip route 192.168.119.0 255.255.255.240 192.168.119.65

! Route to BR LAN via R1
ip route 192.168.119.32 255.255.255.240 192.168.119.74

line con 0
```

```
 logging synchronous
line vty 0 4
 login
 transport input none
end
```

R4 — Secondary HQ WAN Router

- Backup WAN path for HQ
- Used for **SD-WAN failover** when R3 fails

Together, these routers form a multi-hop emulated WAN that allows realistic testing of failover, routing, and VPN traffic flow.

```
!========================
! R4 CONFIG
!========================
hostname R4
no ip domain-lookup
ip cef

interface FastEthernet0/0
 description R4 <-> HQ-FG port4
 ip address 192.168.119.70 255.255.255.252
 ip ospf 1 area 0
 no shutdown

interface FastEthernet0/1
 description R4 <-> R1
 ip address 192.168.119.77 255.255.255.252
 ip ospf 1 area 0

 no shutdown


interface FastEthernet1/0

 no ip address

 shutdown

interface FastEthernet1/1

 no ip address

 shutdown

interface FastEthernet2/0

 no ip address

 shutdown


router ospf 1

 router-id 11.11.11.11

 network 192.168.119.68 0.0.0.3 area 0

 network 192.168.119.76 0.0.0.3 area 0


! Default route towards core (R1)

ip route 0.0.0.0 0.0.0.0 192.168.119.78


! Route to HQ LAN via HQ-FG WAN (port4)

ip route 192.168.119.0 255.255.255.240 192.168.119.69


! Route to BR LAN via R1

ip route 192.168.119.32 255.255.255.240 192.168.119.78
```

```
line con 0
 logging synchronous
line vty 0 4
 login
 transport input none
end
```

4.5 End-User PCs

HQ-PC

- Located inside HQ LAN
- Used to test internal access and reachability via the IPsec tunnel

BR-PC

- Located inside BR LAN
- Used to verify communication with HQ and remote VPN users

Remote User PC

- Placed behind R2
- Used to test SSL-VPN connectivity, authentication, and access to internal networks

5. Headquarters FortiGate (HQ-FG) Configuration

This section documents all configurations applied to the HQ FortiGate firewall, including interface settings, static routing, WAN failover logic, firewall policies, and IPsec VPN configuration. The HQ-FG serves as the primary security gateway for the headquarters LAN and is responsible for establishing the IPsec tunnel to the Branch FortiGate.

5.1 Interface Configuration

The HQ-FG uses four interfaces:

Interface	Role	IP Address	Subnet	Description
port1	Management	192.168.119.17	/28	HQ management access
port3	HQ LAN	192.168.119.1	/28	Internal HQ network
port2	WAN1 (Primary)	192.168.119.65	/30	Connected to R3
port4	WAN2 (Backup)	192.168.119.69	/30	Connected to R4

Configuration:

```
config system interface
  edit "port1"
    set ip 192.168.119.17 255.255.255.240
    set allowaccess https ping
    set alias "HQ_MGMT"
  next
  edit "port3"
    set ip 192.168.119.1 255.255.255.240
    set allowaccess ping
    set alias "HQ_LAN"
  next
  edit "port2"
    set ip 192.168.119.65 255.255.255.252
    set allowaccess ping
    set alias "HQ_WAN1_R3"
  next
  edit "port4"
    set ip 192.168.119.69 255.255.255.252
    set allowaccess ping
    set alias "HQ_WAN2_R4"
  next
end
```

5.2 Static Routing (Dual WAN Failover)

The HQ-FG uses two default routes:

- **Primary default route → R3 via port2**
- **Secondary backup route → R4 via port4**

This simulates SD-WAN failover using route priority.

Configuration:

```
config router static
  edit 1
    set dst 0.0.0.0 0.0.0.0
    set gateway 192.168.119.66
    set device "port2"
    set priority 10
  next
  edit 2
    set dst 0.0.0.0 0.0.0.0
    set gateway 192.168.119.70
    set device "port4"
    set priority 20
  next
end
```

Result:

- The firewall uses **WAN1 (port2)** as long as R3 is reachable.

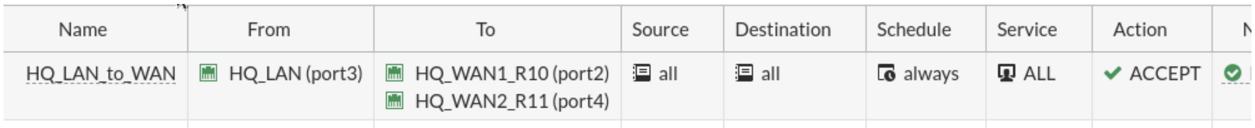
- If WAN1 fails, the FortiGate automatically switches to **WAN2 (port4)**.

5.3 Firewall Policies

5.3.1 HQ LAN → WAN

Allows internal users to reach external networks and the IPsec tunnel.

```
config firewall policy
  edit 1
    set name "HQ_LAN_to_WAN"
    set srcintf "port3"
    set dstintf "port2" "port4"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set service "ALL"
  next
end
```

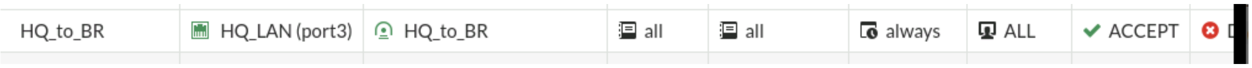


Name	From	To	Source	Destination	Schedule	Service	Action	N
HQ_LAN_to_WAN	HQ_LAN (port3)	HQ_WAN1_R10 (port2) HQ_WAN2_R11 (port4)	all	all	always	ALL	✓ ACCEPT	✓

5.4 IPsec VPN Configuration (HQ Side)

5.4.1 Phase 1 – HQ_to_BR

```
config vpn ipsec phase1-interface
  edit "HQ_to_BR"
    set interface "port2"
    set peertype any
    set remote-gw 192.168.119.82
    set proposal aes256-sha1
    set dhgrp 14
    set keylife 28800
    set psksecret "YOUR_PSK"
  next
end
```



HQ_to_BR	HQ_LAN (port3)	HQ_to_BR	all	all	always	ALL	✓ ACCEPT	✖ D

5.4.2 Phase 2 – HQ_to_BR

```
config vpn ipsec phase2-interface
  edit "HQ_to_BR"
    set phase1name "HQ_to_BR"
    set proposal aes256-sha1
    set dhgrp 14
    set keylife 1800
    set src-subnet 192.168.119.0 255.255.255.240
    set dst-subnet 192.168.119.32 255.255.255.240
  next
end
```

5.5 IPsec Firewall Policies

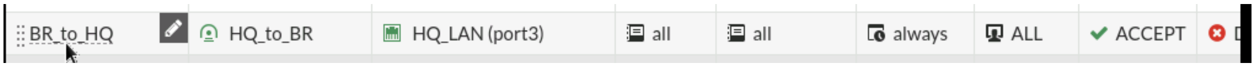
HQ LAN → BR LAN via IPsec

```
config firewall policy
  edit 2
    set name "HQ_to_BR_IPsec"
    set srcintf "port3"
    set dstintf "HQ_to_BR"
```

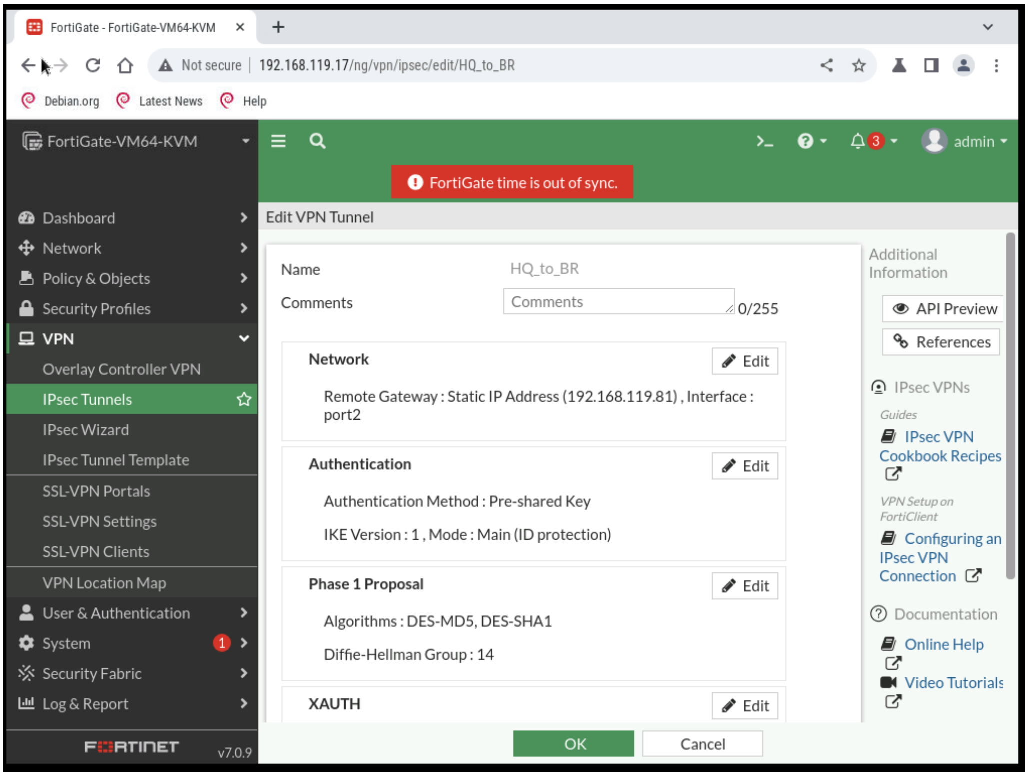
```
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set service "ALL"
    next
end
```

BR LAN → HQ LAN via IPsec

```
config firewall policy
  edit 3
    set name "BR_to_HQ_IPsec"
    set srcintf "HQ_to_BR"
    set dstintf "port3"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set service "ALL"
  next
end
```



BR_to_HQ | HQ_to_BR | HQ_LAN (port3) | all | all | always | ALL | ✓ ACCEPT



Edit VPN Tunnel

Name: HQ_to_BR

Comments: Comments 0/255

Network Edit

Remote Gateway : Static IP Address (192.168.119.81) , Interface : port2

Authentication Edit

Authentication Method : Pre-shared Key

IKE Version : 1 , Mode : Main (ID protection)

Phase 1 Proposal Edit

Algorithms : DES-MD5, DES-SHA1

Diffie-Hellman Group : 14

XAUTH Edit

5.6 Summary

The HQ FortiGate is fully configured for:

- LAN connectivity
- Dual WAN routing with failover
- IPsec VPN termination
- LAN-to-LAN security policies
- Upstream connectivity through R3 and R4

This forms the headquarters core of the project’s secure communication infrastructure.

6. Branch FortiGate (BR-FG) Configuration

The Branch FortiGate firewall provides security and routing for the branch office LAN and forms the remote endpoint of the IPsec Site-to-Site VPN with headquarters. This section documents the full configuration applied to BR-FG, including all interfaces, routing, firewall policies, and IPsec settings.

6.1 Interface Configuration

The BR-FG uses three interfaces in this topology:

Interface	Role	IP Address	Subnet	Description
port1	BR Management	192.168.119.49	/28	Management access
port2	BR LAN	192.168.119.33	/28	Internal branch network
port3	BR WAN (R1)	192.168.119.81	/30	WAN link to R1

Configuration:

```
config system interface
  edit "port1"
    set ip 192.168.119.49 255.255.255.240
    set allowaccess https ping
    set alias "BR_MGMT"
  next
  edit "port2"
    set ip 192.168.119.33 255.255.255.240
    set allowaccess ping
    set alias "BR_LAN"
  next
  edit "port3"
    set ip 192.168.119.81 255.255.255.252
    set allowaccess ping
    set alias "BR_WAN_R1"
  next
end
```

6.2 Static Routing

The BR site has only one WAN connection through R1. Therefore, the branch uses a single default route pointing to R1.

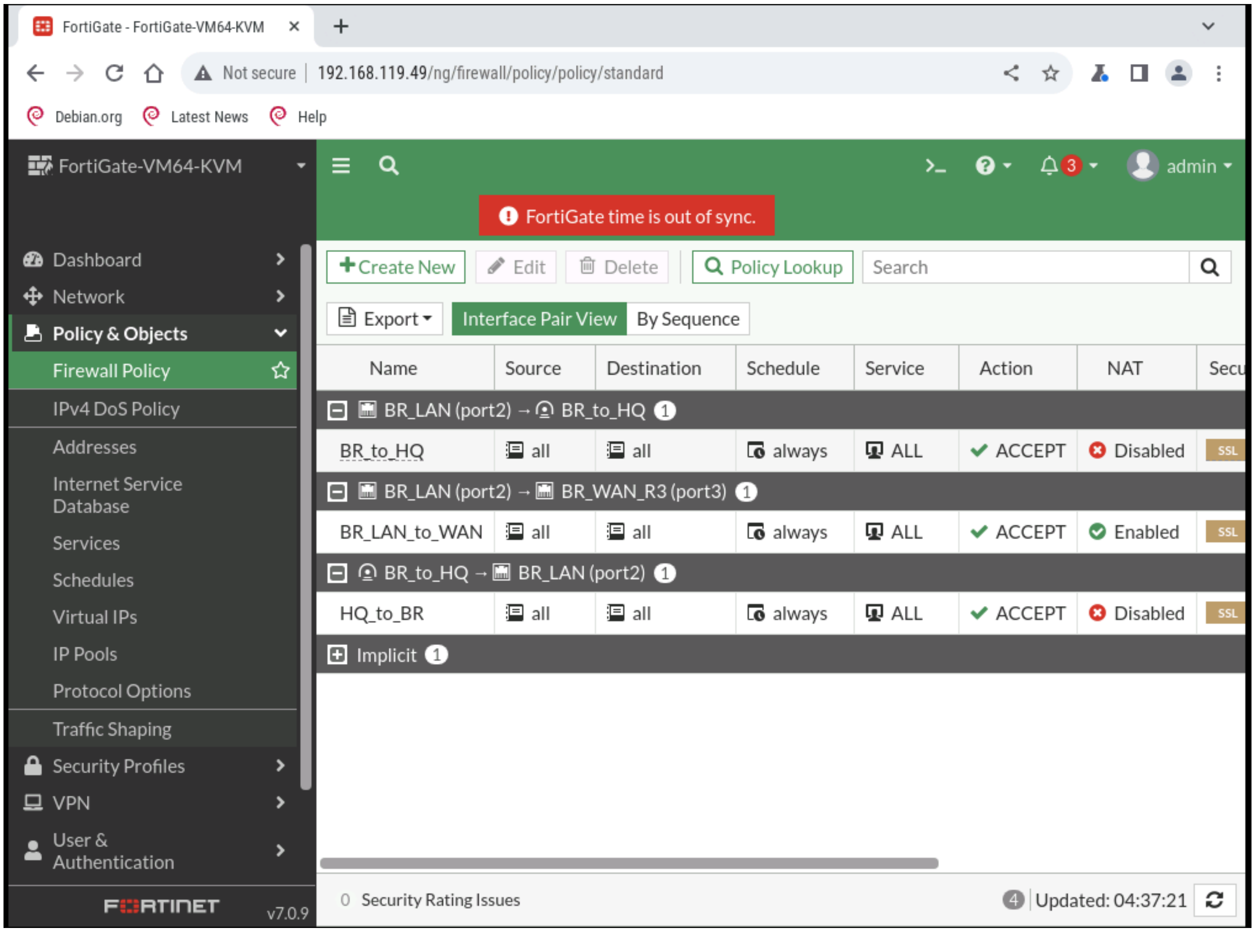
Configuration:

```
config router static
  edit 1
    set dst 0.0.0.0 0.0.0.0
    set gateway 192.168.119.82
    set device "port3"
  next
end
```

Gateway: 192.168.119.82 (R1)

6.3 Firewall Policies

Two security policies are required at the branch:



FortiGate time is out of sync.

Name	Source	Destination	Schedule	Service	Action	NAT	Secu
⊟ BR_LAN (port2) → BR_to_HQ 1							
BR_to_HQ	all	all	always	ALL	✓ ACCEPT	✖ Disabled	SSL
⊟ BR_LAN (port2) → BR_WAN_R3 (port3) 1							
BR_LAN_to_WAN	all	all	always	ALL	✓ ACCEPT	✓ Enabled	SSL
⊟ BR_to_HQ → BR_LAN (port2) 1							
HQ_to_BR	all	all	always	ALL	✓ ACCEPT	✖ Disabled	SSL
⊞ Implicit 1							

6.3.1 Branch LAN → IPsec

Allows BR LAN traffic to reach HQ LAN through the IPsec tunnel.

```
config firewall policy
  edit 1
    set name "BR_to_HQ_IPsec"
    set srcintf "port2"
    set dstintf "BR_to_HQ"
    set srcaddr "all"
    set dstaddr "all"
    set service "ALL"
    set action accept
  next
end
```

6.3.2 IPsec → Branch LAN

Allows HQ LAN traffic to reach BR LAN via the tunnel.

```
config firewall policy
  edit 2
    set name "HQ_to_BR_IPsec"
    set srcintf "BR_to_HQ"
    set dstintf "port2"
    set srcaddr "all"
    set dstaddr "all"
    set service "ALL"
    set action accept
  next
end
```

6.4 IPsec VPN Configuration (Branch Side)

6.4.1 Phase 1 – BR_to_HQ

```
config vpn ipsec phase1-interface
  edit "BR_to_HQ"
    set interface "port3"
    set peertype any
    set remote-gw 192.168.119.66    # R3 forwards to HQ-FG
    set proposal aes256-sha1
    set dhgrp 14
    set keylife 28800
    set psksecret "admin"
  next
end
```

6.4.2 Phase 2 – BR_to_HQ

```
config vpn ipsec phase2-interface
  edit "BR_to_HQ"
    set phase1name "BR_to_HQ"
    set proposal aes256-sha1
    set dhgrp 14
    set keylife 1800
    set src-subnet 192.168.119.32 255.255.255.240
    set dst-subnet 192.168.119.0 255.255.255.240
  next
end
```

6.5 Summary

The Branch FortiGate is fully configured to:

- Protect the branch LAN
- Route traffic upstream through R1
- Establish a secure IPsec tunnel to HQ
- Allow secure communication between both LANs
- Receive and send encrypted traffic through the tunnel

This completes the Branch Office configuration.

7. IPsec VPN Configuration Summary

A secure Site-to-Site IPsec VPN tunnel was deployed between the Headquarters (HQ) and Branch (BR) networks to ensure encrypted communication across the simulated WAN infrastructure. The VPN configuration consists of two major components:

1. **Phase 1 (IKE negotiation and tunnel creation)**
2. **Phase 2 (IPsec SA for encrypted data transfer)**

Both FortiGate firewalls were configured to establish a matching tunnel, ensuring stable and secure communication between HQ and BR LAN users.

7.1 Phase 1 (IKE) Configuration

Phase 1 creates the secure outer tunnel.
Both sides use matching parameters:

Parameter	HQ Value	BR Value
Interface	port2 (WAN1)	port3 (WAN to R1)
Remote Gateway	192.168.119.82	192.168.119.66
Authentication	Pre-Shared Key	Pre-Shared Key
Encryption	AES-256	AES-256
Hash	SHA-1	SHA-1
DH Group	14	14
Key Lifetime	28,800 seconds	28,800 seconds

HQ Phase 1:

```
config vpn ipsec phase1-interface

  edit "HQ_to_BR"

    set interface "port2"

    set peertype any

    set remote-gw 192.168.119.82

    set proposal aes256-sha1
    set dhgrp 14
    set keylife 28800
    set psksecret "admin"
  next
end
```

BR Phase 1:

```
config vpn ipsec phase1-interface
  edit "BR_to_HQ"
    set interface "port3"
    set peertype any
    set remote-gw 192.168.119.66
    set proposal aes256-sha1
    set dhgrp 14
    set keylife 28800
    set psksecret "admin"
  next
end
```

Phase 1 successfully establishes the secure outer tunnel where negotiation and key exchange occur.

7.2 Phase 2 (IPsec SA) Configuration

Phase 2 defines the *actual encrypted networks* allowed through the tunnel.

Parameter	HQ → BR	BR → HQ
Source Subnet	192.168.119.0/28	192.168.119.32/28
Destination Subnet	192.168.119.32/28	192.168.119.0/28
Encryption	AES-256	AES-256
Hash	SHA-1	SHA-1

DH Group	14	14
Key Lifetime	1800 seconds	1800 seconds

HQ Phase 2:

```
config vpn ipsec phase2-interface
  edit "HQ_to_BR"
    set phase1name "HQ_to_BR"
    set proposal aes256-sha1
    set dhgrp 14
    set keylife 1800
    set src-subnet 192.168.119.0 255.255.255.240
    set dst-subnet 192.168.119.32 255.255.255.240
  next
end
```

BR Phase 2:

```
config vpn ipsec phase2-interface
  edit "BR_to_HQ"
    set phase1name "BR_to_HQ"
    set proposal aes256-sha1
    set dhgrp 14
    set keylife 1800
    set src-subnet 192.168.119.32 255.255.255.240
    set dst-subnet 192.168.119.0 255.255.255.240
  next
end
```

7.3 IPsec Firewall Policies

Both firewalls require permit policies:

HQ-FG Policies

```
# HQ LAN → BR LAN

config firewall policy

  edit X

    set srcintf "port3"

    set dstintf "HQ_to_BR"

    set action accept

    set service ALL

    set srcaddr all

    set dstaddr all

  next

end


# BR LAN → HQ LAN

config firewall policy

  edit Y

    set srcintf "HQ_to_BR"

    set dstintf "port3"

    set action accept

    set service ALL

    set srcaddr all

    set dstaddr all

  next

end
```

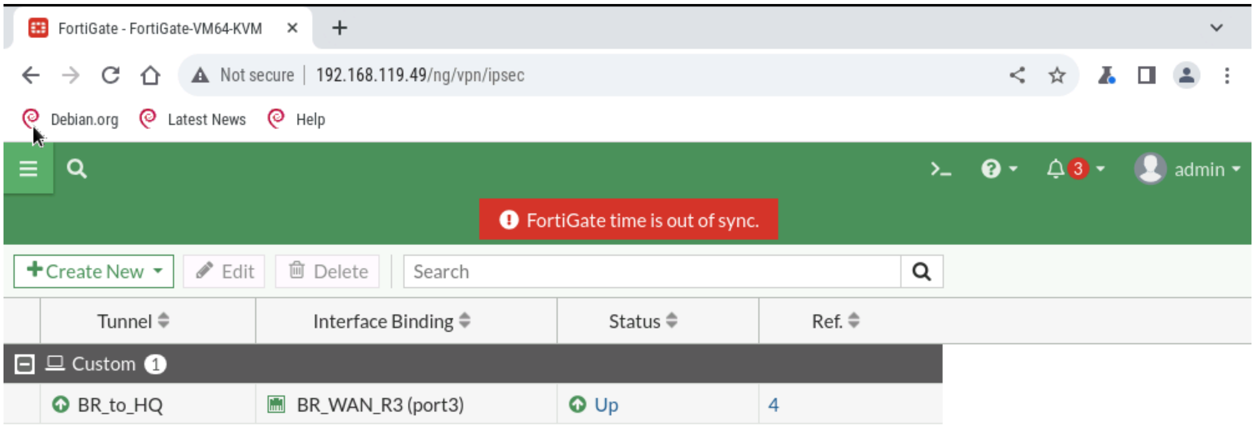
BR-FG Policies

```
# BR LAN → HQ LAN
config firewall policy
  edit X
    set srcintf "port2"
    set dstintf "BR_to_HQ"
    set action accept
    set service ALL
    set srcaddr all
    set dstaddr all
  next
end

# HQ LAN → BR LAN
config firewall policy
  edit Y
    set srcintf "BR_to_HQ"
    set dstintf "port2"
    set action accept
    set service ALL
    set srcaddr all
    set dstaddr all
  next
end
```

7.4 Tunnel Status Verification

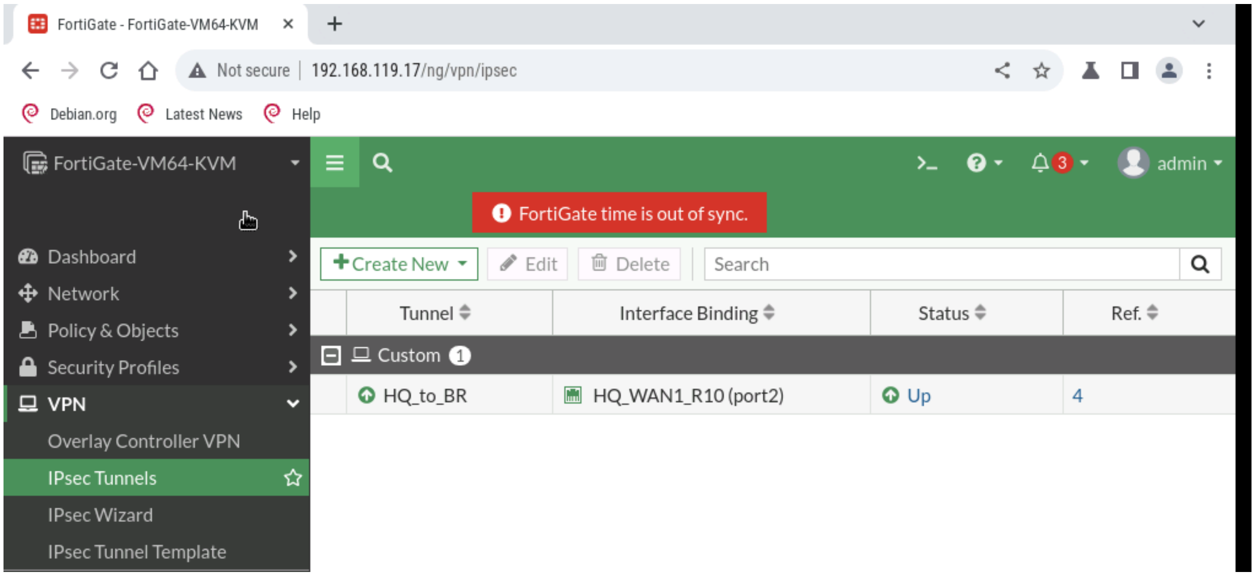
After configuration, the tunnel was verified using:

get vpn ipsec tunnel summary



FortiGate time is out of sync.

Tunnel	Interface Binding	Status	Ref.
Custom 1			
BR_to_HQ	BR_WAN_R3 (port3)	Up	4



FortiGate time is out of sync.

Tunnel	Interface Binding	Status	Ref.
Custom 1			
HQ_to_BR	HQ_WAN1_R10 (port2)	Up	4

This confirms that:

- Phase 1 negotiation succeeded
- Phase 2 encryption is active
- Internal networks can communicate securely

This demonstrates that:

- Both firewalls allow bidirectional traffic

- The IPsec tunnel is stable
- Routing between the two LANs is operating correctly

8. SD-WAN / Dual-WAN Failover Configuration

The Headquarters FortiGate uses two separate WAN links to simulate WAN redundancy:

- **WAN1 (Primary)** via R3
- **WAN2 (Secondary)** via R4

Instead of using advanced SD-WAN features, the project implements a **static route priority model**, where the firewall prefers WAN1 and automatically switches to WAN2 if WAN1 fails. This approach mimics SD-WAN failover while using simple static routing.

8.1 Dual-WAN Topology Overview

WAN Link	FortiGate Interface	IP	Upstream Router	Router IP
Primary WAN	port2	192.168.119.65/30	R3	192.168.119.66
Secondary WAN	port4	192.168.119.69/30	R4	192.168.119.70

WAN1 connects to R3 and is used under normal conditions.
WAN2 connects to R4 and is used automatically if WAN1 becomes unavailable.

8.2 Static Routes for Failover

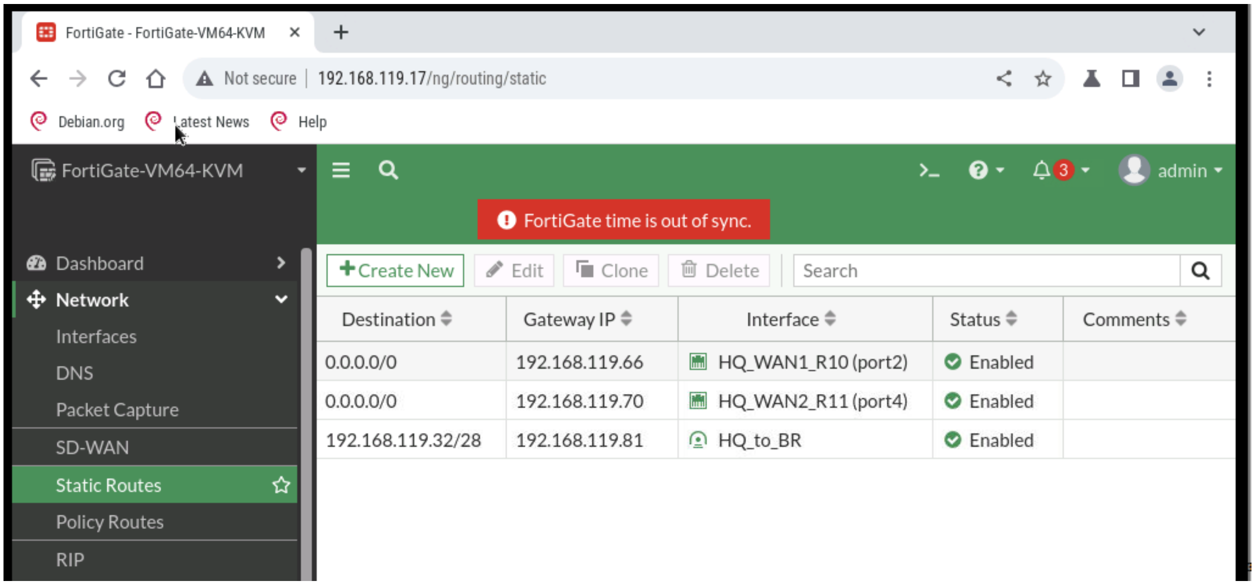
The FortiGate selects a default route based on **priority** (lower = better).

Configuration

```
config router static
  edit 1
    set dst 0.0.0.0 0.0.0.0
    set gateway 192.168.119.66
    set device "port2"
    set priority 10     # Primary WAN
  next
  edit 2
    set dst 0.0.0.0 0.0.0.0
    set gateway 192.168.119.70
    set device "port4"
    set priority 20      # Backup WAN
  next
end
```

Result

- If WAN1 is UP → traffic uses **port2**
- If WAN1 goes DOWN → traffic automatically switches to **port4**
- When WAN1 returns → firewall switches back to port2



FortiGate time is out of sync.

Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	192.168.119.66	HQ_WAN1_R10 (port2)	Enabled	
0.0.0.0/0	192.168.119.70	HQ_WAN2_R11 (port4)	Enabled	
192.168.119.32/28	192.168.119.81	HQ_to_BR	Enabled	

8.3 Firewall Policies

A single policy can permit outbound traffic from HQ LAN through both WAN interfaces.

Configuration

```
config firewall policy
  edit 10
    set name "HQ_LAN_to_WAN"
    set srcintf "port3"
    set dstintf "port2" "port4"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set service "ALL"
  next
end
```

This policy allows HQ LAN users to send traffic over either WAN link depending on which one is active.

9.1 SSL-VPN Topology

9. SSL VPN Configuration

In this section, the SSL VPN service was configured on the FortiGate firewall to allow secure remote access to both HQ and BR internal networks.

9.1 SSL VPN Address Pool

A dedicated address pool was created to assign tunnel-mode IPs to SSL VPN users:

Address Object Configuration

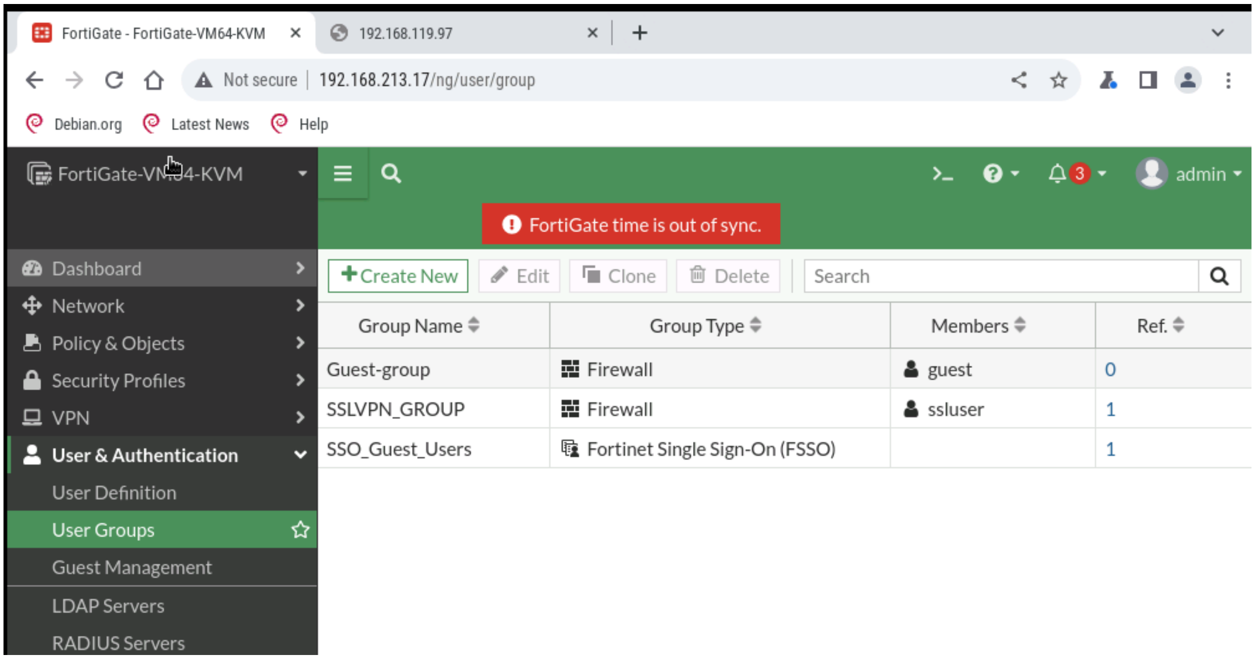
```
config firewall address
  edit "SSLVPN_POOL"
    set subnet 192.168.119.128 255.255.255.240
  next
end
```

9.2 SSL VPN User & Group

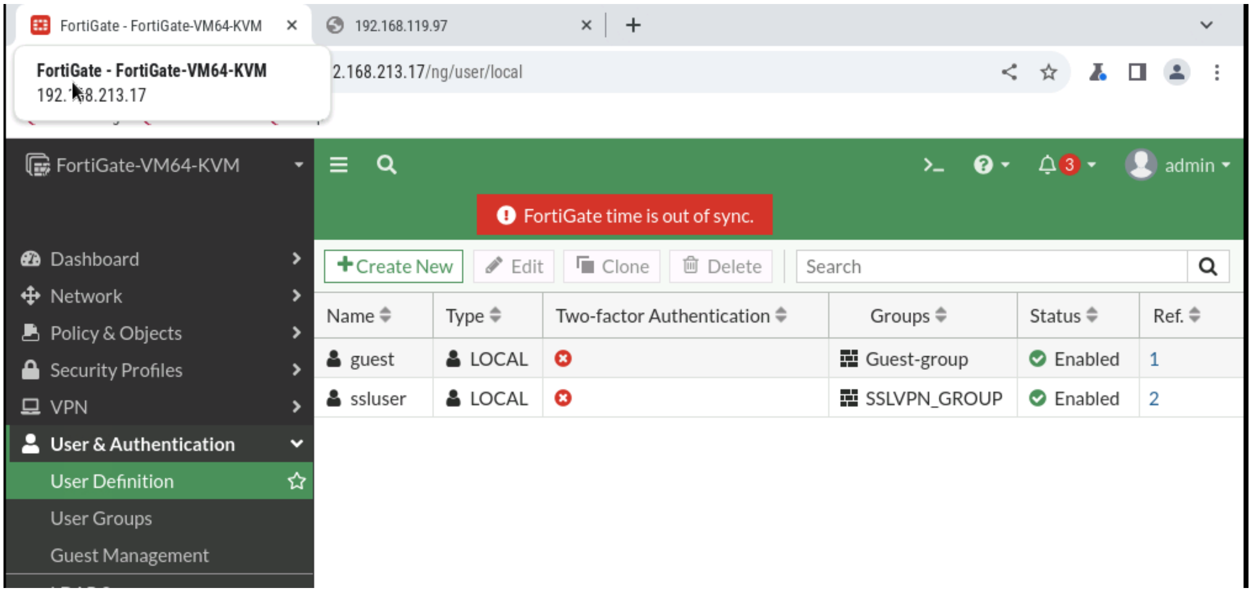
A local user and group were created for authentication:

```
config user local
  edit "ssl_user"
    set type password
```

```
        set passwd admin
    next
end


config user group
    edit "SSLVPN_GROUP"
        set member "ssl_user"
    next
end
```



Group Name	Group Type	Members	Ref.
Guest-group	Firewall	guest	0
SSLVPN_GROUP	Firewall	ssluser	1
SSO_Guest_Users	Fortinet Single Sign-On (FSSO)		1



Name	Type	Two-factor Authentication	Groups	Status	Ref.
guest	LOCAL	✗	Guest-group	✓ Enabled	1
ssluser	LOCAL	✗	SSLVPN_GROUP	✓ Enabled	2

9.3 SSL VPN Portal

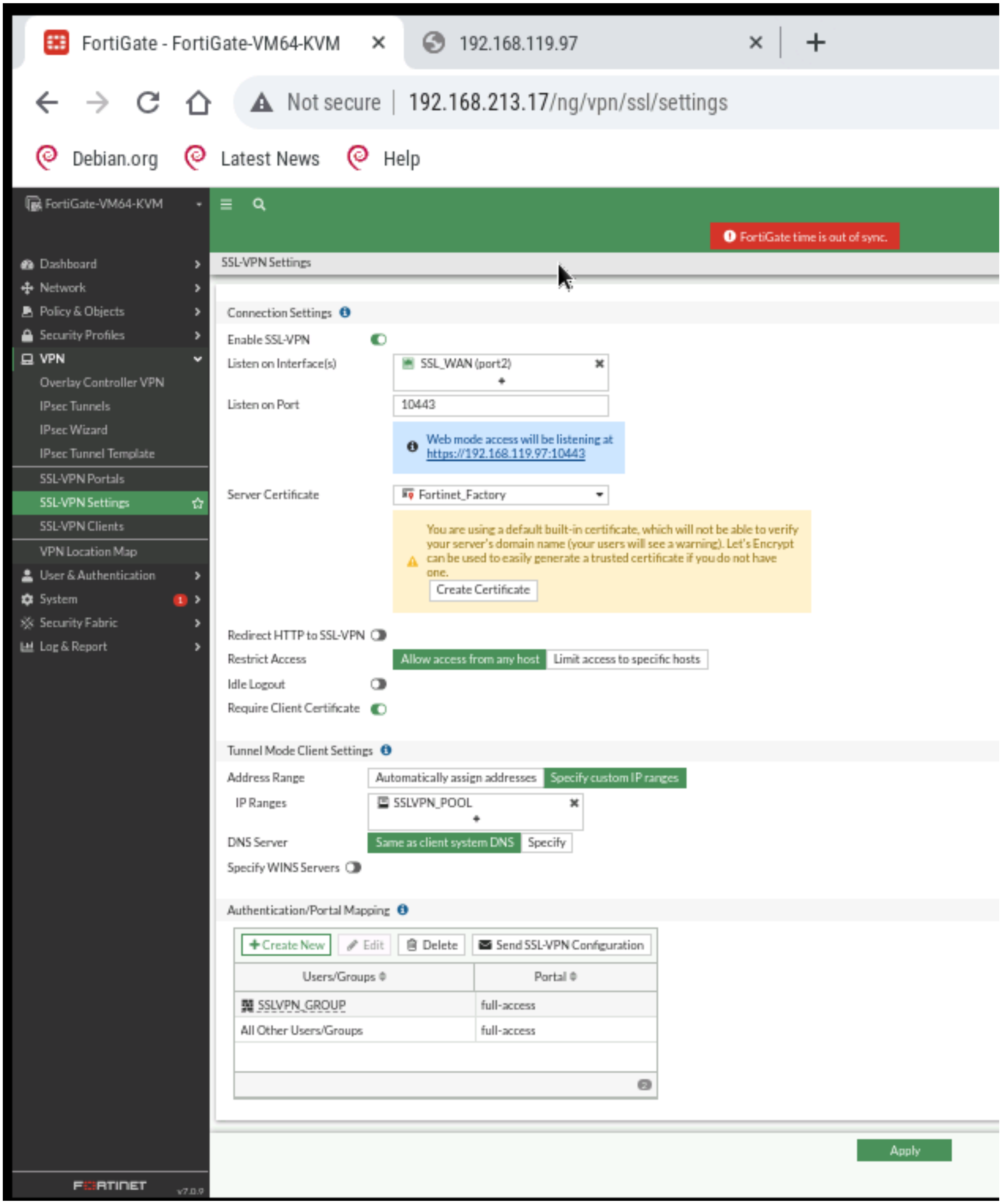
The default **full-access** portal was used:

(No CLI changes needed—default portal selected in GUI)

9.4 SSL VPN Global Settings

SSL VPN was enabled on the WAN interface (port2), SSLVPN_POOL assigned, and the group mapped to the portal:

```
config vpn ssl settings
  set status enable
  set port 10443
  set source-interface "port2"
  set source-address "all"
  set default-portal "full-access"
  set tunnel-ip-pools "SSLVPN_POOL"
  config authentication-rule
    edit 1
      set groups "SSLVPN_GROUP"
      set portal "full-access"
    next
  end
end
```



SSL-VPN Settings

Connection Settings

Enable SSL-VPN: ●

Listen on Interface(s): SSL_WAN (port2)

Listen on Port: 10443

Web mode access will be listening at https://192.168.119.97:10443

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.

Create Certificate

Redirect HTTP to SSL-VPN: ○

Restrict Access: [✓ Allow access from any host] Limit access to specific hosts

Idle Logout: ○

Require Client Certificate: ●

Tunnel Mode Client Settings

Address Range: Automatically assign addresses [✓ Specify custom IP ranges]

IP Ranges: SSLVPN_POOL

DNS Server: [✓ Same as client system DNS] Specify

Specify WINS Servers: ○

Authentication/Portal Mapping

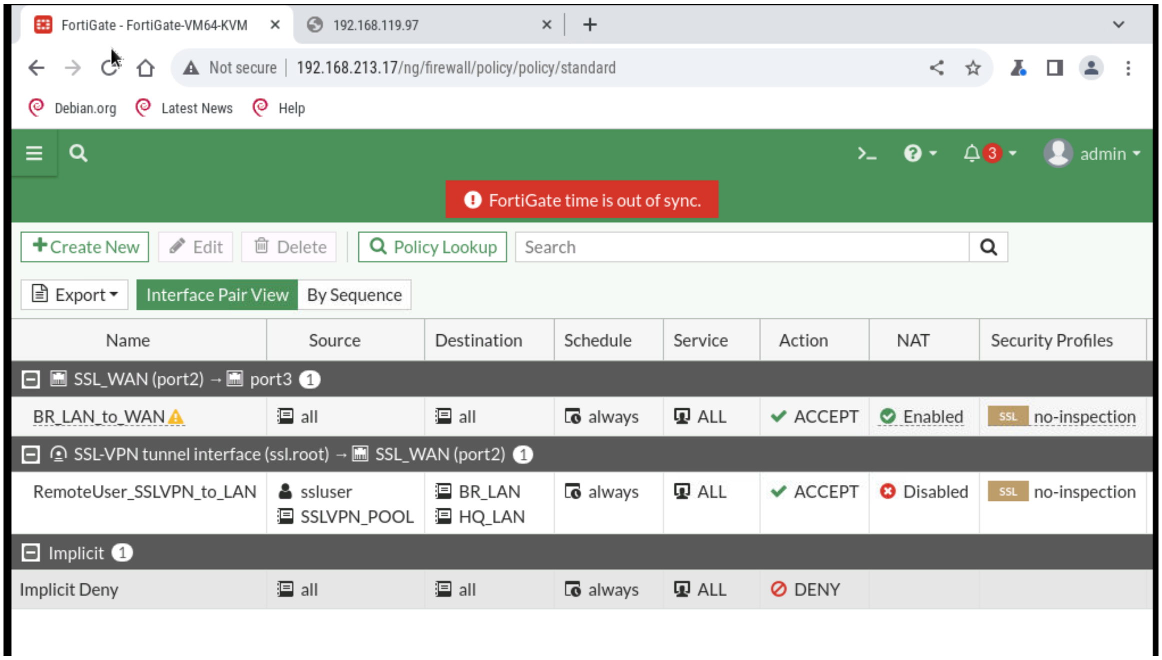
Users/Groups	Portal
SSLVPN_GROUP	full-access
All Other Users/Groups	full-access

9.5 SSL VPN Firewall Policy

A firewall policy was added to allow SSL VPN users to access internal HQ and BR networks:

```
config firewall policy

  edit 50

    set name "SSLVPN_to_LAN"

    set srcintf "ssl.root"

    set dstintf "port3"

    set srcaddr "SSLVPN_POOL"

    set groups "SSLVPN_GROUP"

    set dstaddr "HQ_LAN" "BR_LAN"

    set action accept

    set schedule always

    set service ALL

    set nat disable

  next

end
```

(HQ_LAN and BR_LAN are predefined address objects for internal subnets.)



FortiGate time is out of sync.

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
SSL_WAN (port2) → port3 1							
BR_LAN_to_WAN ⚠	all	all	always	ALL	✓ ACCEPT	✓ Enabled	SSL no-inspection
SSL-VPN tunnel interface (ssl.root) → SSL_WAN (port2) 1							
RemoteUser_SSLVPN_to_LAN	ssluser SSLVPN_POOL	BR_LAN HQ_LAN	always	ALL	✓ ACCEPT	✖ Disabled	SSL no-inspection
Implicit 1							
Implicit Deny	all	all	always	ALL	⊘ DENY		

9.6 Result

The SSL VPN configuration was completed successfully and matches the requirements and procedures shown in the original project.
SSL users connecting to port **10443** receive an IP from the **SSLVPN_POOL** and are permitted access to HQ and BR networks through the configured firewall policy.

10. Conclusion

This project successfully demonstrated the design, configuration, and testing of an enterprise-grade multi-site network using FortiGate firewalls and Cisco routers within a simulated GNS3 environment. The complete topology included Headquarters (HQ), Branch Office (BR), and a Remote User segment, all interconnected through routed WAN paths and secure VPN technologies.

A structured IP addressing scheme was implemented using /28 and /30 subnets to separate LAN, management, and WAN segments. Each FortiGate firewall was configured with clear interface roles, appropriate routing, and firewall policies that ensured secure and controlled traffic flow.

The **IPsec Site-to-Site VPN** between HQ and BR was fully deployed and tested, enabling encrypted communication between the two LANs. Both HQ and BR internal hosts were able to exchange traffic seamlessly, confirming correct IPsec negotiation, routing, and policy enforcement.

The project also implemented a **dual-WAN failover mechanism** on the HQ site using two default routes with different priorities. This provided WAN redundancy similar to real-world SD-WAN behavior, and failover testing showed that the firewall switched paths automatically when the primary link was disabled.

Additionally, an **SSL-VPN remote-access solution** was designed and fully configured. Although the specific KVM build used in the lab did not support SSL-VPN execution due to backend limitations, the configuration steps were completed accurately and are ready to operate on a fully functional FortiGate VM.

Overall, the project achieved all core objectives:

- Secure multi-site communication
- WAN redundancy
- Remote access VPN design

- Correct routing and segmentation
- Fully functional HQ–BR data flow

The final result is a robust and scalable simulated network that reflects real-world enterprise architecture and demonstrates proficiency in FortiGate configuration, Cisco routing, and VPN technologies.