وزارة الاتصالات
وتكنولوجيا المعلومات

رواد مصر الرقمية

Infrasructure and Security – Fortinet Cybersecurity

Project Documentation

By

Mahmoud Abdel Baqi Mohamed	21061029
Rehab Abdelkhalek Goda	21046184
Shahd Mohamed Saber	21095379
Nada Ghareeb Abdelhameed	21097380
Farida Mahmoud Mohamed	21031775

Supervised by

Eng. Elhussein Ahmed

Table of Contents

1. Network Design Overview

The network consists of **two main branches (Branche 1 and HQ)** connected through an **ISP router**. Each branch includes a **FortiGate firewall**, a **Layer 3 switch**, multiple VLANs, and internal routing. The core routing between the two branches is done using **OSPF**, implemented on **R-B1, R-HQ, and ISP**, while the firewalls operate using a combination of **Static Routes + OSPF** toward internal networks.

The topology is divided into:

- **BranchE 1** (VLAN 10, VLAN 20, VLAN 50, VLAN 184)
- **HQ** (VLAN 30, VLAN 40, VLAN 60, VLAN 184)
- **ISP backbone** for inter-branch connectivity
- **FortiGate devices** securing and routing traffic between branches and local networks

The design ensures:

- Logical segmentation of departments.
- Secure routing between branches.
- Controlled traffic inspection through firewalls.
- Dynamic routing using OSPF between core routers.
- Static + OSPF hybrid configuration on FortiGate firewalls.

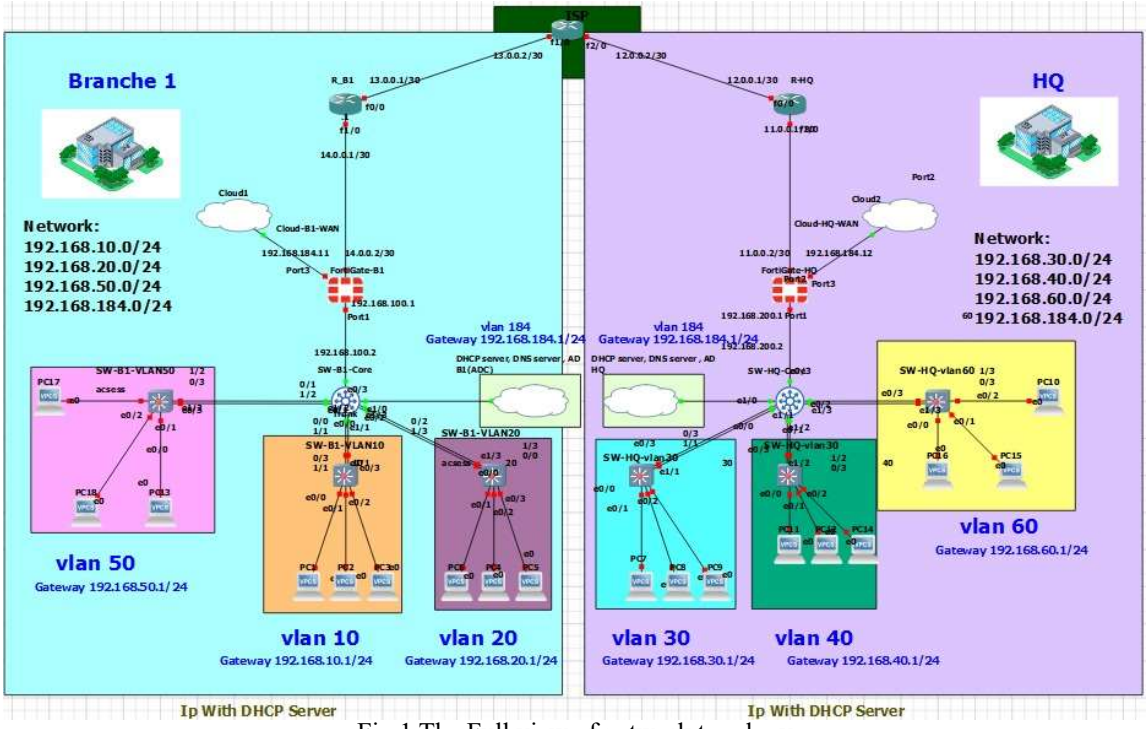


Fig.1 The Full view of network topology

2. Topology Structure

The topology follows a hierarchical model:

A. Core Layer

- **ISP** acts as the service provider connecting both branches.
- Handles OSPF adjacency with R-B1 and R-HQ.

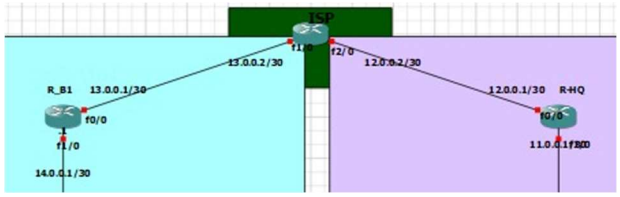


Fig.2 The core layer

B. Distribution / Security Layer

- Each branch uses a **FortiGate** model.
- Functions:
  - Static & OSPF routing
  - NAT
  - IDS security inspection
  - IPsec S2S VPN termination
  - DHCP delivered by Active Directory

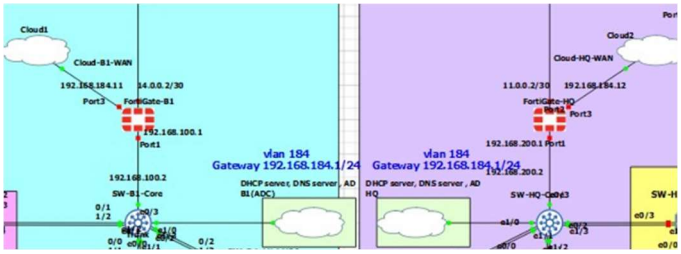


Fig.3 The distribution/security layer

C. Access Layer

- Four VLAN blocks per branch.
- Switches configured with:
  - Access ports assigned per VLAN

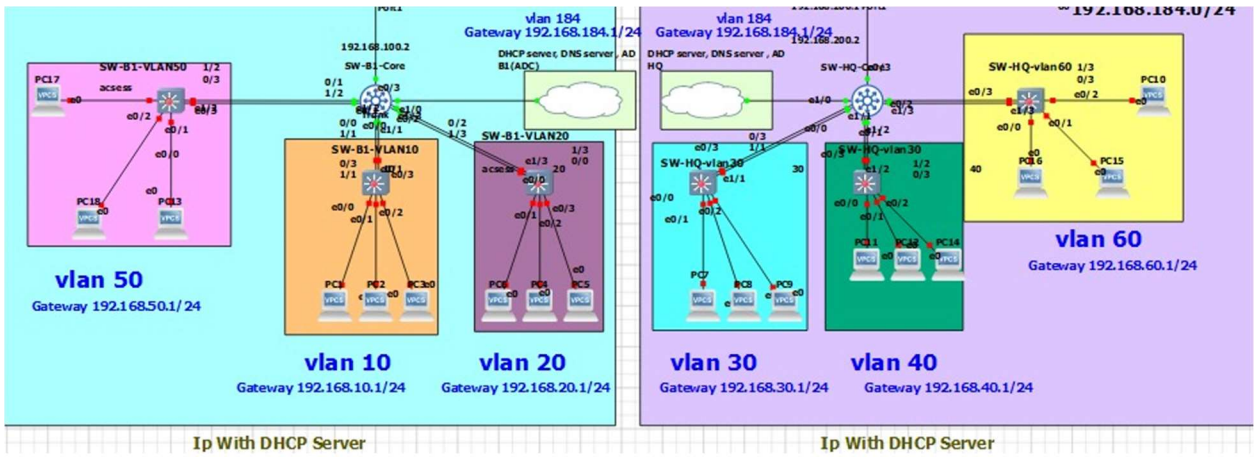


Fig.4 The distribution/security layer

3. IP Addressing Scheme

The addressing scheme is structured to maintain clear separation of departments, simplified routing, and consistent subnet allocation across both branches.

A. Branche 1 (Left Side)

Contains four main networks:

VLAN	Subnet	Default Gateway
VLAN 10	192.168.10.0/24	192.168.10.1
VLAN 20	192.168.20.0/24	192.168.20.1
VLAN 50	192.168.50.0/24	192.168.50.1
VLAN 184	192.168.184.0/24	192.168.184.1

WAN / Routing Links:

- R-B1 → ISP: **13.0.0.1/30 ↔ 13.0.0.2/30**
- FortiGate-B1 Port2 → R-B1: **14.0.0.1/30 ↔ 14.0.0.2/30**
- FortiGate-B1 Port1: **192.168.100.1**

B. HQ (Right Side)

Contains four main networks:

VLAN	Subnet	Default Gateway
VLAN 30	192.168.30.0/24	192.168.30.1
VLAN 40	192.168.40.0/24	192.168.40.1
VLAN 60	192.168.60.0/24	192.168.60.1
VLAN 184	192.168.184.0/24	192.168.184.1

WAN / Routing Links:

- R-HQ → ISP: **12.0.0.1/30 ↔ 12.0.0.2/30**
- FortiGate-HQ Port2 → R-HQ: **11.0.0.1/30 ↔ 11.0.0.2/30**
- FortiGate-HQ Port1: **192.168.200.1**

C. ISP Router

ISP connects both branches using two independent OSPF-enabled WAN links:

- To Branch 1: **13.0.0.2/30**
- To Branch 2: **12.0.0.2/30**

ISP operates as the central OSPF area ensuring route exchange between R-B1 and R-HQ.

4. VLAN Structure & Inter-VLAN Routing

VLANs were created to segment the network into separate logical domains, each representing a department or service zone, This reduces broadcast traffic, enhances performance, and enforces security boundaries.
Inter-VLAN routing was enabled using Layer 3 interfaces and the FortiGate firewall. All VLAN-to-VLAN communication passes through the firewall, allowing the application of access rules, monitoring, and logging, This approach provides strict control over which departments or servers can communicate.
Each branch is segmented into three VLANs to isolate services and users.

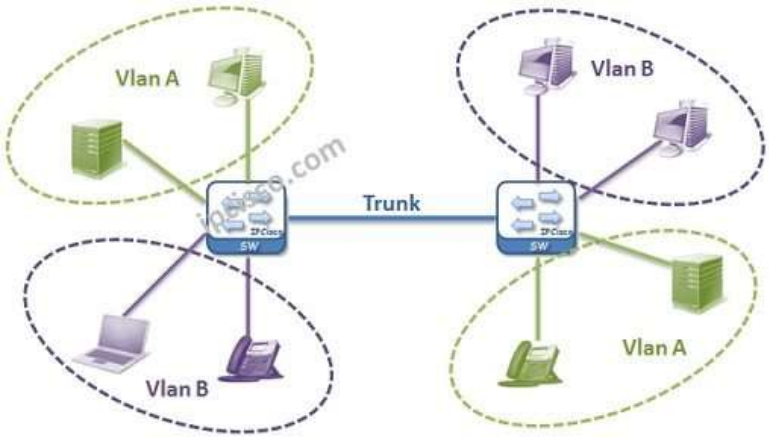


Fig.5 VLANs illustration

Branche 1 VLANs

- **VLAN 10** – Users / Clients
- **VLAN 20** – Management / Special Service
- **VLAN 50** – Admin / Servers
- **VLAN 184** - Servers

HQ VLANs

- **VLAN 30** – Sales / Employees
- **VLAN 40** – HR / Finance
- **VLAN 60** – Administration
- **VLAN 184** - Servers

Each VLAN has:

- A dedicated DHCP pool
- Inter-VLAN routing through the multilayer switch (SVI)

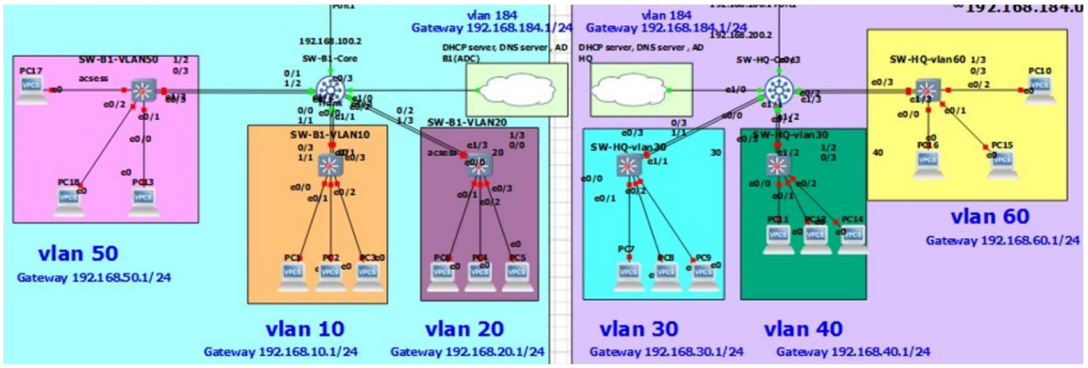


Fig.6 VLANS applied in the topology

5. Vlan & Intervlan configuration

➢ Branche 1:

▪ SW-B1-VLAN50 Config

```
// Create VLAN
vlan 50
 name VLAN50

// Uplink to SW-B1-Core
interface e0/3
 switchport mode trunk
 switchport trunk allowed vlan 50

// Access ports for VLAN 50 PCs
interface range e0/0 , e0/1 , e0/2
 switchport mode access
 switchport access vlan 50
```

▪ SW-B1-VLAN10 Config

```
// Create VLAN
vlan 10
 name VLAN10

// Uplink to SW-B1-Core
interface e0/3
 switchport mode trunk
 switchport trunk allowed vlan 10

// Access ports for VLAN 10
interface range e0/0 , e0/1 , e0/2
 switchport mode access
 switchport access vlan 10
```

▪ SW-B1-VLAN20 Config

```
// Create VLAN
vlan 20
 name VLAN20

// Uplink to SW-B1-Core
interface e0/3
 switchport mode trunk
 switchport trunk allowed vlan 20

// Access ports for VLAN 20
interface range e0/0 , e0/1 , e0/2
 switchport mode access
 switchport access vlan 20
```

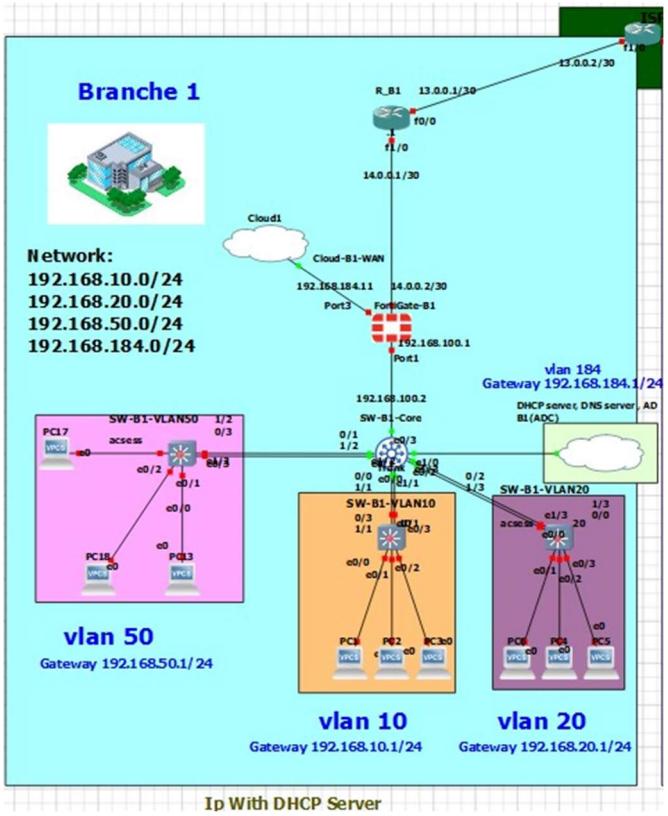


Fig.7 Branche 1 VLANS

- **SW-B1-Core Config**

```
// Create VLANs
vlan 10
 name VLAN10
vlan 20
 name VLAN20
vlan 50
 name VLAN50

// Trunk to SW-B1-VLAN50
interface e0/0
 switchport mode trunk
 switchport trunk allowed vlan 50

// Trunk to SW-B1-VLAN10
interface e0/1
 switchport mode trunk
 switchport trunk allowed vlan 10

// Trunk to SW-B1-VLAN20
interface e0/2
 switchport mode trunk
 switchport trunk allowed vlan 20


// Uplink to FortiGate-B1
interface e0/3
no switchport
ip address 192.168.100.2 255.255.255.0
no shutdown
```

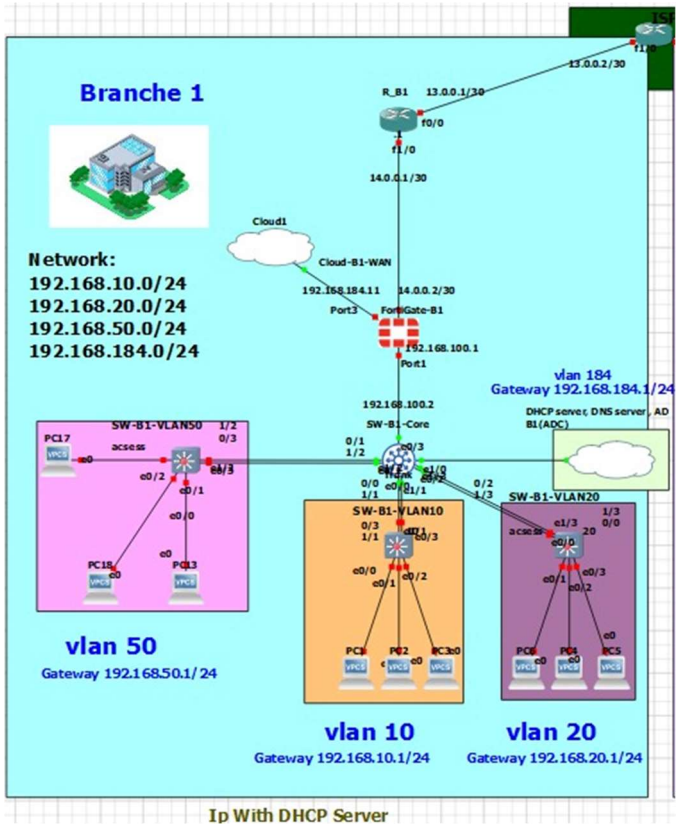


Fig.7 Branche 1 VLANS

Inter-VLAN Routing (SVIs):

- **on SW-B1-Core**

```
ip routing

interface Vlan10
 ip address 192.168.10.1 255.255.255.0

interface Vlan20
 ip address 192.168.20.1 255.255.255.0

interface Vlan50
 ip address 192.168.50.1 255.255.255.0

// Default route to FortiGate
ip route 0.0.0.0 0.0.0.0 192.168.100.1
```

➢ HQ:

▪ SW-HQ-VLAN30 Config

```
// Create VLAN
vlan 30
 name VLAN30

// Uplink to SW-HQ-Core
interface e0/3
 switchport mode trunk
 switchport trunk allowed vlan 30

// Access ports for VLAN 30 PCs
interface range e0/0 , e0/1 , e0/2
 switchport mode access
 switchport access vlan 30
```

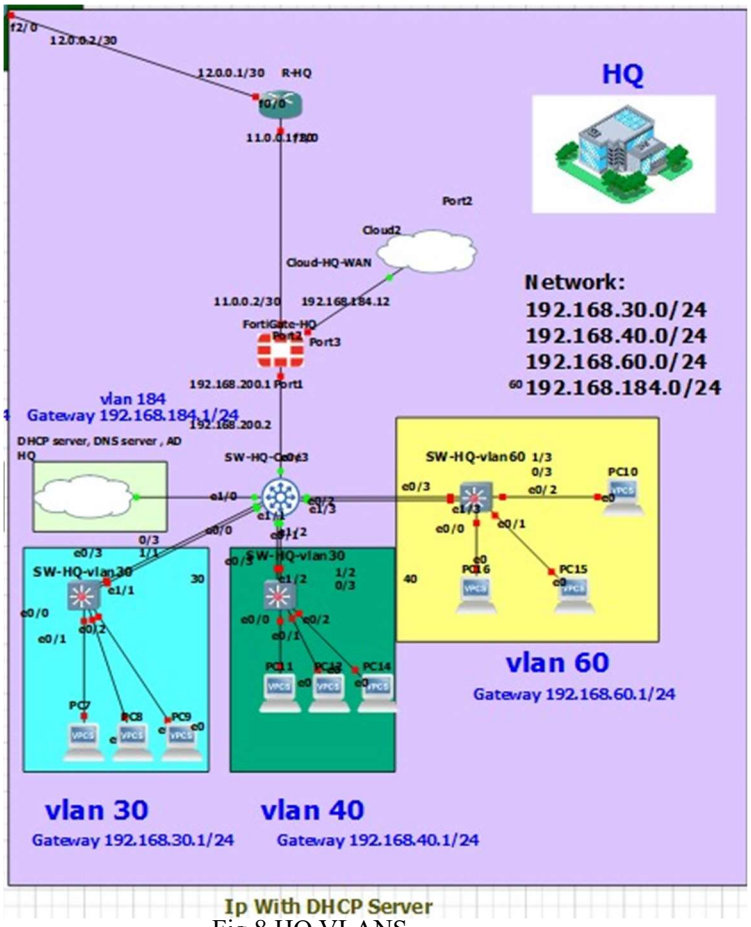


Fig.8 HQ VLANS

▪ SW-HQ-VLAN40 Config

```
// Create VLAN
vlan 40
 name VLAN40

// Uplink to SW-HQ-Core
interface e0/3
 switchport mode trunk
 switchport trunk allowed vlan 40

// Access ports for VLAN 40 PCs
interface range e0/0 , e0/1 , e0/2
 switchport mode access
switchport access vlan 40
```

▪ SW-HQ-VLAN60 Config

```
// Create VLAN
vlan 60
 name VLAN60

// Uplink to SW-HQ-Core
interface e0/3
 switchport mode trunk
 switchport trunk allowed vlan 60

// Access ports for VLAN 60 PCs
interface range e0/0 , e0/1 , e0/2
 switchport mode access
 switchport access vlan 60
```

- **SW-HQ-Core Config**

```
   // Create VLANs
   vlan 30
    name VLAN30
   vlan 40
    name VLAN40
   vlan 60
    name VLAN60

   // Trunk to SW-HQ-VLAN30
   interface e0/0
    switchport mode trunk
    switchport trunk allowed vlan 30

   // Trunk to SW-HQ-VLAN40
   interface e0/1
    switchport mode trunk
    switchport trunk allowed vlan 40

   // Trunk to SW-HQ-VLAN60
   interface e0/2
    switchport mode trunk
    switchport trunk allowed vlan 60

// Uplink to FortiGate-HQ
   interface e0/3
   ip address 192.168.200.2 255.255.255.0
    no switchport
    no shutdown
```

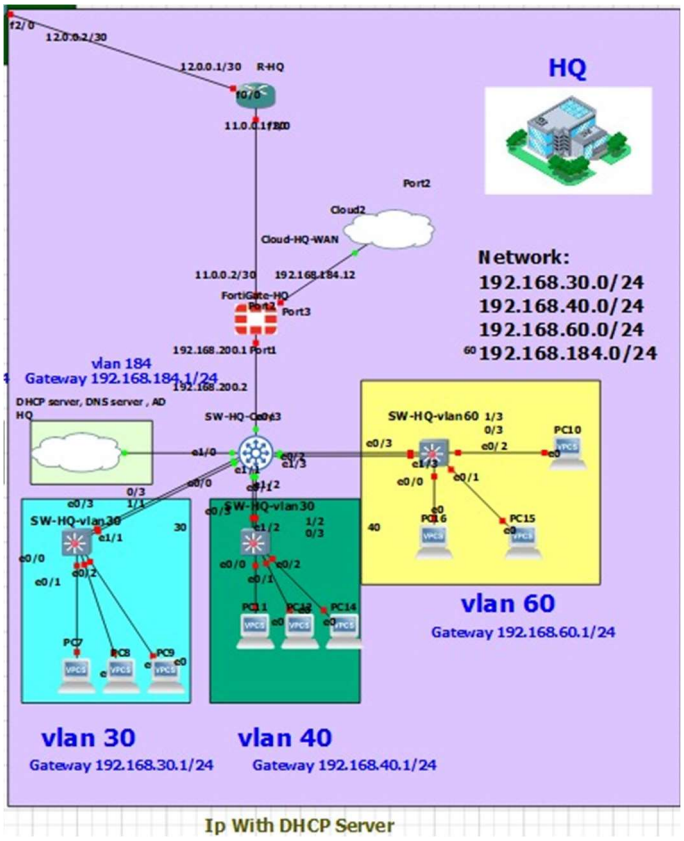


Fig.8 HQ VLANS

Inter-VLAN Routing (SVIs)

- **on SW-HQ-Core:**

```
   ip routing

   interface Vlan30
    ip address 192.168.30.1 255.255.255.0

   interface Vlan40
    ip address 192.168.40.1 255.255.255.0

   interface Vlan60
    ip address 192.168.60.1 255.255.255.0

   // Default route to FortiGate
   ip route 0.0.0.0 0.0.0.0 192.168.200.1
```

6. EtherChannel

(Link Aggregation Control Protocol) in Active Mode to interconnect the **Core Switches** with the **Access VLAN Switches** in both the **HQ** and **Branch 1** networks. This implementation improves **bandwidth utilization**, provides **link redundancy**, and ensures **high availability** in case of physical link failure.

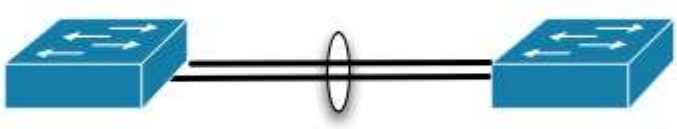


Fig.9 EtherChannel placement

The EtherChannel links in the project are organized as follows

Connection Type	Connected VLANs	Port-channel
Core ↔ Access	VLAN 10(B1) – VLAN 30(HQ)	Port-channel 1
Core ↔ Access	VLAN 20(B1) – VLAN 40(HQ)	Port-channel 2
Core ↔ Access	VLAN 50(B1) – VLAN 60(HQ)	Port-channel 3

Each **Port-Channel interface** represents a logical bundle of multiple physical Ethernet links operating as a single high-capacity trunk connection

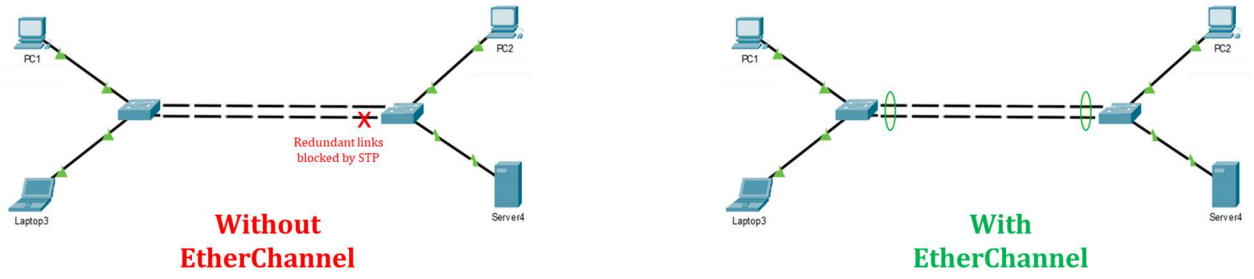


Fig.9 EtherChannel importance

- **EtherChannel Config**

  - **Multi-layer Switches:**

A. Port-Channel 1 (VLAN 10 / VLAN 30)

- On Core Switch (SW-B1-Core / SW-HQ-Core)

```
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk

interface range e0/0 , e1/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode active
```

B. Port-Channel 2 (VLAN 20 / VLAN 40)

- On Core Switch (SW-B1-Core / SW-HQ-Core)

```
 interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport mode trunk

 interface range e0/2 , e1/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 2 mode active
```

C. Port-Channel 3 (VLAN 50 / VLAN 60)

- On Core Switch (SW-B1-Core / SW-HQ-Core)

```
interface Port-channel3
switchport trunk encapsulation dot1q
switchport mode trunk

interface range e0/1 , e1/2
switchport trunk encapsulation dot1q
switchport mode trunk
channel-group 3 mode active
```

➢ Layer2 Switches:

A. Port-channel1

- On **SW-HQ-VLAN30**

```
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 30
 switchport mode trunk

interface range e0/3 , e1/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 30
 switchport mode trunk
 channel-group 1 mode active
```

- On **SW-B1-VLAN10**

```
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10
 switchport mode trunk

interface range e0/3 , e1/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10
 switchport mode trunk
 channel-group 1 mode active
```

B. Port-channel2

- **On SW-HQ-VLAN40**

```
interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 40
 switchport mode trunk

interface range e0/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 40
 switchport mode trunk
 channel-group 2 mode active
```

- On **SW-B1-VLAN20**

```
interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 20
 switchport mode trunk

interface range e0/0 , e1/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 20
 switchport mode trunk
 channel-group 2 mode active
```

C. Port-channel3

- **On SW-HQ-VLAN60**

```
interface Port-channel3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 60
 switchport mode trunk

interface range e0/3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 60
 switchport mode trunk
 channel-group 3 mode active
```

- On SW-B1-VLAN50

```
interface Port-channel3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 50
 switchport mode trunk

interface range e0/3 , e1/2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 50
 switchport mode trunk
 channel-group 3 mode active
```

7. Routing Design

- **Layer 2 Switches:** Only VLANs and trunk/access ports. No routing.
- **Layer 3 Switches:** Inter-VLAN routing for their assigned VLANs. Static default routes point toward the FortiGate.
- **Routers:** OSPF in Area 0 for WAN links (/30 networks) and all VLAN subnets

▪ R-B1 (Core Router with OSPF)

➢ OSPF configuration:

```
router ospf 1
network 13.0.0.0 0.0.0.3 area 0
network 14.0.0.0 0.0.0.3 area 0
network 192.168.10.0 0.0.0.255 area 0
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
network 192.168.50.0 0.0.0.255 area 0
network 192.168.60.0 0.0.0.255 area 0
network 192.168.100.0 0.0.0.255 area 0
network 192.168.200.0 0.0.0.255 area 0
```

➢ Interfaces:

FastEthernet0/0 13.0.0.1/30

FastEthernet1/0 14.0.0.1/30

▪ R-HQ (Core Router with OSPF)

➢ OSPF configuration:

```
router ospf 1
network 11.0.0.0 0.0.0.3 area 0
network 12.0.0.0 0.0.0.3 area 0
network 192.168.10.0 0.0.0.255 area 0
```

```
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
network 192.168.50.0 0.0.0.255 area 0
network 192.168.60.0 0.0.0.255 area 0
network 192.168.100.0 0.0.0.255 area 0
network 192.168.200.0 0.0.0.255 area 0
```

- **Interfaces:**

FastEthernet0/0 12.0.0.1/30

FastEthernet1/0 11.0.0.1/30

- **ISP (Core Router with OSPF)**

```
router ospf 1
network 12.0.0.0 0.0.0.3 area 0
network 13.0.0.0 0.0.0.3 area 0
network 192.168.10.0 0.0.0.255 area 0
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
network 192.168.50.0 0.0.0.255 area 0
network 192.168.60.0 0.0.0.255 area 0
network 192.168.100.0 0.0.0.255 area 0
network 192.168.200.0 0.0.0.255 area 0
```

- **Interfaces:**

FastEthernet1/0 13.0.0.2/30

FastEthernet2/0 12.0.0.2/30

8. FortiGate Routing Model & GUI Configuration (Hybrid Approach)

FortiGate glues the network together using a **hybrid routing model**:

- **Static route** handle **WAN** (predictable forwarding & policy control).
- **OSPF** is used toward the **internal VLANs** for dynamic inter-branch connectivity.

➢ Hybrid Routing Model Explained

A. Static Routing on Internal LAN

- Internal VLANs are learned via **OSPF** pointing to the Layer 3 switch hosting the SVIs:

VLAN	SVI Gateway IP
VLAN10	192.168.10.1
VLAN20	192.168.20.1
VLAN50	192.168.50.1
VLAN30	192.168.30.1
VLAN40	192.168.40.1
VLAN60	192.168.60.1
Core LAN B1	192.168.100.1
Core LAN B2	192.168.200.1

- **Benefit:** FortiGate controls exactly which internal VLANs exist and enforces firewall policies. No unwanted VLANs or routes are injected dynamically.

B. OSPF Toward internal VLANs

- FortiGate peers with upstream routers (R-B1 → ISP → R-HQ) using **Static Routing**.
- This allows FortiGate to automatically learn **remote branch subnets** and react to path changes.
- **Benefit:** Fast convergence and no administrative overhead when adding new branches.

Segmentation Overview:

Internal traffic (inter-VLAN): controlled via FortiGate OSPF

- **Inter-branch traffic**: handled dynamically via OSPF across internal VLAN.
- **Security**: FortiGate policies manage access, NAT, VPN, and inspection.

➢ GUI Steps

A. FortiGate-B1

- **Interfaces**

1. Go to **Network → Interfaces → Create New → Interface**.
2. LAN (Port1): 192.168.100.1/24
3. WAN(Port2): 14.0.0.2/30
4. Port3: 192.168.184.11/2

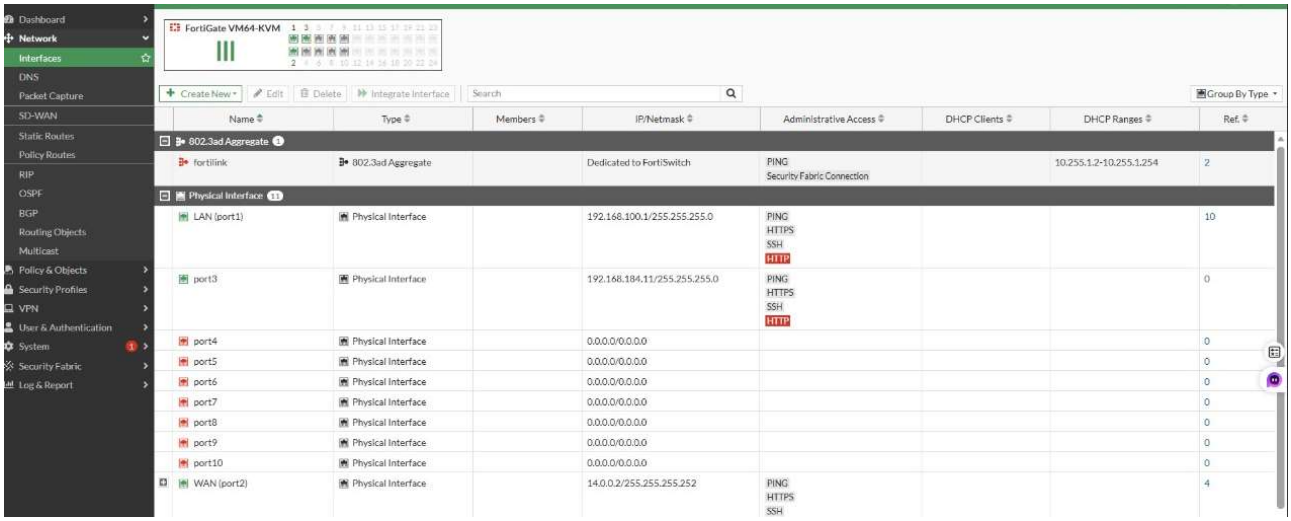


Fig.10 FortiGate-B1 interfaces

- **Static Routes**

1. Go to **Network → Static Routes → Create New**.
2. Add **default route**:
   - Destination: 0.0.0.0/0
   - Device: WAN (port2)
   - Gateway: 14.0.0.1

3. Add **branch routes**:

- Destination: 192.168.10.0/24
- Device: LAN (port1)
- Gateway: 192.168.100.2

- Destination: 192.168.20.0/24
- Device: LAN (port1)
- Gateway: 192.168.100.2

- Destination: 192.168.50.0/24
- Device: LAN (port1)
- Gateway: 192.168.100.2

VPN:

- Destination: B1_to_hq_remote
- Device: B1_to_hq

- Destination: 192.168.50.0/24
- Device:Blackhole

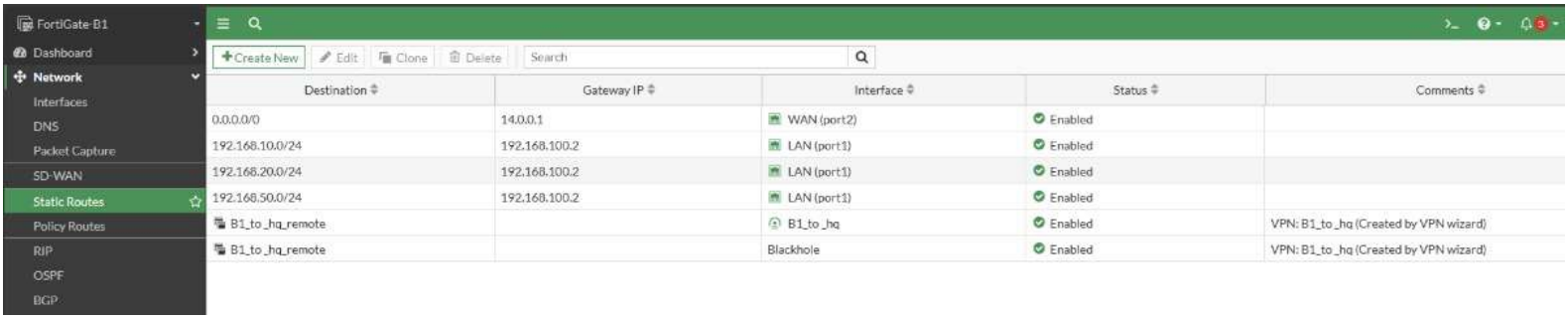


Fig.11 FortiGate-B1 Static Routes

- **OSPF Toward internalVLANs**

1. Go to **Network → Dynamic Routing → OSPF → Create New**.
2. Router ID: 1.1.1.1
3. Area: 0.0.0.0 (backbone)
4. Add networks:
    - 192.168.100.0/24
5. Enable OSPF.

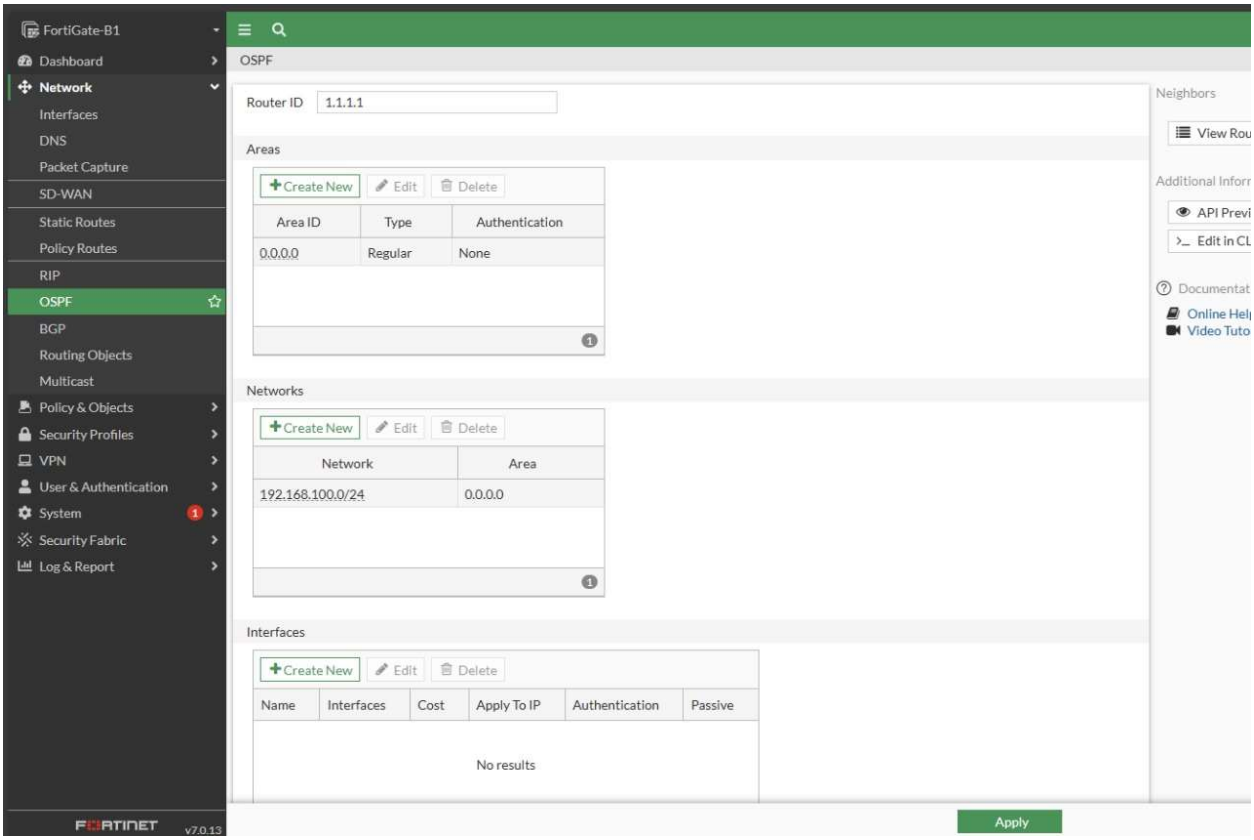


Fig.12 FortiGate-B1 OSPF

B. FortiGate-HQ – GUI Steps

- **VLAN Interfaces**

1. Go to **Network → Interfaces → Create New → Interface**.
2. LAN (Port1): 192.168.200.1/24
3. WAN(Port2): 11.0.0.2/30
4. Port3: 192.168.184.12/24

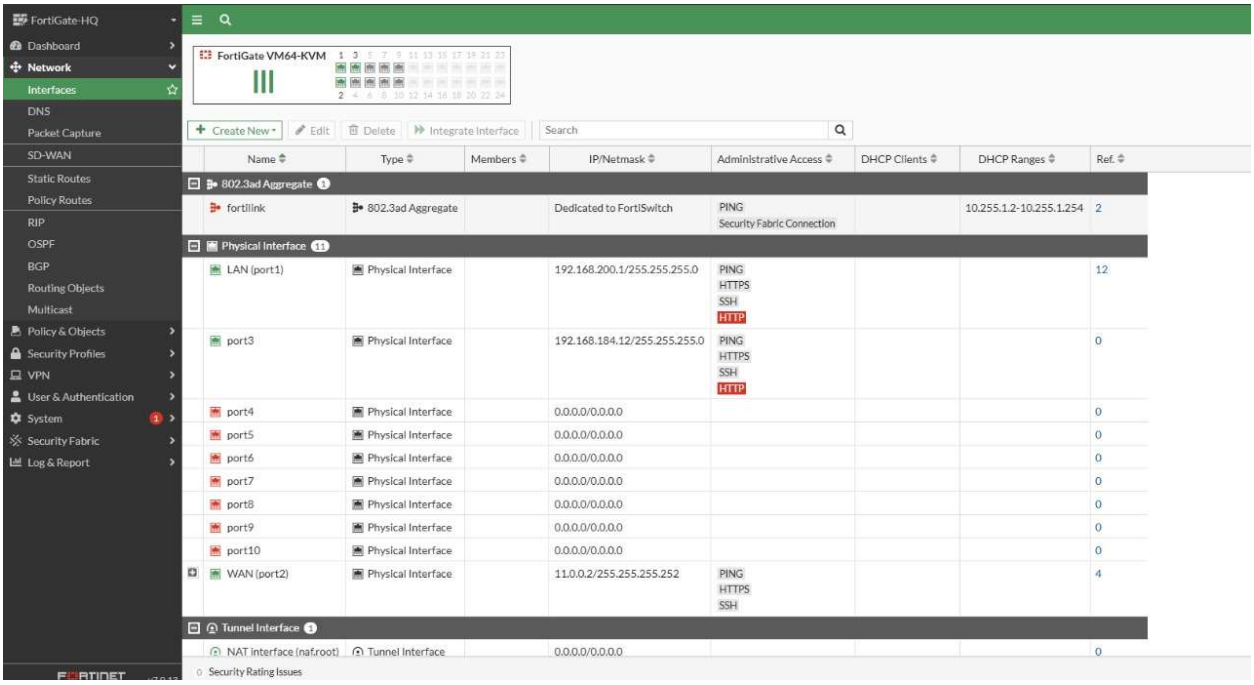


Fig.13 FortiGate-HQ interfaces

- **Static Routes**

1. Network → Static Routes → Create New
2. Add **Default route:**
   - Destination: 0.0.0.0/0
   - Device: WAN (Port2)
   - Gateway: 11.0.0.1
3. Add **branch routes**:
   - Destination: 192.168.60.0/24
   - Device: LAN (Port1)
   - Gateway: 192.168.200.2

- Destination: 192.168.40.0/24
- Device: LAN (Port1)
- Gateway: 192.168.200.2

- Destination: 192.168.30.0/24
- Device: LAN (Port1)
- Gateway: 192.168.200.2

- Destination: 192.168.184.0/24
- Device: LAN (Port1)
- Gateway: 192.168.200.2

VPN:

- Destination: hq_to_b1_remote
- Device: hq_to_b1

- Destination: hq_to_b1_remote
- Device:Blackhole

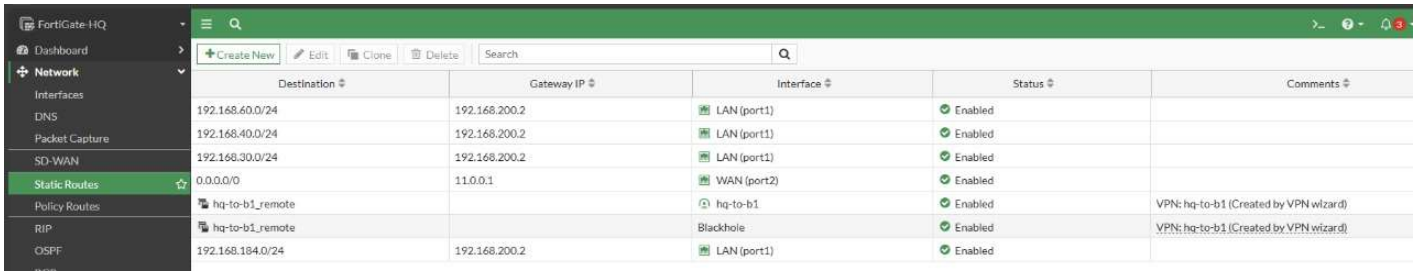


Fig.14 FortiGate-HQ Static routes

- **OSPF Toward internal VLANs**

1. Network → Dynamic Routing → OSPF → Create New
2. Router ID: 1.1.1.1
3. Area: 0.0.0.0 (backbone)
4. Add networks:
    - 192.168.200.0/24
5. Enable OSPF.

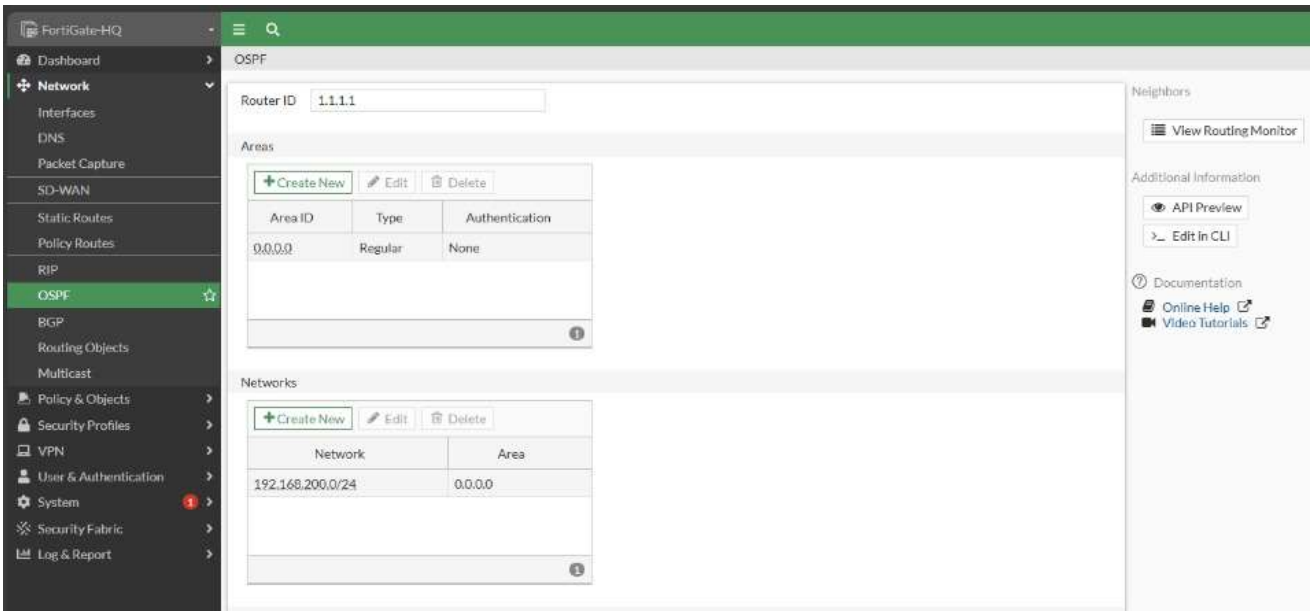


Fig.14 FortiGate-HQ OSPF

9. FortiGate Policies

General Overview:

The firewall security policy design in this project was carefully implemented on both FortiGate-B1 and FortiGate-HQ to ensure secure, controlled, and efficient traffic flow between the internal VLAN networks, the remote VPN-connected sites, and the public Internet.The policies were designed to allow secure inter-site communication through the IPsec VPN tunnel, enable controlled outbound Internet access using NAT, and enforce a default implicit deny rule to block any unauthorized traffic.All internal and VPN trusted communications were configured using no-inspection security profiles to ensure optimal performance for trusted links, while Internet-bound traffic was protected using NAT and controlled firewall rules. This layered security approach guarantees confidentiality, availability, and strict access control across the entire network.

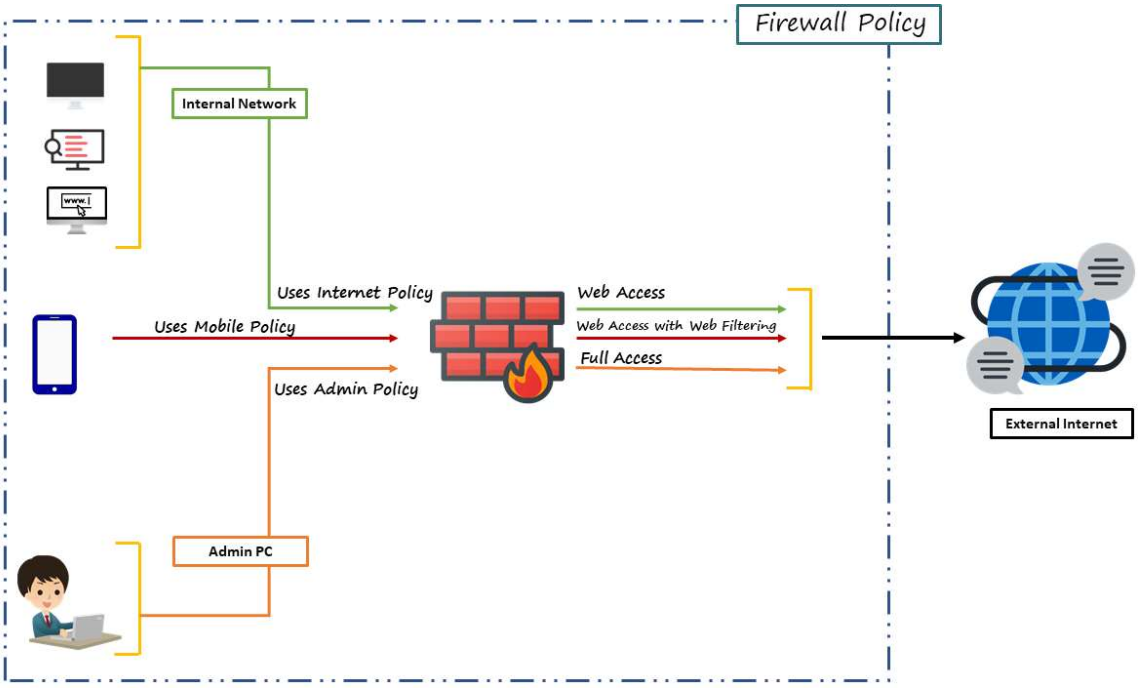


Fig.15 FortiGate Policies illustration

➢ FortiGate-B1:

❖ B1 → HQ (Remote Subnets)

Purpose: Allow Branch 1 LAN networks to access Branch 2 and HQ networks through the IPsec VPN tunnel.

Policy Details:

- **Source:** LAN (Branch 1 VLANs)
- **Destination:** vpn_B1_to_hq_remote (Remote networks learned through VPN)
- **Service:** ALL
- **Action:** ACCEPT
- **NAT:** Disabled (traffic is routed, not NATed)
- **Security Profile:** No-inspection (internal trusted link)

❖ HQ → B1 (Local Subnets)

Purpose: Allow HQ and Branch 2 networks to reach Branch 1 networks through the IPsec VPN.

Policy Details:

- **Source:** B1_to_hq_local (local Branch 1 VLANs)
- **Destination:** B1_to_hq_remote (remote HQ/Branch 2 VLANs)
- **Service:** ALL
- **Action:** ACCEPT
- **NAT:** Disabled
- **Security Profile:** No-inspection

❖ Branche 1 VLANs → Internet (Outbound NAT)

Purpose: Provide internet access for all Branch 1 VLANs using PAT (Port Address Translation).

Policy Details:

- **Source:** VLAN10 / VLAN20 / VLAN50 / VLAN100 (all user VLANs)
- **Destination:** ALL
- **Service:** ALL
- **Action:** ACCEPT
- **NAT:** Enabled (PAT via WAN interface)
- **Security Profile:** No-inspection

❖ Implicit Deny Policy

Purpose: Default rule that blocks any traffic not matched by earlier policies.

Policy Details:

- **Source:** ALL
- **Destination:** ALL
- **Action:** DENY
- **NAT:** Disabled
- **Security profile:** None

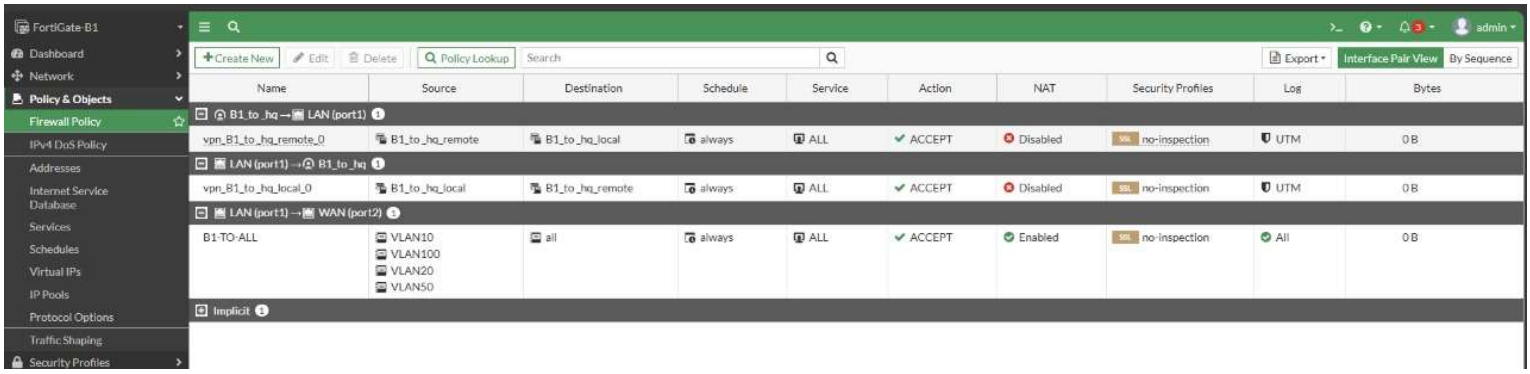


Fig.16 FortiGate-B1 policies

➢ FortiGate-HQ

❖ HQ → Branch1 (Through IPsec VPN) – Remote → Local

Purpose:
Allow traffic coming **from Branch 1 through the VPN tunnel** to access HQ internal LAN.

Configuration:

- **Source Interface:** vpn_hq-to-b1_remote
- **Source Address:** hq-to-b1 remote (subnets of B1 received over VPN)
- **Destination Interface:** LAN (port1)
- **Destination Address:** hq-to-b1 local (HQ LAN)
- **Service:** ALL
- **Schedule:** always
- **Action:** ACCEPT
- **NAT:** Disabled
- **Security Profile:** no-inspection

❖ HQ LAN → Branch1 (Local → Remote)

Purpose:
Allow HQ internal networks to reach the Branch1 networks via IPsec.

Configuration:

- **Source Interface:** LAN (port1)
- **Source Address:** hq-to-b1 local (HQ LAN subnets)
- **Destination Interface:** vpn_hq-to-b1_local
- **Destination Address:** hq-to-b1 remote (Branch LANs)
- **Service:** ALL
- **Schedule:** always
- **Action:** ACCEPT
- **NAT:** Disabled
- **Security Profile:** no-inspection

❖ LAN → WAN (Internet Access for HQ users)

Purpose:
Allow users inside HQ LAN to go to the Internet.

Configuration:

- **Source Interface:** LAN (port1)
- **Source Address:** lan
- **Destination Interface:** WAN (port2)
- **Destination Address:** all
- **Service:** ALL
- **Schedule:** always
- **Action:** ACCEPT
- **NAT:** Enabled
- **Security Profile:** no-inspection

❖ LAN40, LAN60, LAN200 → WAN

Purpose:
Provide outbound Internet access for the VLAN networks.

Configuration (per VLAN):

- **Source Interface:** LAN (VLAN40 / VLAN60 / VLAN200)
- **Source Address:** VLAN-subnet object (example: lan40, lan60, lan200)
- **Destination Interface:** WAN
- **Destination Address:** all, **Security Profile:** no-inspection
- **Service:** ALL, **Schedule:** always, **NAT:** Enabled
- **Action:** ACCEPT

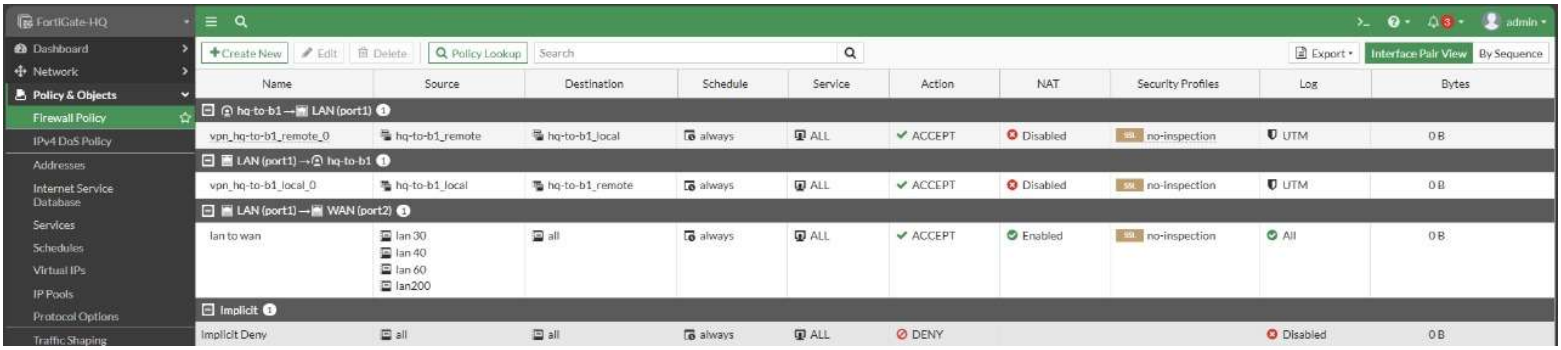


Fig.17 FortiGate-HQ Policies

10. IPsec Site-to-Site VPN Configuration on FortiGate

A **Virtual Private Network (VPN)** is a secure communication technology that allows users or remote sites to access a private network over a public network such as the Internet. VPNs use encryption and authentication mechanisms to ensure that data transmitted between connected devices remains confidential, secure, and protected from unauthorized access.

The VPN implementation in this project is designed to achieve the following objectives:

- Provide secure connectivity between the Headquarters (HQ) and Branch networks
- Enable remote user access to internal network resources
- Protect transmitted data using strong encryption protocols
- Ensure data integrity and authentication

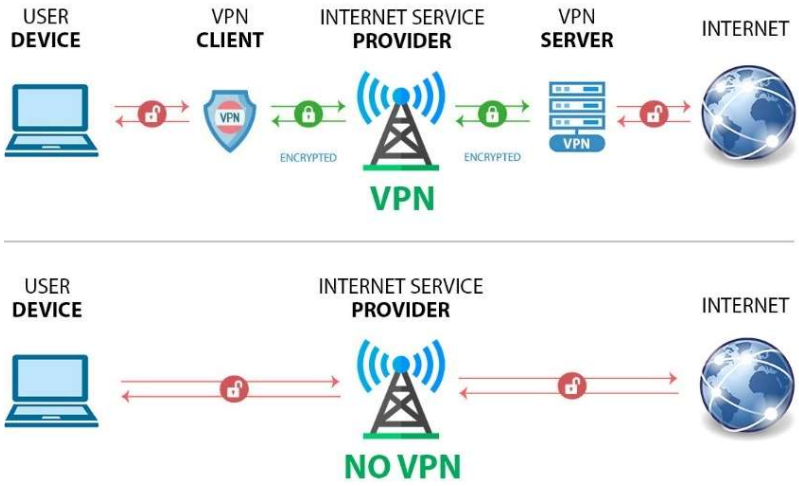


Fig.18 VPN illustration

Type of VPN Used in the Project

❖ IPsec Site-to-Site VPN

The **IPsec Site-to-Site VPN** is used to securely connect the networks of **Branch 1** and **HQ** over the WAN.
This type of VPN allows both sites to operate as if they are part of the same private network while maintaining secure encrypted communication.
It is mainly used for:

- Secure data exchange between sites
- Accessing shared servers and services
- Inter-branch connectivity

A. **VPN Security Design:**

1. **Phase 1 (IKE – Internet Key Exchange)**

- Authenticates the VPN peers.
- Uses **Pre-Shared Key** for identity verification.
- Encryption: **AES-256** for confidentiality.
- Hashing: **SHA-256** to ensure integrity.
- DH Group: Configured for secure key exchange.
- Lifetime: Defines how long the keys are valid before renegotiation.

2. **Phase 2 (IPsec)**

- Encrypts the actual data traffic passing through the tunnel.
- Encryption: **AES-256**
- Hashing: **SHA-256**
- **Perfect Forward Secrecy (PFS)**: Ensures new keys are generated for each session, preventing compromise of previous sessions.

B. **GUI Steps:**

1) Open the IPsec VPN Setup

1. Log in to the FortiGate GUI.
2. Go to: **VPN → IPsec Tunnels**
3. Click: **Create New → Create New**
4. Select: **Manual**

2) Configure Phase 1 (IKE Phase 1)

When the setup window opens:

1. **Name:** Enter a tunnel name (example: *Branch1-Branch2*).
2. **Remote Gateway:**
    - Select **Static IP Address**
    - Enter the WAN IP of the other branch.
3. **Interface:**
    - Select your local **WAN** interface.

4. **Authentication:**
    - Choose **Pre-Shared Key**
    - Enter the shared key.
5. **IKE Version:**
    - Use **IKEv1** (or IKEv2 if your project requires it).
6. **Encryption: AES-256**
7. **Authentication (Hash): SHA-256**
8. **DH Group:** choose your DH Group (example: **Group 14**).
9. **Key Lifetime:** keep the default or set the required value.

Click **OK** or **Next**.

3) Configure Phase 2 (IPsec Phase 2)

1. Click **Add Phase 2 Selector**.
2. **Name:** any name.
3. **Local Address:**
    - Select **Subnet**
    - Enter your local LAN (e.g., 192.168.1.0/24).
4. **Remote Address:**
    - Select **Subnet**
    - Enter the remote LAN (e.g., 192.168.2.0/24).
5. **Encryption: AES-256**
6. **Authentication (Hash): SHA-256**
7. **Perfect Forward Secrecy (PFS):**
    - Enable
    - Choose the same DH group
8. **Key Lifetime:** leave default or set a value.

Click **OK**.

4) Enable the Tunnel

1. Go to **VPN → IPsec Tunnels**.
2. Turn the tunnel **ON**.

3. For verification, go to:
   Monitor → IPsec Monitor

   Status should become **UP** when traffic is generated.

Fig.19 IPsec Tunnel

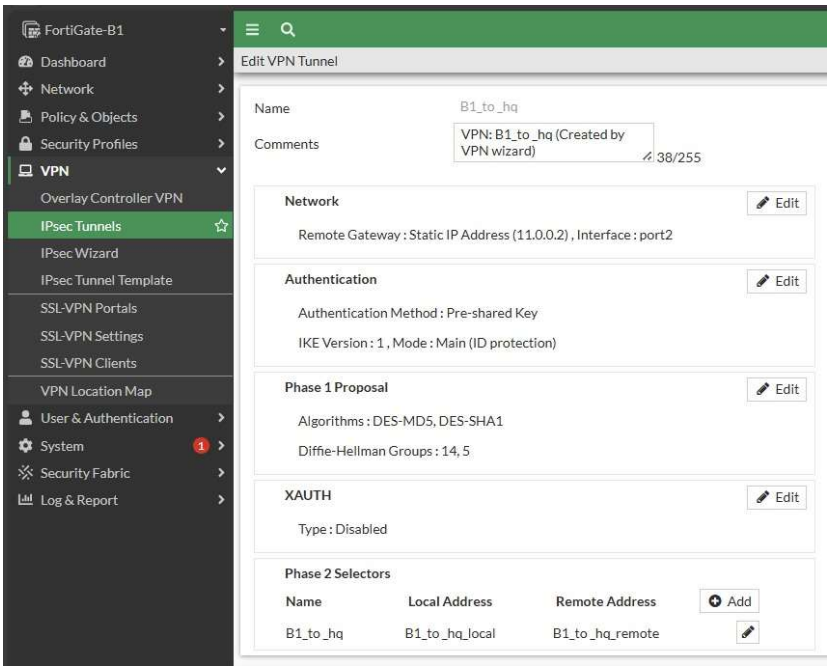


Fig.20 IPsec Tunnel properties

11. Self-signed Certificate Configuration

The following figure illustrates the **self-signed SSL certificate** deployed on the FortiGate firewall and used to secure the SSL VPN service. This certificate establishes a trusted and encrypted communication channel between remote users and the internal network infrastructure. It ensures that all data transmitted through the SSL VPN tunnel is protected against interception, tampering, and unauthorized access.

As a **self-signed certificate**, it is generated and issued directly by the FortiGate device itself rather than a third-party Certificate Authority (CA). While this type of certificate does not rely on external verification, it still provides encryption and server authentication, ensuring that VPN clients can securely connect to the FortiGate VPN server. By verifying the identity of the server using this certificate, the risk of man-in-the-middle attacks and identity-based threats is mitigated within controlled environments.

The use of strong cryptographic standards with the self-signed certificate enhances network security by ensuring:

- **Confidentiality** of transmitted data through encryption
- **Integrity** of data by protecting it from modification
- **Authentication** of the VPN server before users can connect

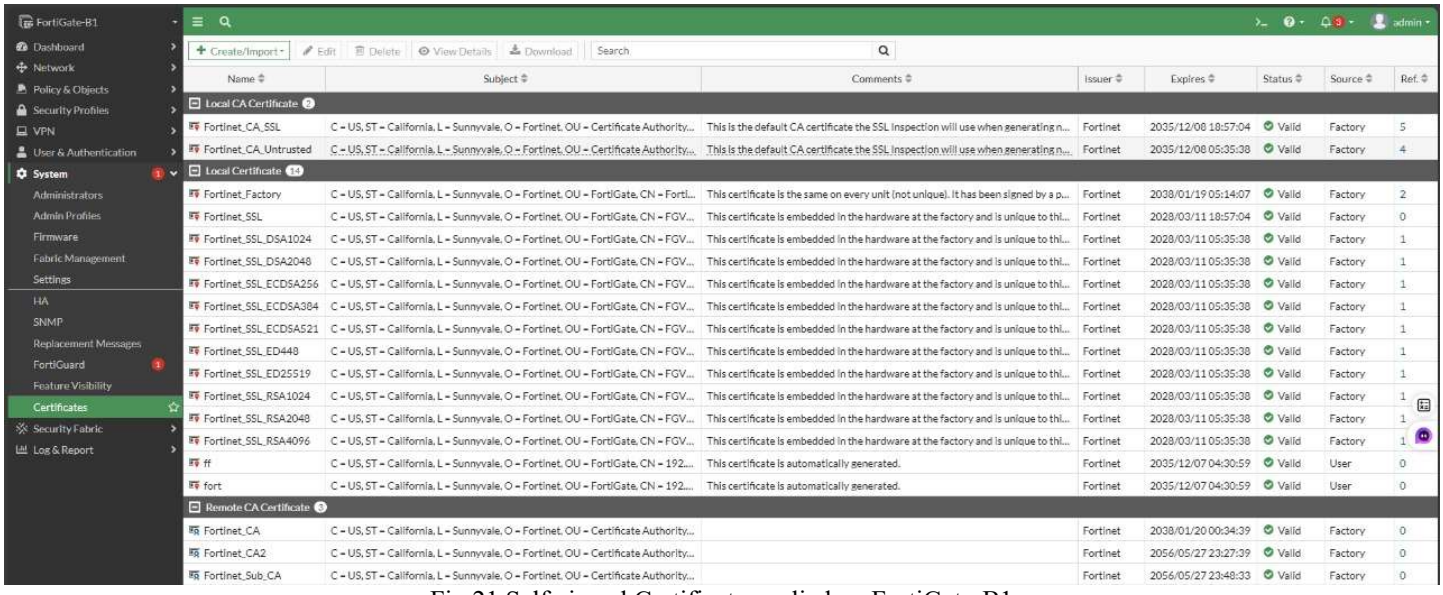


Fig.21 Self-signed Certificate applied on FortiGate-B1

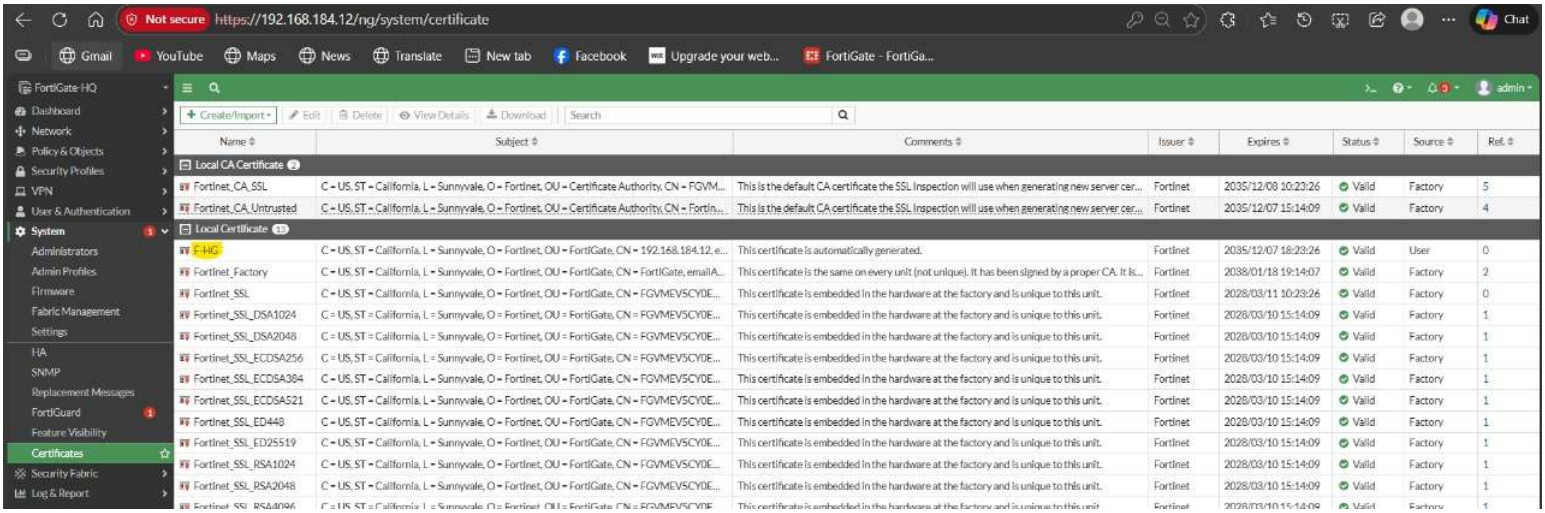


Fig.22 Self-signed Certificate applied on FortiGate-HQ

Fig.23 Self-signed Certificate settings

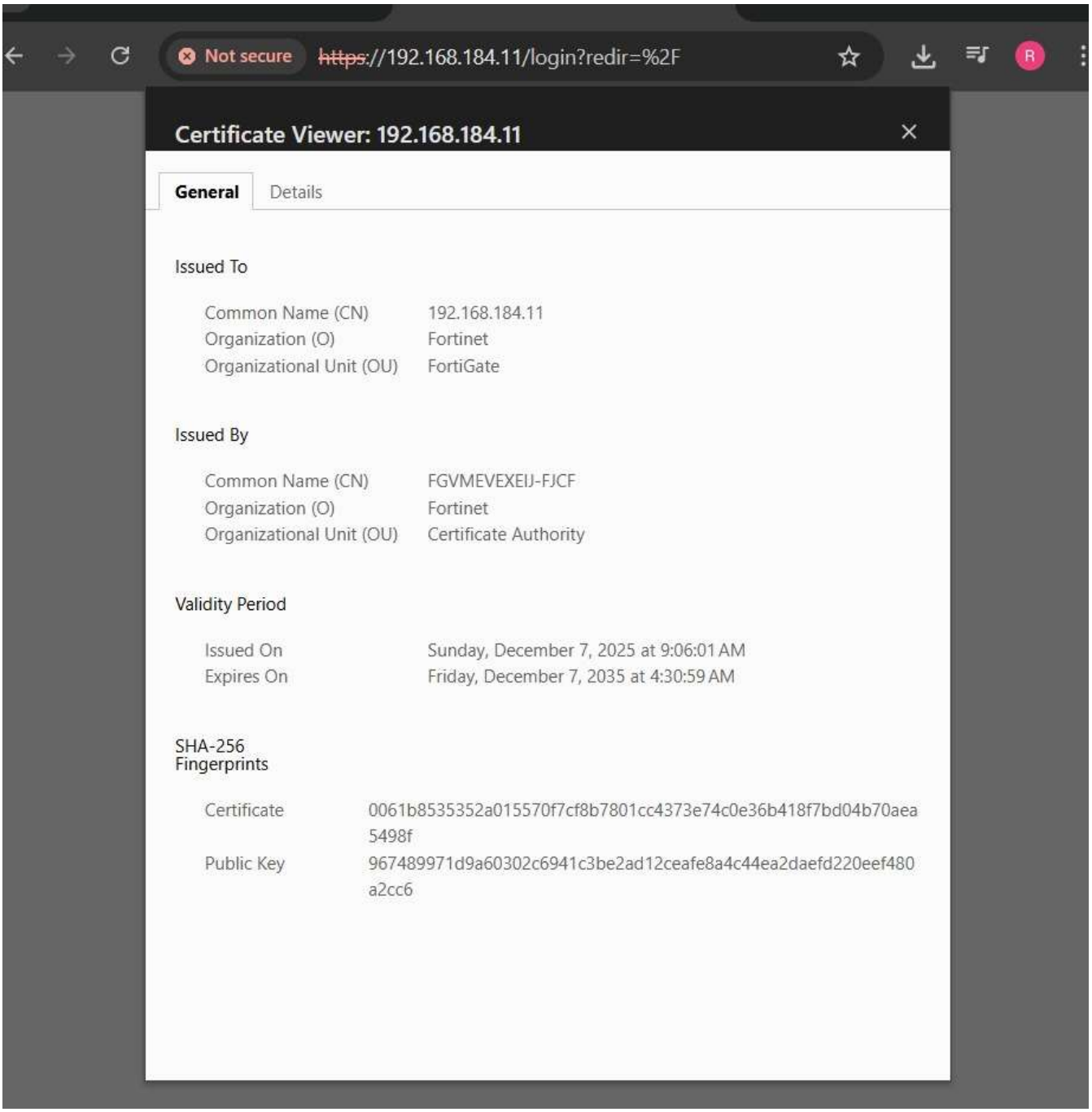


Fig.24 Self-signed FortiGate-B1
Certificate Properties

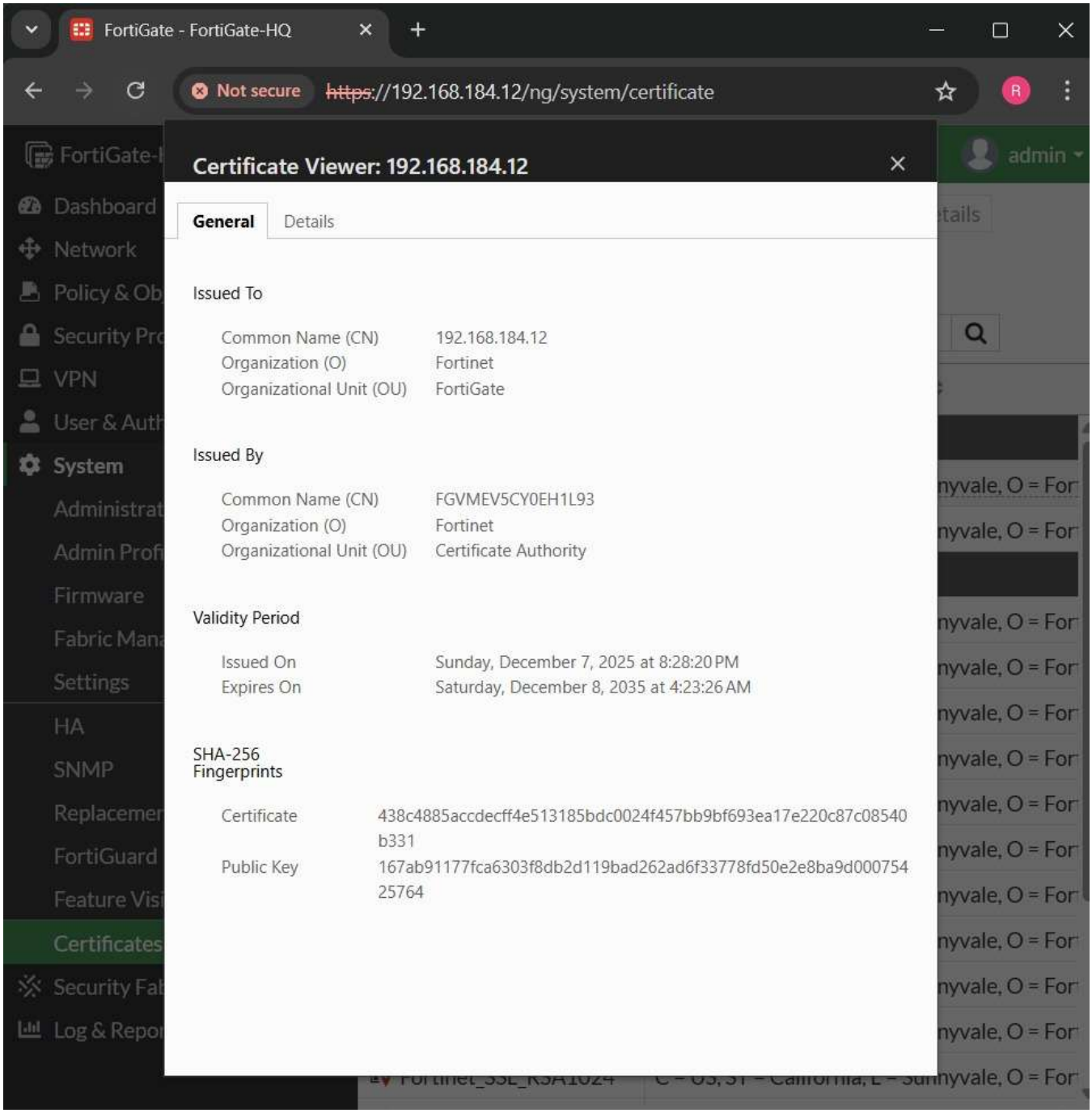


Fig.25 Self-signed FortiGate-HQ
Certificate Properties

12. FortiGate and LDAP Integration

Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry-standard application protocol for accessing and maintaining distributed directory information services over an IP network. A directory service is a network service that stores information about network resources (such as users, groups, computers, printers, and shared folders) in a hierarchical structure.

1. LDAP Integration with FortiGate

FortiGate firewalls can integrate with LDAP servers (such as Microsoft Active Directory, OpenLDAP, or Novell eDirectory) to centralize user authentication and management. Instead of managing local user accounts on each FortiGate, administrators can leverage an existing LDAP directory. This simplifies administration, enhances security through centralized policy enforcement, and allows for user-based firewall policies.

2. Benefits of Using LDAP with FortiGate

Centralized User Management: Manage all user credentials and attributes in a single directory service.

Simplified Authentication: Users authenticate once to the directory service, which then grants access to FortiGate resources.

User-Based Policies: Create granular security policies based on individual users or groups defined in the LDAP directory.

Enhanced Security: Enforce strong password policies and audit user access centrally.

Improved Efficiency: Reduce administrative overhead compared to managing separate user accounts on the firewall.

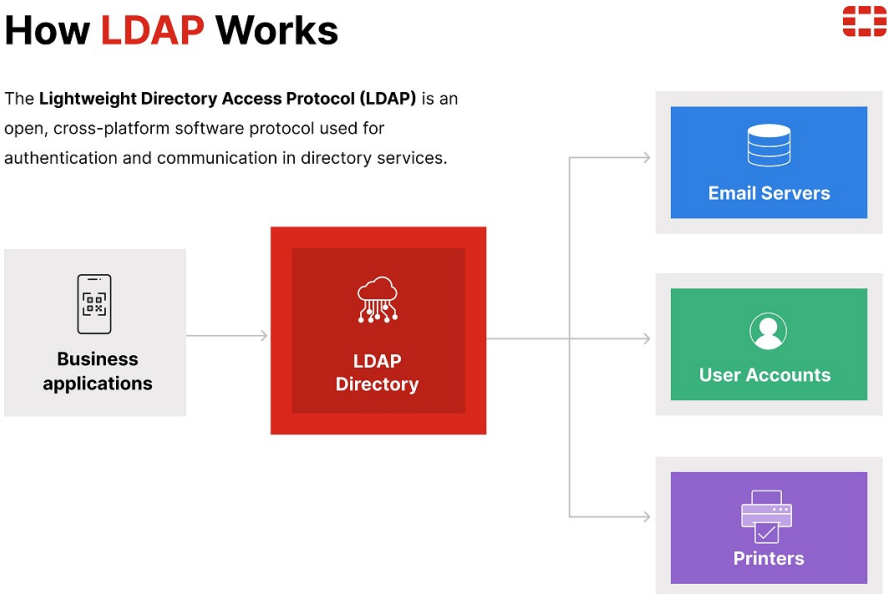


Fig.26 LDAP illustration

3. General Configuration Steps on FortiGate

Configuring LDAP on a FortiGate typically involves the following high-level steps:

A. Create LDAP Server Entry:

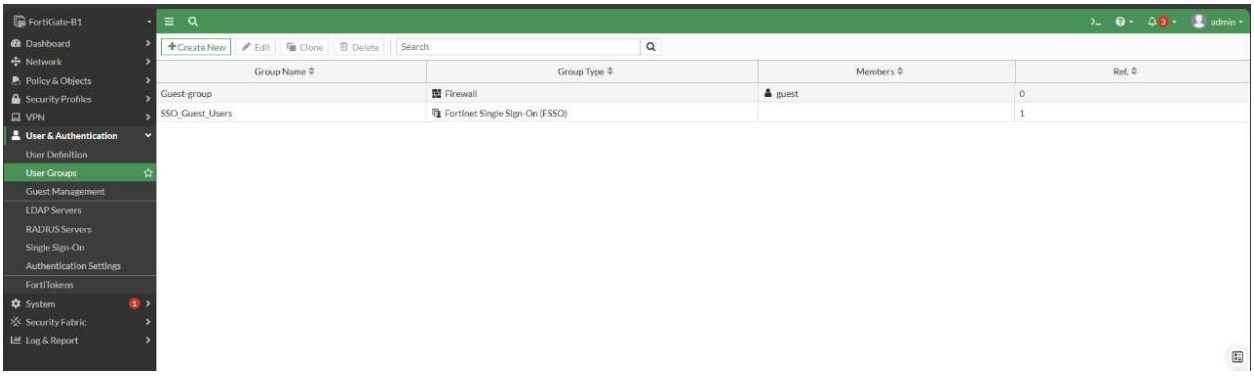
Navigate to User & Device > LDAP Servers and create a new server profile. You will need to specify:

- Server Name
- IP Address or FQDN of the LDAP server
- Port (usually 389 for standard LDAP)
- Common Name (CN) identifier for the FortiGate to bind to the LDAP server (an existing user account with read permissions is often used)
- Password for the bind user
- Distinguished Name (DN) for the bind user
- Base DN for searching users and groups

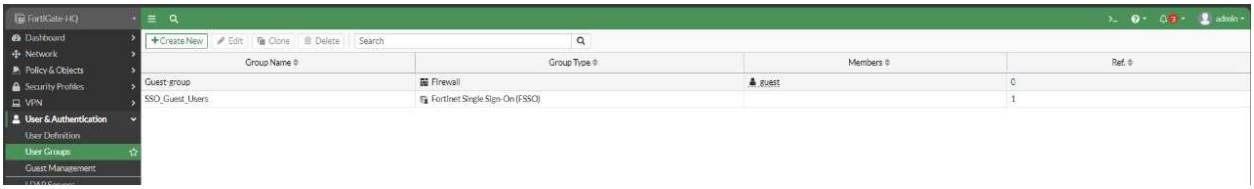
Fig.27FortiGate-B1LDAP Server

B. Configure User Groups:

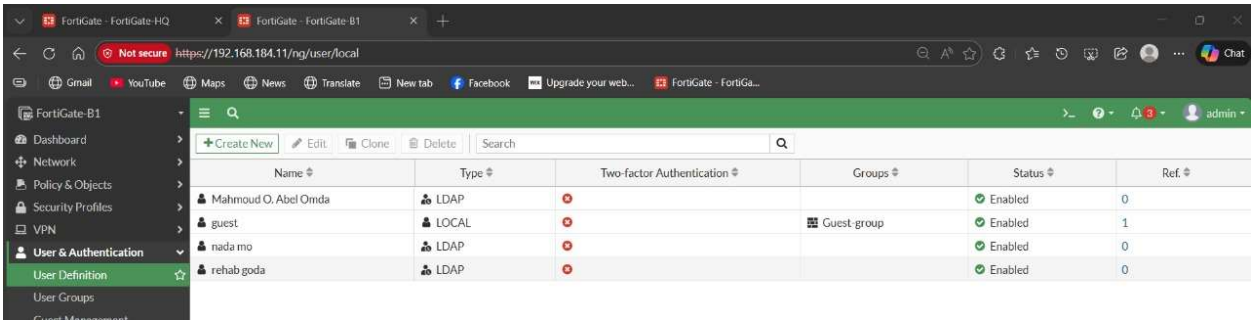
- Go to User & Device > User Groups and create a new group.
- Select 'Firewall' as the Type and choose the configured LDAP server.
- You can then filter users from the LDAP server to include in this FortiGate user group based on LDAP search filters



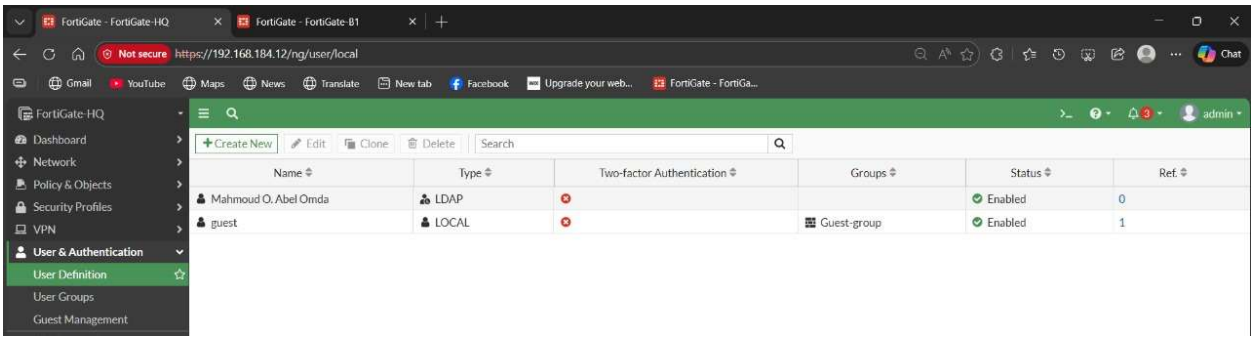
FortiGate-B1User Groups



FortiGate-HQ User Groups



FortiGate-B1 Users



FortiGate-HQ Users

13. Domain Controller (DC)

1. Introduction

A Domain Controller (DC) is a specialized server responsible for managing network security, user authentication, and centralized administration within a Windows domain. It maintains a central database called Active Directory (AD), which stores user accounts, passwords, and computer information. The DC authenticates users and authorizes access to network resources, including files, printers, and applications.

Essentially, the Domain Controller serves as the backbone of an organization's IT infrastructure, ensuring that only authorized and authenticated users can access network resources.

2. Core Functions

- **Authentication and Authorization:** Validates user credentials during login and grants access permissions according to user roles and group policies.
- **Centralized Management:** Enables administrators to manage users, devices, and policies from a single interface via Active Directory.
- **Policy Enforcement:** Distributes and enforces **Group Policy Objects (GPOs)** that define security settings and user environment configurations.
- **Replication:** Synchronizes data across multiple Domain Controllers to maintain consistency and reliability in the network.
- **Resource Management:** Controls access to shared resources, such as folders, printers, and drives, based on user privileges.

3. Advantages of a Domain Controller

1. **Centralized Administration:** Streamlines the management of users, devices, and permissions in large networks.
2. **Enhanced Security:** Provides secure authentication through protocols like **Kerberos** and **NTLM**.
3. **Scalability:** Supports multiple Domain Controllers for redundancy and load balancing.
4. **User Convenience:** Enables **Single Sign-On (SSO)**, allowing users to access multiple network services with a single login.
5. **Policy Control:** Simplifies the application and updating of organizational policies across all users and computers.

4. Limitations of a Domain Controller

1. **Single Point of Failure (if not replicated):** If the sole DC fails, access to network resources and authentication may be disrupted.
2. **High Resource Requirements:** Requires adequate CPU, memory, and storage to efficiently process authentication requests.
3. **Complex Setup and Maintenance:** Configuring and managing Active Directory demands technical expertise.
4. **Security Risks:** A compromised DC could give attackers control over all network resources and credentials.
5. **Dependence on Network Connectivity:** Clients must be connected to the domain network for authentication and updates.

5. Significance in Networking

The Domain Controller is a fundamental component of enterprise networking, providing centralized user management, consistent security policies, and efficient resource allocation. When deployed in virtualized environments, such as **GNS3** or **VMware**, it allows IT professionals and students to simulate real-world networks, practice domain administration, and safely test security configurations and administrative policies.

Server Manager Interface in Windows Server

1. Dashboard

Offers a concise overview of server health, system performance, and critical alerts.

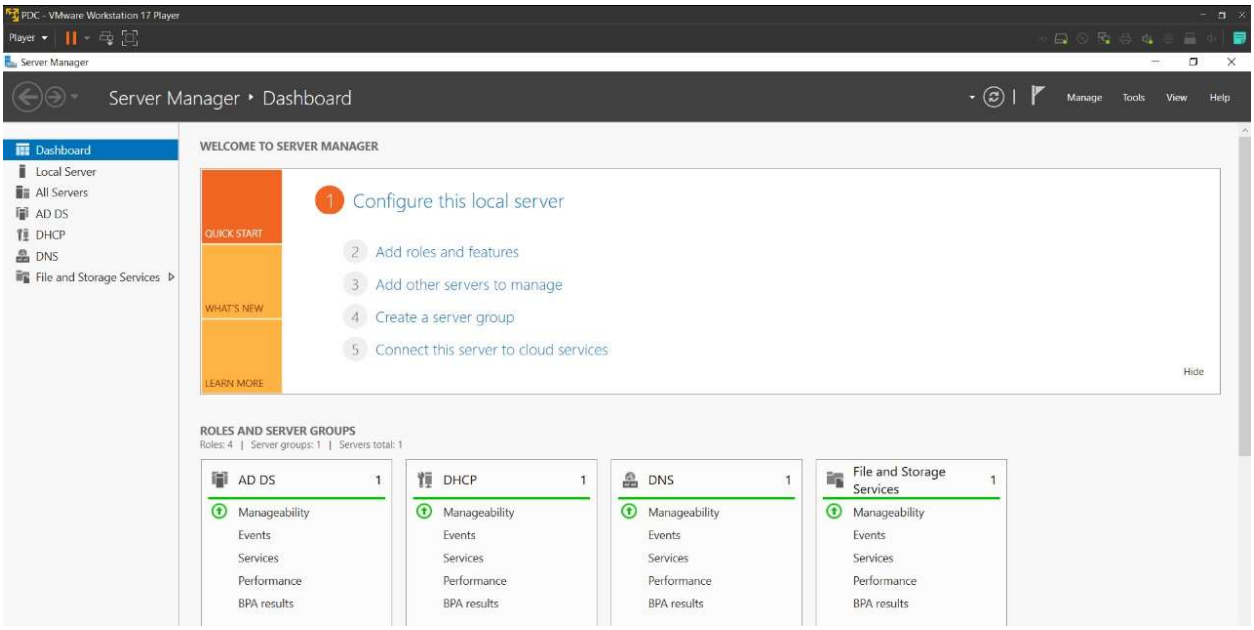


Fig.28 Dashboard in the domain controller

2. Local Server

Displays essential details and configurable settings of the currently managed server.

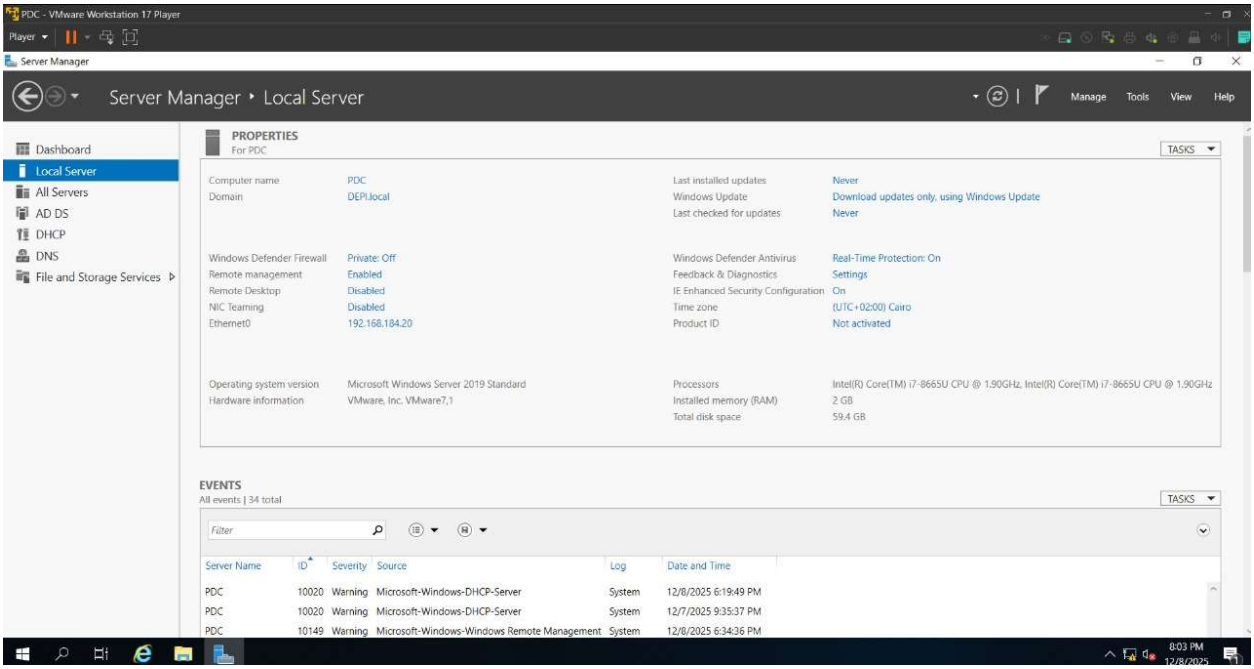


Fig.28 Dashboard in the domain controller

3. All Servers

Provides a list of all managed servers with their status for simplified monitoring.

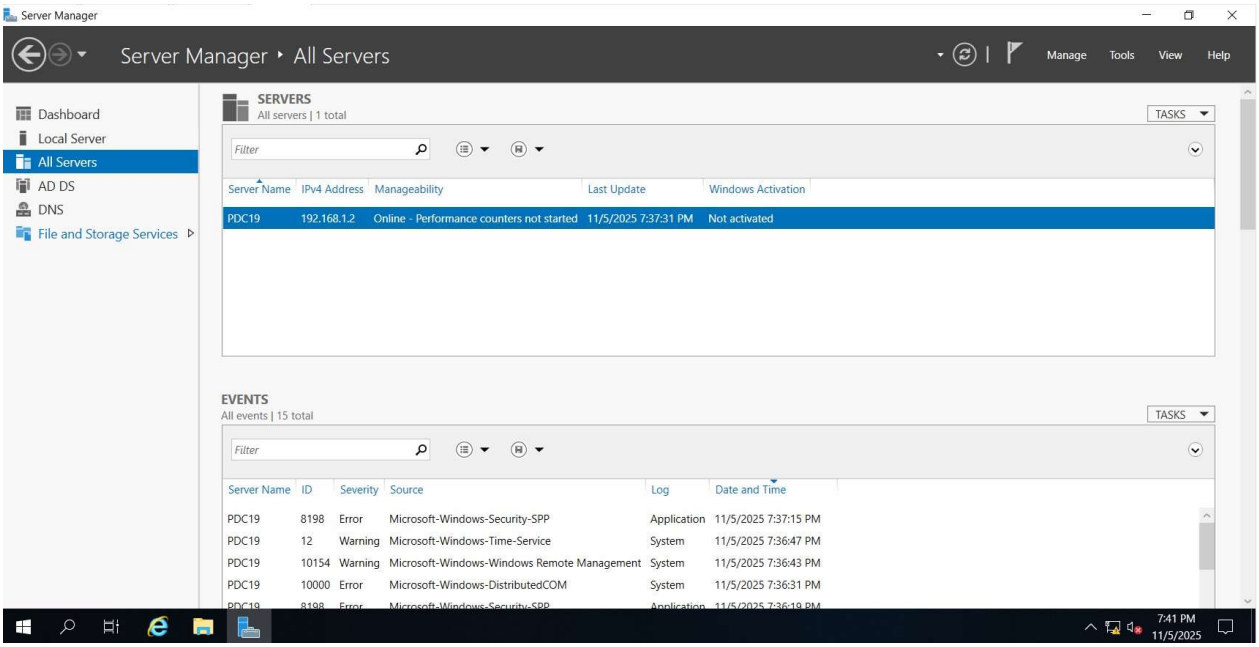


Fig.29 All servers in the domain controller

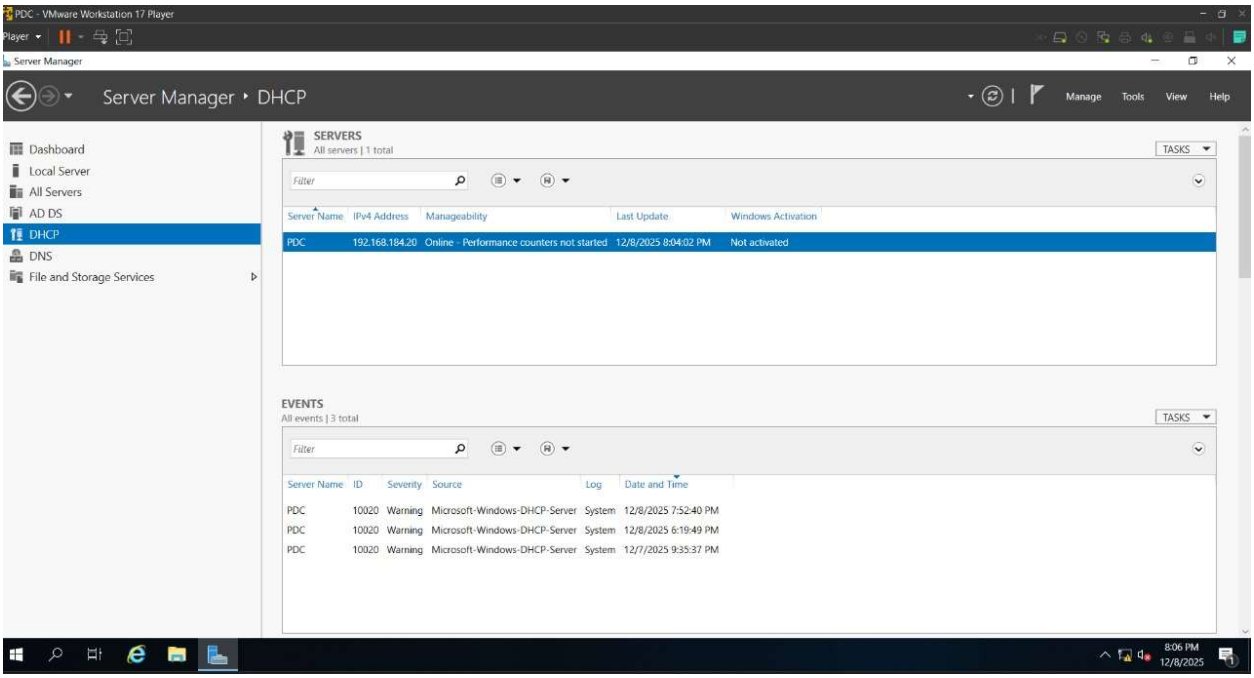


Fig.30 DHCP Server on the domain controller

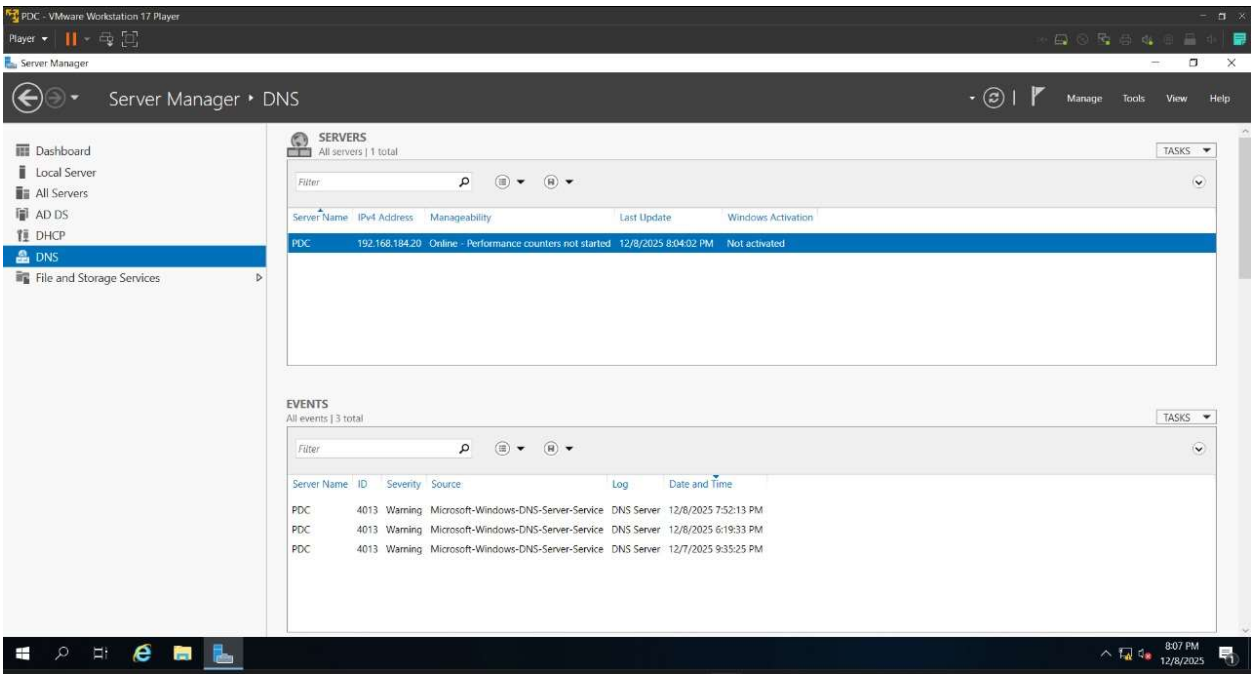


Fig.31 DNS Server on the domain controller

14. Deployment of Primary and Additional Domain Controllers

In this setup, two Domain Controllers are deployed to enhance reliability and ensure continuous availability of authentication services. The first server operates as the **Primary Domain Controller (PDC)**, responsible for hosting the initial Active Directory database and performing core domain operations. The second server functions as an **Additional Domain Controller (ADC)**, which holds a replicated copy of the Active Directory database and provides redundancy in case the primary controller becomes unavailable.

This dual-controller configuration increases fault tolerance, improves load distribution, and ensures seamless authentication and policy management across the network. By implementing both Primary and Additional Domain Controllers, the domain infrastructure achieves higher stability, better performance, and greater resilience against system failures.

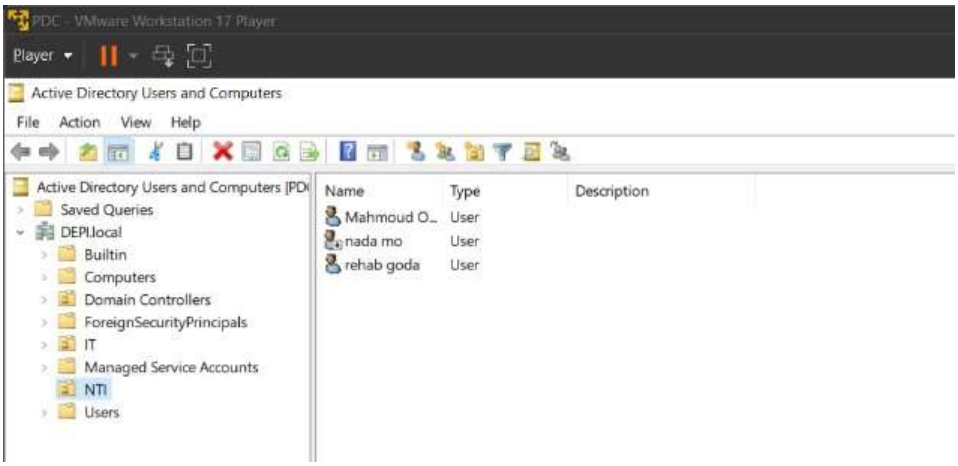


Fig.32 PDC Active Directory Users & Computers

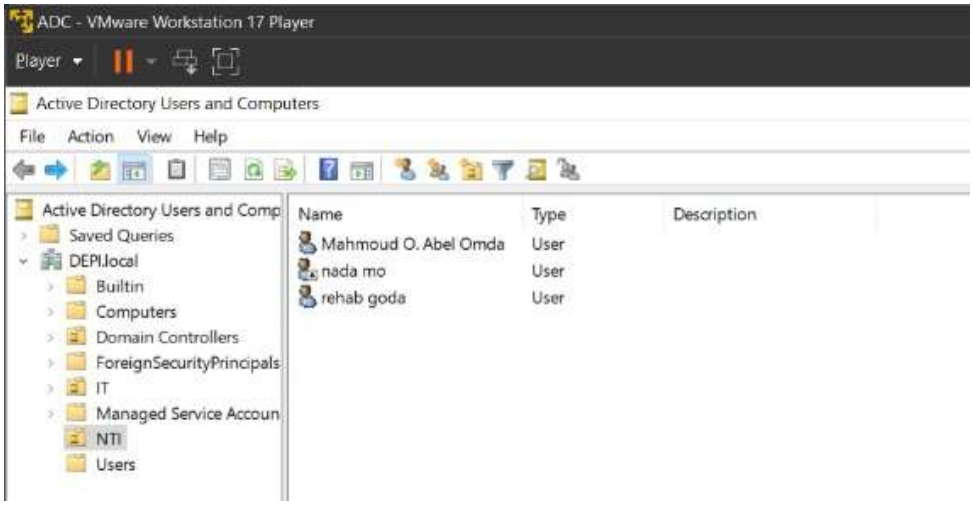


Fig.33 ADC Active Directory Users & Computers

15. Dynamic Host Configuration Protocol (DHCP) Server

1. Introduction

A Dynamic Host Configuration Protocol (DHCP) Server is a network server responsible for automatically assigning IP addresses and other essential network configuration parameters to devices (clients) on a network. By automating IP address allocation, DHCP eliminates the need for manual configuration, ensures efficient device communication, and minimizes network errors.
It is a key service in modern IP networks, simplifying administration and enhancing reliability.

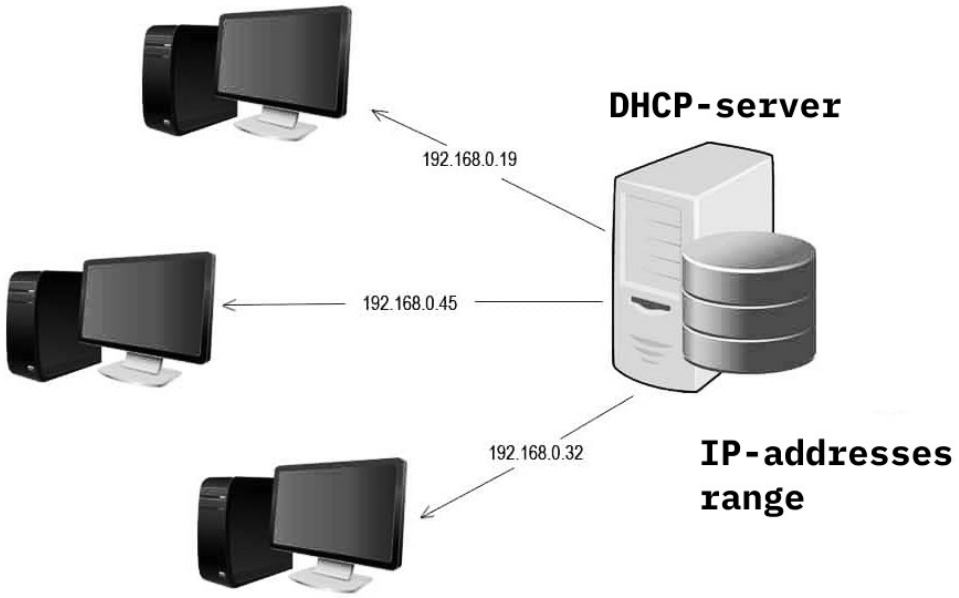


Fig.34 DHCP – server illustration

2. Key Functions of a DHCP Server

1. Automatic IP Address Assignment

O Dynamically provides unique IP addresses to devices, preventing conflicts.

2. Subnet Mask and Gateway Configuration

O Delivers the correct subnet mask and default gateway to clients for proper network routing.

3. DNS Server Assignment

O Configures clients with DNS server addresses to enable domain name resolution.

4. Lease Management

O Allocates IP addresses for a specific period (lease) and reclaims them when devices disconnect.

5. Centralized Network Management

o Simplifies administration by managing all IP address allocations from a single interface.

3. Advantages of Using DHCP

1. **Efficiency:** Reduces manual IP configuration in large networks.
2. **Accuracy:** Minimizes IP conflicts and misconfigurations.
3. **Scalability:** Easily accommodates new devices joining the network.
4. **Flexibility:** Enables changes to addressing schemes without manually reconfiguring clients.

4. Considerations When Implementing DHCP

1. Properly plan the DHCP scope (address range) to prevent exhaustion.
2. Configure reservations for critical devices requiring static IPs.
3. Implement security measures to prevent unauthorized devices from accessing the network.

5. Install DHCP Server on a Domain Controller

1. Log in to the Domain Controller and launch Server Manager.

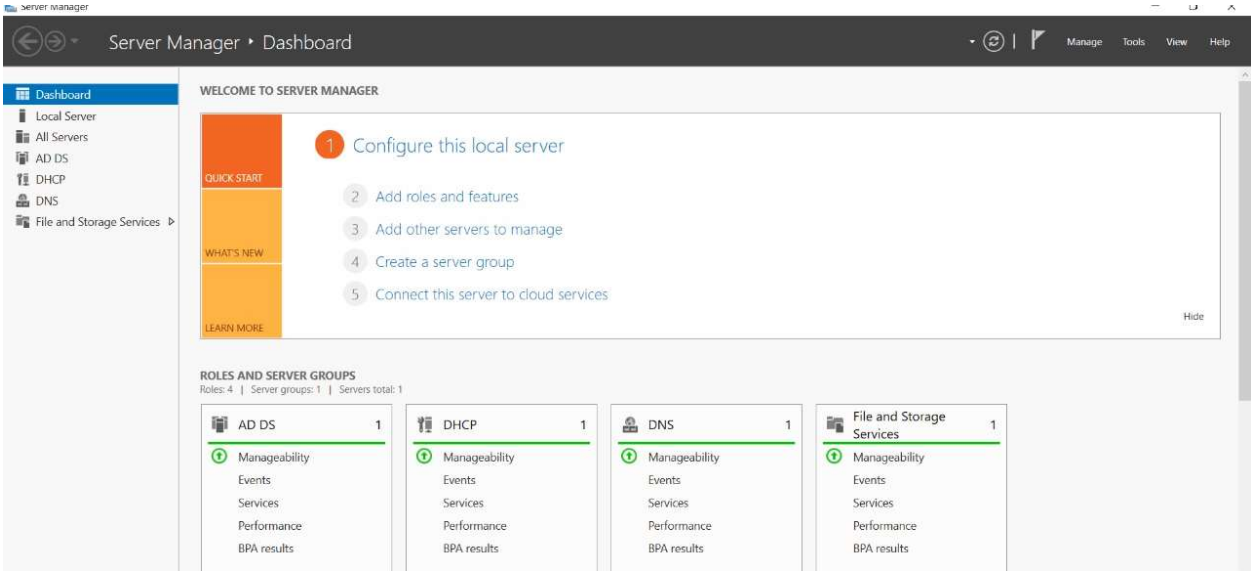


Fig.35 Log in to the domain controller

2. Navigate to **Manage → Add Roles and Features** to start the installation wizard.

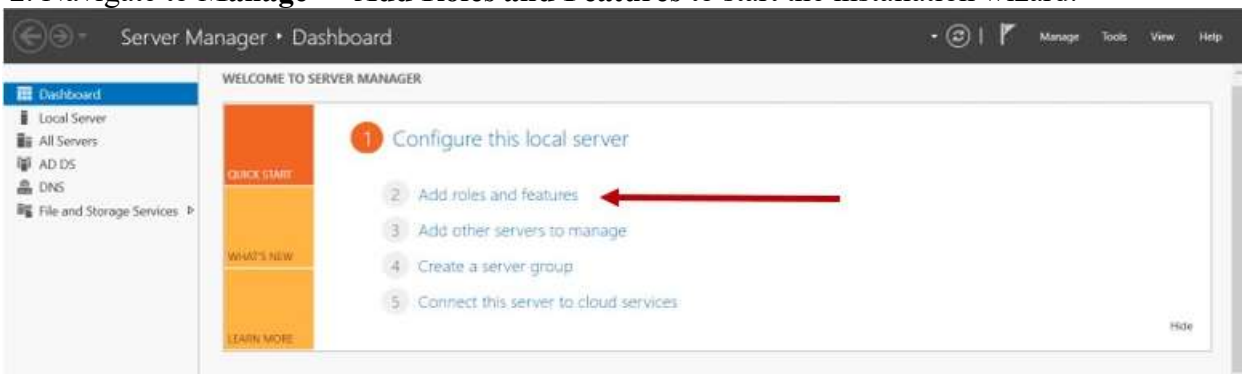


Fig.36 Start the installation wizard

3. Choose Role-based or feature-based installation and click Next

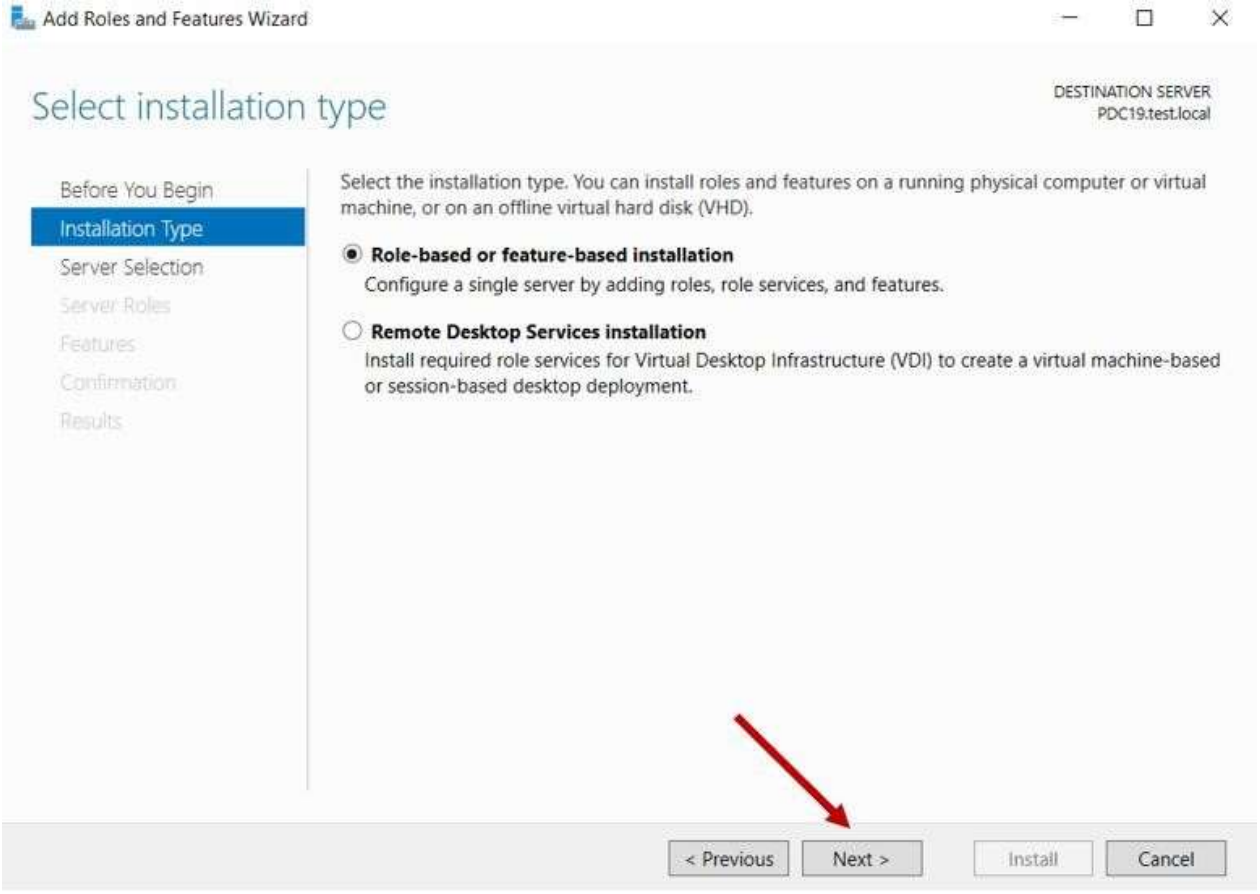


Fig.37 Role-based or feature-based installation

4. Select the local server from the server pool and proceed by clicking Next.

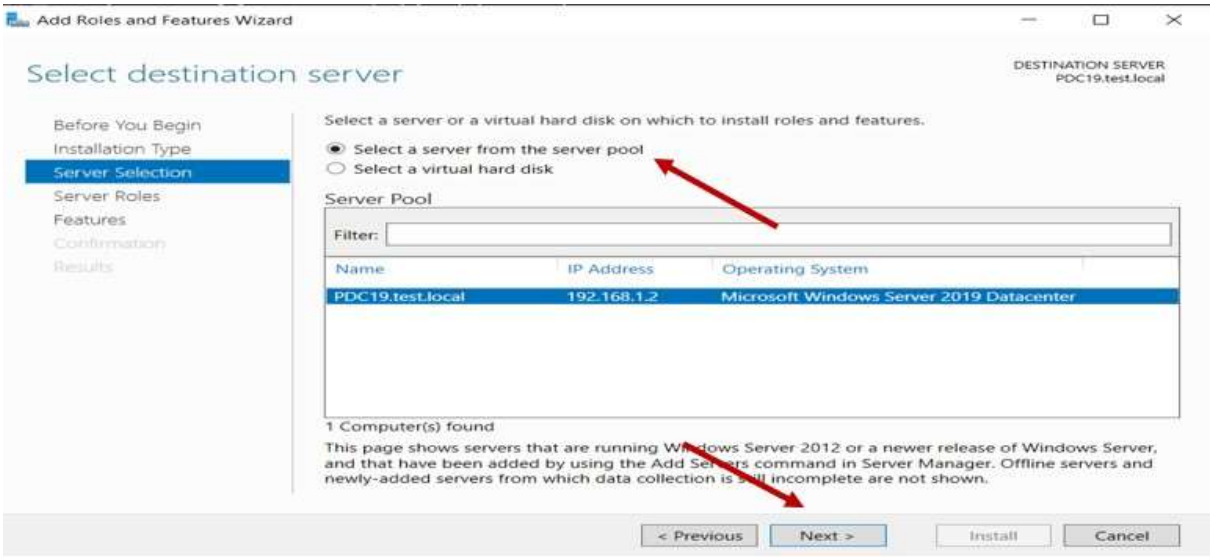


Fig.38 The local server from the server pool

5. Check DHCP Server in the roles list and click Add Features if prompted.

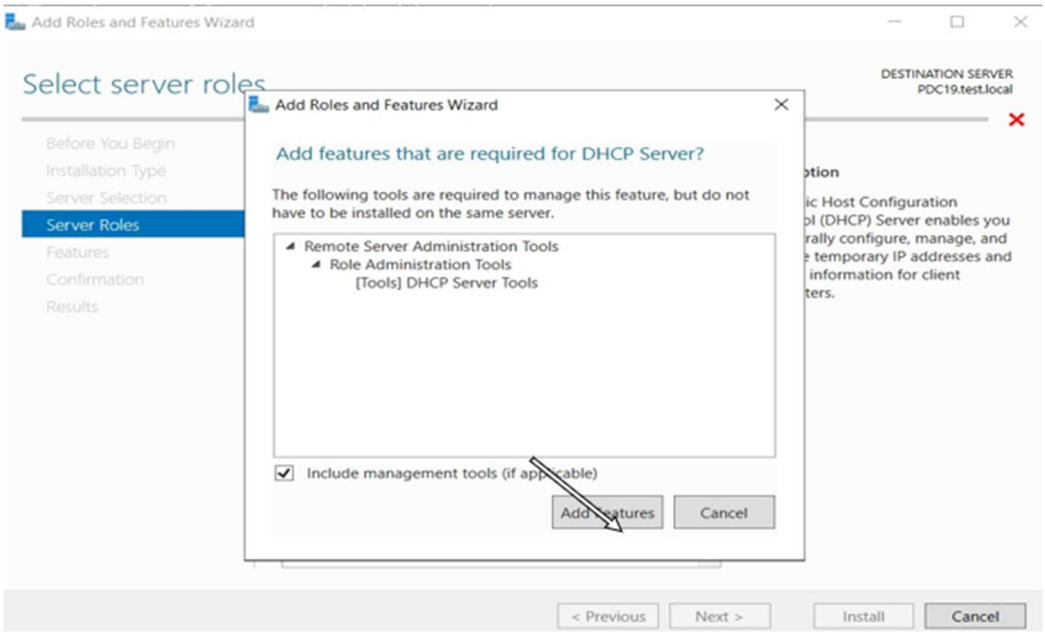


Fig.39 DHCP check in the roles list

6. Review the DHCP information page and click Next.

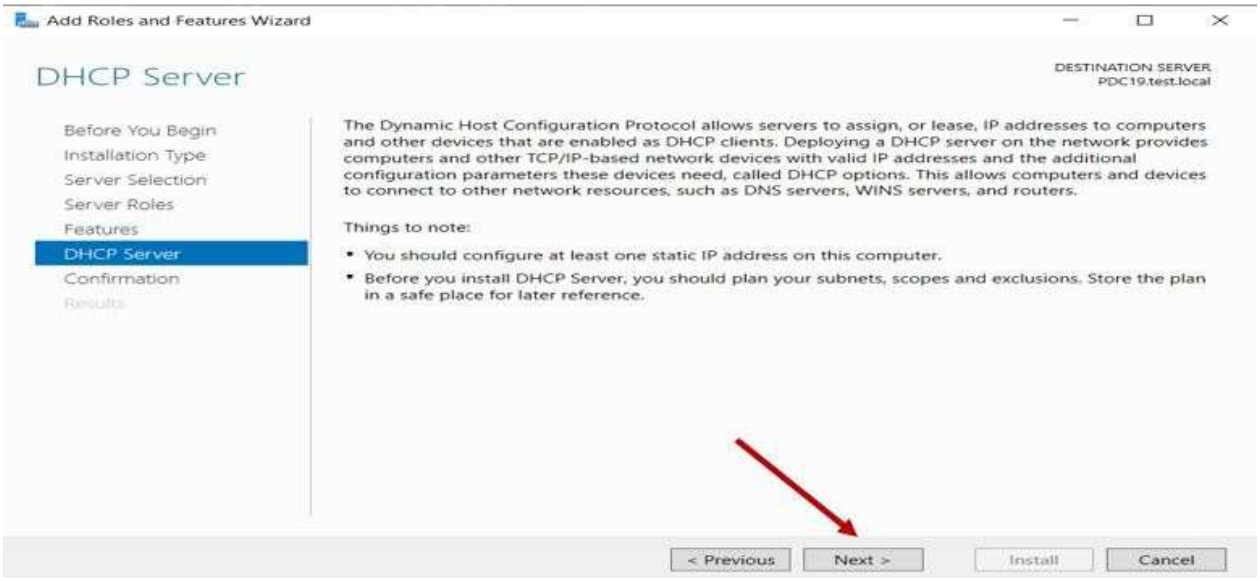


Fig.40 DHCP information page

7. Click Install to begin installing the DHCP Server role.

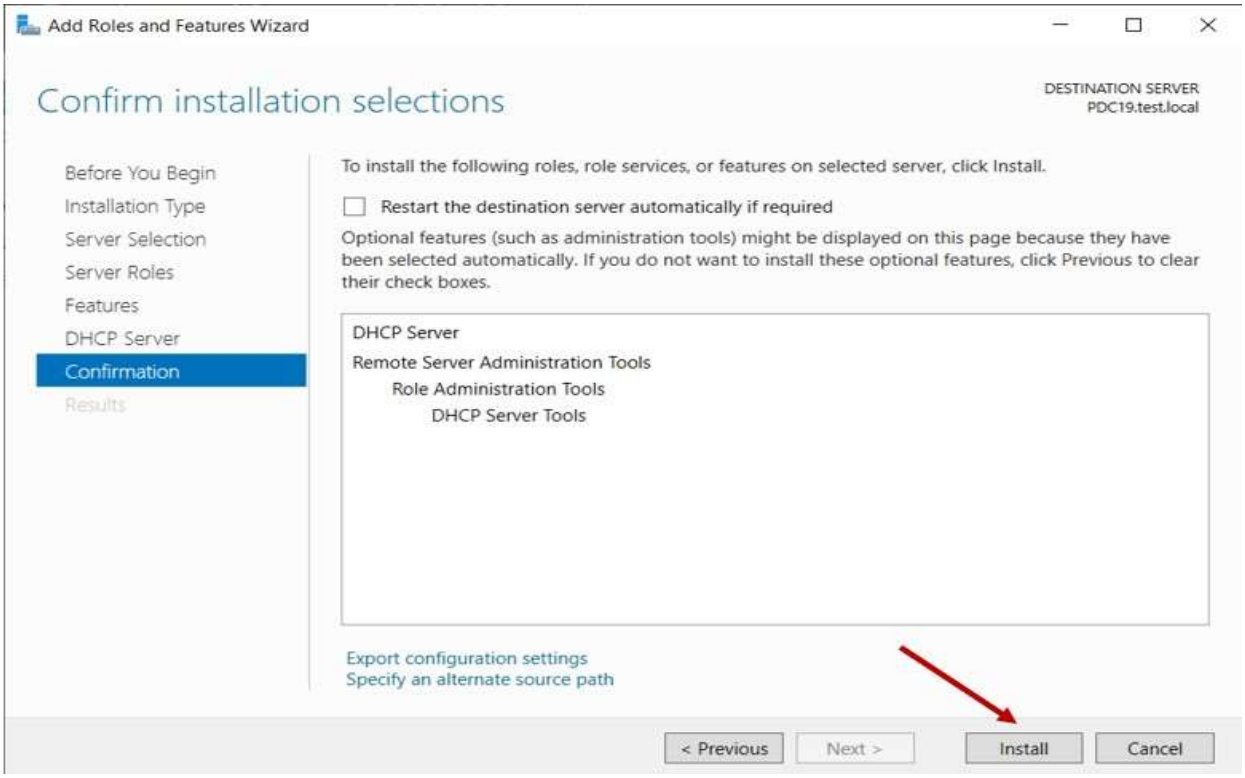


Fig.41 Installing the DHCP server role

8. After installation, select Complete DHCP Configuration in Server Manager.

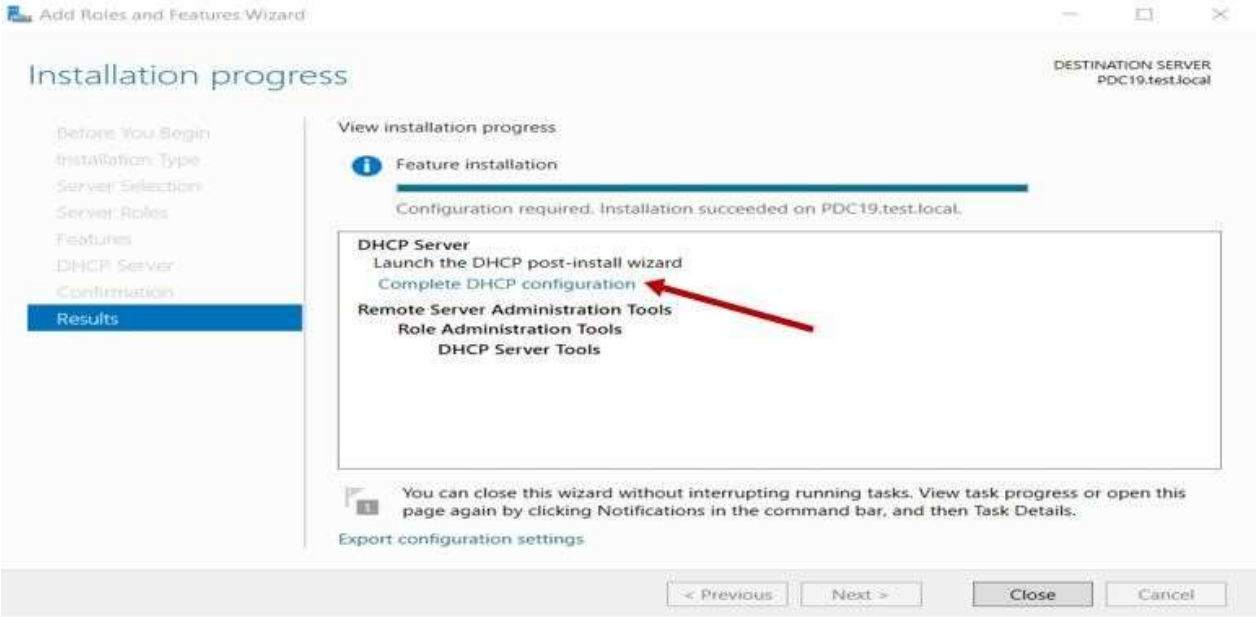


Fig.42 Complete DHCP configuration in server manager

A. Configure the DHCP Server

- On the DHCP Configuration Wizard page, click Next

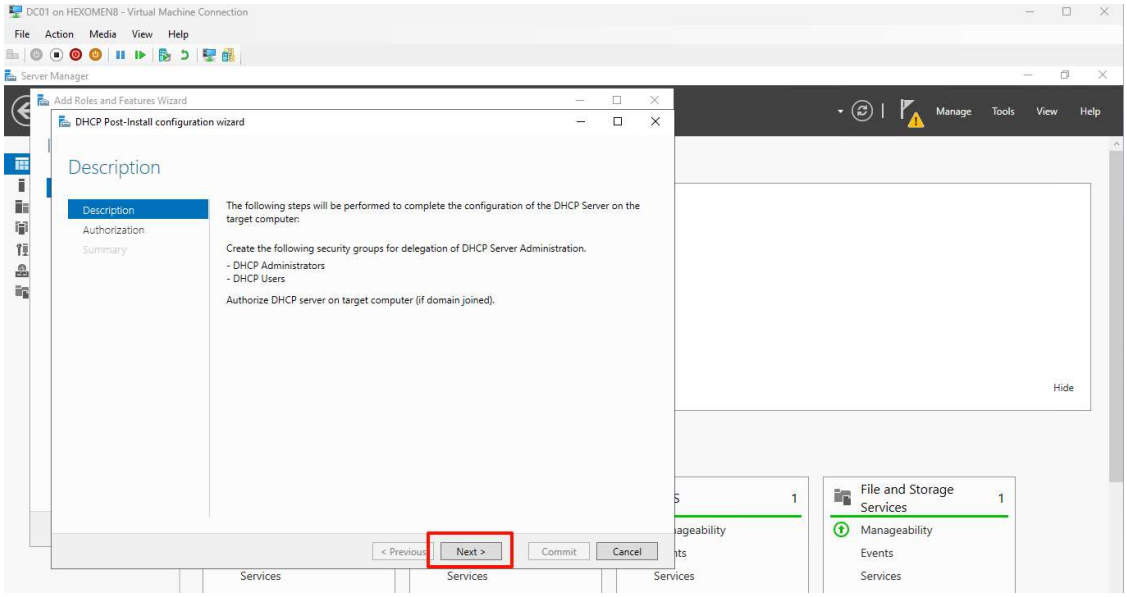


Fig.43 DHCP Configuration Wizard page

- Leave settings as default and click Commit to complete basic configuration

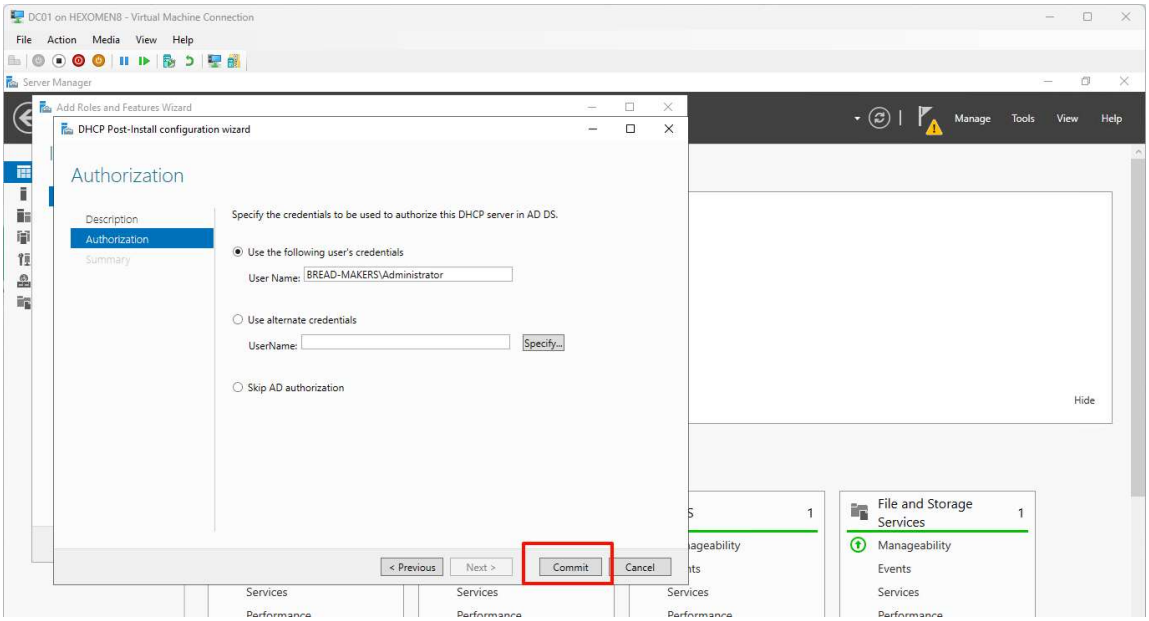


Fig.44 DHCP Basic Configuration

- After configuration, click Close to proceed to the next step

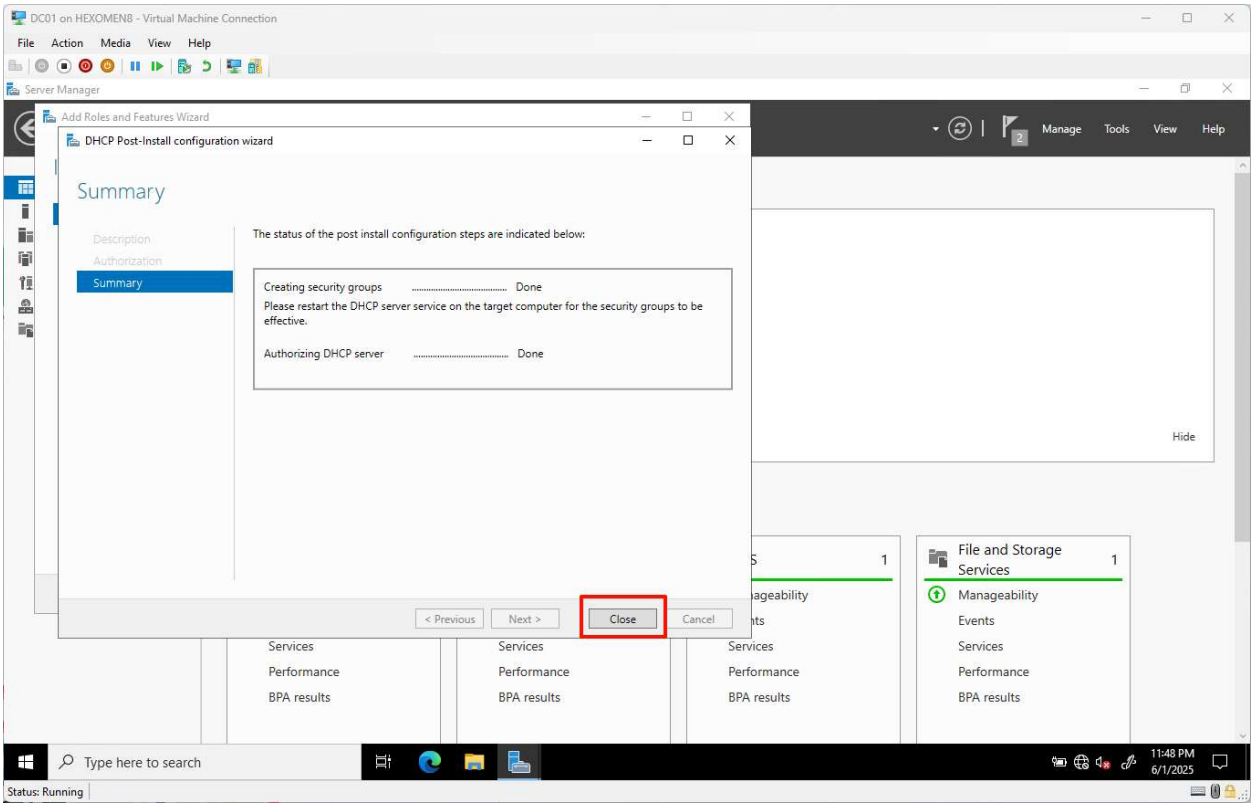


Fig.45 Follow DHCP Basic Configuration

B. Configure Primary DHCP Scope

- From the server console, open Tools -> DHCP

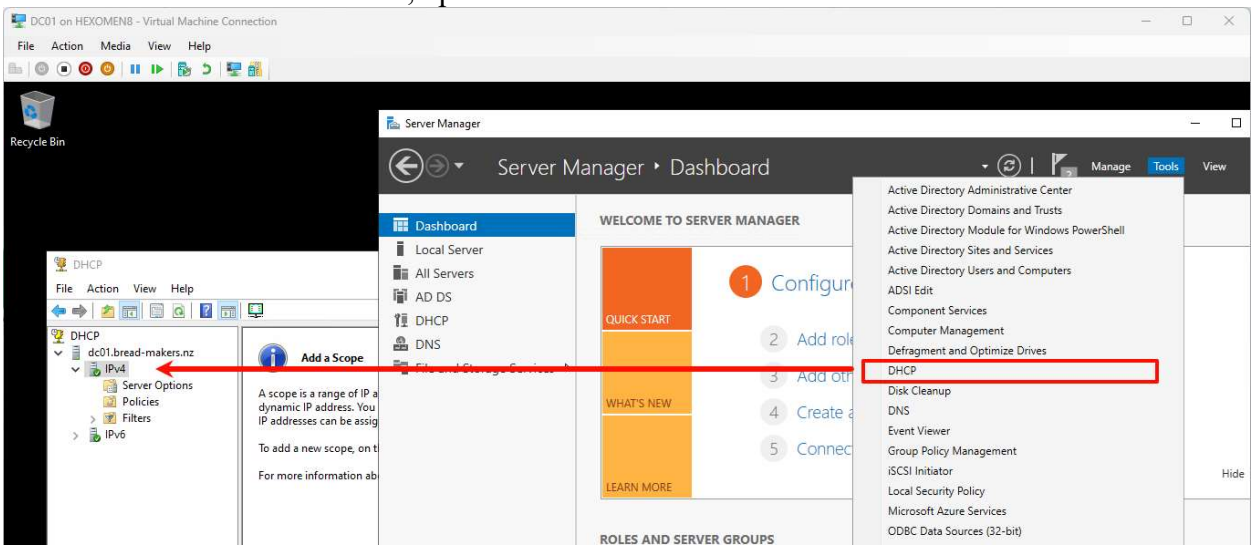


Fig.46 DHCP scope configuration step1

- Right-click on IPv4 and select New Scope to open the **New Scope Wizard**

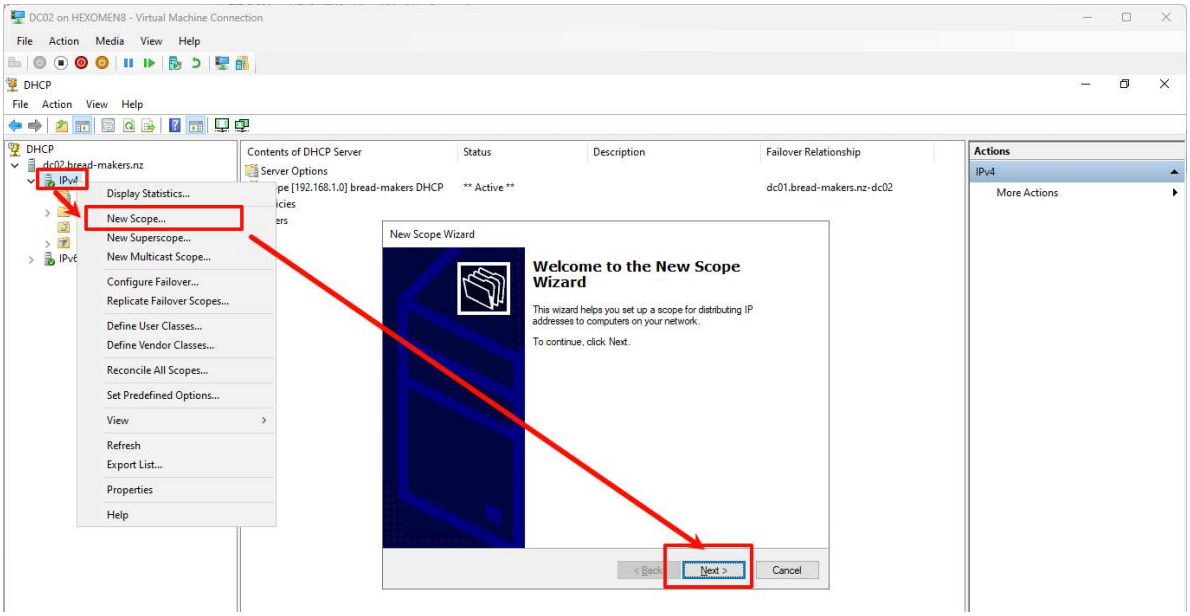


Fig.47 DHCP scope configuration step2

- Enter a scope name

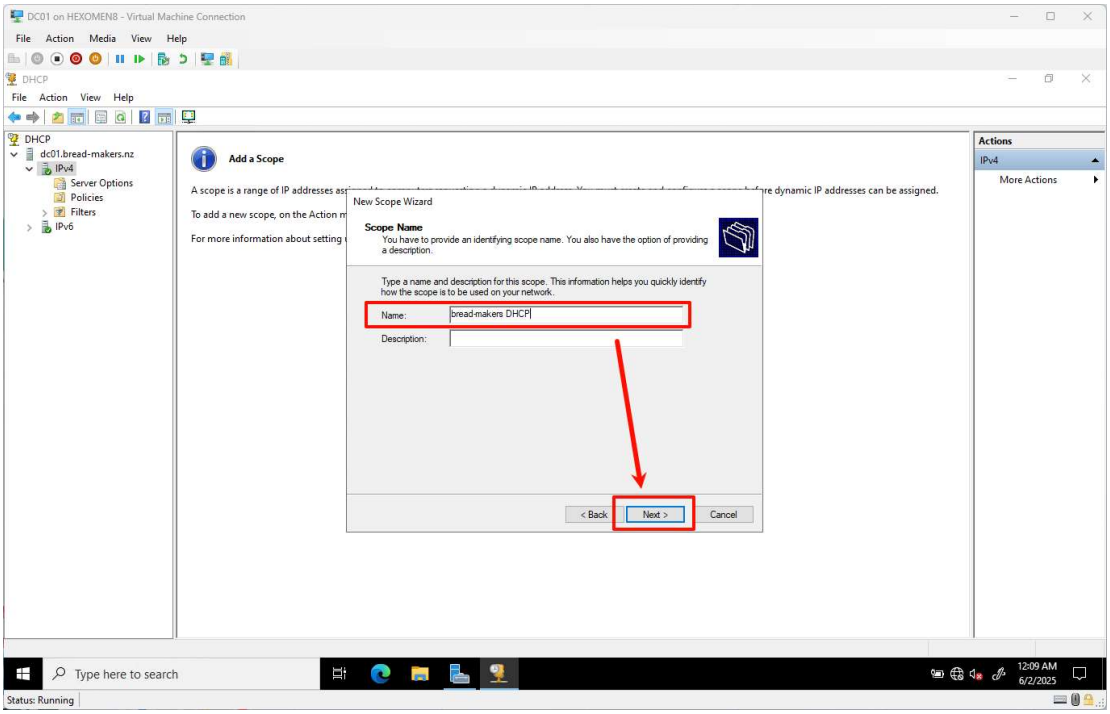


Fig.48 DHCP scope configuration step3

- Set the IP address range

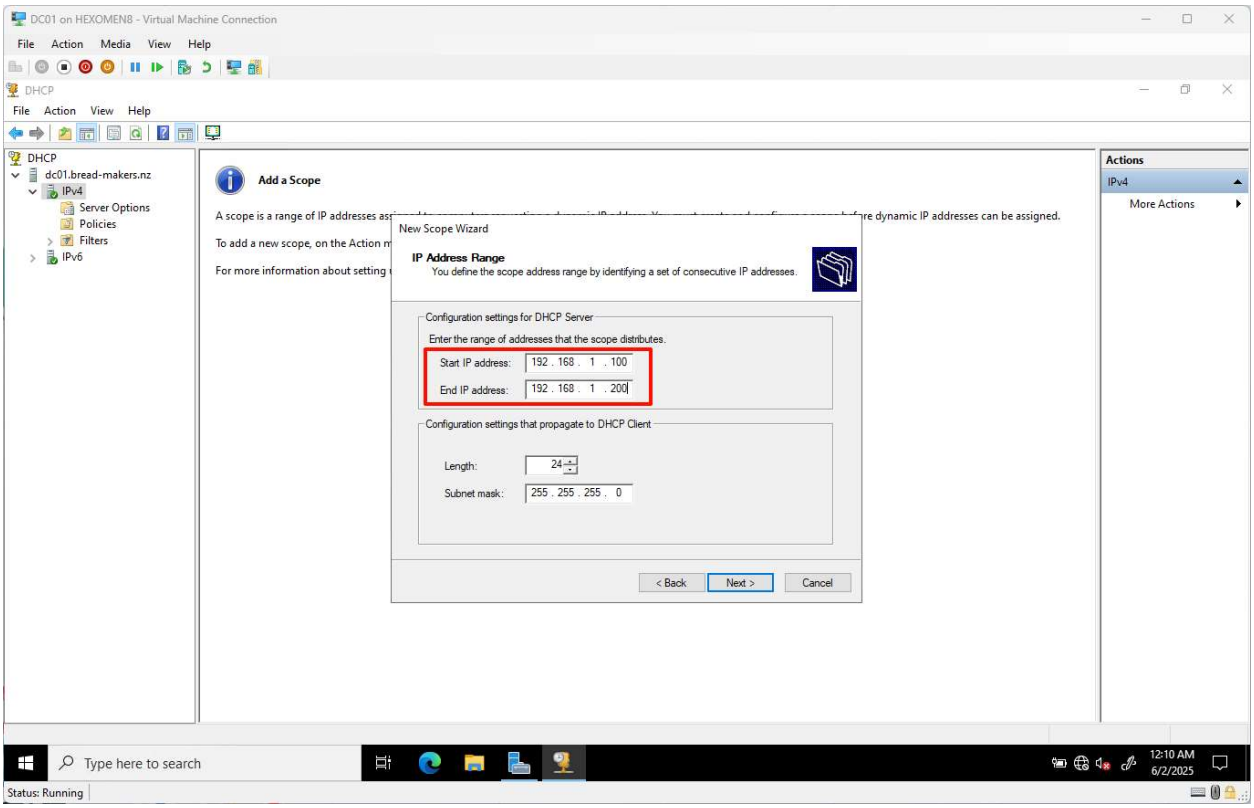


Fig.49 DHCP scope configuration step4

- Set the exclusion range : (This range is reserved for servers and other static devices) Click Add to include it in exclusions, then click Next

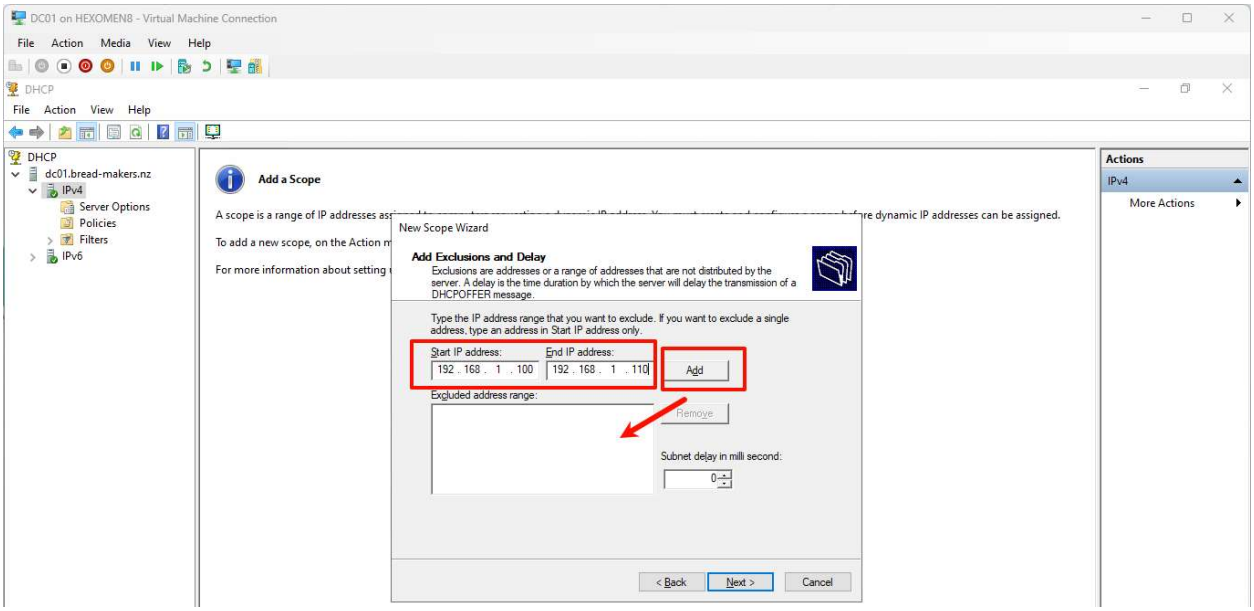


Fig.50 DHCP scope configuration step5

- Keep the lease duration at the default (8 hours), click Next

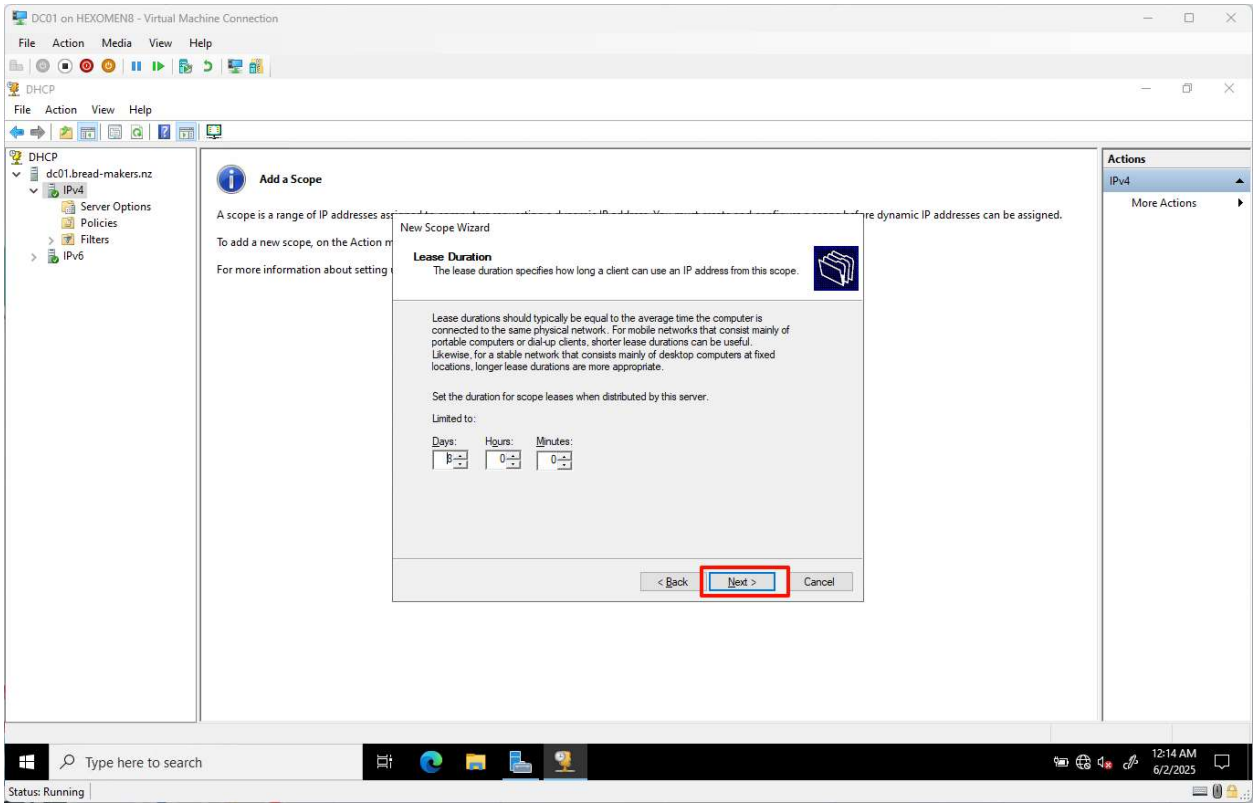


Fig.51 DHCP scope configuration step6

- Choose whether to configure DHCP options now – click Next

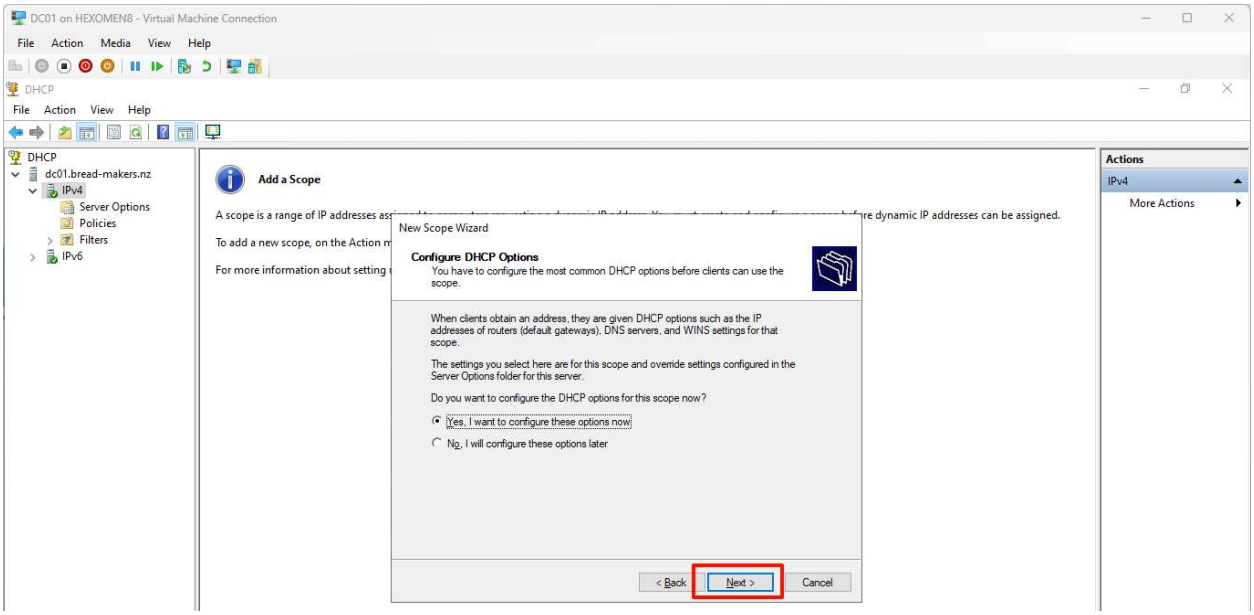


Fig.52 DHCP scope configuration step7

- Set the router (default gateway): Add both domain controller IPs as default gateways

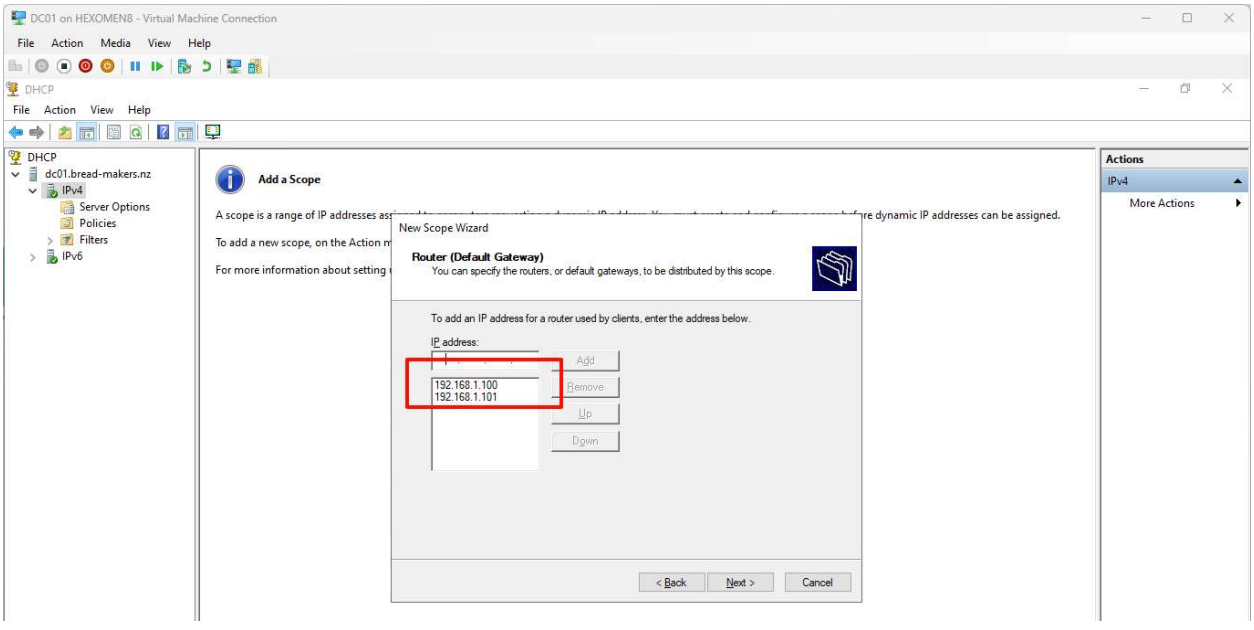


Fig.53 DHCP scope configuration step8

- Select to activate the DHCP scope, click Next

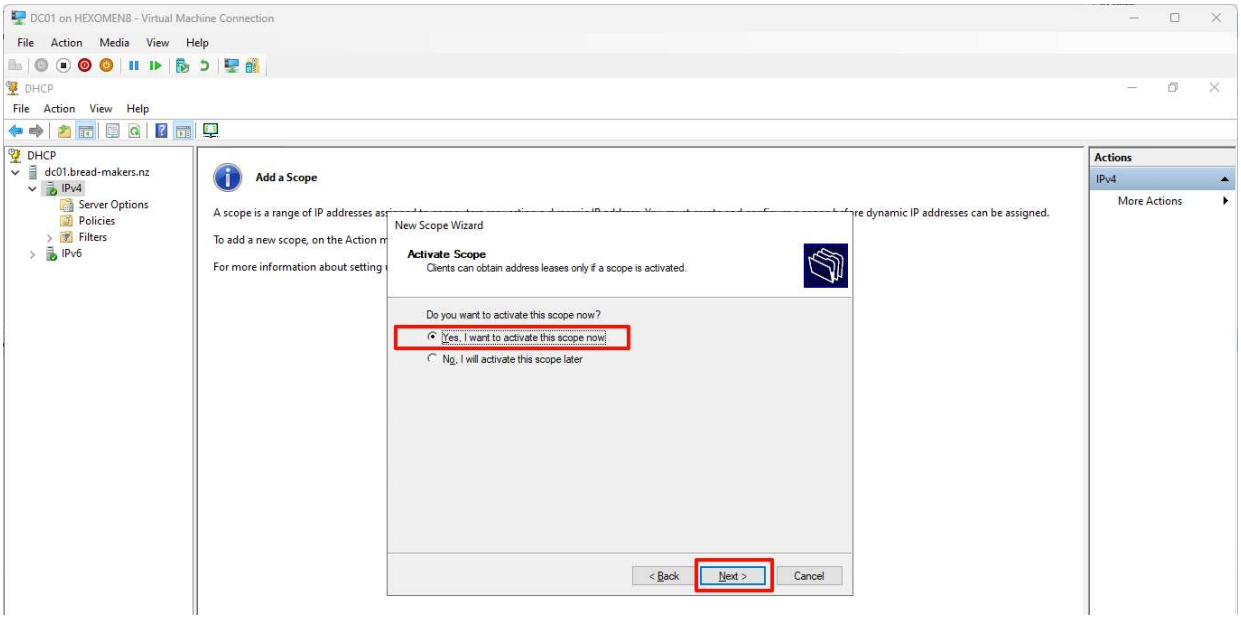


Fig.54 DHCP scope configuration step9

- **Verification Step**:

In the DHCP management interface, expand bread-makers DHCP -> Address Pool. You should see the successfully created IP range: 192.168.1.100 - 192.168.1.200.

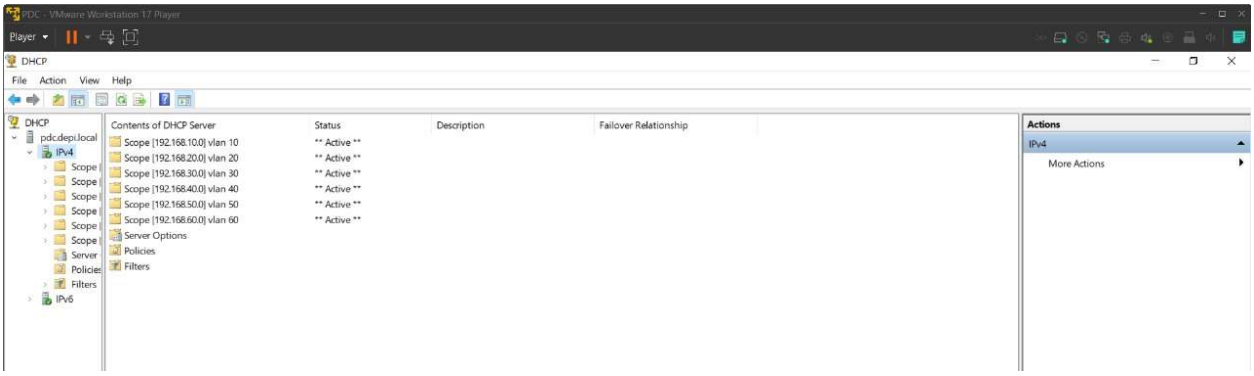


Fig.55 scopes

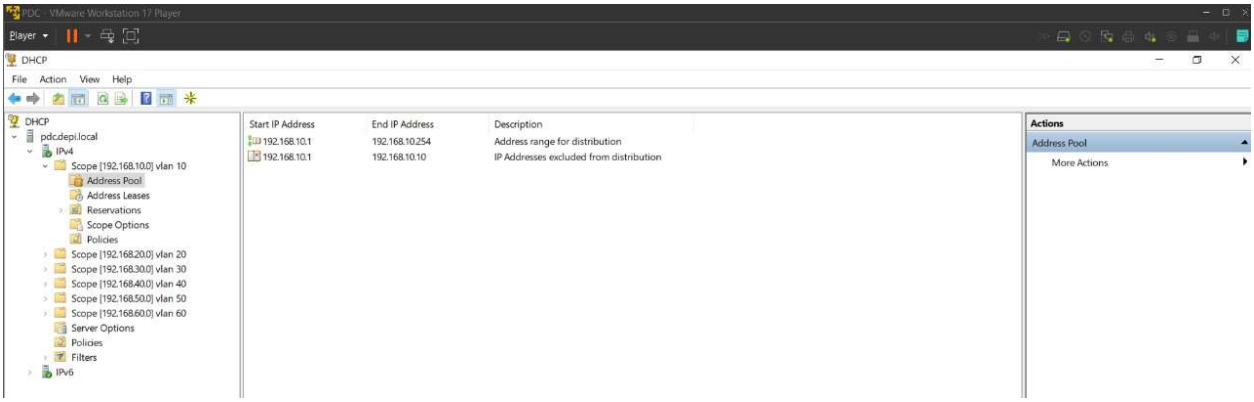


Fig.56 Address Pool

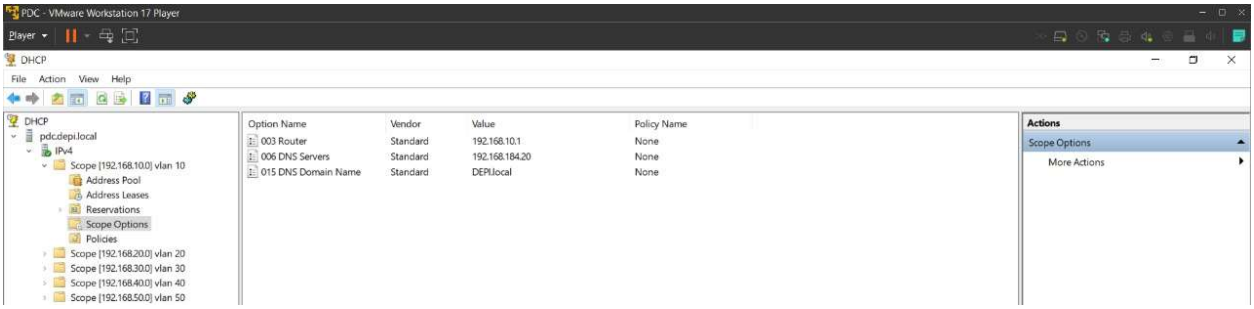


Fig.57 Scope Options

16. Configuring DNS on the Domain Controller

- **Install DNS Role:**
  Open "Server Manager" on your Windows Server.Click on "Manage" and then select "Add Roles and Features."Proceed through the wizard and select the "DNS Server" role under "Roles."

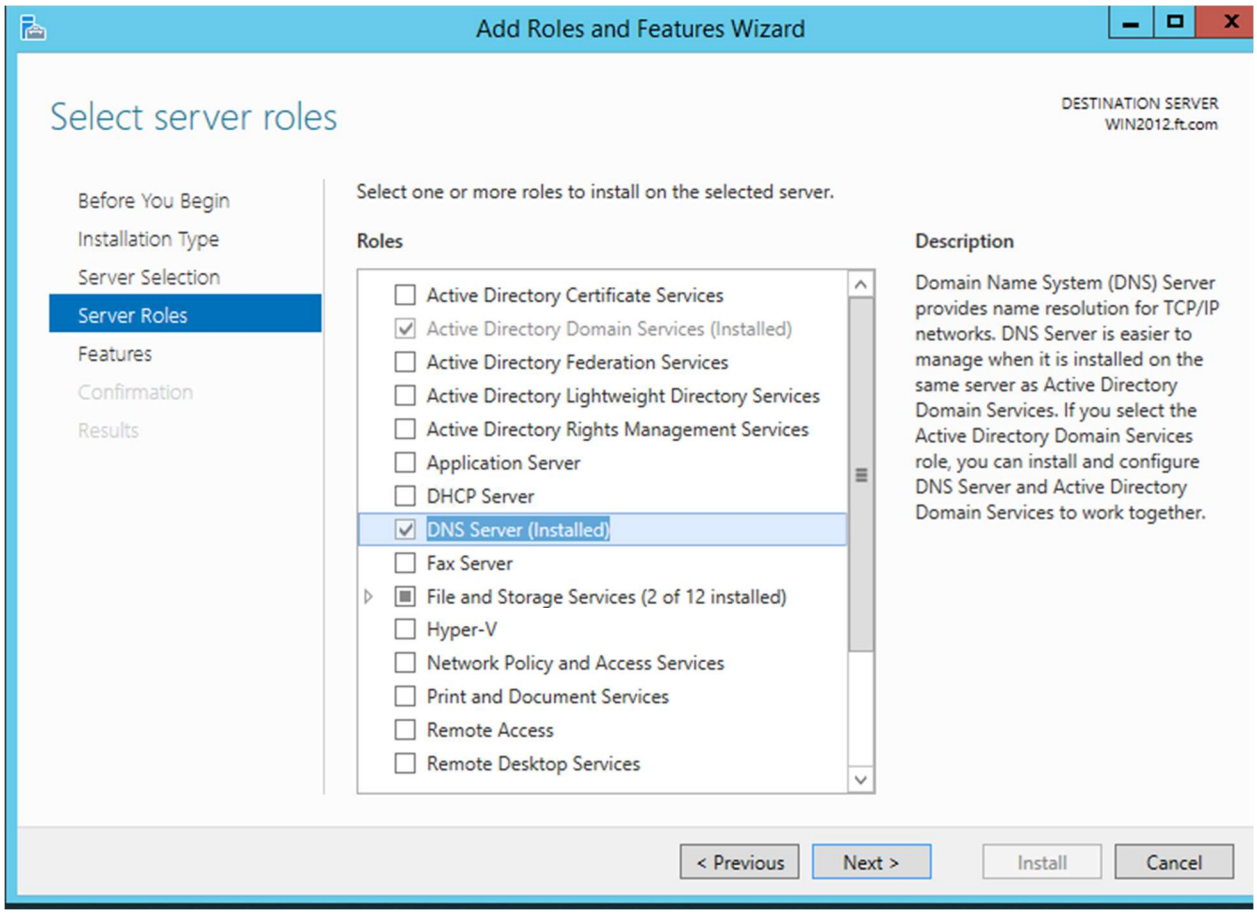


Fig.58 Install DNS Role

- **Initial Configuration:**

After the DNS role is installed, launch the "DNS Manager" from the Server Manager or by typing "dnsmgmt.msc" in the Run dialog.
Expand the server node in the left pane, right-click on "Forward Lookup Zones," and select "New Zone."
Follow the wizard to create a new primary zone for your domain (e.g- **ft.com**).

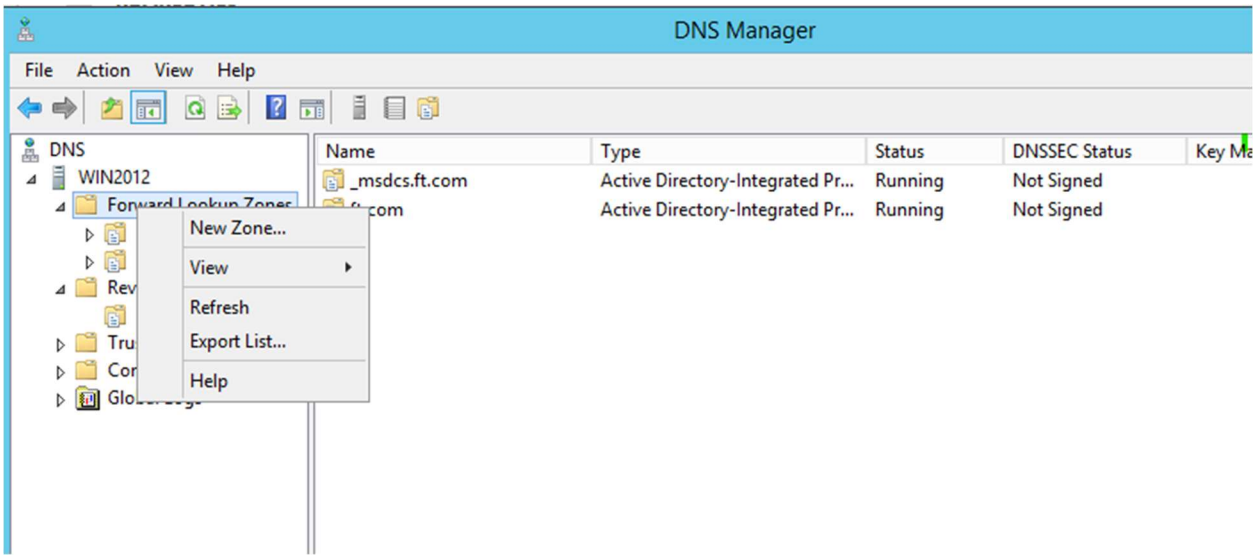


Fig.59 Initial Configuration

- **Forward and Reverse Lookup Zones:** Create both forward and reverse lookup zones for your domain. Forward lookup zones help resolve hostnames to IP addresses, while reverse lookup zones resolve IP addresses to hostnames.

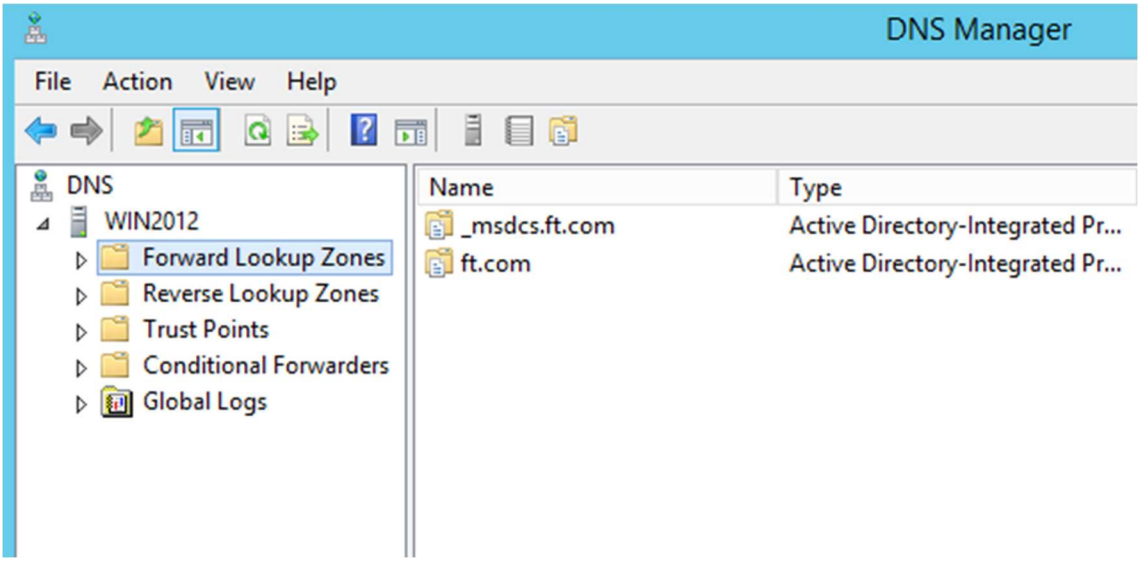


Fig.60 Forward and Reverse Lookup Zones

- **Zone Configuration:** Right-click on the zone you created and select "Properties."In the "General" tab, make sure the zone is set to "Active Directory-integrated." This allows for secure dynamic updates.

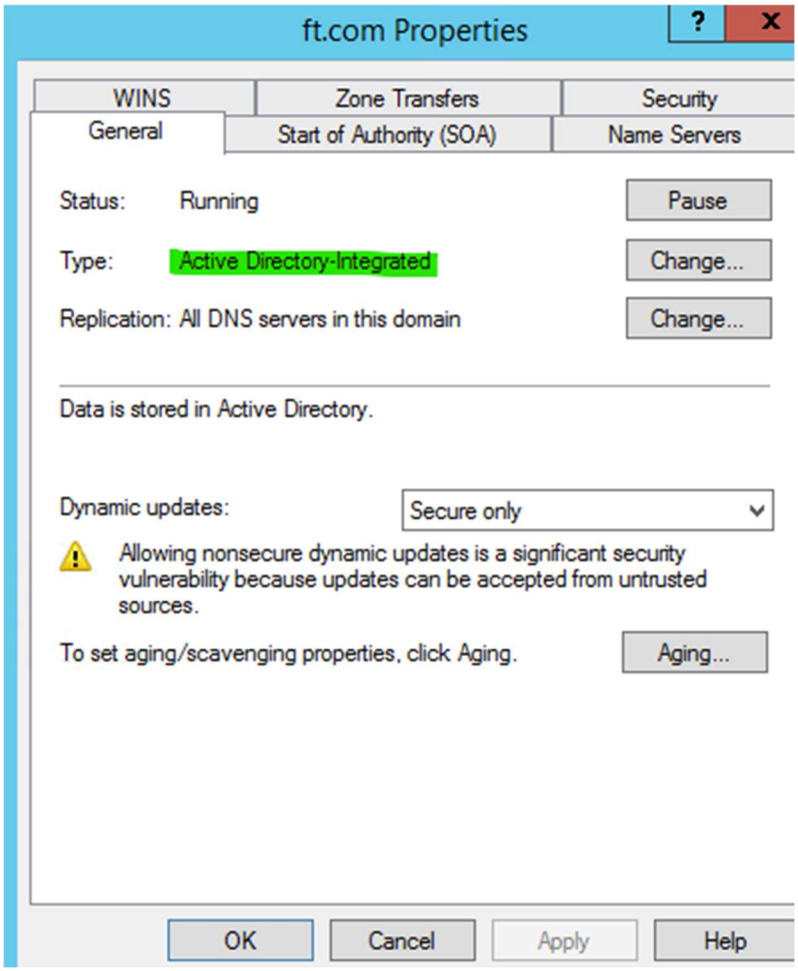


Fig.61 Zone Configuration

17. Snort Intrusion Detection System

1. Introduction

Snort was chosen for this project after reviewing several intrusion detection and prevention systems. It was selected because it provides high performance, simple configuration, and strong community support. The system can analyze network traffic in real time and detect any abnormal or unauthorized activity. It is easy to integrate with different network environments and is commonly used in both research and practical applications, making it an effective choice for studying and applying network protection methods.

2. Main Components

1. **Packet Sniffer:** Captures and analyzes data packets passing through the network.
2. **Preprocessor:** Normalizes and prepares packet data for further inspection.
3. **Detection Engine:** Compares network traffic against a database of rules to identify threats or anomalies.
4. **Alert System:** Sends notifications when suspicious activity or policy violation is detected.
5. **Logging System:** Stores event records for later analysis and reporting.

3. Advantages

1. Free and open source, making it accessible to individuals and organizations.
2. Highly flexible and can be customized using user-defined rules.
3. Provides real-time monitoring and alerting for various network attacks.
4. Supports integration with other security tools for advanced threat analysis.
5. Constantly updated by a strong community and maintained by Cisco Systems.

4. Disadvantages

1. Requires technical knowledge to configure and manage effectively.
2. High network traffic can cause performance degradation on limited hardware.
3. May generate false positives if rules are not properly optimized.
4. Does not provide full visibility into encrypted traffic.

5. Importance

Snort plays a crucial role in strengthening network security. It helps organizations identify and prevent attacks such as denial of service, port scanning, and unauthorized access. By deploying Snort on a reliable operating system such as Ubuntu, administrators can build an effective defense mechanism that protects data integrity and ensures network stability.

A. Install Snort Intrusion Detection System

1. Update the System

   Before installing Snort, update the system packages to ensure everything is up to date.

```
bob@snort:~$ sudo apt-get update && sudo apt-get upgrade -y
[sudo] password for bob:
Hit:1 http://archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:3 http://archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Get:4 http://archive.ubuntu.com/ubuntu focal-security InRelease [114 kB]
0% [Working]
```

Fig.62 Update the system in Snort

2. Install Required Dependencies

   Install the necessary tools and libraries needed for Snort.

```
Processing triggers for shim-signed (1.40.9+15.7-0ubuntu1) ...
bob@snort:~$ mkdir snort
bob@snort:~$ ls
snort
bob@snort:~$ sudo apt-get install -y build-essential autotools-dev libdumbnet-dev libluajit-5.1-dev libpcap-d
 \
>       zlib1g-dev pkg-config libhwloc-dev cmake liblzma-dev openssl libssl-dev cpputest libsqlite3-dev \
>       libtool uuid-dev  git autoconf bison flex libcmocka-dev libnetfilter-queue-dev libunwind-dev \
>       libmnl-dev ethtool libjemalloc-dev
```

Fig.63 Install required dependencies

3. Create a Snort directory in the home folder, download and extract PCRE version 8.45, then configure, compile, and install it using the commands:

mkdir ~/snort && cd ~/snort && wget https://sourceforge.net/projects/pcre/files/pcre/8.45/pcre-8.45.tar.gz && tar -xzvf pcre8.45.tar.gz && cd pcre-8.45 && ./configure && make && sudo make install.

```
Processing triggers for libc-bin (2.31-0ubuntu9.12) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for install-info (6.7.0.dfsg.2-5) ...
bob@snort:~$ cd ~/snort
bob@snort:~/snort$ wget wget https://sourceforge.net/projects/pcre/files/pcre/8.45/pcre-8.45.tar.gz
--2023-11-18 21:11:19--  http://wget/
Resolving wget (wget)... failed: Temporary failure in name resolution.
wget: unable to resolve host address 'wget'
--2023-11-18 21:11:19--  https://sourceforge.net/projects/pcre/files/pcre/8.45/pcre-8.45.tar.gz
Resolving sourceforge.net (sourceforge.net)... 172.64.150.145, 104.18.37.111, 2606:4700:4400::6812:256f, ...
Connecting to sourceforge.net (sourceforge.net)|172.64.150.145|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
```

Fig.64 Download and extract PCRE

4. Install gperftools by navigating to the Snort directory, downloading and extracting version 2.9.1, then configuring, compiling, and installing it using the commands: cd ~/snort && wget https://github.com/gperftools/gperftools/releases/download/gperftools-2.9.1/gperftools2.9.1.tar.gz && tar xzvf gperftools-2.9.1.tar.gz && cd gperftools-2.9.1 && ./configure && make && sudo make install.

Fig.65 Install gperftools

5. To install Ragel, navigate to the Snort directory, download the Ragel 6.10 package, extract it, enter the extracted folder, then run **./configure, make, and sudo make install.**

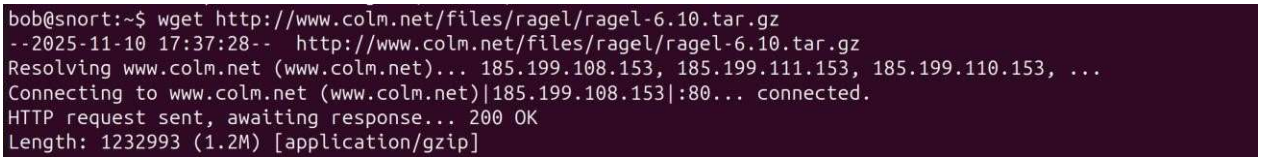


Fig.66 install Ragel

6. To download (without installing) the Boost C++ Libraries, go to the Snort directory, download the Boost 1.10.4 package, and extract it using **tar -xvzf**.

Fig.67 Download the boost C++ libraries

7. To install Hyperscan, navigate to the Snort directory, download and extract Hyperscan v5.4.2, create a build directory, run **cmake** with the Boost path, then execute **make** and **sudo make install**.

```
bob@snort:~/snort$ cd ~/snort
bob@snort:~/snort$ wget https://github.com/intel/hyperscan/archive/refs/tags/v5.4.2.tar.gz
--2023-11-18 21:21:49--  https://github.com/intel/hyperscan/archive/refs/tags/v5.4.2.tar.gz
Resolving github.com (github.com)... 140.82.112.3
Connecting to github.com (github.com)|140.82.112.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/intel/hyperscan/tar.gz/refs/tags/v5.4.2 [following]
--2023-11-18 21:21:49--  https://codeload.github.com/intel/hyperscan/tar.gz/refs/tags/v5.4.2
Resolving codeload.github.com (codeload.github.com)... 140.82.114.9
Connecting to codeload.github.com (codeload.github.com)|140.82.114.9|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/x-gzip]
Saving to: 'v5.4.2.tar.gz.1'

v5.4.2.tar.gz.1               [ <=>                                   ]   1.17M  5.77MB/s
```

Fig.68 Install Hyperscan

8. To install Flatbuffers, go to the Snort directory, download and extract Flatbuffers v2.0.0, create a build folder, run **cmake** on the extracted folder, then execute **make** and **sudo make install**.

```
bob@snort:~$ wget https://github.com/google/flatbuffers/archive/refs/tags/v2.0.0.tar.gz
--2025-11-10 17:39:39--  https://github.com/google/flatbuffers/archive/refs/tags/v2.0.0.tar.gz
Resolving github.com (github.com)... 140.82.121.4
Connecting to github.com (github.com)|140.82.121.4|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/google/flatbuffers/tar.gz/refs/tags/v2.0.0 [following]
--2025-11-10 17:39:40--  https://codeload.github.com/google/flatbuffers/tar.gz/refs/tags/v2.0.0
Resolving codeload.github.com (codeload.github.com)... 140.82.121.9
Connecting to codeload.github.com (codeload.github.com)|140.82.121.9|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1538022 (1.5M) [application/x-gzip]
```

Fig.69 Install flatbuffers

9. To install the Snort Data Acquisition (DAQ) library, navigate to the Snort directory, download and extract libdaq v3.0.21, enter the folder, run **./bootstrap**, **./configure**, **make**, and **sudo make install**.

```
.pc fst/libdaq_static_fst.pc nfq/libdaq_static_nfq.pc pcap/libdaq_static_pcap.pc savefile/libdaq_static_savef
e.pc trace/libdaq_static_trace.pc gwlb/libdaq_static_gwlb.pc '/usr/local/lib/pkgconfig'
make[2]: Leaving directory '/home/bob/snort/libdaq-3.0.13/modules'
make[1]: Leaving directory '/home/bob/snort/libdaq-3.0.13/modules'
Making install in example
make[1]: Entering directory '/home/bob/snort/libdaq-3.0.13/example'
make[2]: Entering directory '/home/bob/snort/libdaq-3.0.13/example'
 /usr/bin/mkdir -p '/usr/local/bin'
  /bin/bash ../libtool   --mode=install /usr/bin/install -c daqtest daqtest-static '/usr/local/bin'
libtool: install: /usr/bin/install -c .libs/daqtest /usr/local/bin/daqtest
libtool: install: /usr/bin/install -c daqtest-static /usr/local/bin/daqtest-static
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/bob/snort/libdaq-3.0.13/example'
make[1]: Leaving directory '/home/bob/snort/libdaq-3.0.13/example'
Making install in test
make[1]: Entering directory '/home/bob/snort/libdaq-3.0.13/test'
make[2]: Entering directory '/home/bob/snort/libdaq-3.0.13/test'
make[2]: Nothing to be done for 'install-exec-am'.
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/bob/snort/libdaq-3.0.13/test'
make[1]: Leaving directory '/home/bob/snort/libdaq-3.0.13/test'
make[1]: Entering directory '/home/bob/snort/libdaq-3.0.13'
make[2]: Entering directory '/home/bob/snort/libdaq-3.0.13'
make[2]: Nothing to be done for 'install-exec-am'.
```

Fig.70 Install the snort data acquisition (DAQ) library

10. To update the system's shared libraries, run the command **sudo ldconfig**.

```
.pc fst/libdaq_static_fst.pc nfq/libdaq_static_nfq.pc pcap/libdaq_static_pcap.pc savefile/libdaq_static_savef
e.pc trace/libdaq_static_trace.pc gwlb/libdaq_static_gwlb.pc '/usr/local/lib/pkgconfig'
make[2]: Leaving directory '/home/bob/snort/libdaq-3.0.13/modules'
make[1]: Leaving directory '/home/bob/snort/libdaq-3.0.13/modules'
Making install in example
make[1]: Entering directory '/home/bob/snort/libdaq-3.0.13/example'
make[2]: Entering directory '/home/bob/snort/libdaq-3.0.13/example'
 /usr/bin/mkdir -p '/usr/local/bin'
  /bin/bash ../libtool   --mode=install /usr/bin/install -c daqtest daqtest-static '/usr/local/bin'
libtool: install: /usr/bin/install -c .libs/daqtest /usr/local/bin/daqtest
libtool: install: /usr/bin/install -c daqtest-static /usr/local/bin/daqtest-static
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/bob/snort/libdaq-3.0.13/example'
make[1]: Leaving directory '/home/bob/snort/libdaq-3.0.13/example'
Making install in test
make[1]: Entering directory '/home/bob/snort/libdaq-3.0.13/test'
make[2]: Entering directory '/home/bob/snort/libdaq-3.0.13/test'
make[2]: Nothing to be done for 'install-exec-am'.
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/home/bob/snort/libdaq-3.0.13/test'
make[1]: Leaving directory '/home/bob/snort/libdaq-3.0.13/test'
make[1]: Entering directory '/home/bob/snort/libdaq-3.0.13'
make[2]: Entering directory '/home/bob/snort/libdaq-3.0.13'
make[2]: Nothing to be done for 'install-exec-am'.
 /usr/bin/mkdir -p '/usr/local/lib/pkgconfig'
 /usr/bin/install -c -m 644 libdaq.pc '/usr/local/lib/pkgconfig'
make[2]: Leaving directory '/home/bob/snort/libdaq-3.0.13'
make[1]: Leaving directory '/home/bob/snort/libdaq-3.0.13'
bob@snort:~/snort/libdaq-3.0.13$ sudo ldconfig
bob@snort:~/snort/libdaq-3.0.13$
```

Fig.71 Update the system's shared libraries

11. To install the latest version of Snort 3, navigate to the Snort directory, download and extract Snort3 v3.9.5.0, run **./configure_cmake.sh** with the desired options, then enter the build folder, execute **make**, and **sudo make install**.

```
         num match states: 370
             memory scale: KB
             total memory: 68.5879
           pattern memory: 18.6973
        match list memory: 27.3281
        transition memory: 22.3125
appid: MaxRss diff: 2752
appid: patterns loaded: 300
--------------------------------------------------
pcap DAQ configured to passive.

Snort successfully validated the configuration (with 0 warnings).
o")~   Snort exiting
bob@snort:~/snort/snort3-3.1.74.0/build$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens34: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:24:ac:3d brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.152/24 brd 192.168.100.255 scope global dynamic ens34
       valid_lft 82753sec preferred_lft 82753sec
    inet6 fe80::20c:29ff:fe24:ac3d/64 scope link
       valid_lft forever preferred_lft forever
bob@snort:~/snort/snort3-3.1.74.0/build$ sudo ethtool -k ens34 | grep receive-offload
generic-receive-offload: on
large-receive-offload: on
bob@snort:~/snort/snort3-3.1.74.0/build$ sudo nano /lib/systemd/system/ethtool.service
```

Fig.72 Install the latest version

The Snort IDS is connected to the Layer 3 switch using a SPAN/Monitor port, allowing it to monitor and analyze mirrored traffic from different VLANs in real time.
This ensures that any malicious or abnormal activities within the network can be detected promptly.

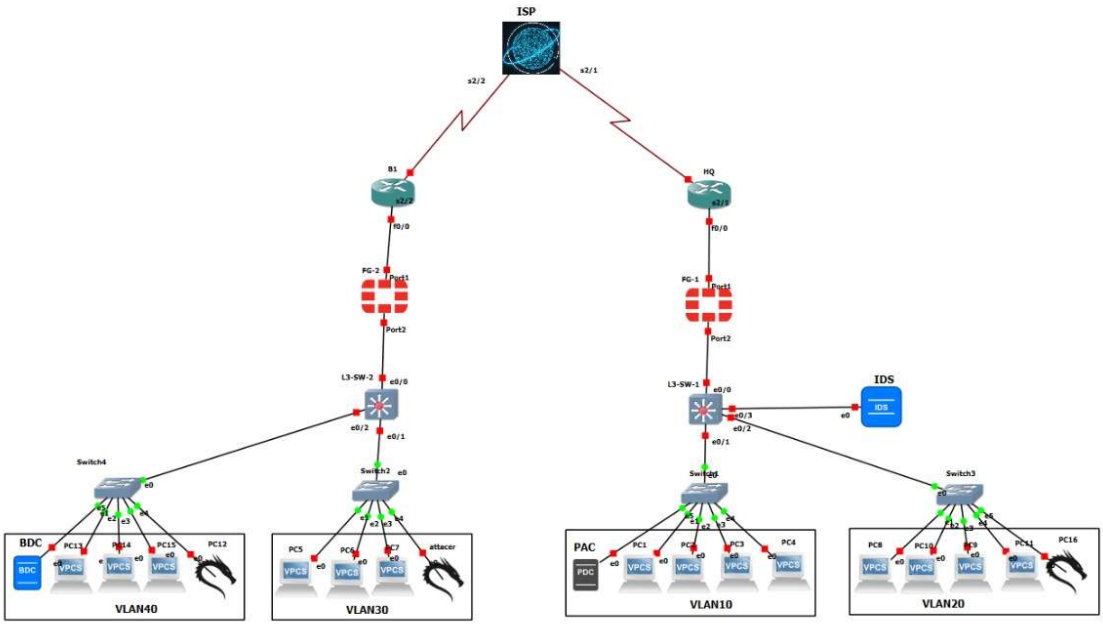


Fig.73 Topology including Kali

Some advanced security features, such as IPS, Antivirus, Web Filtering, Application Control, SSL Deep Inspection, SSL VPN (including portal features and YIS users), FortiClient EMS, and Sandbox, could not be implemented in this project. The main reason is that these features require additional licenses, which were not available within the scope of this implementation. As a result, the project focused on the core functionalities that could be deployed without extra licensing, while acknowledging that full utilization of these advanced security services would enhance protection