Project Document :

VLAN and Inter-VLAN Routing with FortiGate

1. Summary

This project focuses on the design, implementation, and verification of a segmented network infrastructure using a FortiGate Firewall as the core routing and security device. The primary objective is to establish a secure network environment by implementing Virtual Local Area Networks (VLANs) to separate the network into distinct zones: a **DMZ-Zone** for servers (VLAN 100 & 200) and a **TRUST-Zone** for clients (VLAN 10 & 20).

The project involves configuring Layer 2 switching protocols, establishing 802.1Q trunk links, and configuring the FortiGate firewall to handle Inter-VLAN routing using sub-interfaces. Additionally, security policies will be applied to regulate traffic between the different VLANs and to provide controlled internet access for all network segments.

2. Project Timeline and Objectives

The project execution is divided into four distinct phases, as outlined below:

Objective 1: VLAN Configuration Basics

- **Task:** Set up VLANs on the network switches and configure basic inter-VLAN routing capabilities.

Objective 2: FortiGate Integration for VLANs

- **Task:** Configure the FortiGate firewall to support VLANs via sub-interfaces. This includes IP addressing for gateways and defining firewall policies to govern traffic between VLANs.

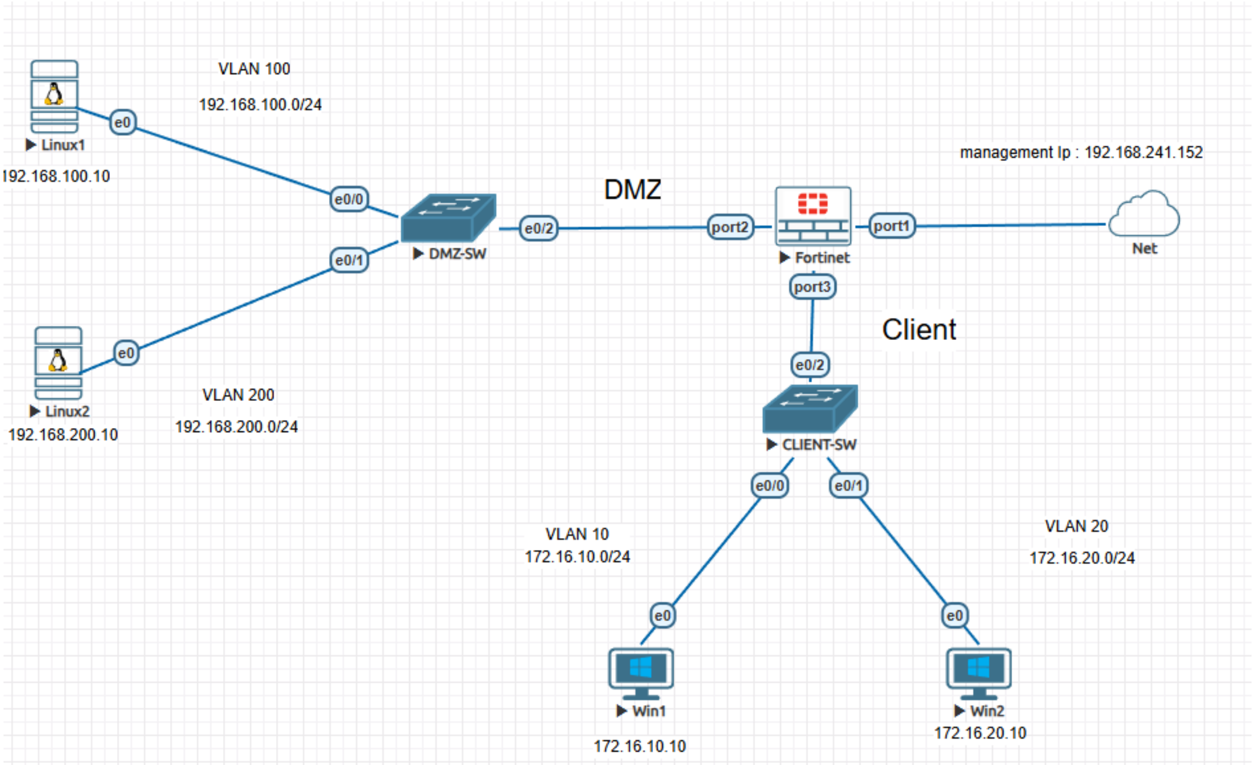
Objective 3: Advanced VLAN Features and Testing

- **Task:** Implement VLAN Trunks between switches and the firewall. rigorous testing of VLAN-to-VLAN communication and connectivity verification (Ping tests).

Objective 4: Presentation and Final Report

- **Task:** Consolidate all findings into a final presentation and report that covers the complete VLAN setup, FortiGate integration steps, and successful testing results.

Topology



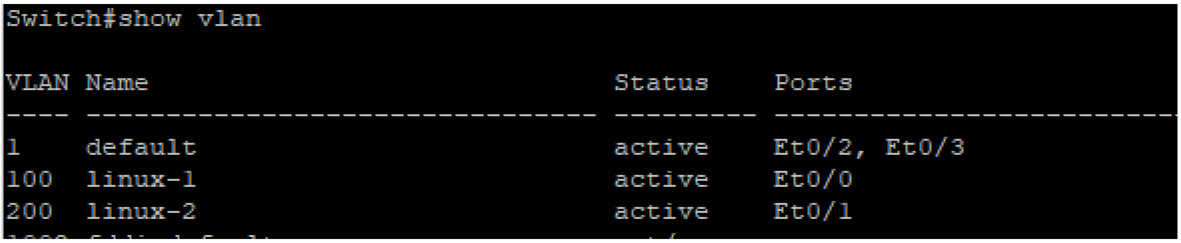
VLAN ID	**Name / Zone**	**Network Subnet**	**Gateway IP (FortiGate)**	**Description**
10	TRUST-Clients-1	172.16.10.0/24	172.16.10.1	Internal Client Access
20	TRUST-Clients-2	172.16.20.0/24	172.16.20.1	Internal Client Access
100	DMZ-Server-1	192.168.100.0/24	192.168.100.1	Public Facing Services
200	DMZ-Server-2	192.168.200.0/24	192.168.200.1	Public Facing Services

Objective 1: VLAN Configuration Basics

First we create VLANs on switches and assign them to interfaces then we configure trunks

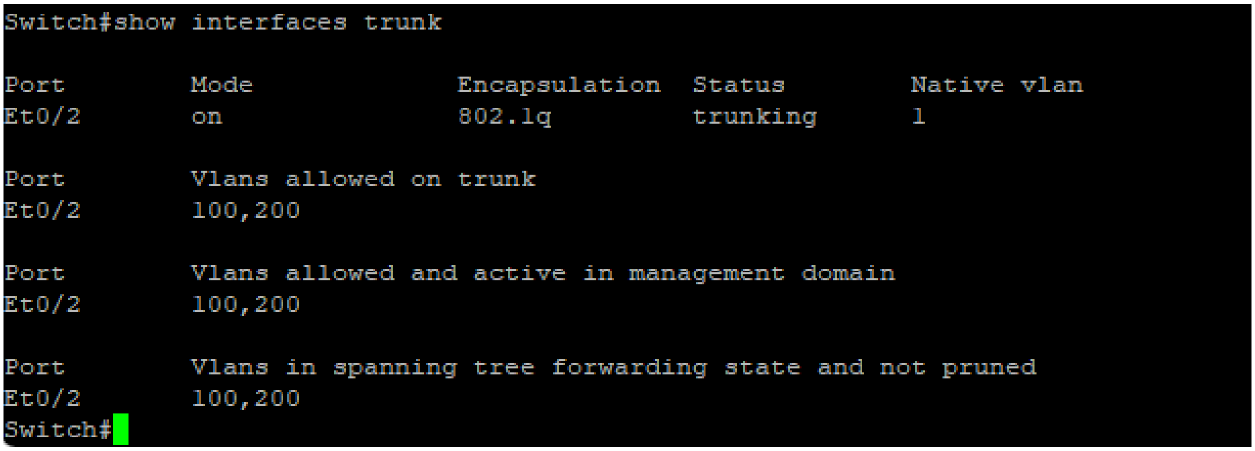
On DMZ-SW:

```
VLAN 100
 name linux-1
VLAN 200
 name linux-2

interface Ethernet0/0
 switchport mode access
 switchport access VLAN 100
 no shutdown
exit

interface Ethernet0/1
 switchport mode access
 switchport access VLAN 200
 no shutdown
exit
```



```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/2, Et0/3
100  linux-1                          active    Et0/0
200  linux-2                          active    Et0/1
```

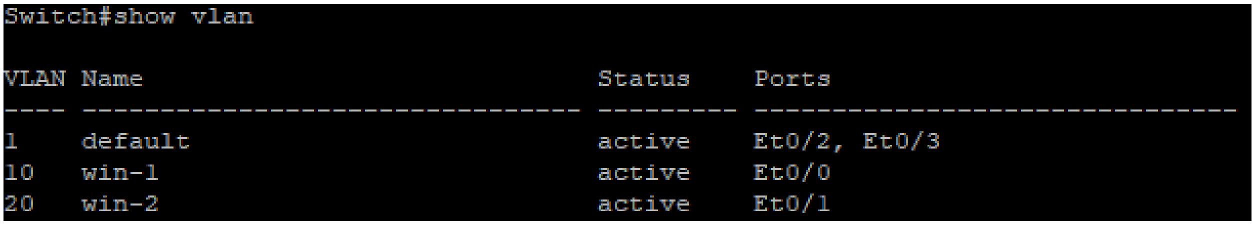
```
interface Ethernet0/2

 switchport trunk encapsulation dot1q

 switchport mode trunk

 switchport trunk allowed VLAN 100,200

 no shutdown

exit
```



```
Switch#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/2       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/2       100,200

Port        Vlans allowed and active in management domain
Et0/2       100,200

Port        Vlans in spanning tree forwarding state and not pruned
Et0/2       100,200
Switch#
```

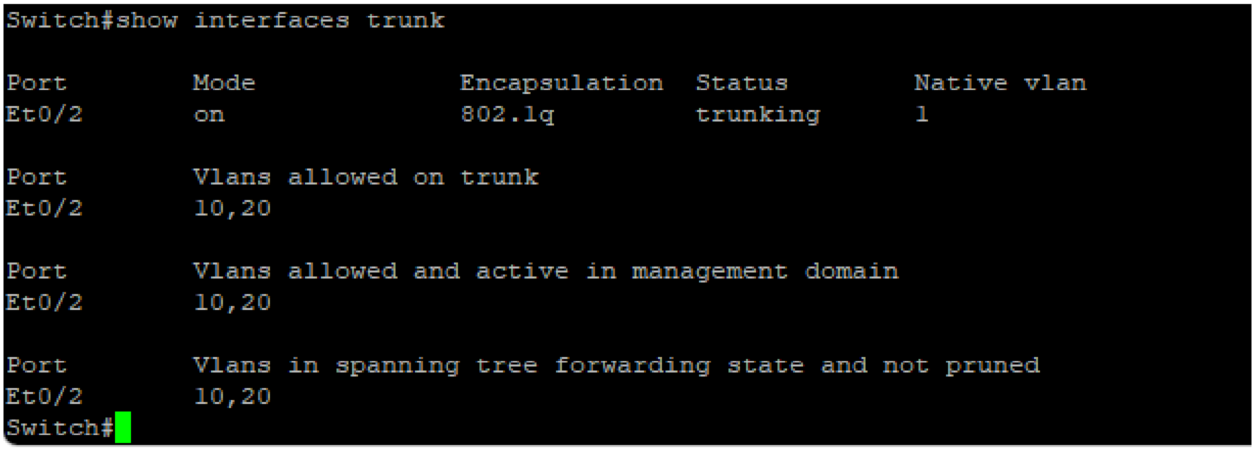
On Client-SW:

```
VLAN 10
 name WIN-1
VLAN 20
 name WIN-2
exit

interface Ethernet0/1
 switchport mode access
 switchport access VLAN 10
 no shutdown
exit

interface Ethernet0/2
switchport mode access
 switchport access VLAN 20
 no shutdown
exit
```



```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/2, Et0/3
10   win-1                            active    Et0/0
20   win-2                            active    Et0/1
```

```
interface Ethernet0/2

 switchport trunk encapsulation dot1q

 switchport mode trunk

 switchport trunk allowed VLAN 10,20

 no shutdown
```



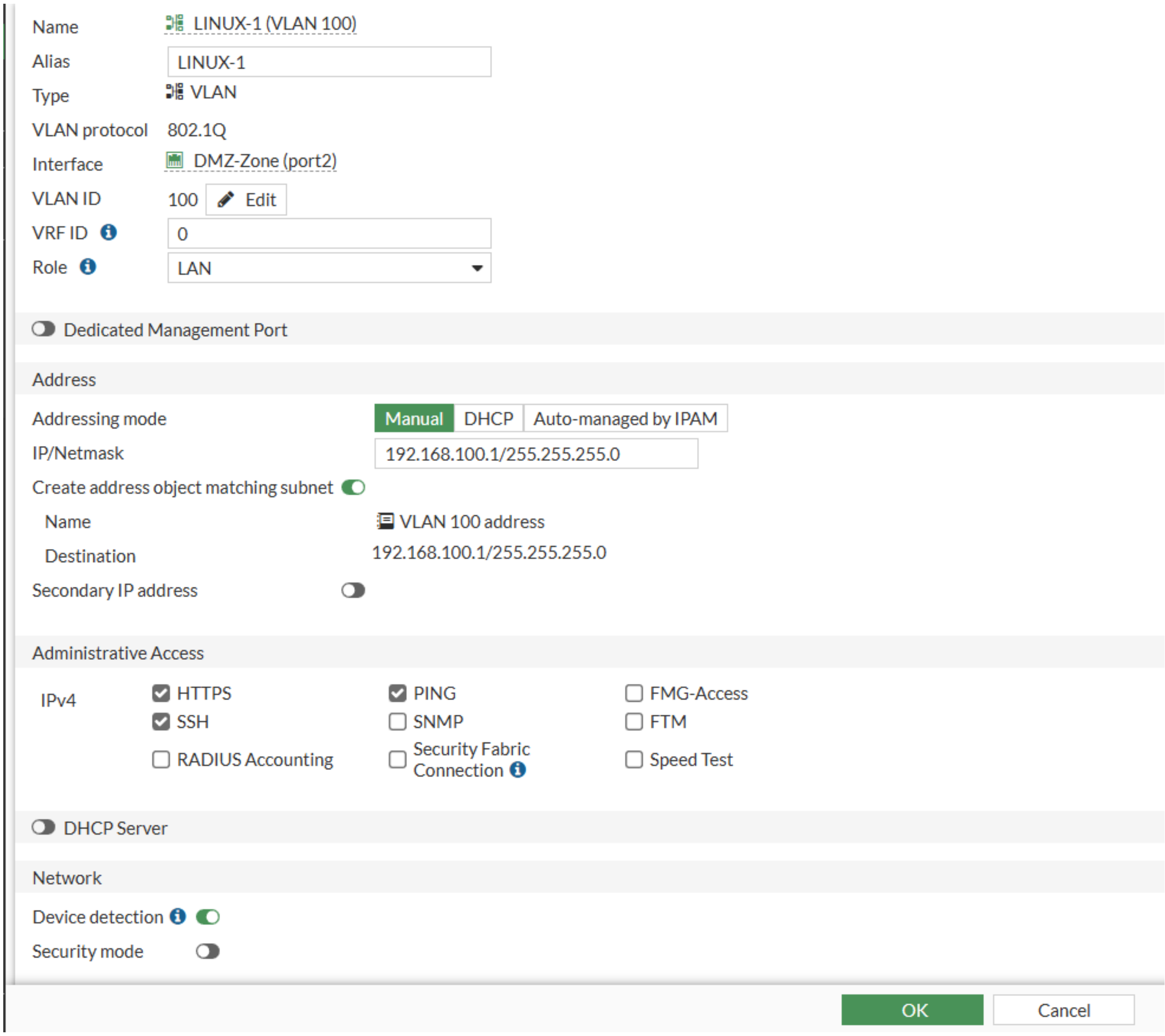
```
Switch#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/2       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/2       10,20

Port        Vlans allowed and active in management domain
Et0/2       10,20

Port        Vlans in spanning tree forwarding state and not pruned
Et0/2       10,20
Switch#
```

Objective 2: FortiGate Integration for VLANs

First we configure sub interfaces for each VLAN with IP addressing

In network > interfaces > create new interface

For VLAN 100 :



Name	LINUX-1 (VLAN 100)
Alias	LINUX-1
Type	VLAN
VLAN protocol	802.1Q
Interface	DMZ-Zone (port2)
VLAN ID	100 Edit
VRF ID	0
Role	LAN

○ Dedicated Management Port

Address

Addressing mode	[✓ Manual] DHCP Auto-managed by IPAM
IP/Netmask	192.168.100.1/255.255.255.0
Create address object matching subnet	●
Name	VLAN 100 address
Destination	192.168.100.1/255.255.255.0
Secondary IP address	○

Administrative Access

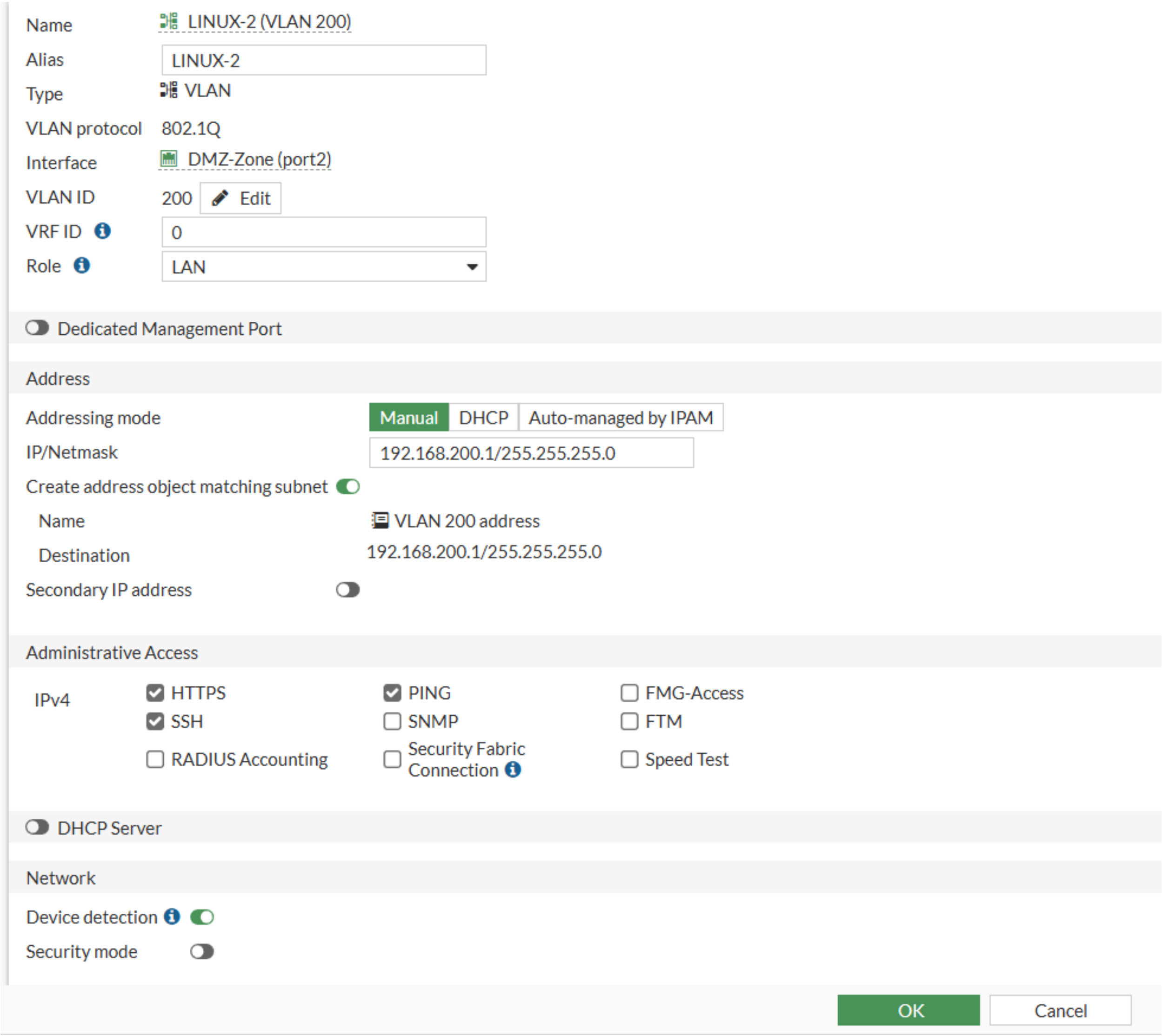
IPv4
☑ HTTPS ☑ PING □ FMG-Access
☑ SSH □ SNMP □ FTM
□ RADIUS Accounting □ Security Fabric Connection □ Speed Test

○ DHCP Server

Network

Device detection	●
Security mode	○

For VLAN 200 :



Name	LINUX-2 (VLAN 200)
Alias	LINUX-2
Type	VLAN
VLAN protocol	802.1Q
Interface	DMZ-Zone (port2)
VLAN ID	200 Edit
VRF ID	0
Role	LAN

○ Dedicated Management Port

Address

Addressing mode	[✓ Manual] DHCP Auto-managed by IPAM
IP/Netmask	192.168.200.1/255.255.255.0
Create address object matching subnet	●
Name	VLAN 200 address
Destination	192.168.200.1/255.255.255.0
Secondary IP address	○

Administrative Access

IPv4

☑ HTTPS
☑ SSH
□ RADIUS Accounting

☑ PING
□ SNMP
□ Security Fabric Connection

□ FMG-Access
□ FTM
□ Speed Test

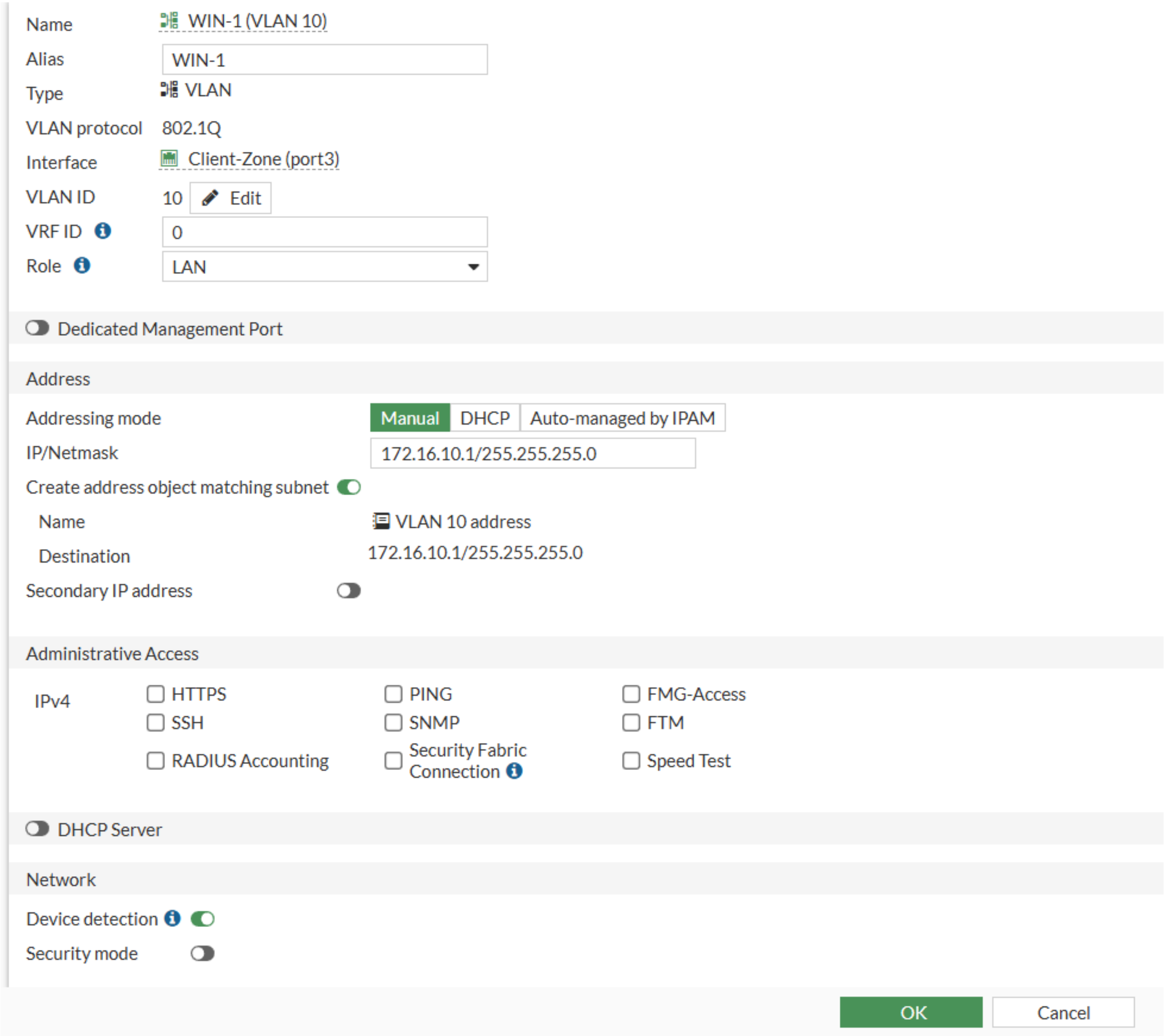
○ DHCP Server

Network

Device detection ●

Security mode ○

For VLAN 10 :



Name	WIN-1 (VLAN 10)
Alias	WIN-1
Type	VLAN
VLAN protocol	802.1Q
Interface	Client-Zone (port3)
VLAN ID	10 Edit
VRF ID ℹ	0
Role ℹ	LAN

○ Dedicated Management Port

Address

Addressing mode	[✓ Manual] DHCP Auto-managed by IPAM
IP/Netmask	172.16.10.1/255.255.255.0
Create address object matching subnet	●
Name	VLAN 10 address
Destination	172.16.10.1/255.255.255.0
Secondary IP address	○

Administrative Access

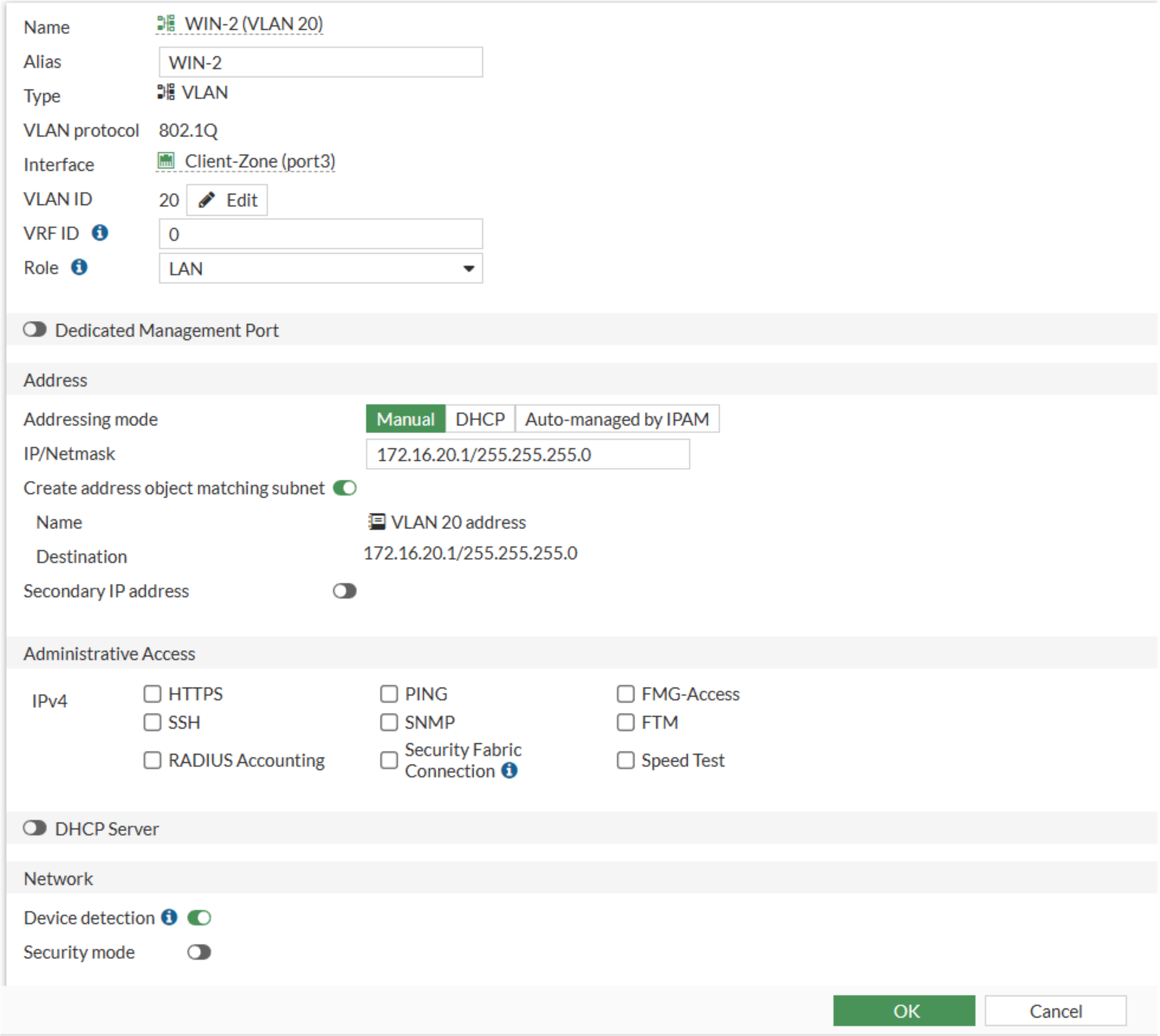
IPv4
□ HTTPS □ PING □ FMG-Access
□ SSH □ SNMP □ FTM
□ RADIUS Accounting □ Security Fabric Connection ℹ □ Speed Test

○ DHCP Server

Network

Device detection ℹ ●
Security mode ○

For VLAN 20 :



Name	WIN-2 (VLAN 20)
Alias	WIN-2
Type	VLAN
VLAN protocol	802.1Q
Interface	Client-Zone (port3)
VLAN ID	20 Edit
VRF ID	0
Role	LAN

Dedicated Management Port

Address

Addressing mode	[✓ Manual] DHCP Auto-managed by IPAM
IP/Netmask	172.16.20.1/255.255.255.0
Create address object matching subnet	●
Name	VLAN 20 address
Destination	172.16.20.1/255.255.255.0
Secondary IP address	○

Administrative Access

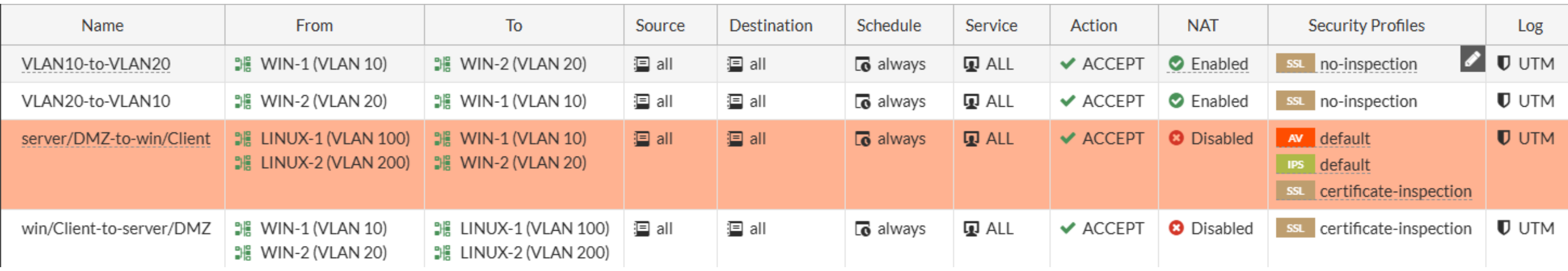
IPv4
- □ HTTPS
- □ SSH
- □ RADIUS Accounting
- □ PING
- □ SNMP
- □ Security Fabric Connection
- □ FMG-Access
- □ FTM
- □ Speed Test

DHCP Server

Network

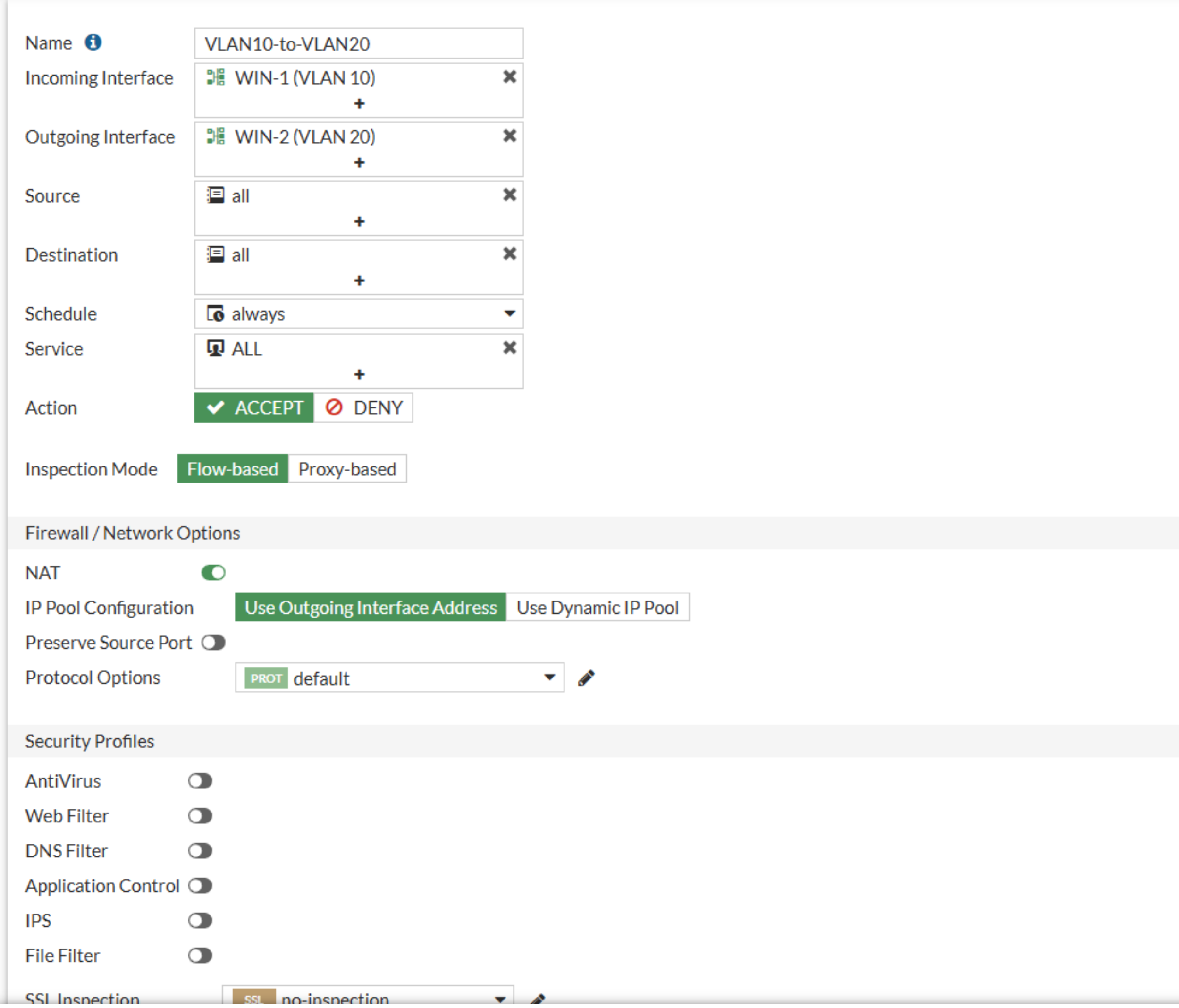
Device detection	●
Security mode	○

Firewall policies



Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
VLAN10-to-VLAN20	WIN-1 (VLAN 10)	WIN-2 (VLAN 20)	all	all	always	ALL	✓ ACCEPT	✓ Enabled	SSL no-inspection	UTM
VLAN20-to-VLAN10	WIN-2 (VLAN 20)	WIN-1 (VLAN 10)	all	all	always	ALL	✓ ACCEPT	✓ Enabled	SSL no-inspection	UTM
server/DMZ-to-win/Client	LINUX-1 (VLAN 100) LINUX-2 (VLAN 200)	WIN-1 (VLAN 10) WIN-2 (VLAN 20)	all	all	always	ALL	✓ ACCEPT	✖ Disabled	AV default IPS default SSL certificate-inspection	UTM
win/Client-to-server/DMZ	WIN-1 (VLAN 10) WIN-2 (VLAN 20)	LINUX-1 (VLAN 100) LINUX-2 (VLAN 200)	all	all	always	ALL	✓ ACCEPT	✖ Disabled	SSL certificate-inspection	UTM

Vlan 10 to Vlan 20



Name	VLAN10-to-VLAN20
Incoming Interface	WIN-1 (VLAN 10)
Outgoing Interface	WIN-2 (VLAN 20)
Source	all
Destination	all
Schedule	always
Service	ALL
Action	[✓ ACCEPT] DENY
Inspection Mode	[✓ Flow-based] Proxy-based

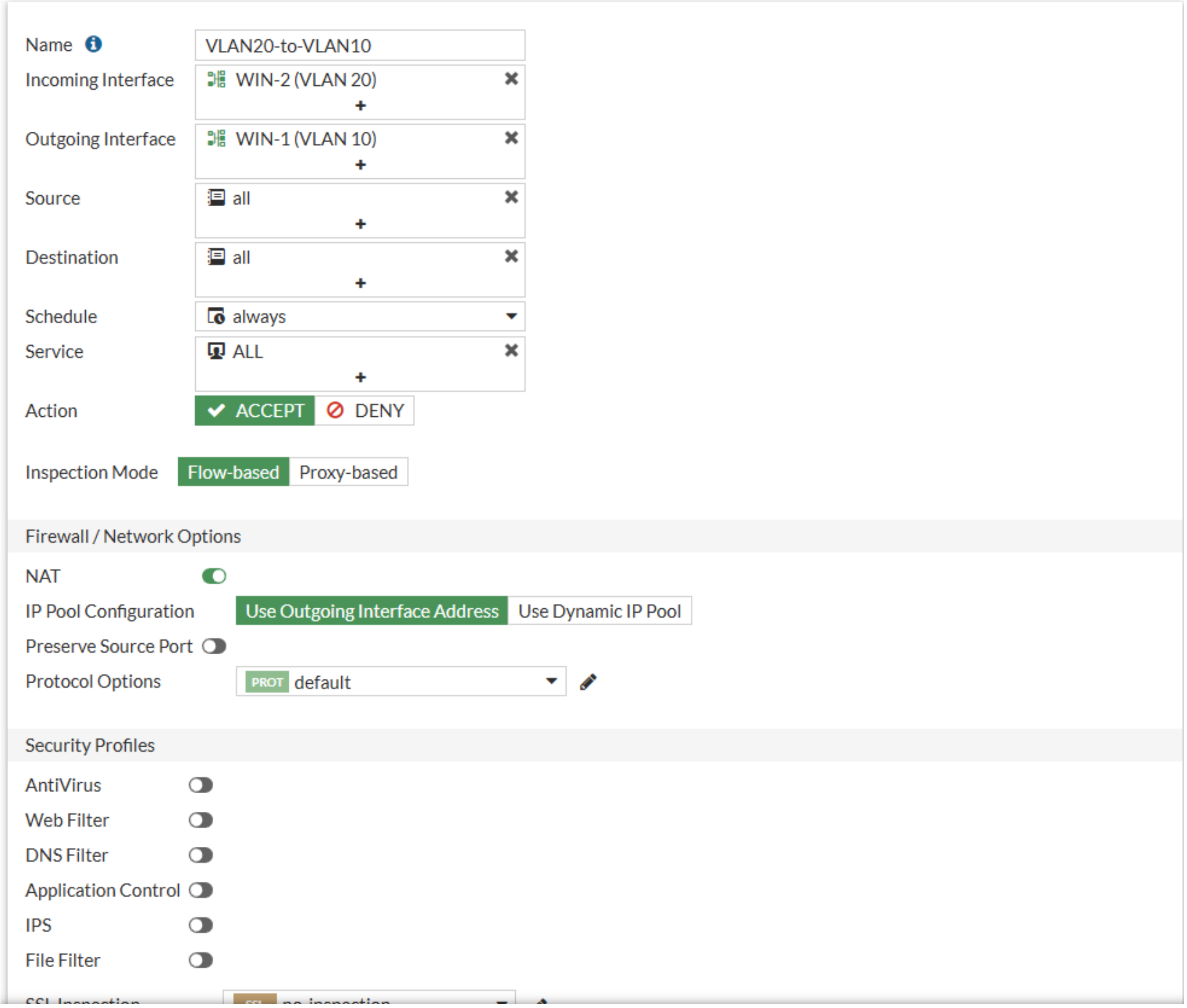
Firewall / Network Options

NAT	●
IP Pool Configuration	[✓ Use Outgoing Interface Address] Use Dynamic IP Pool
Preserve Source Port	○
Protocol Options	PROT default

Security Profiles

AntiVirus	○
Web Filter	○
DNS Filter	○
Application Control	○
IPS	○
File Filter	○
SSL Inspection	SSL no-inspection

Vlan 20 to Vlan 10



Name VLAN20-to-VLAN10

Incoming Interface WIN-2 (VLAN 20)

Outgoing Interface WIN-1 (VLAN 10)

Source all

Destination all

Schedule always

Service ALL

Action [✓ ACCEPT] DENY

Inspection Mode [✓ Flow-based] Proxy-based

Firewall / Network Options

NAT ●

IP Pool Configuration [✓ Use Outgoing Interface Address] Use Dynamic IP Pool

Preserve Source Port ○

Protocol Options PROT default

Security Profiles

AntiVirus ○

Web Filter ○

DNS Filter ○

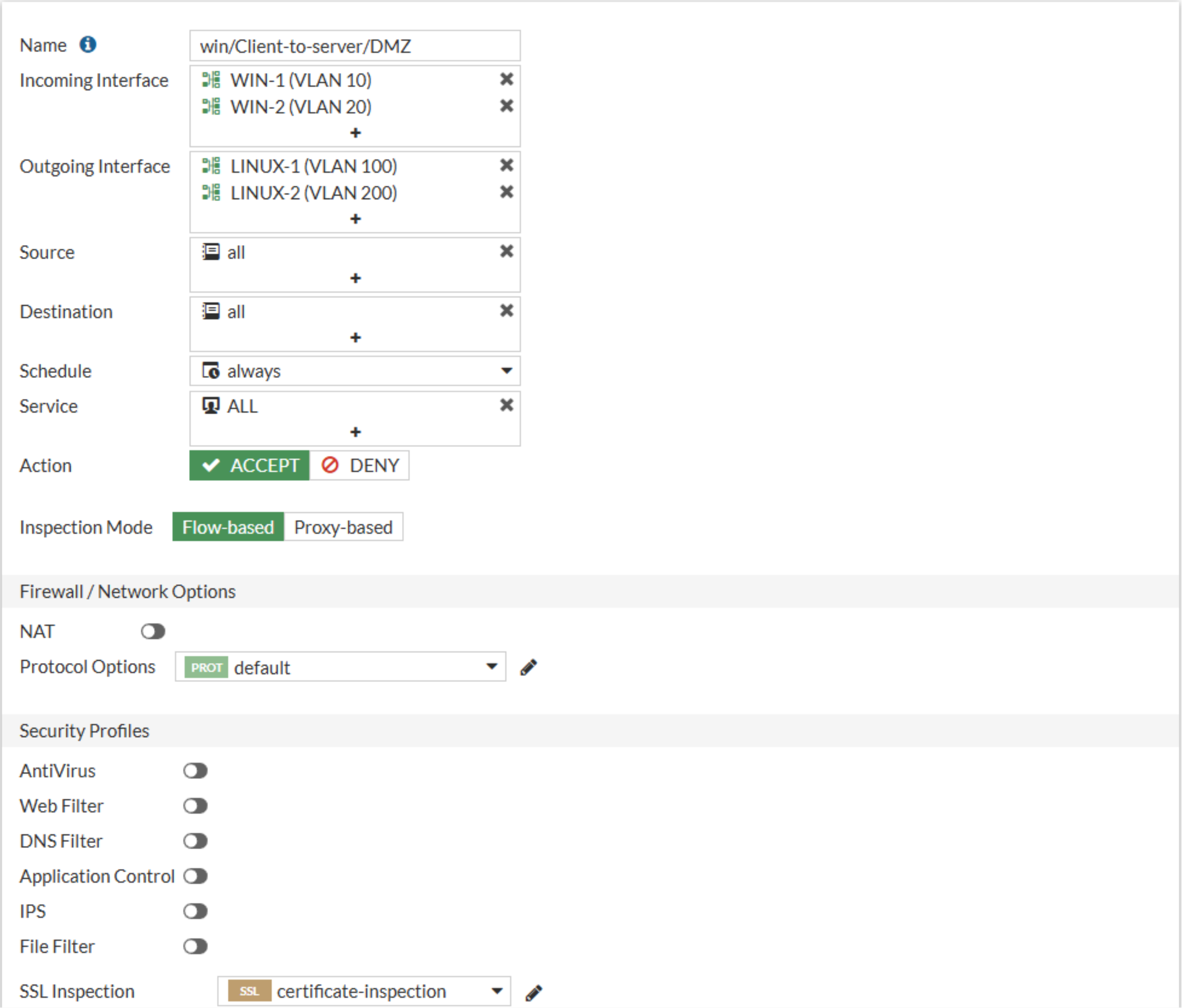
Application Control ○

IPS ○

File Filter ○

SSL Inspection SSL no-inspection

VLAN 10 or 20 to VLAN 100 or 200



Name	win/Client-to-server/DMZ
Incoming Interface	WIN-1 (VLAN 10) WIN-2 (VLAN 20)
Outgoing Interface	LINUX-1 (VLAN 100) LINUX-2 (VLAN 200)
Source	all
Destination	all
Schedule	always
Service	ALL
Action	[✓ ACCEPT] DENY
Inspection Mode	[✓ Flow-based] Proxy-based

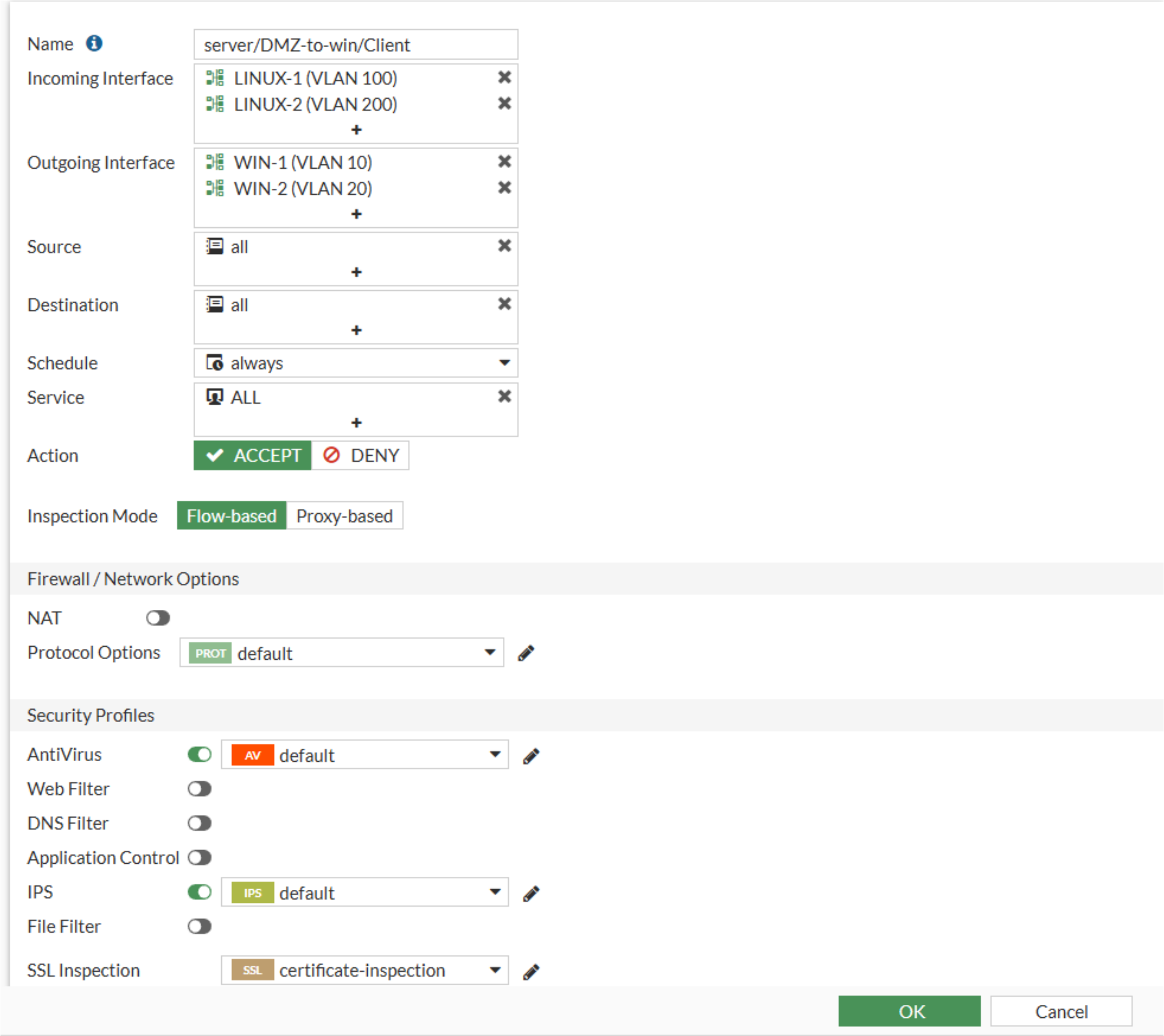
Firewall / Network Options

NAT	○
Protocol Options	PROT default

Security Profiles

AntiVirus	○
Web Filter	○
DNS Filter	○
Application Control	○
IPS	○
File Filter	○
SSL Inspection	SSL certificate-inspection

VLAN 100 or 200 to VLAN 10 or 20



Name: server/DMZ-to-win/Client

Incoming Interface: LINUX-1 (VLAN 100), LINUX-2 (VLAN 200)

Outgoing Interface: WIN-1 (VLAN 10), WIN-2 (VLAN 20)

Source: all

Destination: all

Schedule: always

Service: ALL

Action: [✓ ACCEPT] DENY

Inspection Mode: [✓ Flow-based] Proxy-based

Firewall / Network Options

NAT: ○

Protocol Options: PROT default

Security Profiles

AntiVirus: ● AV default

Web Filter: ○

DNS Filter: ○

Application Control: ○

IPS: ● IPS default

File Filter: ○

SSL Inspection: SSL certificate-inspection

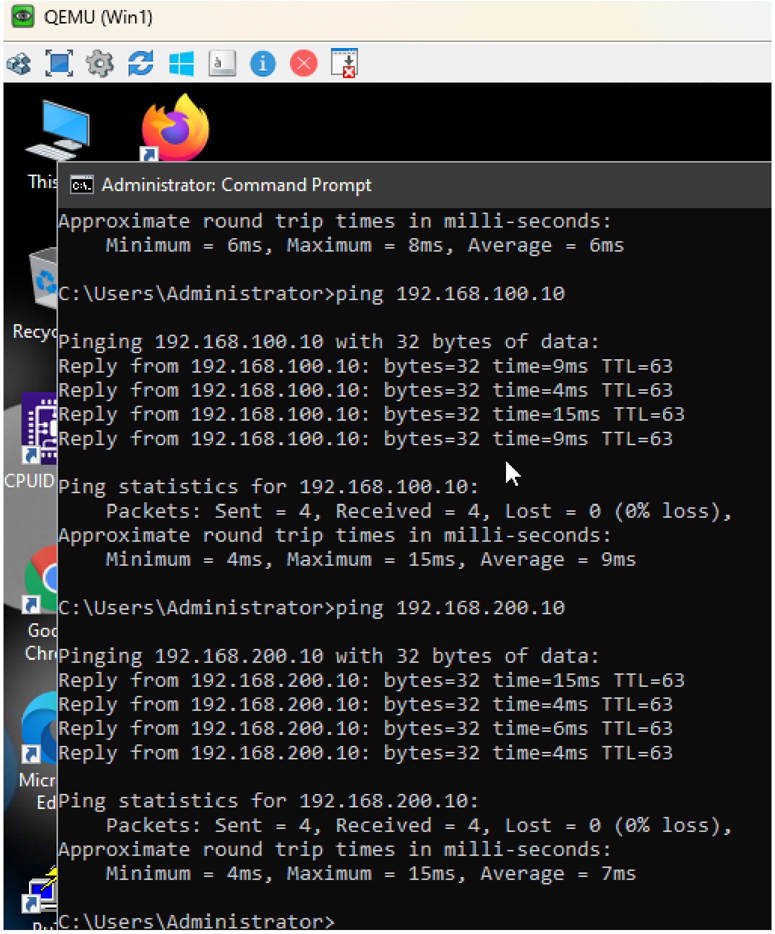
Objective 3: Advanced VLAN Features and Testing

Trunks have already been configured in objective 1 so we proceed into testing

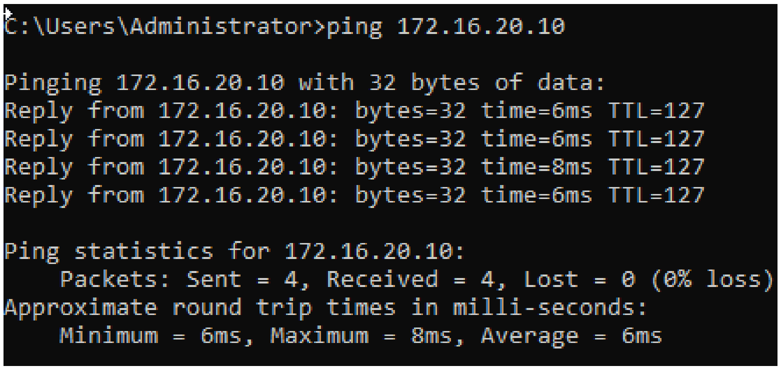
Device Name	Interface	VLAN ID	IP Address	Subnet Mask	Default Gateway
Linux1	eth0	100	**192.168.100.10**	255.255.255.0	192.168.100.1
Linux2	eth0	200	**192.168.200.10**	255.255.255.0	192.168.200.1
Win1	Ethernet0	10	**172.16.10.10**	255.255.255.0	172.16.10.1
Win2	Ethernet0	20	**172.16.20.10**	255.255.255.0	172.16.20.1
Fortinet	port1 (Mgmt)	N/A	**192.168.241.152**	255.255.255.0	192.168.241.152
Fortinet	port2.100	100	**192.168.100.1**	255.255.255.0	N/A
Fortinet	port2.200	200	**192.168.200.1**	255.255.255.0	N/A
Fortinet	port3.10	10	**172.16.10.1**	255.255.255.0	N/A
Fortinet	port3.20	20	**172.16.20.1**	255.255.255.0	N/A

Source (From)	Destination (To)	Traffic Type	Expected Result	Actual result
VLAN 10 (Win1)	VLAN 20 (Win2)	Ping	**Success**	**Success**
VLAN 10 (Win1)	VLAN 100 (Linux1)	Ping	**Success**	**Success**
VLAN 10 (Win1)	VLAN 200 (Linux2)	Ping	**Success**	**Success**
VLAN 20 (Win2)	VLAN 10 (Win1)	Ping	**Success**	**Success**
VLAN 20 (Win2)	VLAN 100 (Linux1)	Ping	**Success**	**Success**
VLAN 20 (Win2)	VLAN 200 (Linux2)	Ping	**Success**	**Success**
VLAN 100 (Linux1)	VLAN 10 (Win1)	Ping	**Success**	**Success**
VLAN 100 (Linux1)	VLAN 20 (Win2)	Ping	**Success**	**Success**
VLAN 100 (Linux1)	VLAN 200 (Linux2)	Ping	**Fail**	**Fail**
VLAN 200 (Linux2)	VLAN 10 (Win1)	Ping	**Success**	**Success**
VLAN 200 (Linux2)	VLAN 20 (Win2)	Ping	**Success**	**Success**
VLAN 200 (Linux2)	VLAN 100 (Linux1)	Ping	**Fail**	**Fail**

VLAN 10 (WIN-1) results :

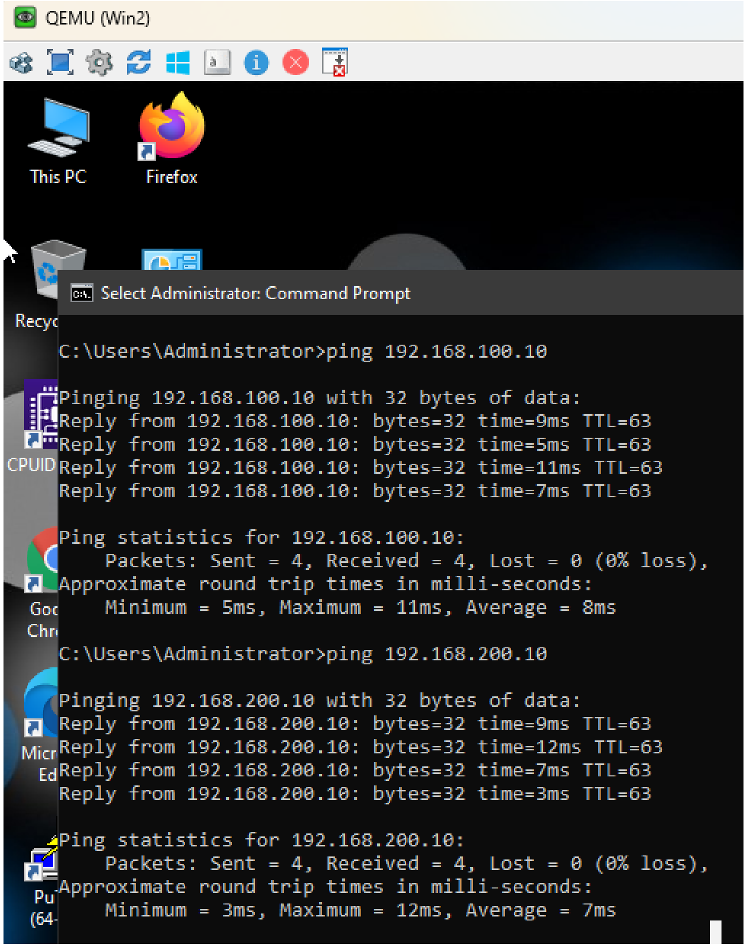


```
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 8ms, Average = 6ms

C:\Users\Administrator>ping 192.168.100.10

Pinging 192.168.100.10 with 32 bytes of data:
Reply from 192.168.100.10: bytes=32 time=9ms TTL=63
Reply from 192.168.100.10: bytes=32 time=4ms TTL=63
Reply from 192.168.100.10: bytes=32 time=15ms TTL=63
Reply from 192.168.100.10: bytes=32 time=9ms TTL=63

Ping statistics for 192.168.100.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 15ms, Average = 9ms

C:\Users\Administrator>ping 192.168.200.10

Pinging 192.168.200.10 with 32 bytes of data:
Reply from 192.168.200.10: bytes=32 time=15ms TTL=63
Reply from 192.168.200.10: bytes=32 time=4ms TTL=63
Reply from 192.168.200.10: bytes=32 time=6ms TTL=63
Reply from 192.168.200.10: bytes=32 time=4ms TTL=63

Ping statistics for 192.168.200.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 15ms, Average = 7ms

C:\Users\Administrator>
```

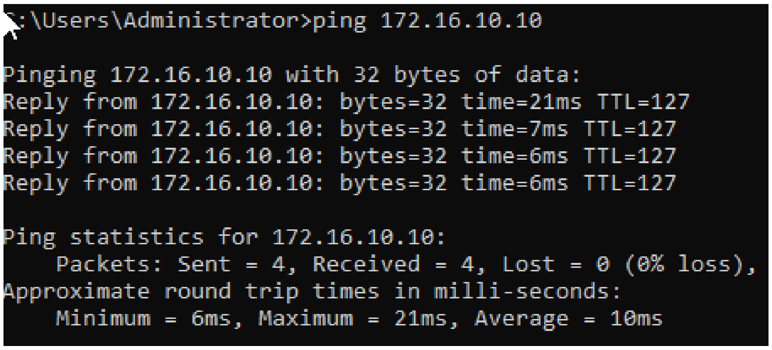


```
C:\Users\Administrator>ping 172.16.20.10

Pinging 172.16.20.10 with 32 bytes of data:
Reply from 172.16.20.10: bytes=32 time=6ms TTL=127
Reply from 172.16.20.10: bytes=32 time=6ms TTL=127
Reply from 172.16.20.10: bytes=32 time=8ms TTL=127
Reply from 172.16.20.10: bytes=32 time=6ms TTL=127

Ping statistics for 172.16.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 8ms, Average = 6ms
```

VLAN 20 (WIN-2) results :

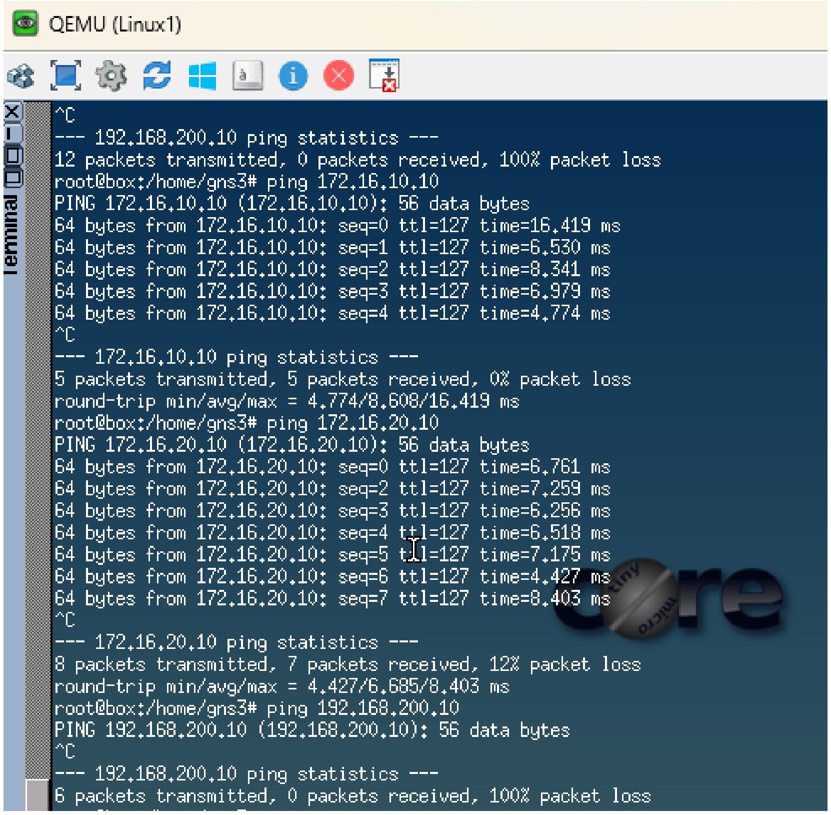


```
C:\Users\Administrator>ping 192.168.100.10

Pinging 192.168.100.10 with 32 bytes of data:
Reply from 192.168.100.10: bytes=32 time=9ms TTL=63
Reply from 192.168.100.10: bytes=32 time=5ms TTL=63
Reply from 192.168.100.10: bytes=32 time=11ms TTL=63
Reply from 192.168.100.10: bytes=32 time=7ms TTL=63

Ping statistics for 192.168.100.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 11ms, Average = 8ms

C:\Users\Administrator>ping 192.168.200.10

Pinging 192.168.200.10 with 32 bytes of data:
Reply from 192.168.200.10: bytes=32 time=9ms TTL=63
Reply from 192.168.200.10: bytes=32 time=12ms TTL=63
Reply from 192.168.200.10: bytes=32 time=7ms TTL=63
Reply from 192.168.200.10: bytes=32 time=3ms TTL=63

Ping statistics for 192.168.200.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 12ms, Average = 7ms
```



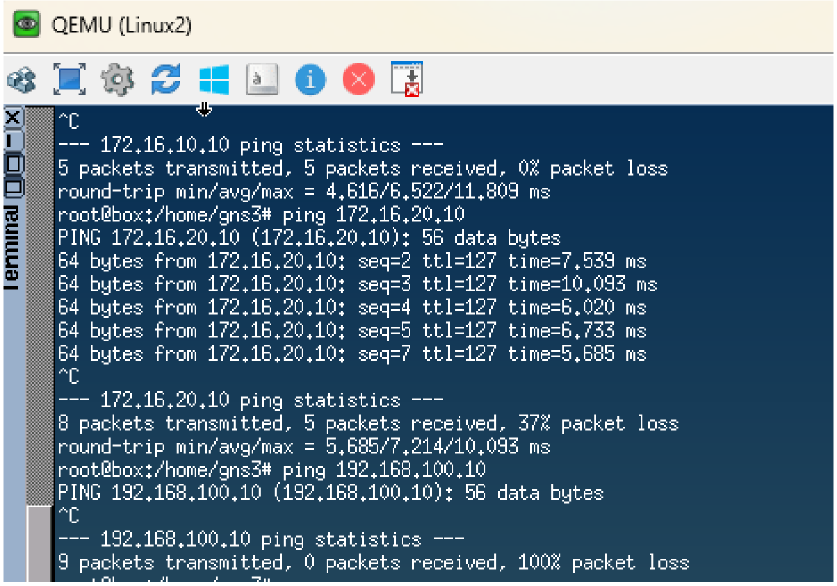
```
C:\Users\Administrator>ping 172.16.10.10

Pinging 172.16.10.10 with 32 bytes of data:
Reply from 172.16.10.10: bytes=32 time=21ms TTL=127
Reply from 172.16.10.10: bytes=32 time=7ms TTL=127
Reply from 172.16.10.10: bytes=32 time=6ms TTL=127
Reply from 172.16.10.10: bytes=32 time=6ms TTL=127

Ping statistics for 172.16.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 21ms, Average = 10ms
```

VLAN 100 results :



```
^C
--- 192.168.200.10 ping statistics ---
12 packets transmitted, 0 packets received, 100% packet loss
root@box:/home/gns3# ping 172.16.10.10
PING 172.16.10.10 (172.16.10.10): 56 data bytes
64 bytes from 172.16.10.10: seq=0 ttl=127 time=16.419 ms
64 bytes from 172.16.10.10: seq=1 ttl=127 time=6.530 ms
64 bytes from 172.16.10.10: seq=2 ttl=127 time=8.341 ms
64 bytes from 172.16.10.10: seq=3 ttl=127 time=6.979 ms
64 bytes from 172.16.10.10: seq=4 ttl=127 time=4.774 ms
^C
--- 172.16.10.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 4.774/8.608/16.419 ms
root@box:/home/gns3# ping 172.16.20.10
PING 172.16.20.10 (172.16.20.10): 56 data bytes
64 bytes from 172.16.20.10: seq=0 ttl=127 time=6.761 ms
64 bytes from 172.16.20.10: seq=2 ttl=127 time=7.259 ms
64 bytes from 172.16.20.10: seq=3 ttl=127 time=6.256 ms
64 bytes from 172.16.20.10: seq=4 ttl=127 time=6.518 ms
64 bytes from 172.16.20.10: seq=5 ttl=127 time=7.175 ms
64 bytes from 172.16.20.10: seq=6 ttl=127 time=4.427 ms
64 bytes from 172.16.20.10: seq=7 ttl=127 time=8.403 ms
^C
--- 172.16.20.10 ping statistics ---
8 packets transmitted, 7 packets received, 12% packet loss
round-trip min/avg/max = 4.427/6.685/8.403 ms
root@box:/home/gns3# ping 192.168.200.10
PING 192.168.200.10 (192.168.200.10): 56 data bytes
^C
--- 192.168.200.10 ping statistics ---
6 packets transmitted, 0 packets received, 100% packet loss
```

VLAN 200 results :



```
^C
--- 172.16.10.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 4.616/6.522/11.809 ms
root@box:/home/gns3# ping 172.16.20.10
PING 172.16.20.10 (172.16.20.10): 56 data bytes
64 bytes from 172.16.20.10: seq=2 ttl=127 time=7.539 ms
64 bytes from 172.16.20.10: seq=3 ttl=127 time=10.093 ms
64 bytes from 172.16.20.10: seq=4 ttl=127 time=6.020 ms
64 bytes from 172.16.20.10: seq=5 ttl=127 time=6.733 ms
64 bytes from 172.16.20.10: seq=7 ttl=127 time=5.685 ms
^C
--- 172.16.20.10 ping statistics ---
8 packets transmitted, 5 packets received, 37% packet loss
round-trip min/avg/max = 5.685/7.214/10.093 ms
root@box:/home/gns3# ping 192.168.100.10
PING 192.168.100.10 (192.168.100.10): 56 data bytes
^C
--- 192.168.100.10 ping statistics ---
9 packets transmitted, 0 packets received, 100% packet loss
```