VLAN and Inter-VLAN Routing with FortiGate

Fortinet Cyber Security Engineer - Digital Egyptian Pioneer (DEPI)

Team Members

- Rinad Samy Abdel Samad **ID:** 21032755
- Mario George Kamal **ID:** 21075137
- Marina Magdy Khalil **ID:** 21070617
- Mennatullah Mohamed Islam **ID:** 21045185
- Mostafa Kamel Helmy **ID:** 21042500
- Sherry Romany Abdel Malak **ID:** 21070357
- Antonios Farid Fouad Said **ID:** 21032607

Table of Contents

List of Figures 03

List of Tables 03

1. Introduction 05

1.1 Project Overview 04

1.2 Aims and Objectives 04

2. Network Design and Topology 05

2.1 Network Topology 05

2.2 Device Description and Roles 05

2.3 IP Addressing Plan 05

3. VLAN Basic Configuration 07

3.1 VLAN Creation 07

3.2 Inter-VLAN Routing Foundation 07

3.3 Testing and Verification 08

4. FortiGate Integration 09

4.1 Interfaces Configuration 09

4.2 Firewall Policy Design 10

4.3 Connectivity Testing 11

5. Advanced VLAN Features and Testing 12

5.1 Implementing VLAN Trunking 12

5.2 VLAN Communication Tests 12

5.3 Troubleshooting Findings 12

6. Final Result and Analysis 14

6.1 Summary of Configuration Success 14

6.2 Security Implications 14

6.3 Strengths and Limitations 14

7. Conclusion 15

7.1 Key Learnings 15

7.2 Network Expansion Opportunities 15

List of Figures

Figure2.1 Network Full Topology 05
Figure 3.1.a Creating VLAN.....07
Figure 3.1.b Assigning ports to VLANs 07
Figure 3.1.c Trunk Port Configuration.....07
Figure 3.2.a SVI Configuration 07
Figure 3.2.b DHCP Configuration 08
Figure 3.2.b routing through l3 switch.....08
Figure 3.3.a VPCs IP Assignment.....08
Figure 3.3.b Communication Testing.....08
Figure 4.1.a Port3 Configuration 09
Figure 4.1.b VLAN sub interfaces configuration 09
Figure 4.1.c Port4 Configuration 09
Figure 4.1.d Addresses and Group Addresses.....10
Figure 4.2.b NAT IP Pool.....10
Figure 4.2.c FortiGate Policies Implementation 11
Figure 4.3.a VLAN to Gateway Connectivity 12
Figure 4.3.b.a Inter-VLAN Connectivity.....12
Figure 4.3.b.b To-Brach VLAN Connectivity 12
Figure 5.1.b Native VLAN 13
Figure 5.3.a Interfaces Issue resolved.....13
Figure 5.3.b NAT Issue resolved.....14

List of Tables

Table 2.3.1 FortiGate Firewall IP Addressing Table 06
Table 2.3.2 L3 Switch IP Adrressing Table 06
Table 2.3.3 Router IP Adrressing Table 06
Table 2.3.4 VPCs IP Adrressing Table.....06
Table 4.2.c FortiGate Policies Implementation 11
Table 5.2 VLAN Communication Tests.....13

1. Introduction

1.1.Project Overview

This Comprehensive network infrastructure project focuses on designing and implementing a secure, segmented network architecture using VLAN technology integrated with FortiGate next-generation firewall capabilities. The project establishes a robust network foundation that segregates departmental traffic between Human Resources (HR) and Information Technology (IT) divisions while maintaining controlled inter-departmental communication. By leveraging FortiGate's advanced security features, the implementation provides granular control over network traffic flows, ensuring both operational efficiency and security compliance. The solution demonstrates enterprise-grade network segmentation principles that can accommodate future organizational growth and additional departmental requirements.

1.2.Aims and Objectives

The primary objectives of this project encompass both technical implementation and security governance:

Network Segmentation & VLAN Implementation
Creating clearly defined network boundaries between departments stood as our primary technical goal. We established separate VLANs for HR and IT teams, ensuring that each department operates within its own dedicated network space.

Inter-VLAN Routing & Security
Establish controlled communication between VLANs through firewall policies with service-level access controls.

Internet & External Connectivity
Provide secure internet access with proper NAT configuration and external router communication.

Operational Management & Monitoring
Develop comprehensive documentation and testing procedures for ongoing network management.

2. Network Design and Topology

2.1.Network Topology

The implemented network architecture features a hierarchical design with clear separation between internal departmental networks and external connectivity, providing both security and scalability for future expansion.

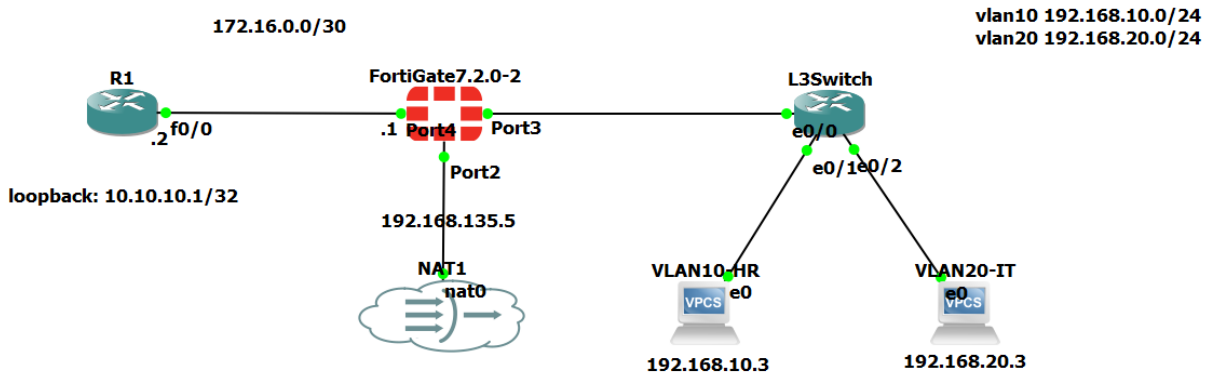


Figure2.1 Network Full Topology

2.2.Device Description and Roles

- **FortiGate Firewall:** Primary security enforcement point and inter-VLAN router
- **Cisco L3 Switch**: VLAN access layer and DHCP services
- **Cisco Router**: External network simulation and internet gateway
- **HR Department Workstations:** VLAN 10 devices for Human Resources
- **IT Department Workstations:** VLAN 20 devices for Information Technology

2.3.IP Addressing Plan

The implemented network architecture features a hierarchical design with clear separation between internal departmental networks and external connectivity, providing both security and scalability for future expansion.

2.3.1 FortiGate Firewall

	IP address	Subnet Mask	Purpose
Port2	192.168.135.5	255.255.255.0	WAN Connection to Internet and Management Access
Port3	NA	NA	VLAN Trunk to Switch
	192.168.10.1	255.255.255.0	VLAN10 - HR Department Gateway
	192.168.20.1	255.255.255.0	VLAN20 - IT Department Gateway
Port4	172.16.0.1	255.255.255.252	LAN Connection to Router (Another Branch)

Table 2.3.1 FortiGate Firewall IP Adrressing Table

2.3.2 Cisco L3 Switch

	Type	IP address	Subnet Mask	Purpose
e0/0	Trunk	NA	NA	To FortiGate port3
e0/1	Access	NA	NA	HR Department Access
e0/2	Access	NA	NA	IT Department Access
VLAN10	SVI	192.168.10.2	255.255.255.0	DHCP Services
VLAN20	SVI	192.168.20.2	255.255.255.0	DHCP Services

Table 2.3.2 L3 Switch IP Adrressing Table

2.3.3 Cisco Router

	Type	IP address	Subnet Mask	Purpose
f0/0	Physical	172.16.0.2	255.255.255.252	To FortiGate port4
Loopback	Logical	10.10.10.1	255.255.255.255	Management

Table 2.3.3 Router IP Adrressing Table

	VLAN	VPC IP address	Subnet Mask	Gateway
HR	10	192.168.10.3	255.255.255.0	192.168.10.1
IT	20	1192.168.20.3	255.255.255.1	192.168.20.1

2.3.4 End Devices

Table 2.3.4 VPCs IP Adrressing Table

3. VLAN Configuration Basics

3.1.VLAN Creation

a. Creating VLANs

```
L3Switch(config)#vlan 10
L3Switch(config-vlan)#name HR
L3Switch(config-vlan)#vlan 20
L3Switch(config-vlan)#name IT
```

Figure 3.1.a Creating VLAN

b. Assigning ports to VLANs

```
L3Switch(config-if)#int e0/1
L3Switch(config-if)#switchport mode access
L3Switch(config-if)#switchport access vlan 10
L3Switch(config-if)#no shutdown
```

```
L3Switch(config-if)#int e0/2
L3Switch(config-if)#switchport mode access
L3Switch(config-if)#switchport access vlan 20
L3Switch(config-if)#no shutdown
```

Figure 3.1.b Assigning ports to VLANs

c. Trunk port Configuration

```
L3Switch(config)#int e0/0
L3Switch(config-if)#switchport mode trunk
L3Switch(config-if)#switchport trunk allowed vlan 10,20
L3Switch(config-if)#no shutdown
L3Switch(config-if)#
```

Figure 3.1.c Trunk port Configuration

3.2.Inter-VLAN routing Foundation

a. SVI Configuration

Switch Virtual Interfaces (SVIs) were configured to provide IP management access and DHCP services for each VLAN while maintaining FortiGate as the default gateway.

```
L3Switch(config-if)#int vlan10
L3Switch(config-if)#ip add 192.168.10.2 255.255.255.0
L3Switch(config-if)#no shutdown
L3Switch(config-if)#
L3Switch(config-if)#int vlan20
L3Switch(config-if)#ip add 192.168.20.2 255.255.255.0
L3Switch(config-if)#no shutdown
```

Figure 3.2.a SVI Configuration

b. DHCP Configuration

```
L3Switch(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.2
L3Switch(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.2
L3Switch(config)#ip dhcp pool HR
L3Switch(dhcp-config)#network 192.168.10.0 255.255.255.0
L3Switch(dhcp-config)#default-router 192.168.10.1
L3Switch(dhcp-config)#dns-server 8.8.8.8
L3Switch(dhcp-config)#
L3Switch(dhcp-config)#ip dhcp pool IT
L3Switch(dhcp-config)#network 192.168.20.0 255.255.255.0
L3Switch(dhcp-config)#default-router 192.168.20.1
L3Switch(dhcp-config)#dns-server 8.8.8.8
L3Switch(dhcp-config)#
L3Switch(dhcp-config)#end
```

Figure 3.2.b DHCP Configuration

As a foundation for inter-VLAN routing we will make L3 switch responsible for the routing, but in the next phases FortiGate will be the component responsible for it.

```
L3Switch(config-if)#ip routing
```

Figure 3.2.b routing through l3 switch

3.3. Testing and Verification

a. VPCs IP assignment

```
VLAN10-HR> dhcp
DDORA IP 192.168.10.3/24 GW 192.168.10.1
```

```
VLAN20-IT> dhcp
DDORA IP 192.168.20.3/24 GW 192.168.20.1
```

Figure 3.3.a VPCs IP Assignment

b. Inter-VLAN Communication

```
VLAN10-HR> ping 192.168.20.3
84 bytes from 192.168.20.3 icmp_seq=1 ttl=63 time=3.666 ms
84 bytes from 192.168.20.3 icmp_seq=2 ttl=63 time=2.727 ms
84 bytes from 192.168.20.3 icmp_seq=3 ttl=63 time=2.347 ms
84 bytes from 192.168.20.3 icmp_seq=4 ttl=63 time=1.666 ms
```

```
VLAN20-IT> ping 192.168.10.3
84 bytes from 192.168.10.3 icmp_seq=1 ttl=63 time=1.529 ms
84 bytes from 192.168.10.3 icmp_seq=2 ttl=63 time=1.593 ms
84 bytes from 192.168.10.3 icmp_seq=3 ttl=63 time=1.583 ms
84 bytes from 192.168.10.3 icmp_seq=4 ttl=63 time=1.657 ms
```

Figure 3.3.b Communication Testing

4. FortiGate Integration

4.1. Interfaces Configuration

a. Port3

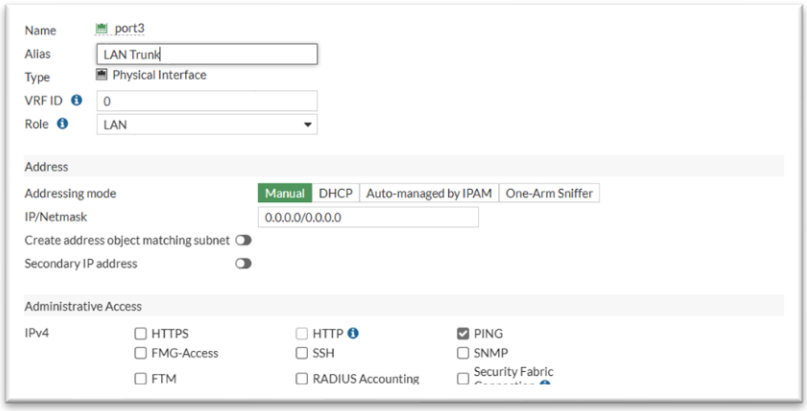


Figure 4.1.a Port3 Configuration

b. VLAN sub interfaces configuration

Figure 4.1.b VLAN sub interfaces configuration

c. Port4 (The other branch)

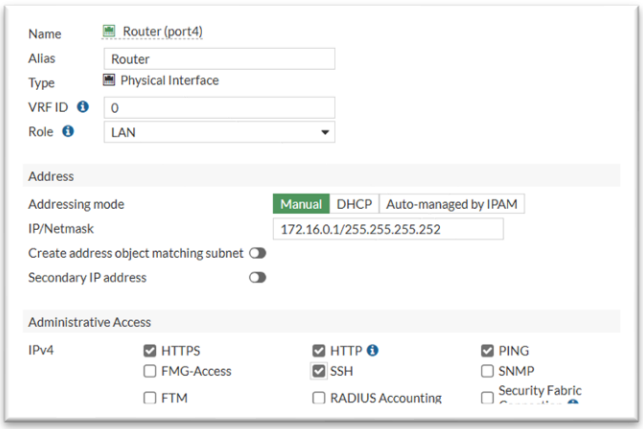


Figure 4.1.c Port4 Configuration

d. Configuring addresses and group addresses for R1 (physical interface and Loopback) and VLANS (HR and IT) for the ease of use in policies

Figure 4.1.d Addresses and Group Addresses

4.2. Firewall Policy Design

a. Key policies requirements:

- Inter-VLAN communication with service-level restrictions
- Internet access for both departments with protocol restrictions
- External router connectivity for management and testing
- Administrative access controls
- Default deny for all other traffic

b. NAT Configuration

Before applying the firewall policies, a NAT IP Pool was created to support outbound traffic from internal VLANs toward the external router. The pool defines the translated IP range *(192.168.135.6 – 192.168.135.10)* used for internet-bound sessions, enabling scalable address translation and efficient traffic handling.

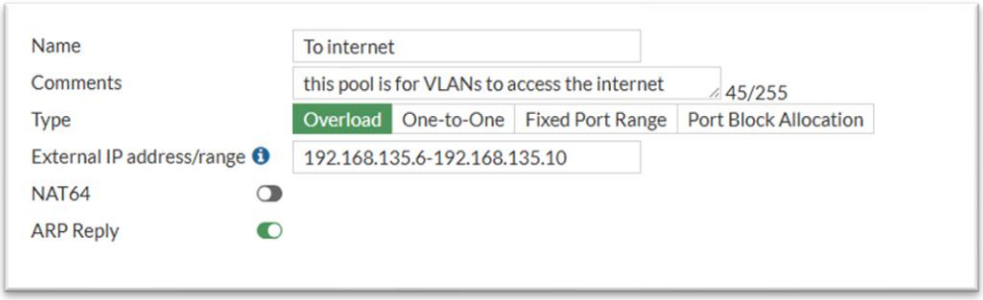
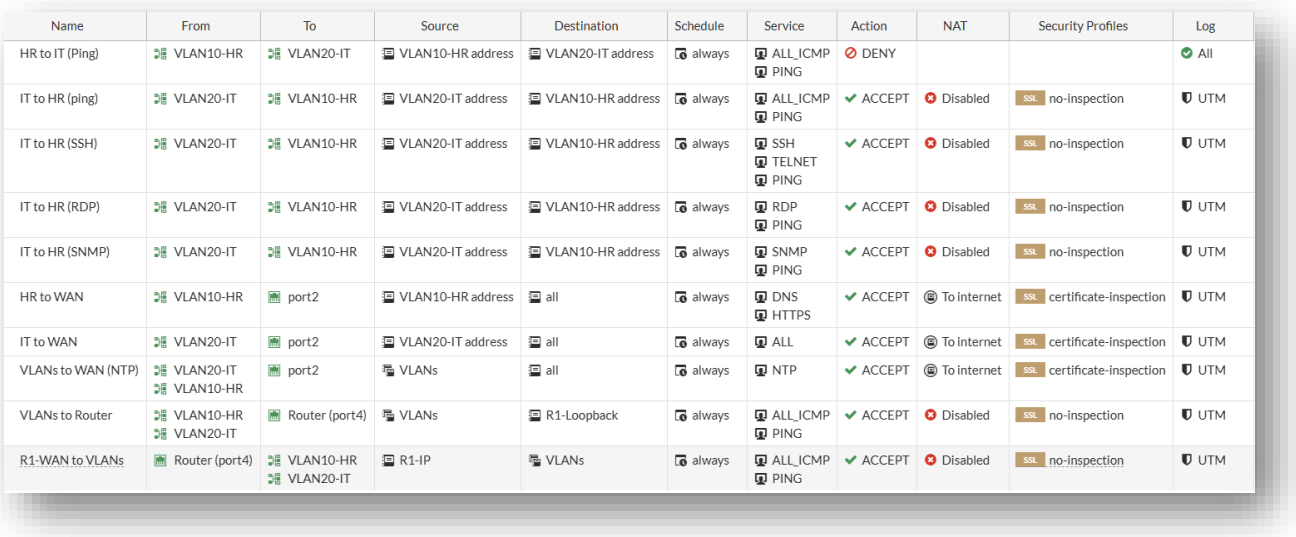


Figure 4.2.b NAT IP Pool

a. Policy Implementation

	Source	Destination	Service	Action	NAT	Description
Internal > Internal	HR	IT	ALL ICMP, PING	DENY	disabled	Block HR to ping IT
	IT	HR	ALL ICMP, PING	ACCEPT	disabled	allow IT to ping HR
	IT	HR	SSH, TELNET	ACCEPT	disabled	allow IT to access HR for internal support
	IT	HR	RDP	ACCEPT	disabled	IT is accessing HR's pcs
	IT	HR	SNMP	ACCEPT	disabled	allows IT monitoring HR equipment
	Both	R1	ALL ICMP, PING	ACCEPT	disabled	testing connection from both departments to R1
	R1	Both	ALL ICMP, PING	ACCEPT	disabled	testing connection from R1 to both departments
Internal > External	HR	all	HTTPS, DNS	ACCEPT	enabled	HR restricted internet access
	IT	all	ALL	ACCEPT	enabled	IT full internet access
	Both	all	NTP	ACCEPT	enabled	Both IT and HR departments sync time via internet

Table 4.2.c FortiGate Policies Implementation



Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
HR to IT (Ping)	VLAN10-HR	VLAN20-IT	VLAN10-HR address	VLAN20-IT address	always	ALL_ICMP PING	DENY			All
IT to HR (ping)	VLAN20-IT	VLAN10-HR	VLAN20-IT address	VLAN10-HR address	always	ALL_ICMP PING	ACCEPT	Disabled	no-inspection	UTM
IT to HR (SSH)	VLAN20-IT	VLAN10-HR	VLAN20-IT address	VLAN10-HR address	always	SSH TELNET PING	ACCEPT	Disabled	no-inspection	UTM
IT to HR (RDP)	VLAN20-IT	VLAN10-HR	VLAN20-IT address	VLAN10-HR address	always	RDP PING	ACCEPT	Disabled	no-inspection	UTM
IT to HR (SNMP)	VLAN20-IT	VLAN10-HR	VLAN20-IT address	VLAN10-HR address	always	SNMP PING	ACCEPT	Disabled	no-inspection	UTM
HR to WAN	VLAN10-HR	port2	VLAN10-HR address	all	always	DNS HTTPS	ACCEPT	To internet	certificate-inspection	UTM
IT to WAN	VLAN20-IT	port2	VLAN20-IT address	all	always	ALL	ACCEPT	To internet	certificate-inspection	UTM
VLANs to WAN (NTP)	VLAN20-IT VLAN10-HR	port2	VLANs	all	always	NTP	ACCEPT	To internet	certificate-inspection	UTM
VLANs to Router	VLAN10-HR VLAN20-IT	Router (port4)	VLANs	R1-Loopback	always	ALL_ICMP PING	ACCEPT	Disabled	no-inspection	UTM
R1-WAN to VLANs	Router (port4)	VLAN10-HR VLAN20-IT	R1-IP	VLANs	always	ALL_ICMP PING	ACCEPT	Disabled	no-inspection	UTM

Figure 4.2.c FortiGate Policies Implementation

4.3.Connectivity Testing

a. VLANs to FortiGate

```
VLAN10-HR> ping 192.168.10.1
84 bytes from 192.168.10.1 icmp_seq=1 ttl=255 time=2.932 ms
84 bytes from 192.168.10.1 icmp_seq=2 ttl=255 time=1.879 ms
84 bytes from 192.168.10.1 icmp_seq=3 ttl=255 time=2.003 ms
84 bytes from 192.168.10.1 icmp_seq=4 ttl=255 time=1.496 ms
```

```
VLAN20-IT> ping 192.168.20.1
84 bytes from 192.168.20.1 icmp_seq=1 ttl=255 time=3.834 ms
84 bytes from 192.168.20.1 icmp_seq=2 ttl=255 time=2.767 ms
84 bytes from 192.168.20.1 icmp_seq=3 ttl=255 time=3.470 ms
84 bytes from 192.168.20.1 icmp_seq=4 ttl=255 time=2.229 ms
```

Figure 4.3.a VLAN to Gateway Connectivity

b. VLANs Connectivity

a. Internal Connectivity (From HR to IT and vice versa)

```
VLAN10-HR> ping 192.168.20.3
192.168.20.3 icmp_seq=1 timeout
192.168.20.3 icmp_seq=2 timeout
192.168.20.3 icmp_seq=3 timeout
192.168.20.3 icmp_seq=4 timeout
```

```
VLAN20-IT> ping 192.168.10.3
192.168.10.3 icmp_seq=1 timeout
192.168.10.3 icmp_seq=2 timeout
84 bytes from 192.168.10.3 icmp_seq=3 ttl=63 time=4.383 ms
84 bytes from 192.168.10.3 icmp_seq=4 ttl=63 time=1.903 ms
84 bytes from 192.168.10.3 icmp_seq=5 ttl=63 time=2.535 ms
```

Figure 4.3.b.a Inter-VLAN Connectivity

b. The Other Branch Connectivity

```
VLAN10-HR> ping 172.16.0.2
84 bytes from 172.16.0.2 icmp_seq=1 ttl=254 time=49.558 ms
84 bytes from 172.16.0.2 icmp_seq=2 ttl=254 time=16.678 ms
84 bytes from 172.16.0.2 icmp_seq=3 ttl=254 time=17.569 ms
84 bytes from 172.16.0.2 icmp_seq=4 ttl=254 time=17.254 ms
```

```
VLAN20-IT> ping 172.16.0.2
84 bytes from 172.16.0.2 icmp_seq=1 ttl=254 time=32.761 ms
84 bytes from 172.16.0.2 icmp_seq=2 ttl=254 time=17.103 ms
84 bytes from 172.16.0.2 icmp_seq=3 ttl=254 time=16.324 ms
84 bytes from 172.16.0.2 icmp_seq=4 ttl=254 time=17.075 ms
```

Figure 4.3.b.b To-Branch VLAN Connectivity

5. Advanced VLAN Features and Testing

5.1. Implementing VLAN Trunking

a. Switch to FortiGate Configuration

The 802.1Q trunk between the L3 switch and FortiGate was successfully implemented to carry multiple VLANs across a single physical connection while maintaining segmentation.

Mentioned in ***Figure 3.1.c*** and ***Figure 4.1.a***

b. Native VLAN Considerations

The native VLAN was explicitly configured to avoid security risks associated with default VLAN 1

```
L3Switch(config-if)#int e0/0
L3Switch(config-if)#switchport trunk native vlan 911
L3Switch(config-if)#
```

Figure 5.1.b Native VLAN

5.2. VLAN Communication Tests

Traffic Flow	Service	Expected Result	Actual Result	Policy Reference
VLAN10 > Router	ICMP	Allow	Allow	HR to R1
VLAN20 > Router	ICMP	Allow	Allow	IT to R1
VLAN10 > VLAN 20	ICMP	Deny	Deny	HR to IT (PING)
VLAN20 > VLAN20	ICMP	Allow	Allow	IT to HR (PING)
VLAN10 > VLAN20	SSH	ALlow	Allow	IT to HR (SSH, Telnet)

Table 5.2 VLAN Communication Tests

5.3. Troubleshooting Findings

a. Issue: VLAN devices could not reach router interfaces

Root Cause: Using physical interface (port3) instead of VLAN interfaces for routing

Resolution:

- Used VLAN10-HR and VLAN20-IT interfaces for internal traffic
- Used port4 exclusively for router communication

```
VLAN10-HR> ping 172.16.0.2
172.16.0.2 icmp_seq=1 timeout
172.16.0.2 icmp_seq=2 timeout
172.16.0.2 icmp_seq=3 timeout
172.16.0.2 icmp_seq=4 timeout
```

```
VLAN10-HR>
VLAN10-HR> ping 172.16.0.2
84 bytes from 172.16.0.2 icmp_seq=1 ttl=254 time=49.558 ms
84 bytes from 172.16.0.2 icmp_seq=2 ttl=254 time=16.678 ms
84 bytes from 172.16.0.2 icmp_seq=3 ttl=254 time=17.569 ms
84 bytes from 172.16.0.2 icmp_seq=4 ttl=254 time=17.254 ms
```

Figure 5.3.a Interfaces Issue resolved

b. Issue: Inconsistent NAT settings breaking return traffic

Root Cause:

- NAT enabled for internal-to-internal communication

Resolution:

- Enabled NAT for internal→external traffic
- Disabled NAT for internal↔internal traffic

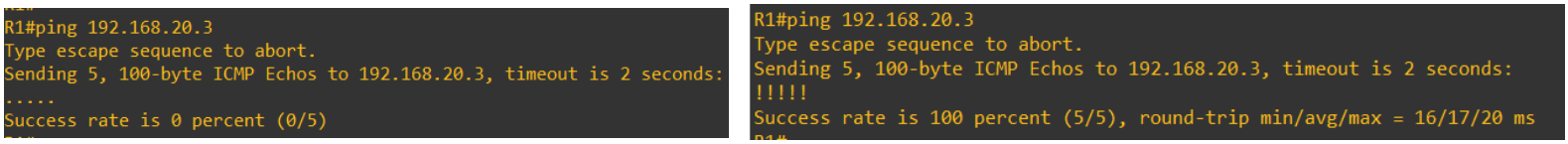


Figure 5.3.b NAT Issue resolved

6. Final Results and Analysis

6.1.Summary of Configuration Success

The project successfully delivered a fully functional segmented network infrastructure meeting all specified requirements:

All Objectives Achieved:

- VLAN segmentation between HR and IT departments
- Controlled inter-VLAN routing through firewall policies
- Secure internet and external router access
- Comprehensive monitoring and management capabilities

6.2.Security Implications

a. Enhanced security posture

- Departmental isolation preventing lateral movement
- Service-level access controls enforcing least privilege
- Centralized security policy enforcement
- Audit trail through comprehensive logging.

b. Risk mitigation

- Unauthorized inter-department access prevented
- External attack surface minimized
- Administrative access properly restricted

6.3.Strengths and Limitations

Strengths

- Centralized Management: Single point for security policy enforcement
- Scalability: Easy addition of new VLANs and departments
- Flexibility: Granular control over service-level communications
- Performance: Efficient routing through dedicated security device

Limitations

- Single Point of Failure: FortiGate as central router
- Bandwidth Constraints: Trunk interface capacity limits
- Complexity: Firewall policy management overhead

7. Conclusion

7.1.Key Learnings

- VLAN design and implementation strategies
- FortiGate firewall policy configuration and management
- Inter-VLAN routing security principles
- Network troubleshooting methodology

7.2.Network Expansion Opportunities

a. Immediate Enhancements

- Additional departmental VLANs (Finance, Operations, etc.)
- Guest network with captive portal authentication
- DMZ zone for public-facing services

b. Advanced Features

- High availability FortiGate cluster
- Intrusion Prevention System (IPS) implementation
- Web filtering and application control
- VPN remote access capabilities

Thank You!