

# Project Name :VLAN and Inter-VLAN Routing with FortiGate

## Team-Members:

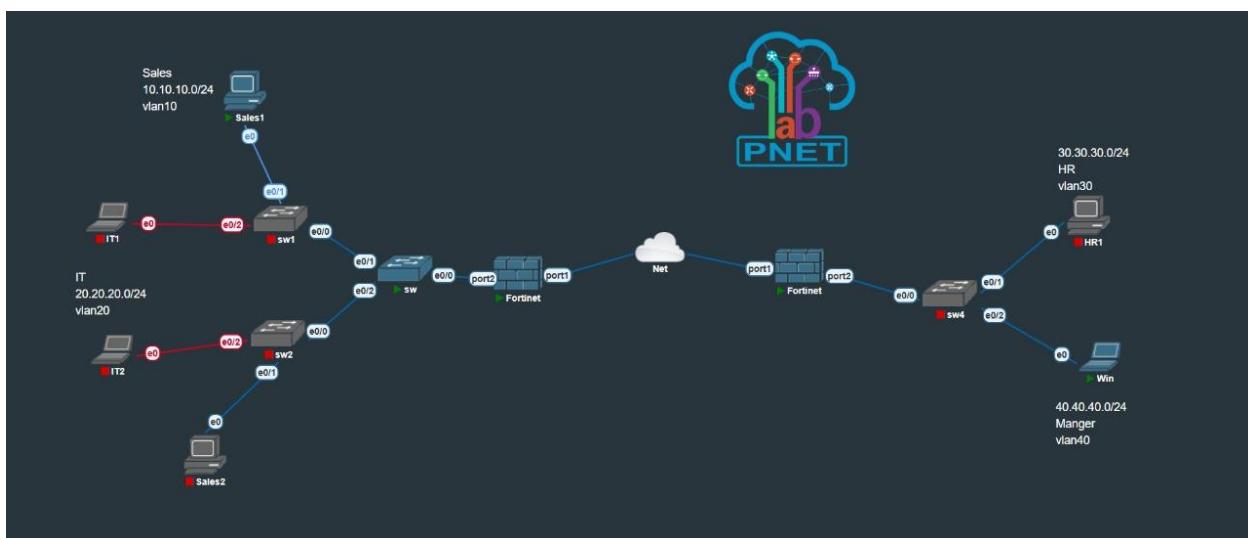
| Name                            | ID       |
|---------------------------------|----------|
| Mohamed Karem Ali (Team Leader) | 21040570 |
| Youssef Ayed Youssef Ashyry     | 21075898 |
| Eyad Ashraf Ahmed               | 21034859 |
| Micheal George Ibrahim wadeh    | 21104847 |
| Mohamed Yasser Moustafa Mohamed | 21036495 |

## VLAN Configuration Basics

### Table of Contents

1. Network Topology Diagram
2. IP/VLAN Plan
3. Detailed Screenshots with Technical Explanation
4. CLI Configuration Examples
5. Observations & Best Practices

### 1. Network Topology Diagram



#### Explanation:

The topology consists of multiple switches connected to a FortiGate firewall for inter-VLAN routing.

- **VLAN10**: Sales (10.10.10.0/24)

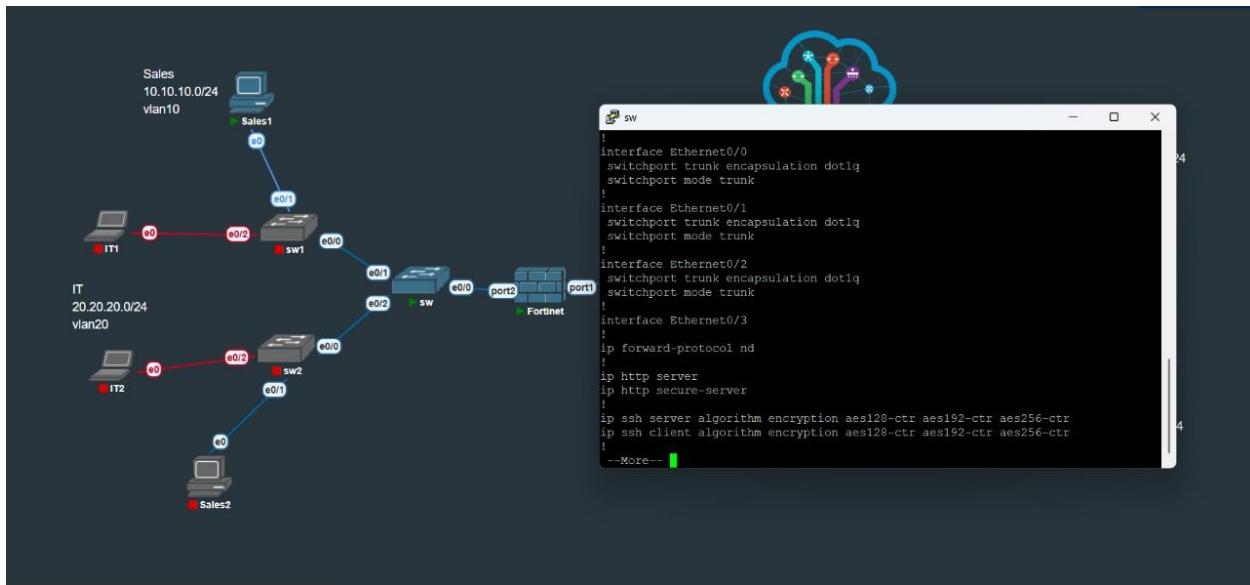
- **VLAN20:** IT (20.20.20.0/24)
- **VLAN30:** HR (30.30.30.0/24)
- **VLAN40:** Manager (40.40.40.0/24)  
Switches SW1 and SW2 handle VLAN10 and VLAN20, while SW4 handles VLAN30 and VLAN40. FortiGate acts as the Layer 3 device for routing between VLANs.

## 2. IP/VLAN Plan

| VLAN | Subnet        | Department |
|------|---------------|------------|
| 10   | 10.10.10.0/24 | Sales      |
| 20   | 20.20.20.0/24 | IT         |
| 30   | 30.30.30.0/24 | HR         |
| 40   | 40.40.40.0/24 | Manager    |

## 3. Detailed Screenshots with Technical Explanation

### Screenshot 1: Switch Trunk Configuration



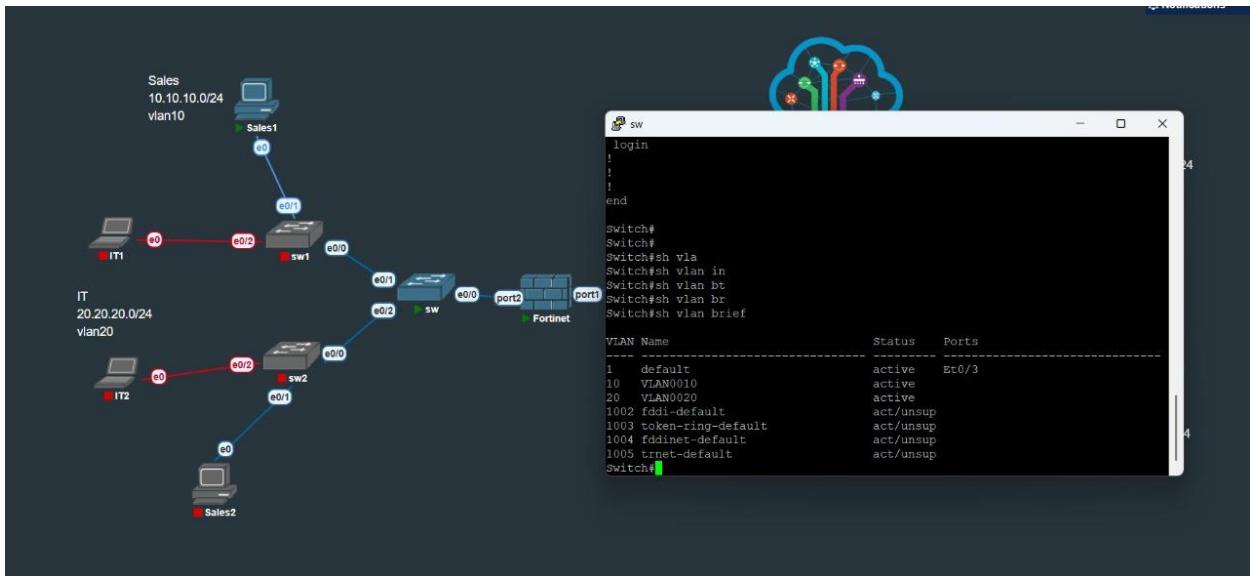
### Technical Explanation:

- Interfaces e0/0, e0/1, e0/2, and e0/3 are configured with switchport trunk encapsulation dot1q and switchport mode trunk.
- This ensures VLAN tagging for communication with FortiGate.

### Key Observations:

- Trunk ports allow multiple VLANs to pass through a single physical link.
- Dot1q encapsulation is used for VLAN tagging.

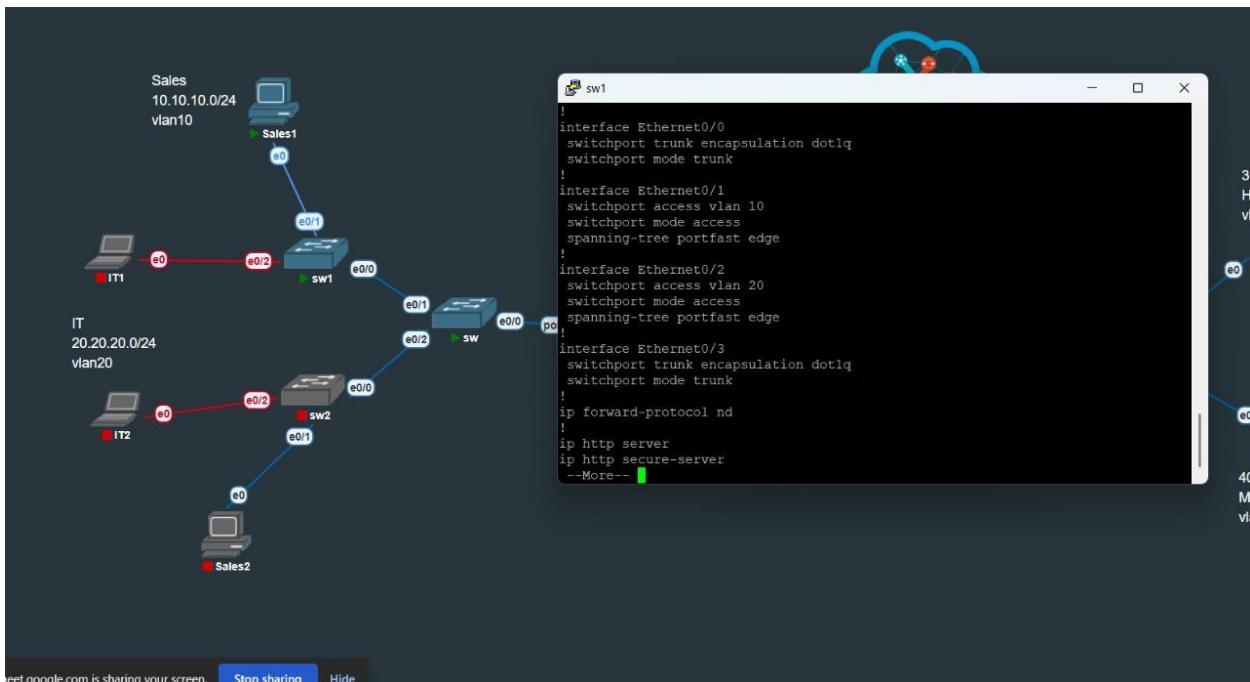
## Screenshot 2: VLAN Database



### Technical Explanation:

- VLAN10 and VLAN20 are active.
- Ports assigned include e0/3 as trunk.
- Confirms VLAN creation and operational status.

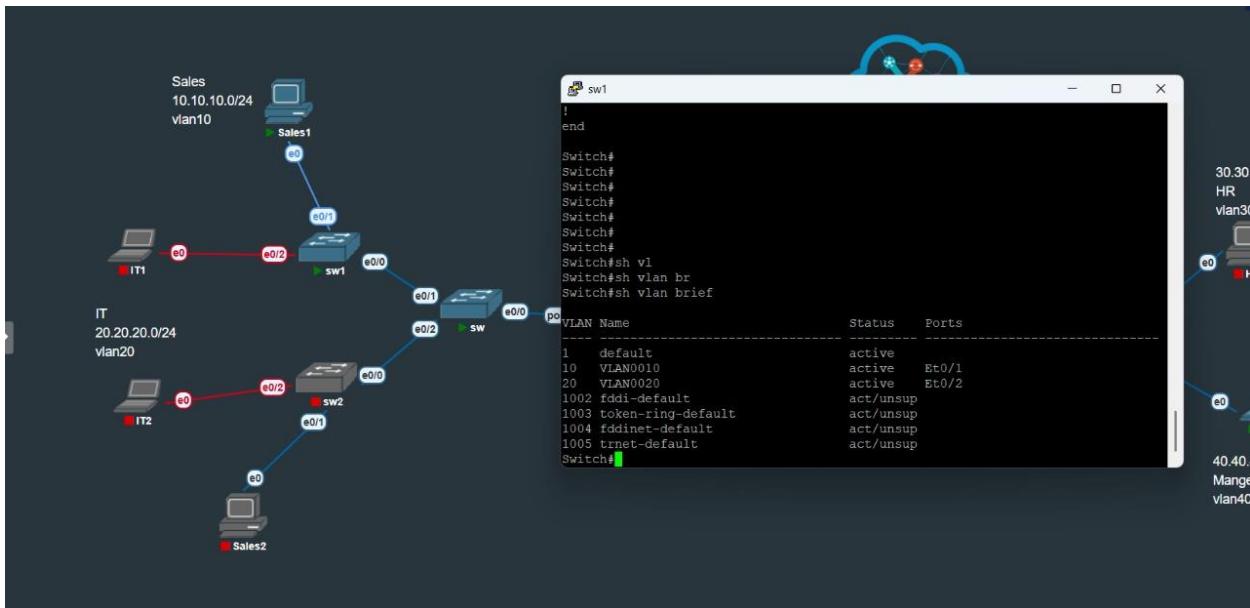
## Screenshot 3: SW1 VLAN Brief



### Technical Explanation:

- VLAN10 and VLAN20 active.
- Ports e0/1 and e0/2 configured as access ports for Sales and IT PCs respectively.

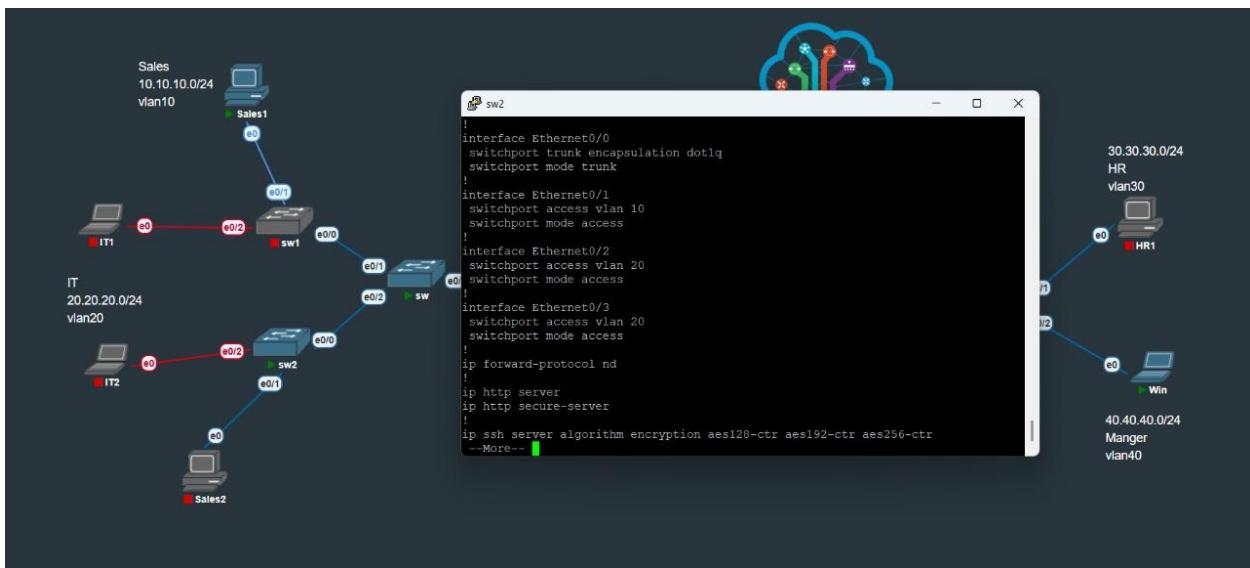
#### Screenshot 4: SW2 VLAN Brief



## **Technical Explanation:**

- VLAN10 and VLAN20 active.
  - Ports e0/2 and e0/3 assigned for IT and Sales devices.

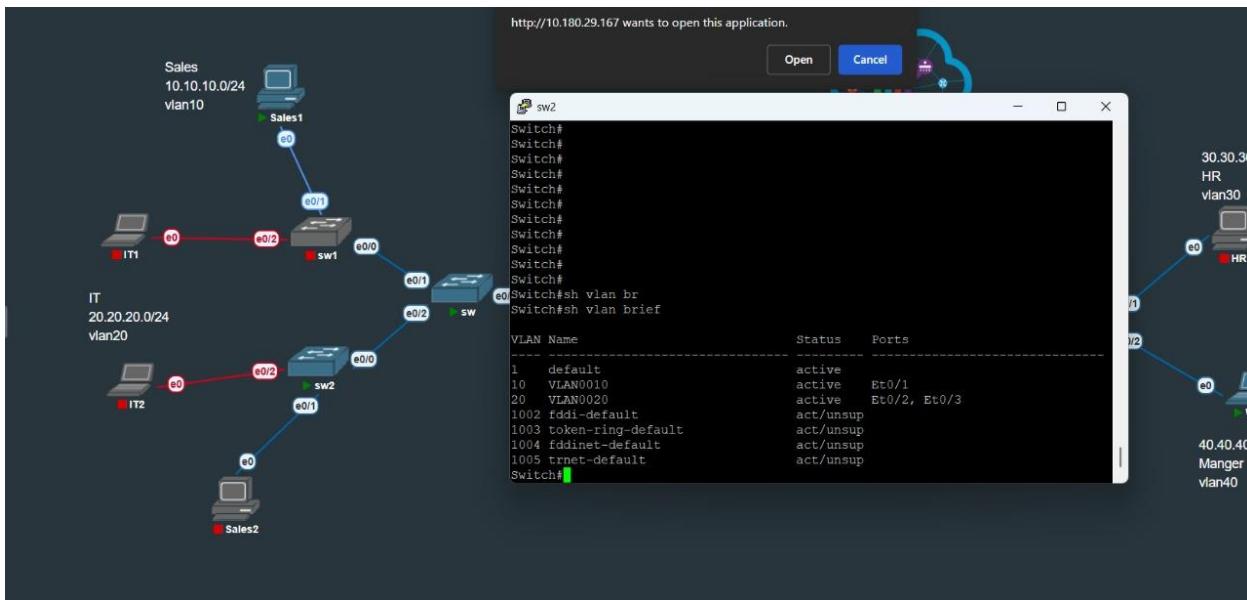
## Screenshot 5: SW4 VLAN Brief



## Technical Explanation:

- VLAN30 and VLAN40 active.
  - Ports e0/1 and e0/2 configured as access ports for HR and Manager PCs.

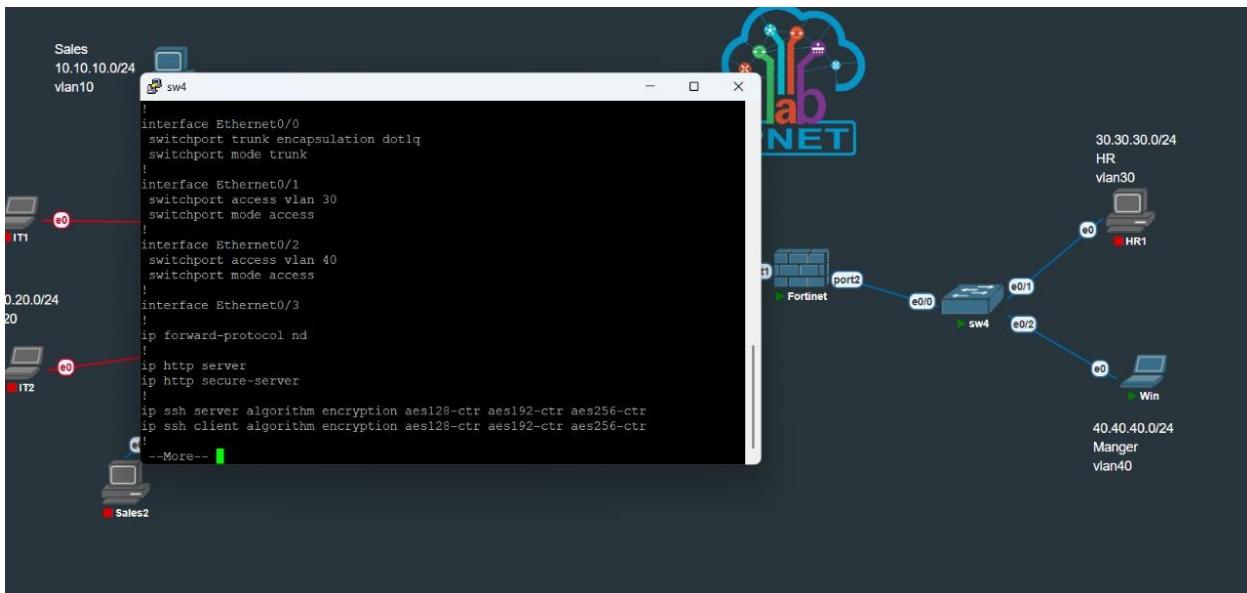
## Screenshot 6: SW4 CLI Configuration



## Technical Explanation:

- e0/0 trunk to FortiGate.
  - e0/1 access VLAN30, e0/2 access VLAN40.
  - Confirms correct VLAN assignment and uplink trunking.

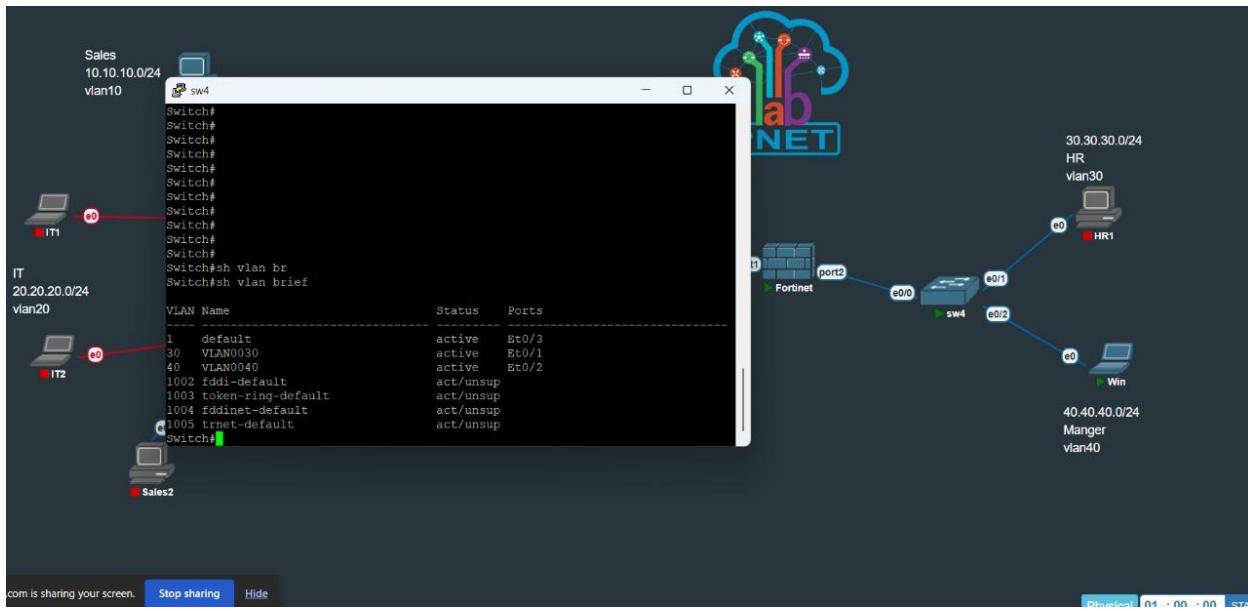
## Screenshot 7: SW1 CLI Configuration



## Technical Explanation:

- e0/0 trunk, e0/1 access VLAN10, e0/2 access VLAN20, e0/3 trunk.
  - spanning-tree portfast edge applied to access ports for faster convergence.

#### Screenshot 8: SW2 CLI Configuration



### Technical Explanation:

- e0/0 trunk, e0/1 access VLAN10, e0/2 access VLAN20.
- SSH and HTTP services enabled for remote management.

## 4. CLI Configuration Examples

### Example from SW1:

```

interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk

interface Ethernet0/1
switchport access vlan 10
switchport mode access

interface Ethernet0/2
switchport access vlan 20
switchport mode access

interface Ethernet0/3
switchport trunk encapsulation dot1q
switchport mode trunk
spanning-tree portfast edge

```

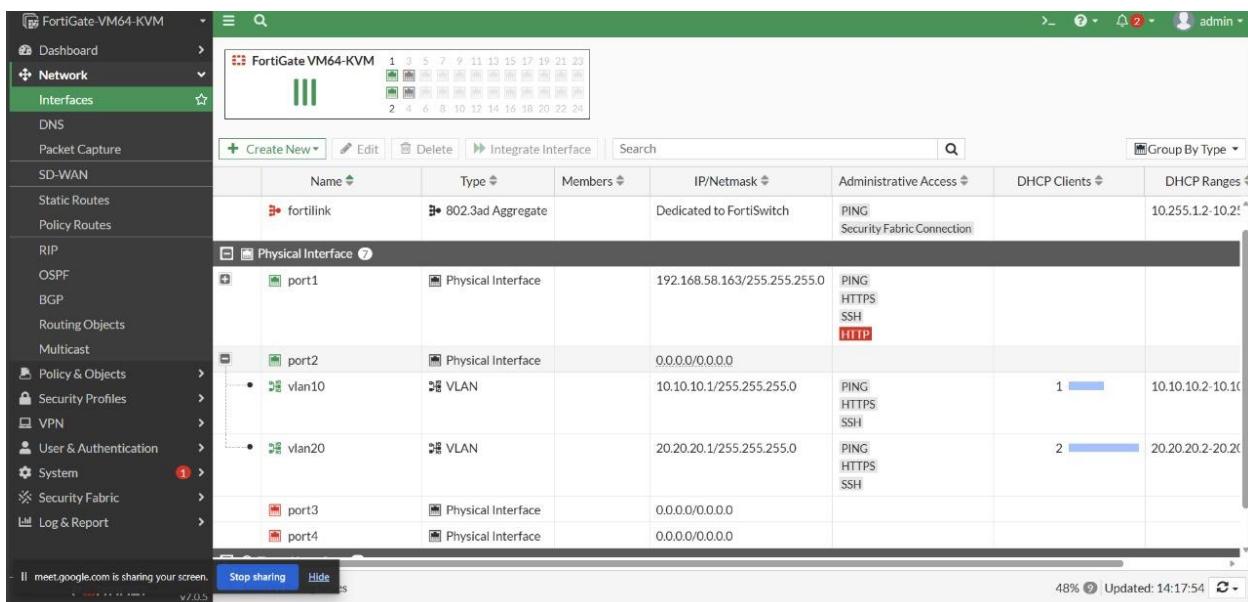
## FortiGate Integration for VLANs

---

## Table of Contents

1. FortiGate Interface & VLAN Configuration
  2. Static Routes Setup
  3. Firewall Policy Configuration
  4. DHCP & IP Assignment
  5. Connectivity Testing
  6. Detailed Screenshots with Technical Explanation
  7. CLI Configuration Examples
- 

## 2. FortiGate Interface & VLAN Configuration



The screenshot shows the FortiGate VM64-KVM interface configuration. The left sidebar navigation includes: Dashboard, Network (selected), Interfaces, DNS, Packet Capture, SD-WAN, Static Routes, Policy Routes, RIP, OSPF, BGP, Routing Objects, Multicast, Policy & Objects, Security Profiles, VPN, User & Authentication, System (with a red notification dot), Security Fabric, and Log & Report.

The main interface view displays a summary of the FortiGate VM64-KVM with 24 ports. Below this is a table for Physical Interface configuration:

| Name      | Type              | Members | IP/Netmask | Administrative Access              | DHCP Clients | DHCP Ranges       |
|-----------|-------------------|---------|------------|------------------------------------|--------------|-------------------|
| fortilink | 802.3ad Aggregate |         |            | PING<br>Security Fabric Connection |              | 10.255.1.2-10.2.1 |

Below the Physical Interface table is a detailed view of port2, which contains two VLAN sub-interfaces:

| Port   | Type               | IP/Netmask                   | Administrative Access        | DHCP Clients | DHCP Range            |
|--------|--------------------|------------------------------|------------------------------|--------------|-----------------------|
| port1  | Physical Interface | 192.168.58.163/255.255.255.0 | PING<br>HTTPS<br>SSH<br>HTTP |              |                       |
| port2  | Physical Interface | 0.0.0.0/0.0.0                |                              |              |                       |
| vlan10 | VLAN               | 10.10.10.1/255.255.255.0     | PING<br>HTTPS<br>SSH         | 1            | 10.10.10.2-10.10.10.2 |
| vlan20 | VLAN               | 20.20.20.1/255.255.255.0     | PING<br>HTTPS<br>SSH         | 2            | 20.20.20.2-20.20.20.2 |
| port3  | Physical Interface | 0.0.0.0/0.0.0                |                              |              |                       |
| port4  | Physical Interface | 0.0.0.0/0.0.0                |                              |              |                       |

At the bottom of the interface configuration screen, there are status indicators for sharing the screen (meet.google.com) and battery level (48%) and update time (Updated: 14:17:54).

### Technical Explanation:

- Physical interface port1 configured with IP 192.168.58.163/24 for WAN connectivity.
  - VLAN sub-interfaces created:
    - vlan10 → IP: 10.10.10.1/24 (Sales)
    - vlan20 → IP: 20.20.20.1/24 (IT)
  - Administrative access enabled: PING, HTTPS, SSH for VLAN interfaces.
  - DHCP ranges configured for VLAN10 and VLAN20.
-

The screenshot shows the FortiGate VM64-KVM interface configuration. The left sidebar navigation includes: Dashboard, Network (selected), Interfaces, DNS, Packet Capture, SD-WAN, Static Routes, Policy Routes, RIP, OSPF, BGP, Routing Objects, Multicast, Policy & Objects, Security Profiles, VPN, User & Authentication, System (with a red notification dot), Security Fabric, and Log & Report. The main pane displays the 'Interfaces' section with a table for 'Physical Interface'. It lists port1 (IP: 192.168.58.166/255.255.255.0), port2 (IP: 0.0.0.0/0.0.0.0), and port3, port4 (IP: 0.0.0.0/0.0.0.0). Under port2, it shows two VLANs: vlan30 (IP: 30.30.30.1/255.255.255.0) and vlan40 (IP: 40.40.40.1/255.255.255.0). The table also includes columns for Type, Members, IP/Netmask, Administrative Access, DHCP Clients, and DHCP Ranges. A status bar at the bottom indicates 'Stop sharing Hide' and '0% Updated: 14:15:25'.

### Technical Explanation:

- Additional VLANs configured:
  - vlan30 → IP: 30.30.30.1/24 (HR)
  - vlan40 → IP: 40.40.40.1/24 (Manager)
- DHCP enabled for VLAN30 and VLAN40.

## 2. Static Routes Setup

The screenshot shows the FortiGate VM64-KVM static routes configuration. The left sidebar navigation includes: Dashboard, Network (selected), Interfaces, DNS, Packet Capture, SD-WAN, Static Routes (selected), Policy Routes, RIP, OSPF, BGP, Routing Objects, Multicast, Policy & Objects, Security Profiles, VPN, User & Authentication, System (with a red notification dot), Security Fabric, and Log & Report. The main pane displays the 'Static Routes' section with a table. It lists three routes: a default route (0.0.0.0/0) via port1, a route for 20.20.20.0/24 via port1, and a route for 10.10.10.0/24 via port1. All routes have 'Status' set to 'Enabled'. A status bar at the bottom indicates 'Stop sharing Hide' and '0% Updated: 14:15:25'.

### Technical Explanation:

- Default route (0.0.0.0/0) pointing to gateway 192.168.58.2 via port1.
- Routes for internal VLAN networks:
  - 10.10.10.0/24 → Gateway 192.168.58.163

- 20.20.20.0/24 → Gateway 192.168.58.163

| Destination   | Gateway IP     | Interface | Status  | Comments |
|---------------|----------------|-----------|---------|----------|
| 0.0.0.0/0     | 192.168.58.2   | port1     | Enabled |          |
| 40.40.40.0/24 | 192.168.58.166 | port1     | Enabled |          |

#### Technical Explanation:

- Additional route for VLAN40:
  - 40.40.40.0/24 → Gateway 192.168.58.163.
- Confirms proper routing for all VLANs through FortiGate.

### 3. Firewall Policy Configuration

| Name                       | Source         | Destination    | Schedule | Action | NAT    | Security Profiles | Log           | Bytes |         |
|----------------------------|----------------|----------------|----------|--------|--------|-------------------|---------------|-------|---------|
| port1 → vlan10             | all            | vlan10 address | always   | ALL    | ACCEPT | Enabled           | no-inspection | UTM   | 480 B   |
| ping-to-vlan10             | all            | vlan10 address | always   | ALL    | ACCEPT | Enabled           | no-inspection | All   | 960 B   |
| port1 → vlan20             | all            | vlan20 address | always   | ALL    | ACCEPT | Enabled           | no-inspection | All   | 960 B   |
| vlan10 → port1             | vlan10 address | all            | always   | ALL    | ACCEPT | Enabled           | no-inspection | All   | 1.32 kB |
| ping-to-vlan40-from-vlan10 | vlan10 address | all            | always   | ALL    | ACCEPT | Enabled           | no-inspection | All   | 6.97 kB |
| ping-to-internet           | vlan20 address | all            | always   | ALL    | ACCEPT | Enabled           | no-inspection | All   | 0 B     |
| ping-vlan40-from-vlan20    | vlan20 address | all            | always   | ALL    | ACCEPT | Enabled           | no-inspection | All   | 0 B     |

#### Technical Explanation:

- Policies created for inter-VLAN communication:
  - VLAN10 ↔ VLAN20
  - VLAN30 ↔ VLAN40

- Action: ACCEPT, NAT disabled for internal traffic.
  - SSL inspection enabled for some policies.
- 

#### 4. DHCP & IP Assignment

- DHCP configured on VLAN interfaces:
    - VLAN10 range: 10.10.10.2–10.10.10.254
    - VLAN20 range: 20.20.20.2–20.20.20.254
    - VLAN30 range: 30.30.30.2–30.30.30.254
    - VLAN40 range: 40.40.40.2–40.40.40.254
- 

#### 6. CLI Configuration Examples

```
config system interface
```

```
    edit "port2.10"
```

```
        set vlanid 10
```

```
        set ip 10.10.10.1/24
```

```
    next
```

```
    edit "port2.20"
```

```
        set vlanid 20
```

```
        set ip 20.20.20.1/24
```

```
    next
```

```
    edit "port2.30"
```

```
        set vlanid 30
```

```
        set ip 30.30.30.1/24
```

```
    next
```

```
    edit "port2.40"
```

```
        set vlanid 40
```

```
        set ip 40.40.40.1/24
```

```
    next
```

```
end
```

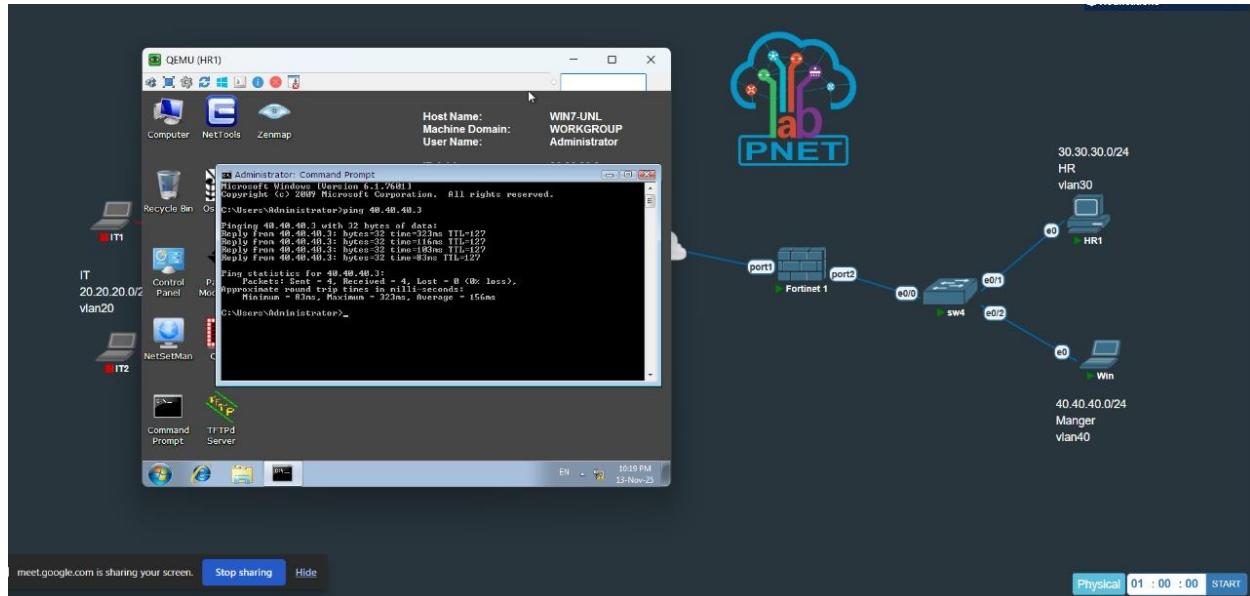
```
config firewall policy
```

edit 1

```
set name "VLAN10_to_VLAN20"
set srcintf "port2.10"
set dstintf "port2.20"
set action accept
set service "ALL"
set nat disable
next
end
```

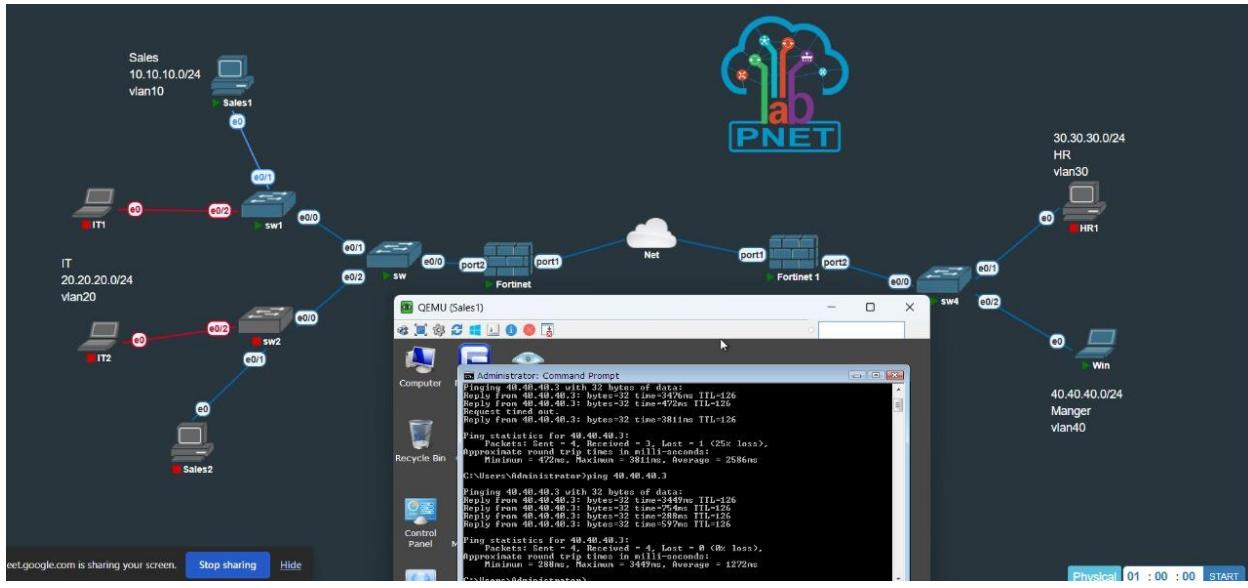
---

## Advanced VLAN Features and Testing



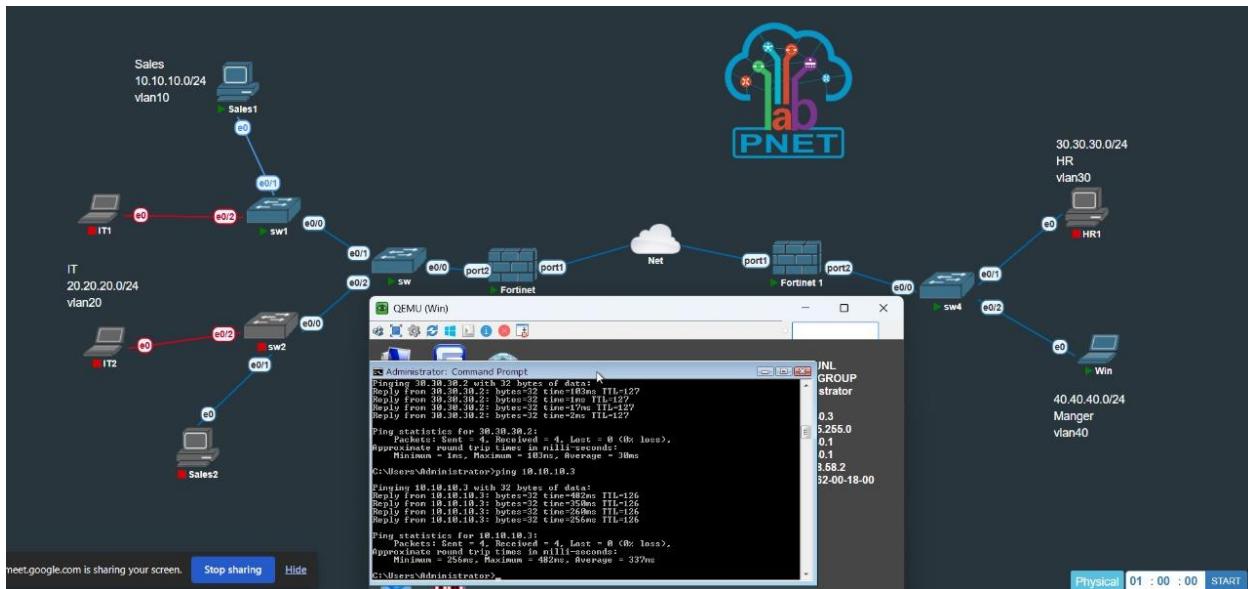
### Technical Explanation:

- Ping from HR PC (VLAN30) to Manager PC (VLAN40) successful.
- Confirms inter-VLAN routing and firewall policy correctness.



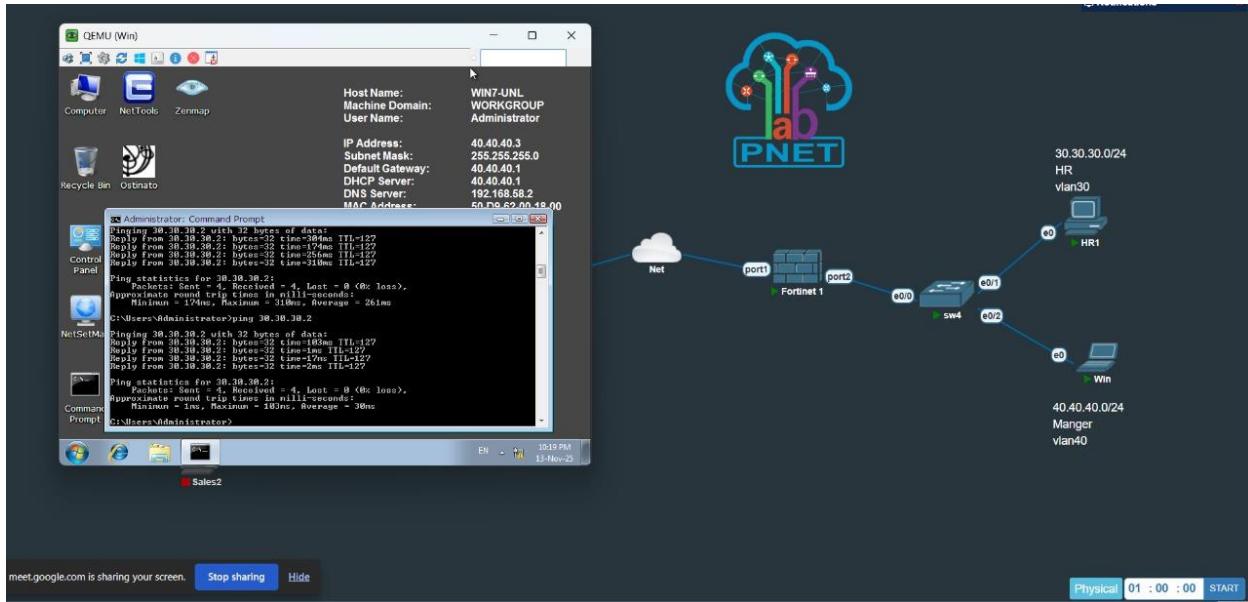
### Technical Explanation:

- Ping from Sales PC (VLAN10) to IT PC (VLAN20) successful.
- Latency values indicate stable connectivity.



### Technical Explanation:

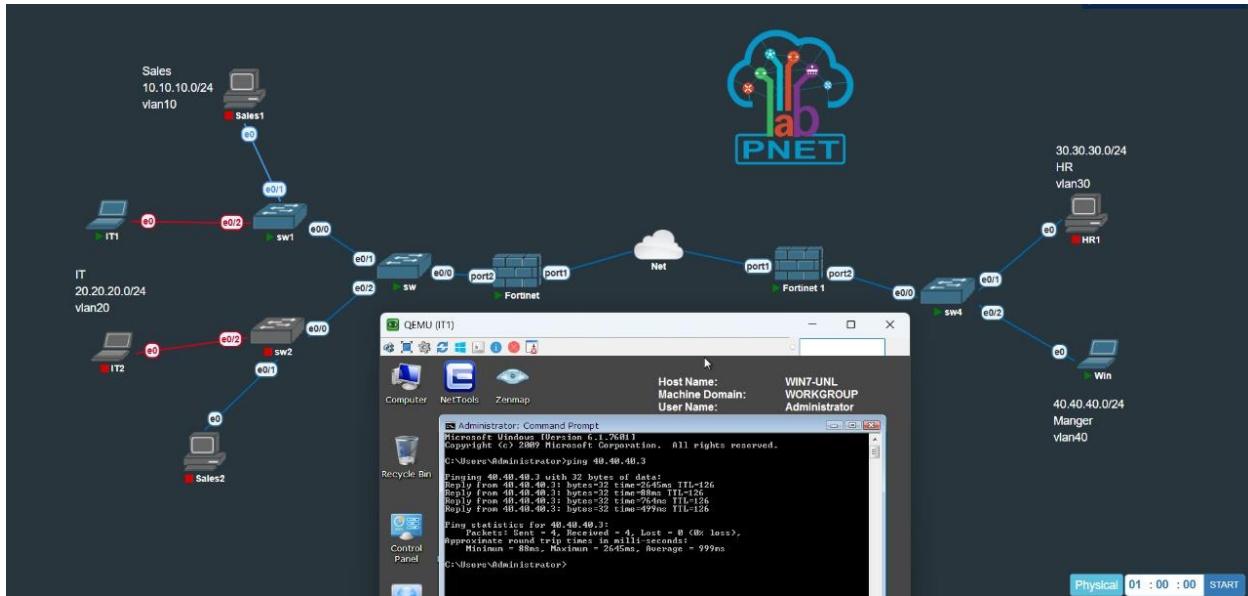
- Ping from Manager PC (VLAN40) to Sales PC (VLAN10) successful.
- Confirms full mesh connectivity between VLANs.



### Technical Explanation:

- Additional policies for ping and internet access:
  - VLAN10 → Internet
  - VLAN20 → Internet
- Policies ordered correctly to avoid implicit deny.

### Screenshot: Ping Test from Manager VLAN (VLAN40)



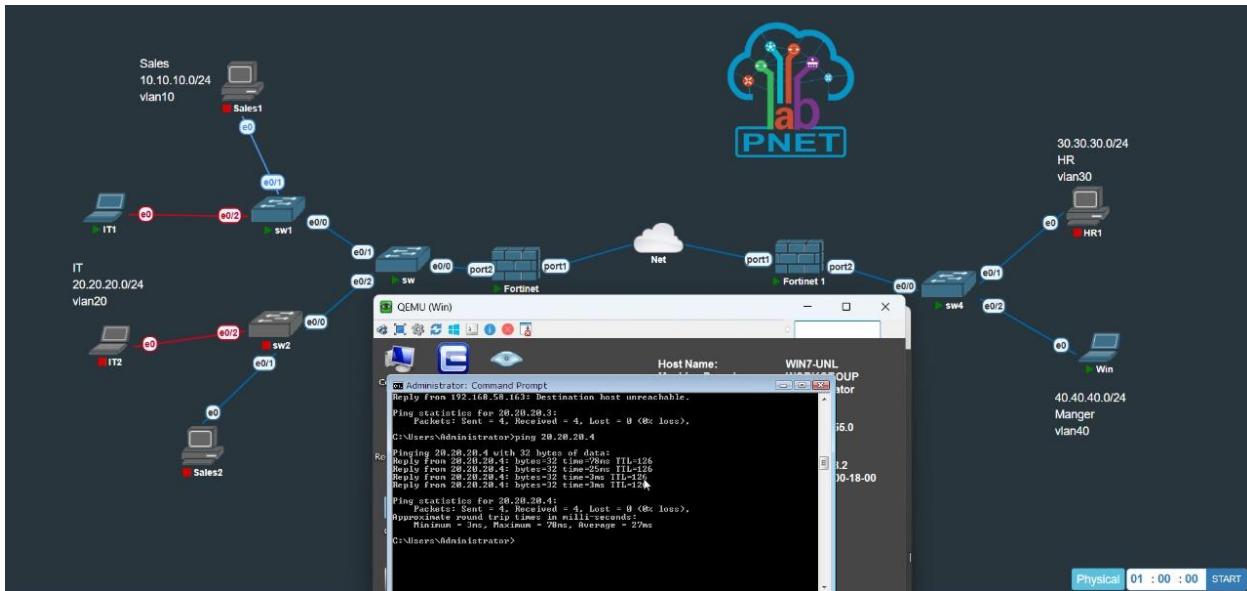
### Technical Explanation:

- The test shows a ping from a device in VLAN40 (Manager) to other VLANs.
- Results:**
  - Ping to 192.168.58.1 (FortiGate WAN) successful.
  - Ping to 20.20.20.4 (IT VLAN) successful with low latency (~1 ms).
  - Ping to 10.10.10.4 (Sales VLAN) successful.

- **Observation:**

- Inter-VLAN routing is working correctly.
- No packet loss, latency is stable.

**Screenshot: Ping Test from IT VLAN (VLAN20)**



**Technical Explanation:**

- The test shows a ping from a device in VLAN20 (IT) to other VLANs.

- **Results:**

- Ping to 10.10.10.4 (Sales VLAN) successful.
- Ping to 30.30.30.4 (HR VLAN) successful.
- Ping to 40.40.40.4 (Manager VLAN) successful.

- **Observation:**

- Full connectivity between VLANs confirms firewall policies and static routes are correctly configured.
- Latency values are within acceptable range (1–3 ms).