



# **VLAN and Inter-VLAN Routing with FortiGate**

## **Final Report**

Created BY :

Mohamed Ayman

Mohamed Nader

Moaz Mahmoud

Osama Ahmed



# INTRODUCTION

A virtual local area network (VLAN) is a local area network broadcast domain that is partitioned and isolated in a virtual network at the data link layer, A VLAN behaves like a virtual network switch or network link that can share the same physical structure with other VLANs while staying logically separate from them. (Logical Partition)

The objective of this project was to design, configure, and validate a VLAN-based network that supports inter-VLAN routing, centralized security, and proper segmentation. The project was completed in four stages: VLAN configuration, FortiGate integration, trunk implementation, and final reporting.

## Project Overview

### **Week 1** — VLAN Configuration Basics:

Create VLANS on the switch, and assigning them Ports/IP.

### **Week 2** — FortiGate VLAN Integration:

Create VLAN interfaces on Fortigate, Build Firewall Policies

### **Week 3** — Advanced Features & Testing:

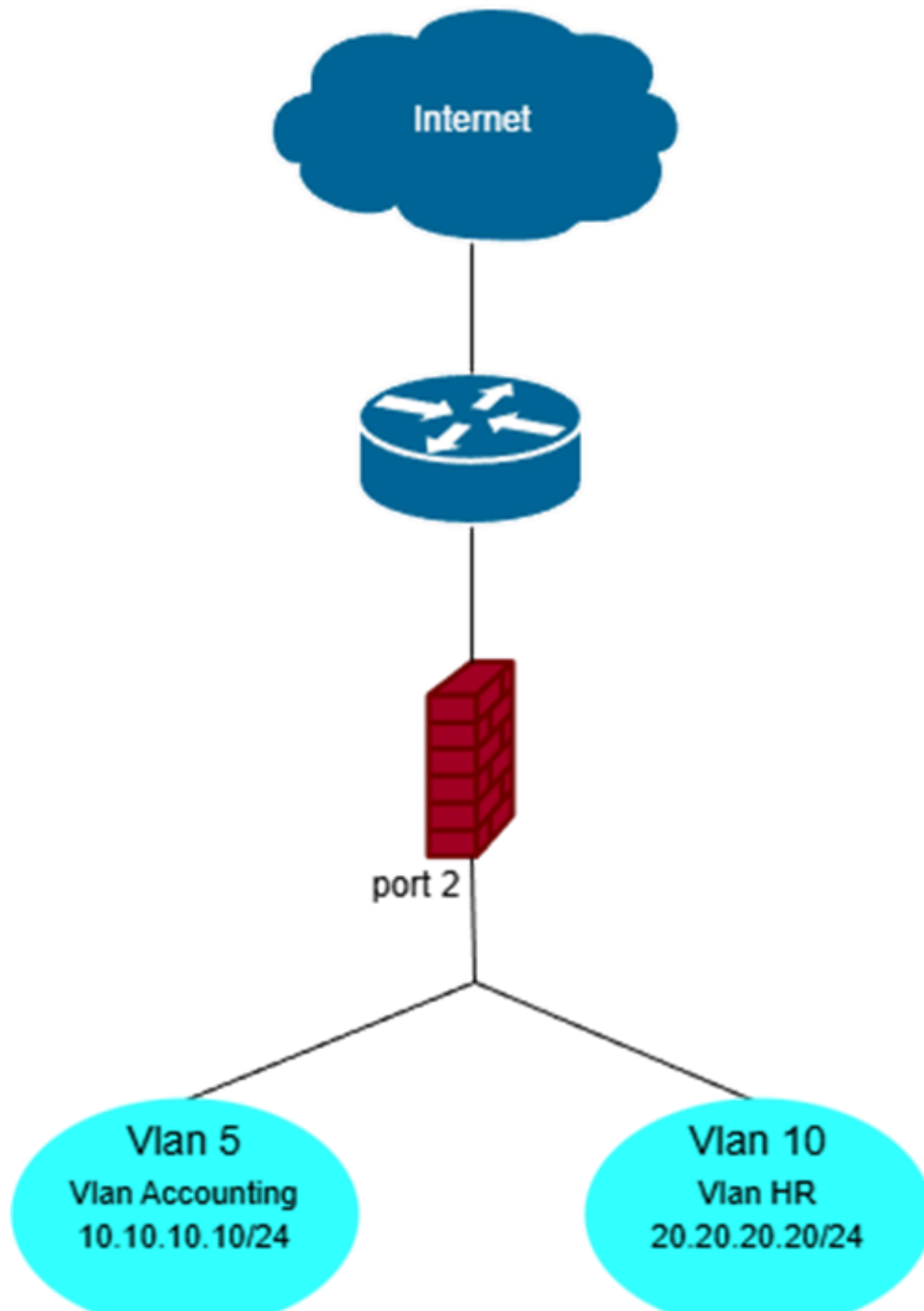
Implement VLAN trunks, and verify InterVLAN communication, Status and Connectivity

### **Week 4** — Final Report & Presentation

Documentation of all steps and Progress up until final completion



# NETWORK TOPOLOGY





# VLAN CONFIGURATION

The first Phase of the implementation was creating the actual VLANs and then configuring them.

The final Decision was to implement two VLANS

- 1.VLAN\_Accounting
2. VLAN\_Hr

both on port 2 , ordered in this priority, the following snapshots contain the configuration settings for both.

Admin Access: HTTPS, SSH, Ping

## VLAN\_Accounting

New Interface

FortiGate

HQ-NGFW-1

Additional Information

API Preview

Edit in CLI

Online Guides

Relevant Documentation

Video Tutorials

Fortinet Community

AWS Fortigate WAN IP

3 Answers 0 Votes 599 Views

CHANGED SUBNET FROM LAN TO WAN

5 Answers 0 Votes 401 Views

External interface drops every 10 minutes

9 Answers 0 Votes 499 Views

See More

Name: VLAN\_Accounting

Alias:

Type: VLAN

VLAN protocol: 802.1Q 802.1AD

Interface: port2

VLAN ID: 5

VRF ID: 0

Role: LAN

Address

Addressing mode: Manual IPAM DHCP PPPoE One-Arm Sniffer

IP/Netmask: 10.10.10.0/24

Create address object matching subnet: ☒

Name: VLAN\_Accounting address

Destination: 10.10.10.0/24

Secondary IP address: ☐

OK Cancel

## VLAN\_Hr

New Interface

FortiGate

HQ-NGFW-1

Additional Information

API Preview

Edit in CLI

Online Guides

Relevant Documentation

Video Tutorials

Fortinet Community

AWS Fortigate WAN IP

3 Answers 0 Votes 599 Views

CHANGED SUBNET FROM LAN TO WAN

5 Answers 0 Votes 401 Views

External interface drops every 10 minutes

9 Answers 0 Votes 499 Views

See More

Name: VLAN\_Hr

Alias:

Type: VLAN

VLAN protocol: 802.1Q 802.1AD

Interface: port2

VLAN ID: 10

VRF ID: 0

Role: LAN

Address

Addressing mode: Manual IPAM DHCP PPPoE One-Arm Sniffer

IP/Netmask: 20.20.20.0/24

Create address object matching subnet: ☒

Name: VLAN\_Hr address

Destination: 20.20.20.0/24

Secondary IP address: ☐

OK Cancel



Inter-VLAN routing is automatically implemented on the FortiGate lab environment, in which the project was done.

## Firewall Policy

Even though routing exists, FortiGate requires explicit policies to allow traffic between interfaces. This ensures proper segmentation and security.

Two Security Profiles were created:

- VLAN\_Accounting → VLAN\_Hr
- VLAN\_Hr→ VLAN\_Accounting

These policies allowed ping tests and general connectivity between the two VLAN networks.

VLAN\_Accounting → VLAN\_Hr Policy Snapshot

Create New Policy

Name ⓘAccounting\_to\_Hr

Schedulealways

Action

✓ ACCEPT

✗ DENY

Incoming interfaceVLAN\_Accounting

Outgoing interfaceVLAN\_Hr

Source & DestinationShow logic

SourceVLAN\_Accounting address

User/group

DestinationVLAN\_Hr address

ServiceALL

Additional Information

API Preview

Online Guides

Relevant Documentation

Video Tutorials

Consolidated Policy Configuration

Fortinet Community

Trouble with firewall policies

8 Answers0 Votes1,499 Views

Firewall policy denying all traffic question

4 Answers0 Votes1,600 Views

Assistance to allow external access to your IIS server

11 Answers0 Votes1,499 Views

See More

VLAN\_Accounting → VLAN\_Hr  
Policy Snapshot

VLAN\_Hr→ VLAN\_Accounting  
Policy Snapshot

Create New Policy

Name ⓘHr\_to\_Accounting

Schedulealways

Action

✓ ACCEPT

✗ DENY

Incoming interfaceVLAN\_Hr

Outgoing interfaceVLAN\_Accounting

Source & DestinationShow logic

SourceVLAN\_Hr address

User/group

DestinationVLAN\_Accounting address

ServiceALL

Additional Information

API Preview

Online Guides

Relevant Documentation

Video Tutorials

Consolidated Policy Configuration

Fortinet Community

Trouble with firewall policies

8 Answers0 Votes1,499 Views

Firewall policy denying all traffic question

4 Answers0 Votes1,600 Views

Assistance to allow external access to your IIS server

11 Answers0 Votes1,499 Views

See More



# Verification

To prove that both VLANs were up and running independent of each other , two pings were preformed

```
HQ-NGFW-1 # execute ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10): 56 data bytes
64 bytes from 10.10.10.10: icmp_seq=0 ttl=255 time=0.0 ms
64 bytes from 10.10.10.10: icmp_seq=1 ttl=255 time=0.0 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 10.10.10.10: icmp_seq=3 ttl=255 time=0.0 ms
64 bytes from 10.10.10.10: icmp_seq=4 ttl=255 time=0.0 ms

--- 10.10.10.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

HQ-NGFW-1 # execute ping 20.20.20.20
PING 20.20.20.20 (20.20.20.20): 56 data bytes
64 bytes from 20.20.20.20: icmp_seq=0 ttl=255 time=0.0 ms
64 bytes from 20.20.20.20: icmp_seq=1 ttl=255 time=0.0 ms
64 bytes from 20.20.20.20: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 20.20.20.20: icmp_seq=3 ttl=255 time=0.0 ms
64 bytes from 20.20.20.20: icmp_seq=4 ttl=255 time=0.0 ms

--- 20.20.20.20 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

The successful pings indicate that both VLANs were working, separately of each other, in the next sections we shall verify their inter-communication.

## VLAN Trunking & Testing

A VLAN trunk allows multiple VLANs to be carried over a single physical link. In this Project, The switch uplink port 2 is configured as a trunk, this ensures the VLAN tagging is maintained end to end.

Trunk Implementation Snapshot:

<input type="checkbox"/>	port2	Physical Interface	100.65.0.101/255.255.255.0	PING HTTPS SSH HTTP
<input type="checkbox"/>	VLAN_Accounting	VLAN	10.10.10.10/255.255.255.0	PING HTTPS SSH
<input type="checkbox"/>	VLAN_Hr	VLAN	20.20.20.20/255.255.255.0	PING HTTPS SSH

handling multiple VLANs on the same physical port which means trunking is active





## INTER-VLAN COMMUNICATION

After Previously testing both VLANs independently of each other , we needed to make sure their communication is open between one another , and that inter-VLAN routing is active.

This was done using two pings , where each VLAN alternated being the source and the receiver

Testing Snapshots:

```
HQ-NGFW-1 # execute ping-options source 20.20.20.20

HQ-NGFW-1 # execute ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10): 56 data bytes
64 bytes from 10.10.10.10: icmp_seq=0 ttl=255 time=0.0 ms
64 bytes from 10.10.10.10: icmp_seq=1 ttl=255 time=0.0 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 10.10.10.10: icmp_seq=3 ttl=255 time=0.0 ms
64 bytes from 10.10.10.10: icmp_seq=4 ttl=255 time=0.0 ms

--- 10.10.10.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

HQ-NGFW-1 #
```

```
HQ-NGFW-1 # execute ping-options source 10.10.10.10

HQ-NGFW-1 # execute ping 20.20.20.20
PING 20.20.20.20 (20.20.20.20): 56 data bytes
64 bytes from 20.20.20.20: icmp_seq=0 ttl=255 time=0.0 ms
64 bytes from 20.20.20.20: icmp_seq=1 ttl=255 time=0.0 ms
64 bytes from 20.20.20.20: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 20.20.20.20: icmp_seq=3 ttl=255 time=0.0 ms
64 bytes from 20.20.20.20: icmp_seq=4 ttl=255 time=0.1 ms

--- 20.20.20.20 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.1 ms

HQ-NGFW-1 #
```

Testing Results:

Connectivity between VLANs was achieved successfully. All routing was performed by FortiGate using VLAN and firewall policy controls.



## CONCLUSION

A fully functional VLAN-based network was designed and implemented.

The FortiGate firewall handled inter-VLAN routing, security policies, and management access.

Trunk ports were configured successfully, and all connectivity tests passed.

This project demonstrated the full design and implementation of VLAN segmentation using modern best practices. With the use of FortiGate as a Layer 3 switch.