Step-by-Step VLAN Setup on FortiGate

with Cisco Switch and Multiple PCs

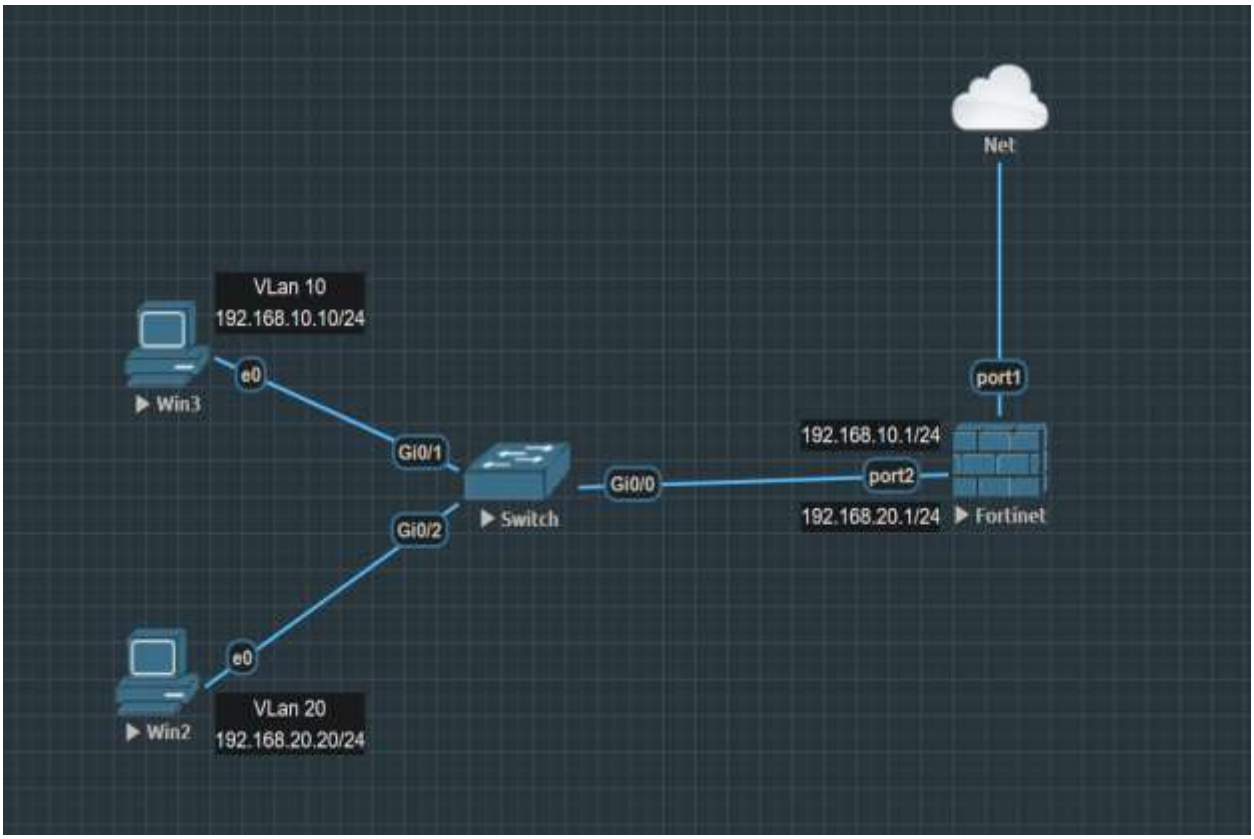
✅ Objectives

This document will cover how to create VLANs in a FortiGate firewall for network segmentation. In this setup, a Cisco switch is used to extend VLANs, and two PCs are connected to different VLANs (PC1 in VLAN 10 and PC2 in VLAN 20). The goal is to demonstrate basic VLAN configuration, trucking between FortiGate and the switch, and verifying device isolation across VLANs.

✅ Scope

This document focuses on configuring VLANs on a FortiGate firewall and integrating them with a Cisco switch to achieve proper network segmentation.

This guide covers basic VLAN functionality only, and does not include advanced routing, DHCP, or firewall policies beyond basic connectivity testing.



🔧 Network Design Overview

In this setup, we are using two ports on the Fortinet firewall:

- Port 1 for management access
- Port 2 to connect the LAN (Cisco switch)

We will assign 192.168.10.1 and 192.168.20.1 to VLAN interfaces on Port 2, as this port will handle both VLANs (VLAN 10 and VLAN 20).

On the Cisco switch, we will create:

- VLAN 10 (for Win 3 PC)
- VLAN 20 (for Win 2PC)

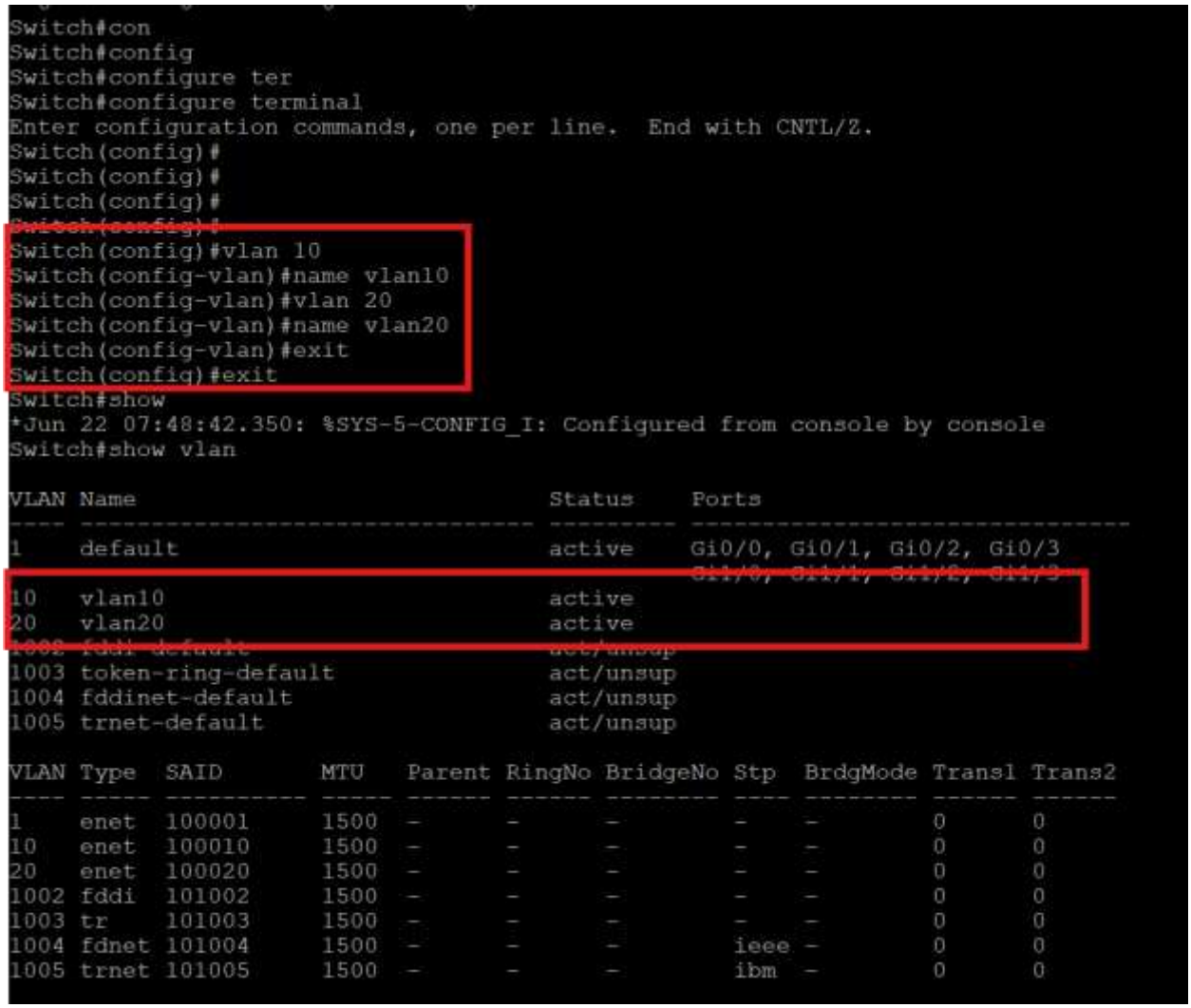
Port gi0/1 will be configured as an access port for VLAN 10
Port gi0/2 will be configured as an access port for VLAN 20

- Win 3 PC (VLAN10-PC) is connected to gi0/1, assigned to VLAN 10
- Another Win 2 PC (VLAN20-PC) is connected to gi0/2, assigned to VLAN 20
- Port gi0/0 on the Cisco switch is connected to Firewall Port 2 and will be configured as a trunk port to carry both VLANs

This configuration allows the firewall to route between VLANs while maintaining proper segmentation between devices on VLAN 10 and VLAN 20.

✅ Step 1 – Creating VLAN 10 and VLAN 20 on the Cisco Switch

Access the Cisco switch using console or SSH and enter the following commands to create the VLANs.



This step creates two VLANs on the switch that will later be used to segment the network between the two PCs

✅ Step 2 – Assign Ports to VLANs

In this step, we'll assign:

- **Port gi0/1** to **VLAN 10**
- **Port gi0/2** to **VLAN 20**

Both ports will be configured as **access ports**, which means each port will carry traffic for **only one VLAN**.

```
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#swi
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport mode access
Switch(config-if)#switch
Switch(config-if)#switchport acc
Switch(config-if)#switchport access vlan
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#inter
Switch(config)#interface gi
Switch(config)#interface gigabitEthernet 0/2
Switch(config-if)#swit
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport mode access
Switch(config-if)#swit
Switch(config-if)#switchport access
Switch(config-if)#switchport access val
Switch(config-if)#switchport access vlan
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch#show
Switch#show
*Jun 22 07:55:04.380: %SYS-5-CONFIG_I: Configured from console by console
% Type "show ?" for a list of subcommands
Switch#show
Switch#show vla
Switch#show vlan br
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/0, Gi0/3, Gi1/0, Gi1/1
10   vlan10                           active    Gi0/1
20   vlan20                           active    Gi0/2
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
Switch#
```

📌 Access ports are typically used for end devices like PCs, ensuring they are placed into the correct VLAN

✅ Step 3 – Configuring Trunk Port on Cisco Switch

In this step, we'll configure **port gi0/0** on the Cisco switch as a **trunk port**. This port connects to the FortiGate firewall and allows traffic from **multiple VLANs (VLAN 10 and VLAN 20)** to pass through. We will specify the **encapsulation method as 802.1Q (dot1q)**, which is the standard VLAN tagging protocol.

```
Switch(config)#inter
Switch(config)#interface gi
Switch(config)#interface gigabitEthernet 0/0
Switch(config-if)#swi
Switch(config-if)#switchport mode trunk
Switch(config-if)#switch
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#
Switch(config-if)#
Switch(config-if)#
```

📌 A trunk port is used to carry multiple VLANs between network devices such as switches, routers, and firewalls.

📌 The **dot1q encapsulation** ensures VLAN tags are added to Ethernet frames, allowing multiple VLANs to be carried on the same physical link.

✅ Step 4 – Assign Static IP Addresses to PCs

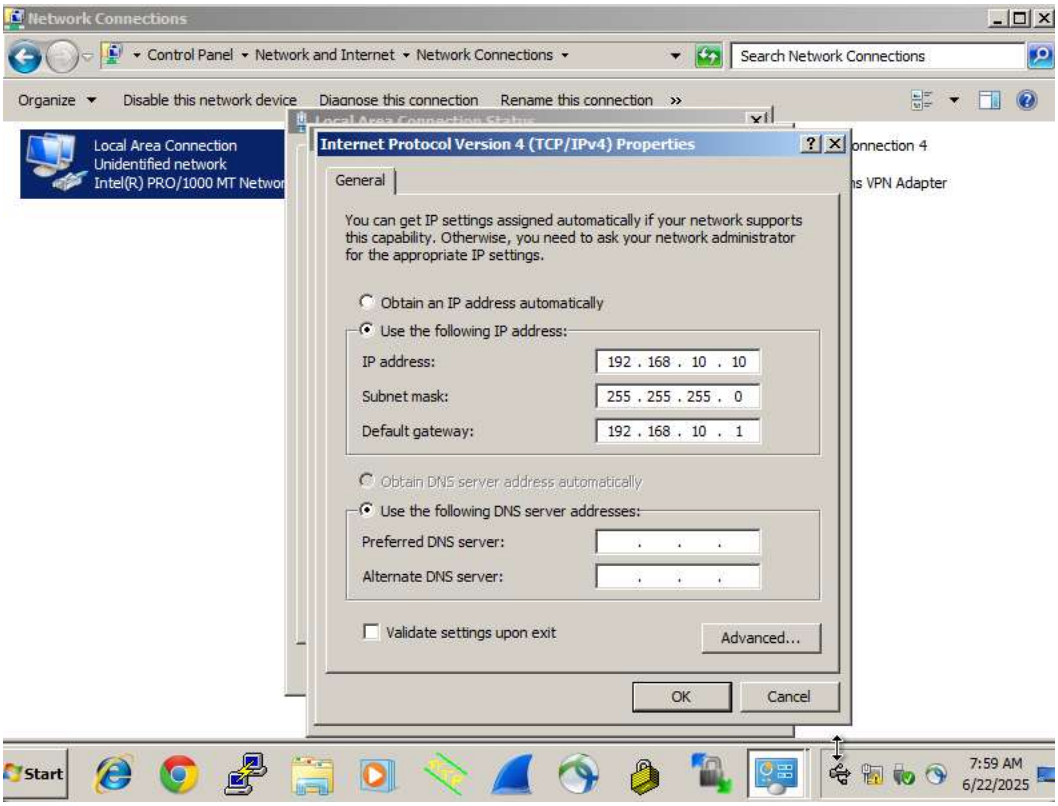
In this step, we will assign static IP addresses to the PCs in their respective VLANs to ensure proper network communication.

- **PC in VLAN 10 (Win3 PC):** Assign IP address **192.168.10.10** with subnet mask **255.255.255.0**
- **PC in VLAN 20 (Win2 PC):** Assign IP address **192.168.20.20** with subnet mask **255.255.255.0**

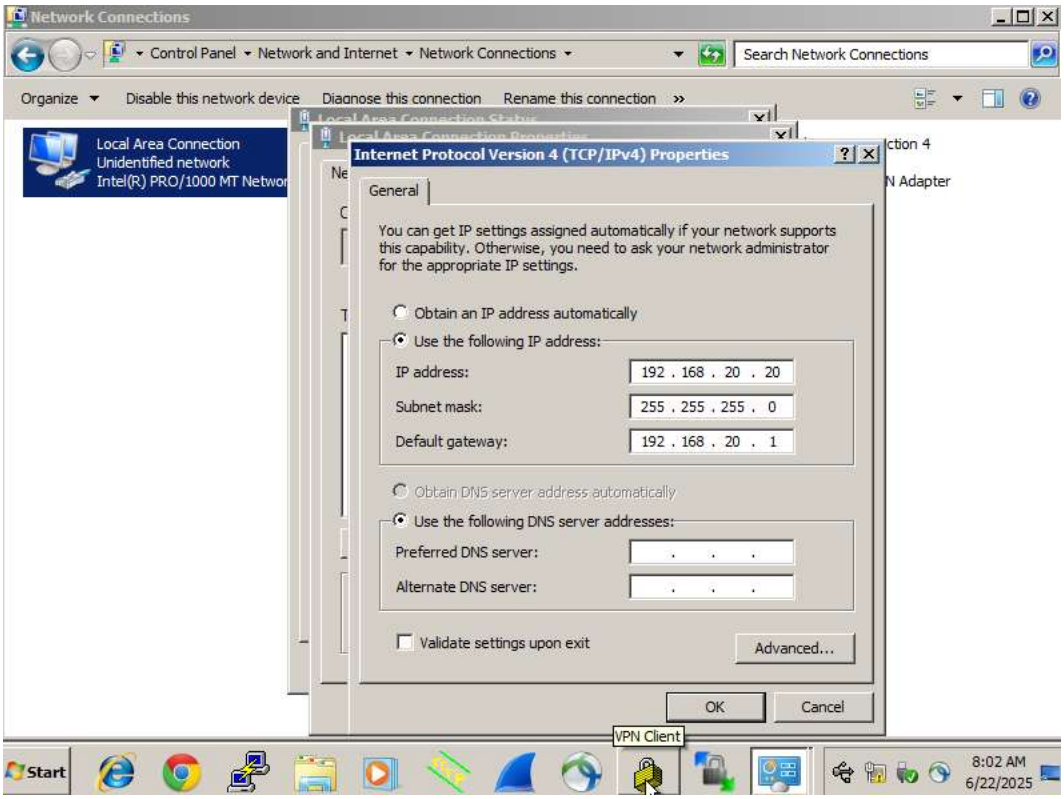
- **How to Assign Static IP (Windows PC):**

1. Open **Network Settings**
2. Navigate to **Change adapter options**
3. Right-click the active network adapter and select **Properties**
4. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**
5. Choose **Use the following IP address:**
    - Enter the IP address, subnet mask, and default gateway (firewall VLAN interface IP)
6. Click **OK** to save changes

VLAN 10 PC



VLAN 20 PC

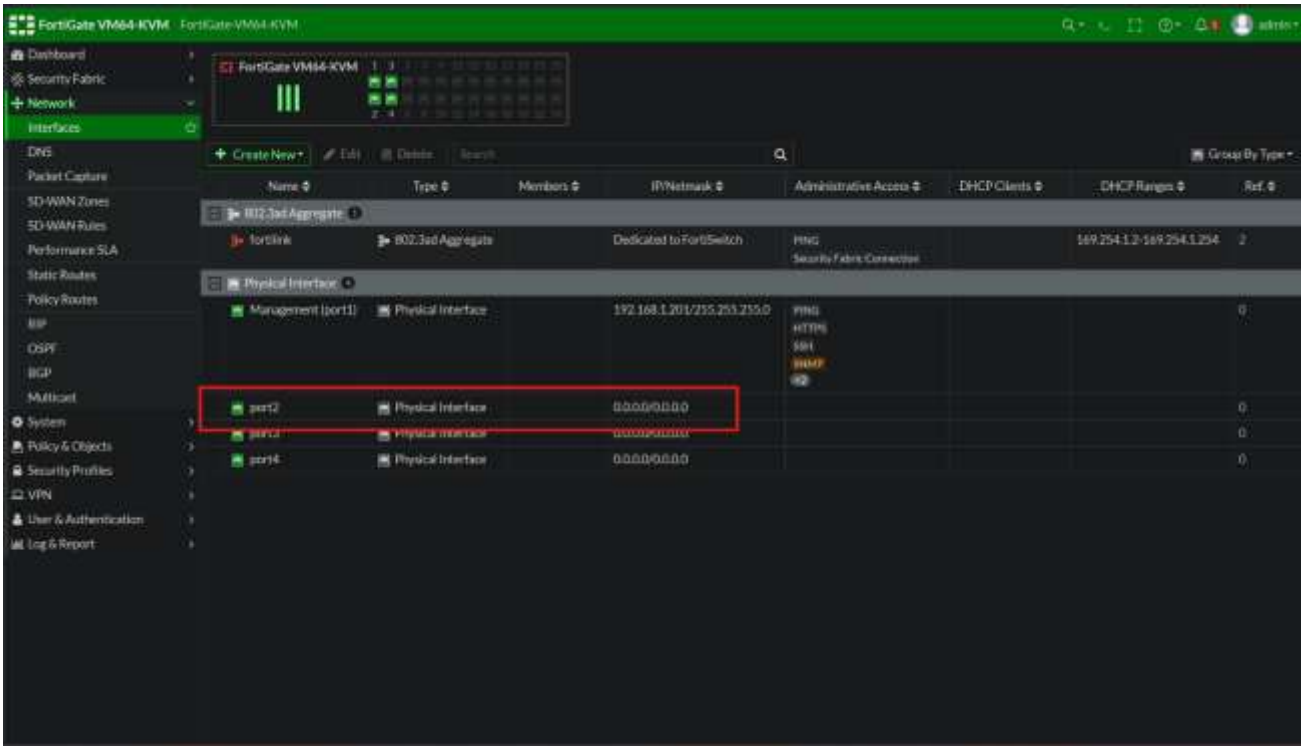


✅ Step 5 – Assign LAN Role to FortiGate Port

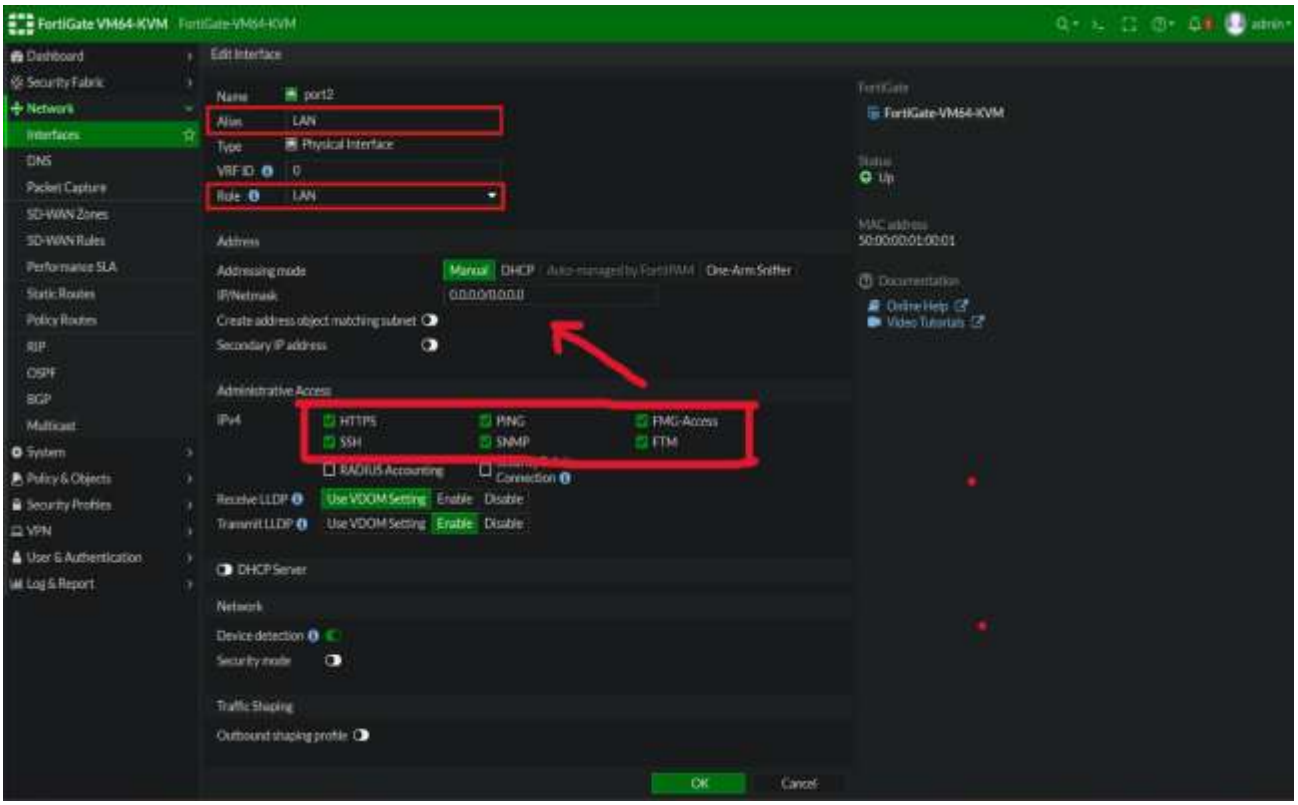
In this step, we configure **Port 2** on the FortiGate firewall and assign it the **LAN role**. This port connects to the Cisco switch and handles the VLAN traffic (VLAN 10 and VLAN 20).

- **Steps:**

1. Log in to the **FortiGate GUI**
2. Go to **Network > Interfaces**
3. Click on **Port2** to edit it or double-click to open its configuration settings.

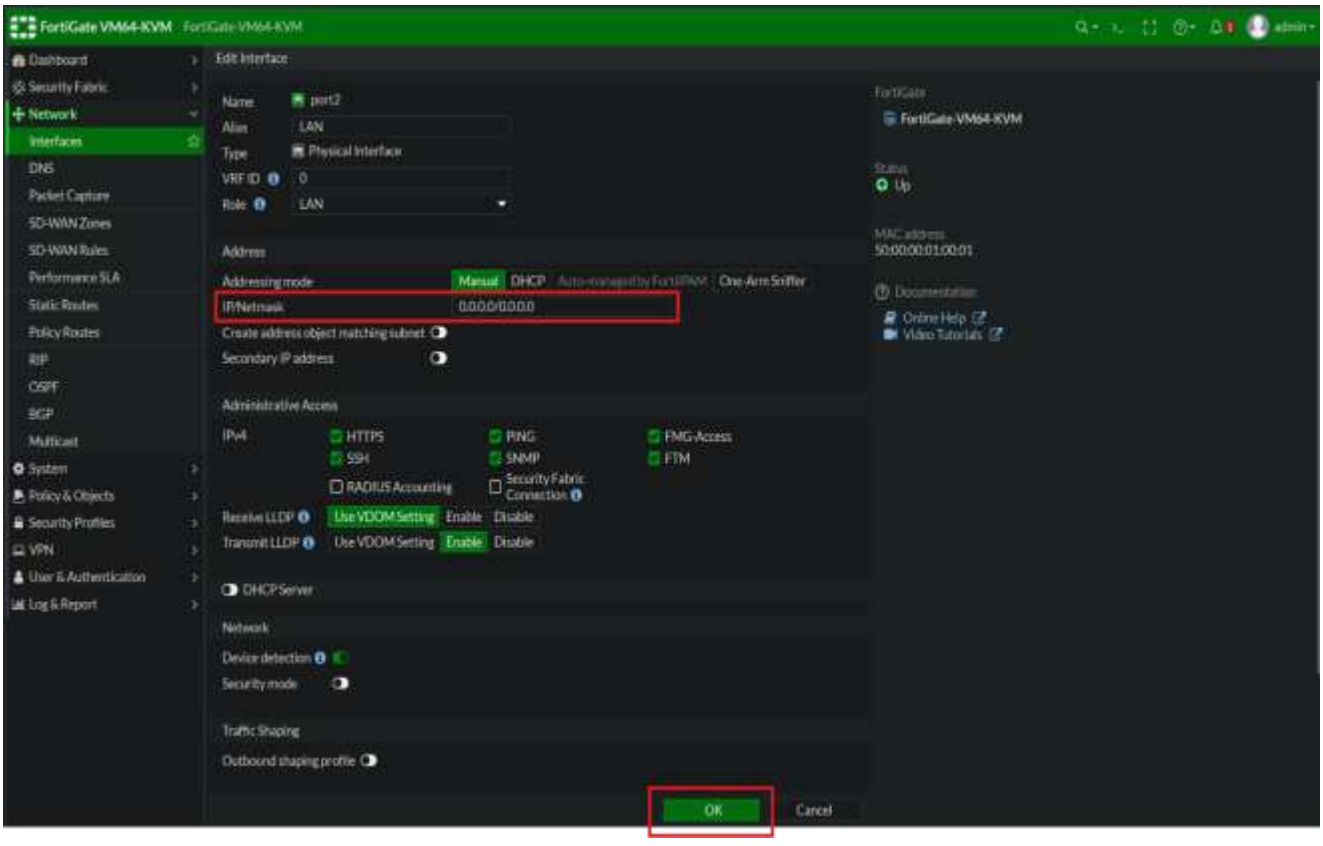


4. In the interface settings:



1. **Under Role**, select LAN and set the *Alias* to LAN for easier identification
2. **Administrative Access:** Enable only the necessary services like:
    1. **HTTPS**
    2. **HTTP**
    3. **PING**
    4. **SSH**
    5. **SNMP** *(if needed for monitoring)*

5. Leave the **IP address field blank**, since Port 2 will act as a trunk and the IPs will be assigned to VLAN sub-interfaces.



6. Click **OK** to save the configuration

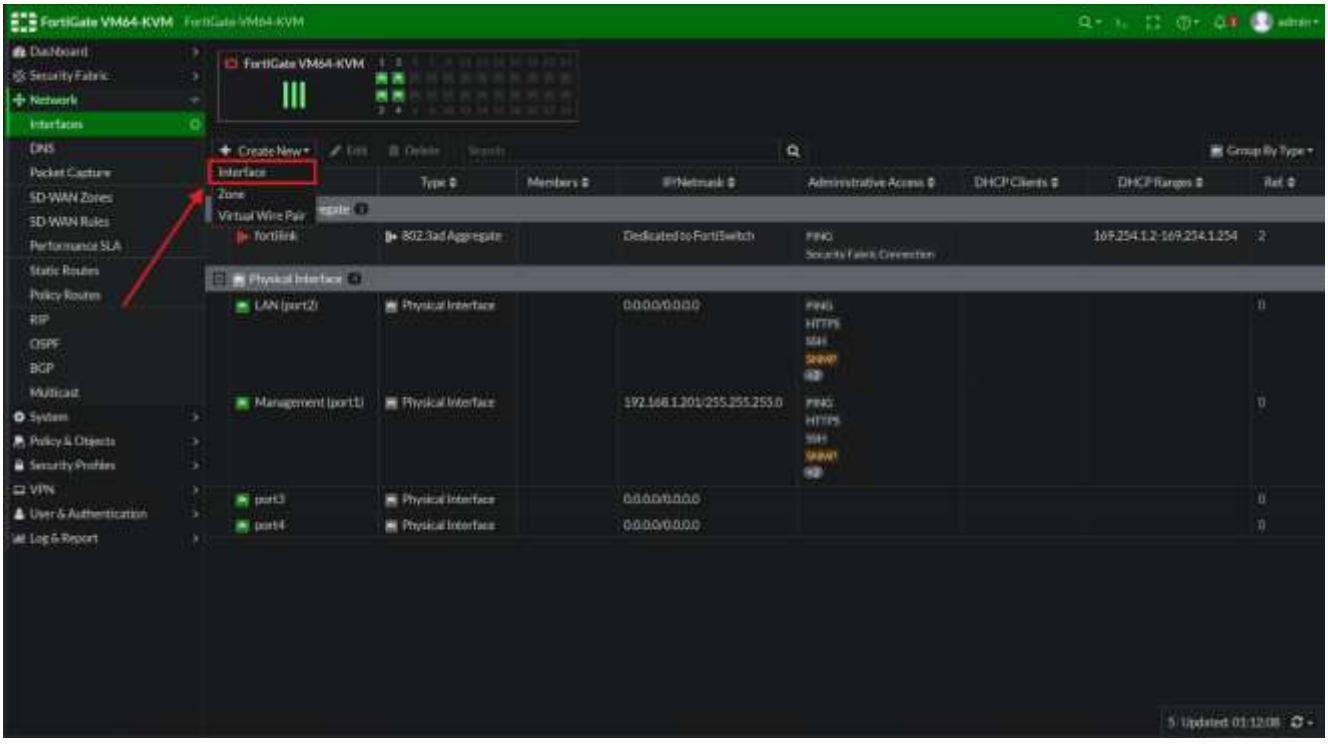
📌 This step prepares Port 2 to carry VLAN traffic without directly assigning it an IP address. VLAN interfaces will handle the IP addressing for each subnet.

✅ Step 6 – Configuring VLAN Interfaces for VLAN 10 and VLAN 20 on FortiGate

In this step, we will create VLAN sub-interfaces on Port2 of the FortiGate firewall. These sub-interfaces will handle traffic for VLAN 10 and VLAN 20. Port2 acts as the physical trunk port for both VLANs.

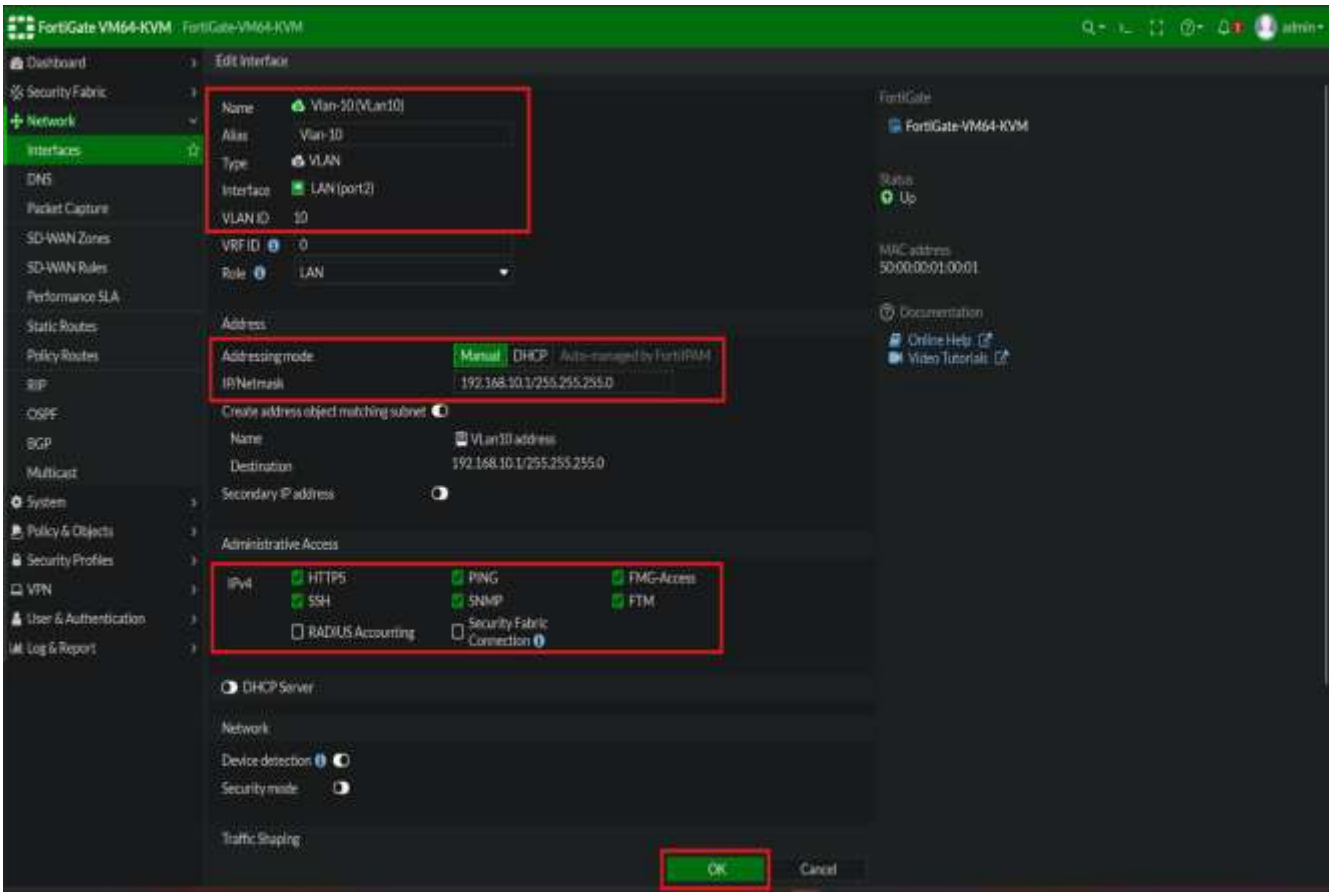
🔹 Steps to Create VLAN 10 Interface:

1. Go to **Network > Interfaces**
2. Click the Create New button and select **Interface**



3. In the interface configuration window:
    - Name: vlan10
    - Alias: VLAN-10
    - Type: VLAN

- Interface: Port2 (this will bind the VLAN to the physical port)
- VLAN ID: 10
- IP/Netmask: 192.168.10.1/255.255.255.0
- Administrative Access: Select options as needed (e.g., HTTPS, PING, SSH)

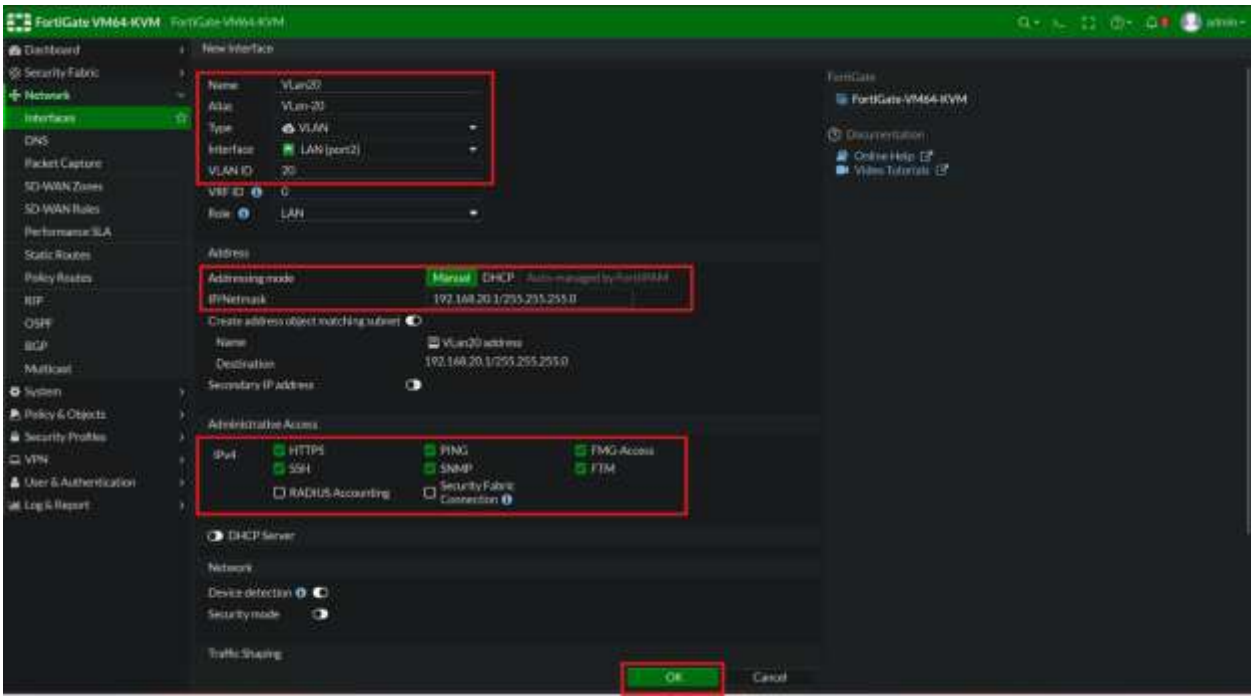


4. Click OK to save the VLAN 10 interface

Steps to Create VLAN 20 Interface:

1. Repeat the above steps to create another interface
2. Use the following settings:
   - Name: vlan20

- Alias: VLAN-20
- Type: VLAN
- Interface: Port2
- VLAN ID: 20
- IP/Netmask: 192.168.20.1/255.255.255.0
- Administrative Access: Enable as required



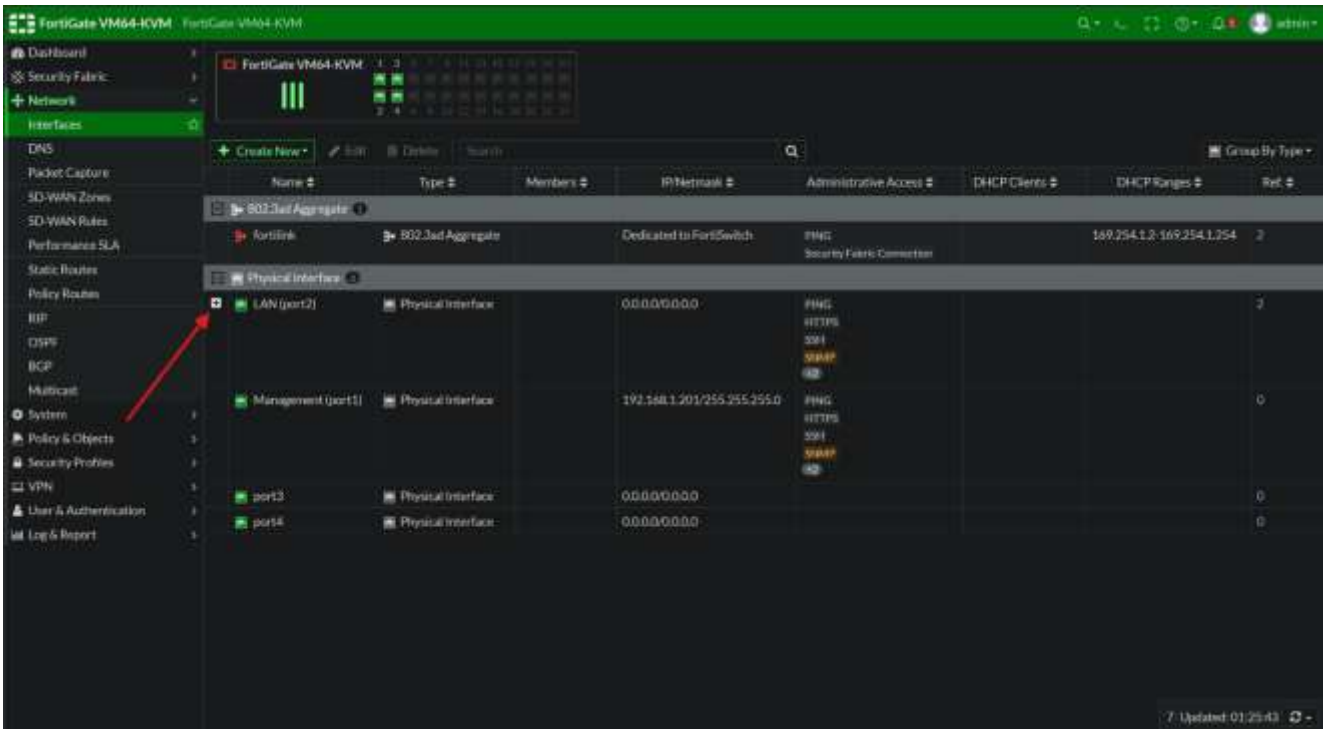
3. Click OK to save the VLAN 20 interface

📌 These VLAN interfaces act as the **default gateways** for devices in their respective VLANs.
If inter-VLAN routing is configured, communication between VLANs will be possible through the FortiGate firewall.

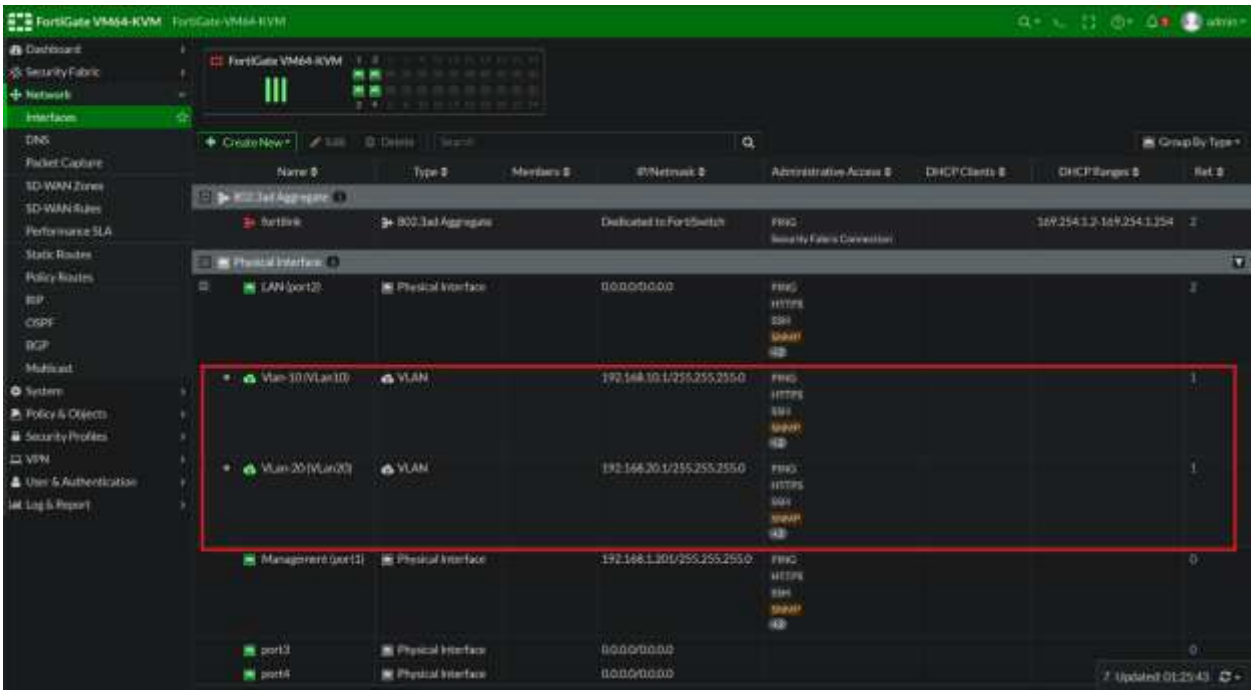
However, in this setup, we are **not configuring inter-VLAN routing**, so **devices in VLAN 10 and VLAN 20 will remain isolated** from each other unless explicit firewall policies are created.

Verifying VLAN Interfaces:

After creating both VLAN interfaces, go back to **Network > Interfaces** and **expand Port2**.



You will now see both **vlan10** and **vlan20** listed under Port2, indicating they are sub-interfaces associated with that physical port.



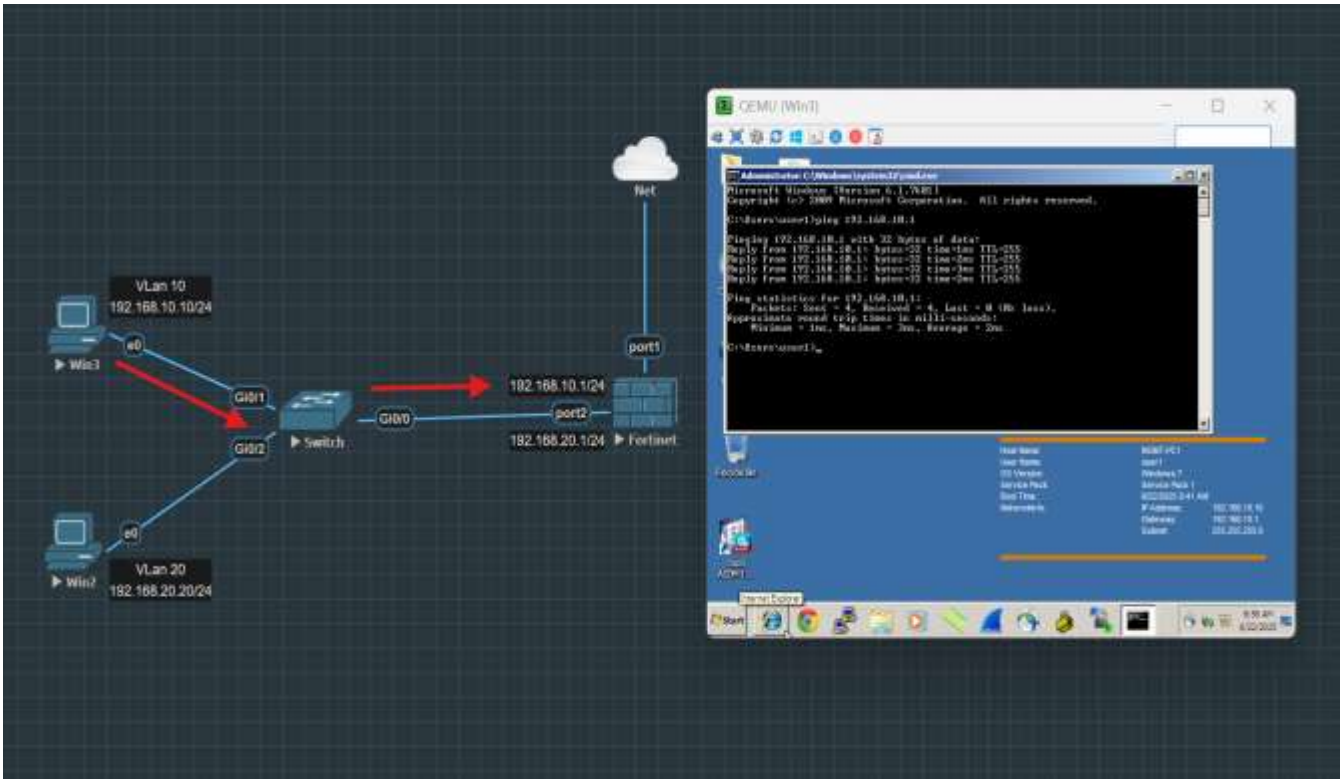
📌 This confirms that Port2 is now acting as a **trunk port**, carrying traffic for both VLANs.

✅ Step 7 – Testing the Connectivity

After completing the VLAN and interface configuration, the next step is to verify basic network connectivity between the PCs and the firewall.

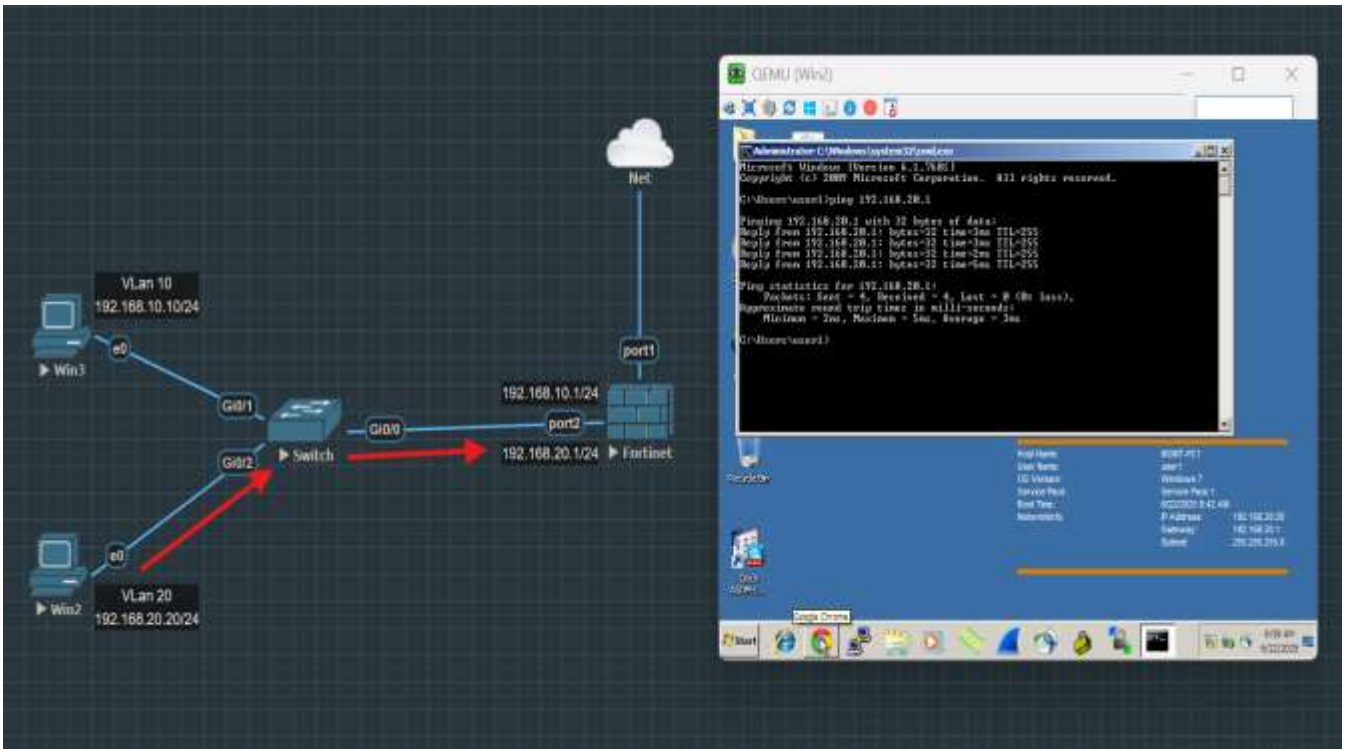
From VLAN 10 PC (192.168.10.10)

- Ping the firewall VLAN 10 interface: 192.168.10.1



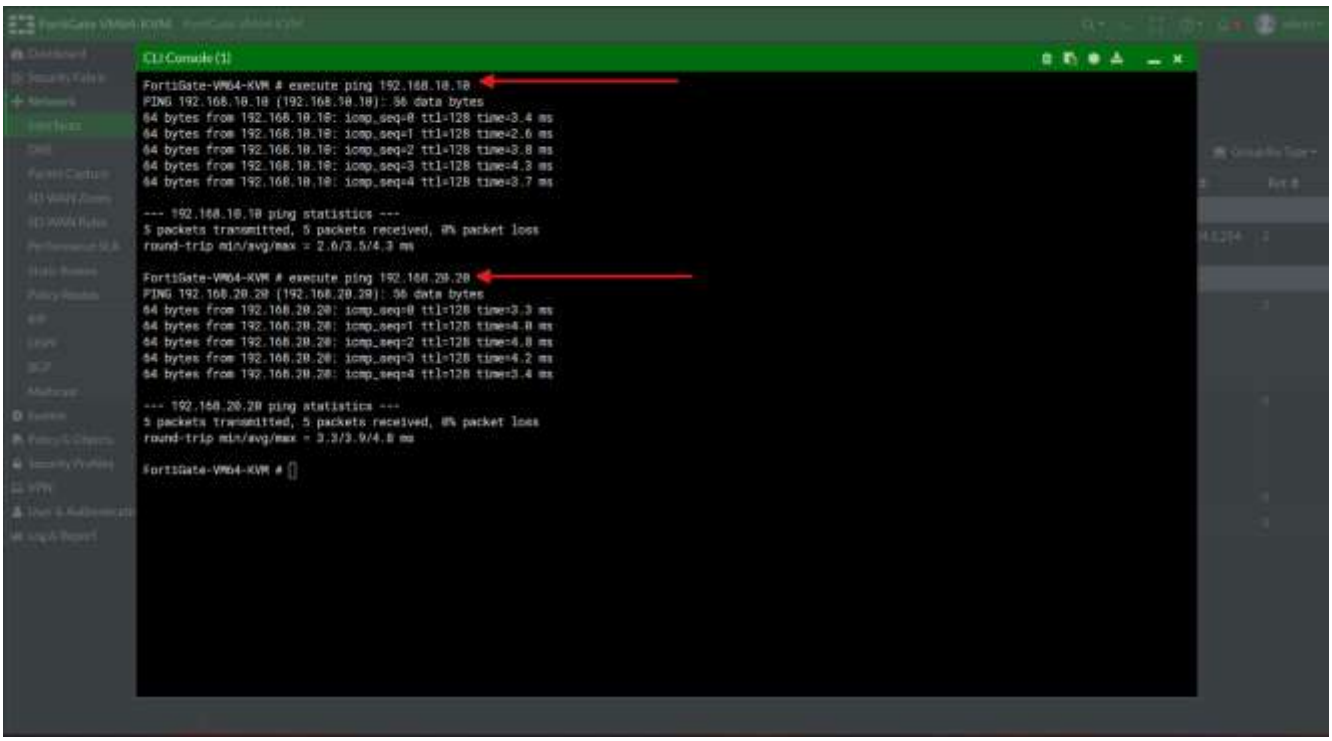
From VLAN 20 PC (192.168.20.20)

- Ping the firewall VLAN 20 interface: 192.168.20.1



From Firewall CLI (optional):

- Use the FortiGate CLI or GUI to ping both PCs to verify reachability:



📌 If all pings are successful, it confirms that the VLANs are properly configured, interfaces are reachable, and connectivity between the **firewall and the PCs** is working correctly.

⚠️ Note: Since we have **not configured inter-VLAN routing**, the PCs in VLAN 10 and VLAN 20 **cannot communicate with each other**, which is expected.

Thanks
for your time!

Keep learning, and keep growing!....