PROJECT 2:
VLAN
&
INTER-VLAN
ROUTING

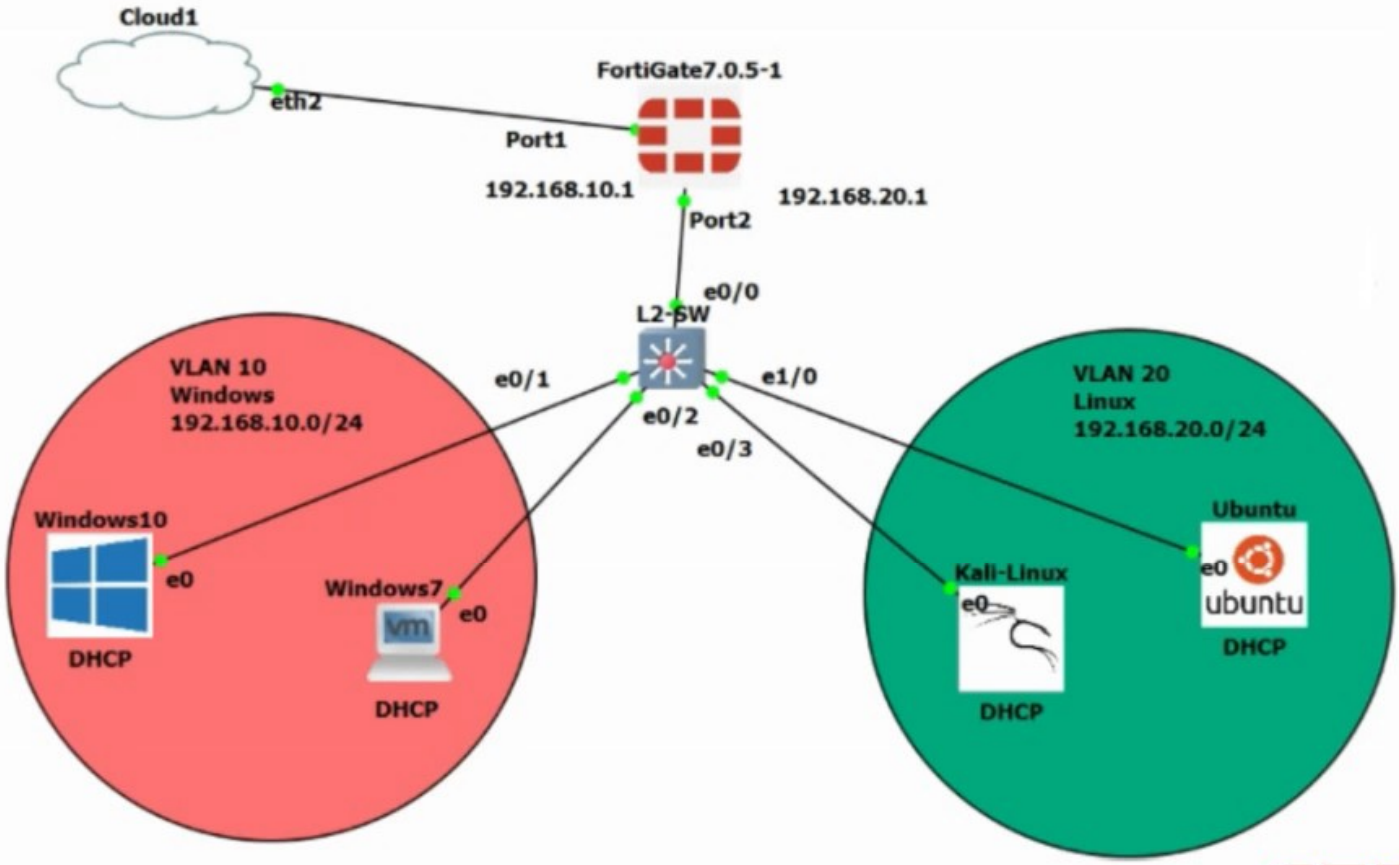
ONL3_ISS8_S3
Group A:
Noureen Khaled 21043876
Mariam Abdou 21069532
Youssef Alaa 21092776
Omar Abdrabo 21051923
Karim Khaled 21081010
Ahmed Zaher 21090718

TABLE OF CONTENTS

01 Topology

In our given VLAN scenario, we created 2 different VLANs, one of which consists two devices that operate Windows Operating System, and the other Linux Operating System.

The VLAN structure is demonstrated in below topology



02 VLANs on Switch

Basic VLANs Configuration

```
ter configuration commands, one per line.  End with CNTL/Z.
2-SW(config)#hostname SW
W(config)#vlan 10
W(config-vlan)#name windows
W(config-vlan)#vlan 20
W(config-vlan)#name linux
W(config-vlan)#exit
W(config)#do show vlan

LAN Name                             Status    Ports
--- -------------------------------- --------- -------------------------------
    default                          active    Et0/0, Et0/1, Et0/2, Et0/3
                                               Et1/0, Et1/1, Et1/2, Et1/3
                                               Et2/0, Et2/1, Et2/2, Et2/3
                                               Et3/0, Et3/1, Et3/2, Et3/3
0   windows                          active
0   linux                            active
002 fddi-default                     act/unsup
003 token-ring-default               act/unsup
004 fddinet-default                  act/unsup
005 trnet-default                    act/unsup

LAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
--- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
    enet  100001     1500  -      -      -        -    -        0      0
0   enet  100010     1500  -      -      -        -    -        0      0
0   enet  100020     1500  -      -      -        -    -        0      0
002 fddi  101002     1500  -      -      -        -    -        0      0
003 tr    101003     1500  -      -      -        -    -        0      0
004 fdnet 101004     1500  -      -      -        ieee -        0      0
005 trnet 101005     1500  -      -      -        ibm  -        0      0
```

1)Bringing topology to real life, creating 2 VLANs on the Switch with previously provided Names and IDs.

2) Double Checking VLANs creation.

Setting ports:

- e0/1
- e0/2
- e0/3
- e1/0

to ‘Access Mode’ in order to belong to a single VLAN, and assigning each port to its corresponding VLAN

```
W(config)#int r e0/1-2
W(config-if-range)#switchport mode acc
W(config-if-range)#switchport mode access
W(config-if-range)#switchport access vlan 10
W(config-if-range)#exit
W(config)#int e0/3
W(config-if)#switchport mode access
W(config-if)#switchport access vlan 20
W(config-if)#int e1/0
W(config-if)#switchport mode access
W(config-if)#switchport access vlan 20
```

```
W(config)#int e0/0
W(config-if)#swi
W(config-if)#switchport mode trunk
ommand rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.
W(config-if)#swi
W(config-if)#switchport trunk en
W(config-if)#switchport trunk encapsulation dot1
W(config-if)#switchport trunk encapsulation dot1q
W(config-if)#switchport mode trunk
W(config-if)#
Nov 28 20:48:00.776: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
W(config-if)#
ov 28 20:48:05.708: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
```

Setting port:

- e0/0

to ‘Trunk Mode’ as it carries traffic for multiple VLANs to the FortiGate Firewall

```
SW(config)#int e0/0
SW(config-if)#switchport trunk allowed vlan 10,20
SW(config-if)#exit
SW(config)#do show int tr

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/0       10,20

Port        Vlans allowed and active in management domain
Et0/0       10,20

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       20
```

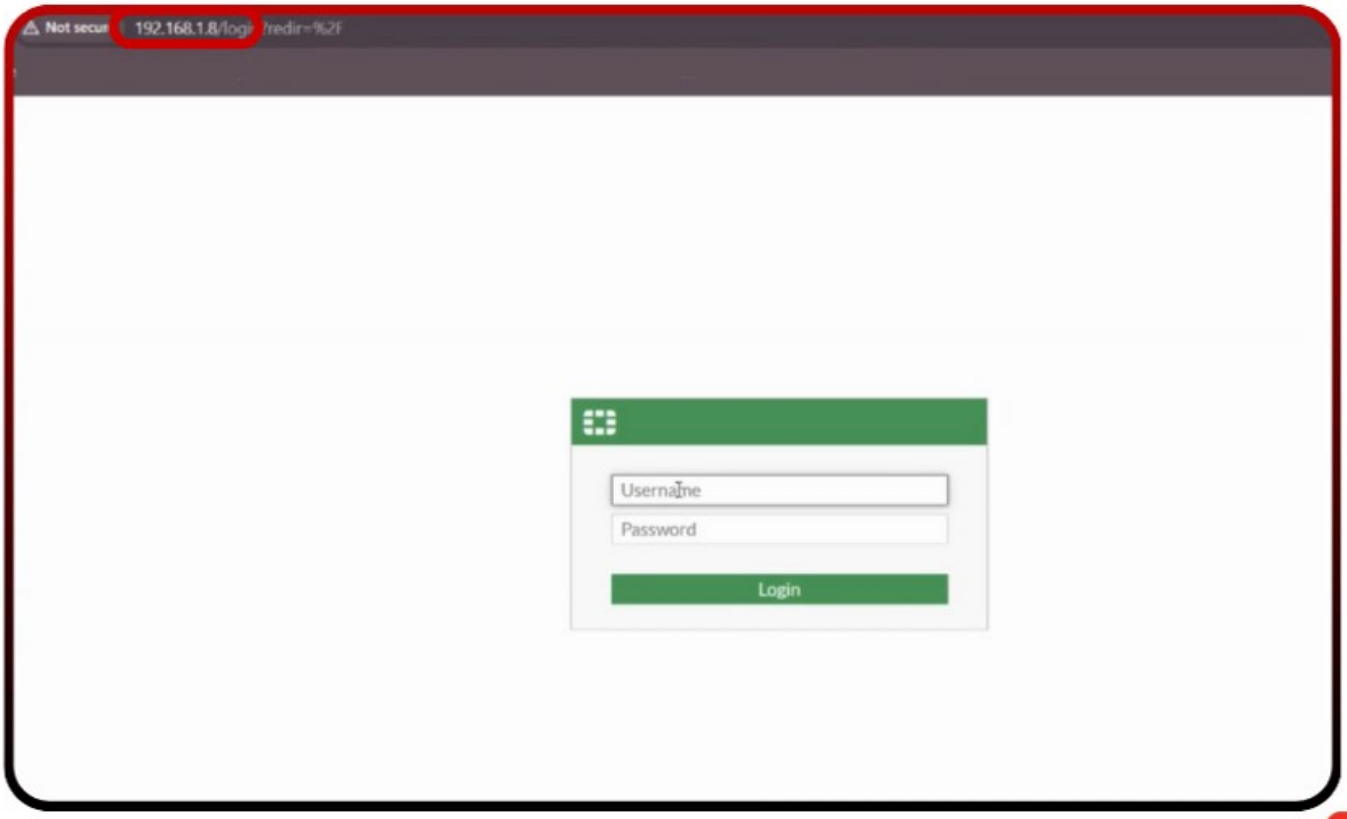
Allowing only VLAN 10 and VLAN 20 to pass through the Trunk port for security purposes

Viewing the Firewall's IP Address that was given via the host, in this scenario, the machine that's operating all scenario's virtual machines.

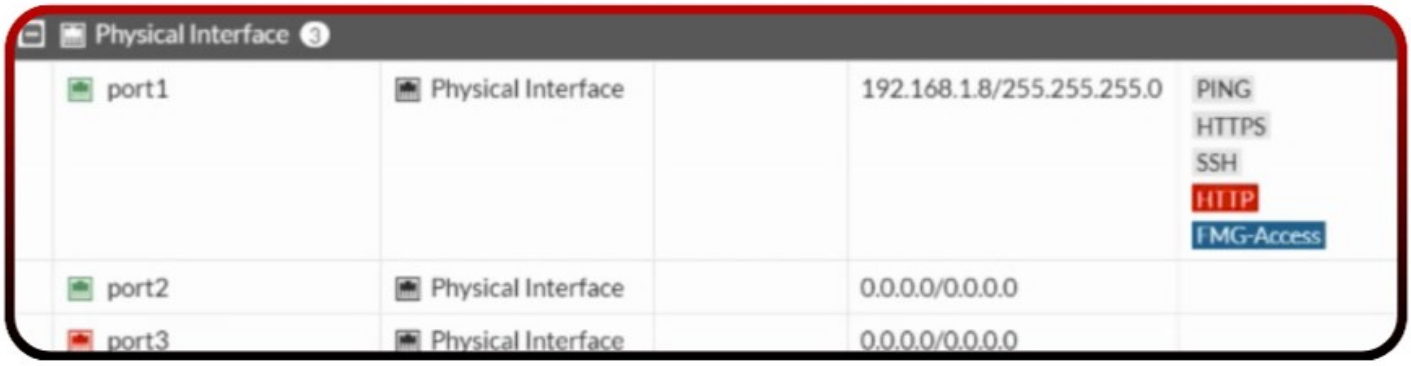
- This IP Address will be used to connect to the FortiGate GUI for further configuration.

```
ortiGate-VM64-KVM login: admin
assword:
ou are forced to change your password. Please input a new password.
ew Password:
onfirm Password:
elcome!

ortiGate-VM64-KVM # get sys int ph
= [onboard]
        ==[port1]
                mode: dhcp
                ip: 192.168.1.8 255.255.255.0
                ipv6: ::/0
                status: up
                speed: 1000Mbps (Duplex: full)
                FEC: none
                FEC_cap: none
        ==[port2]
                mode: static
                ip: 0.0.0.0 0.0.0.0
                ipv6: ::/0
                status: up
                speed: 1000Mbps (Duplex: full)
                FEC: none
                FEC_cap: none
        ==[port3]
                mode: static
                ip: 0.0.0.0 0.0.0.0
                ipv6: ::/0
                status: down
                speed: n/a
                FEC: none
```



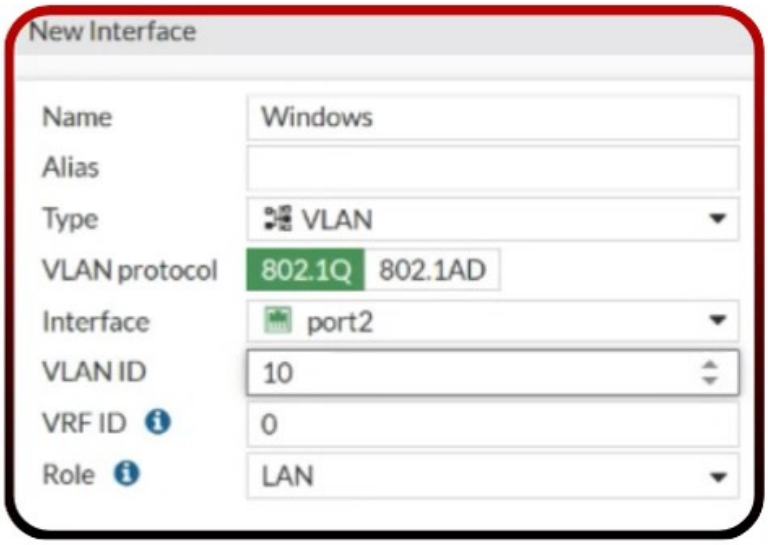
03 VLANs on FortiGate

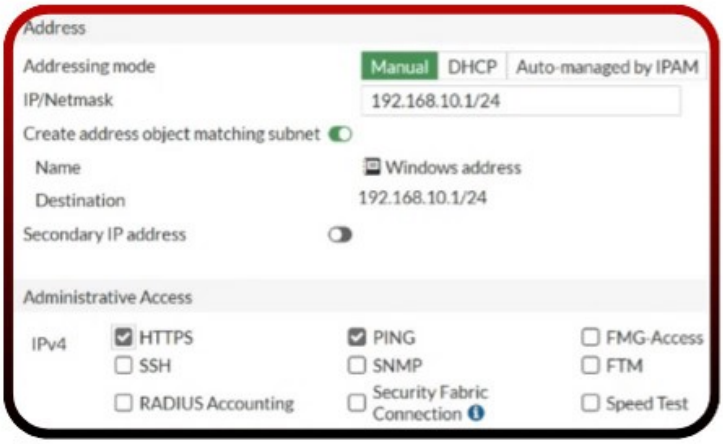


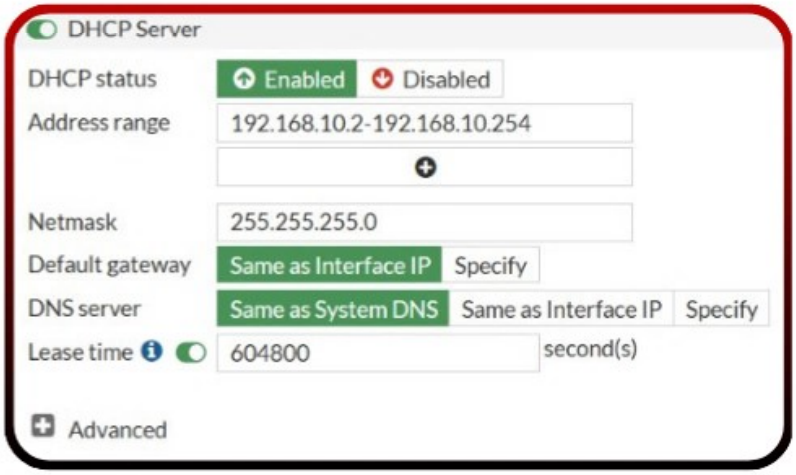
Our physical interfaces on the FortiGate firewall prior to VLAN configuration

Creating both VLANs:

VLAN 10



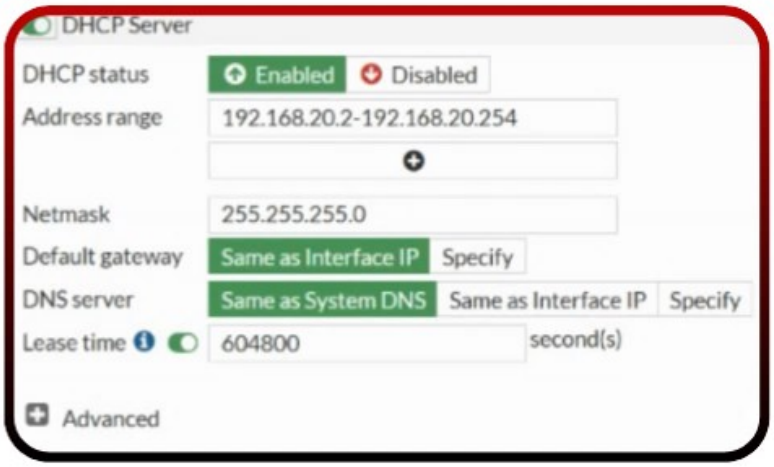




We gave our VLAN its Name, ID, Network Address, and the capability to give devices on that VLAN IP Addresses using the DHCP Server option

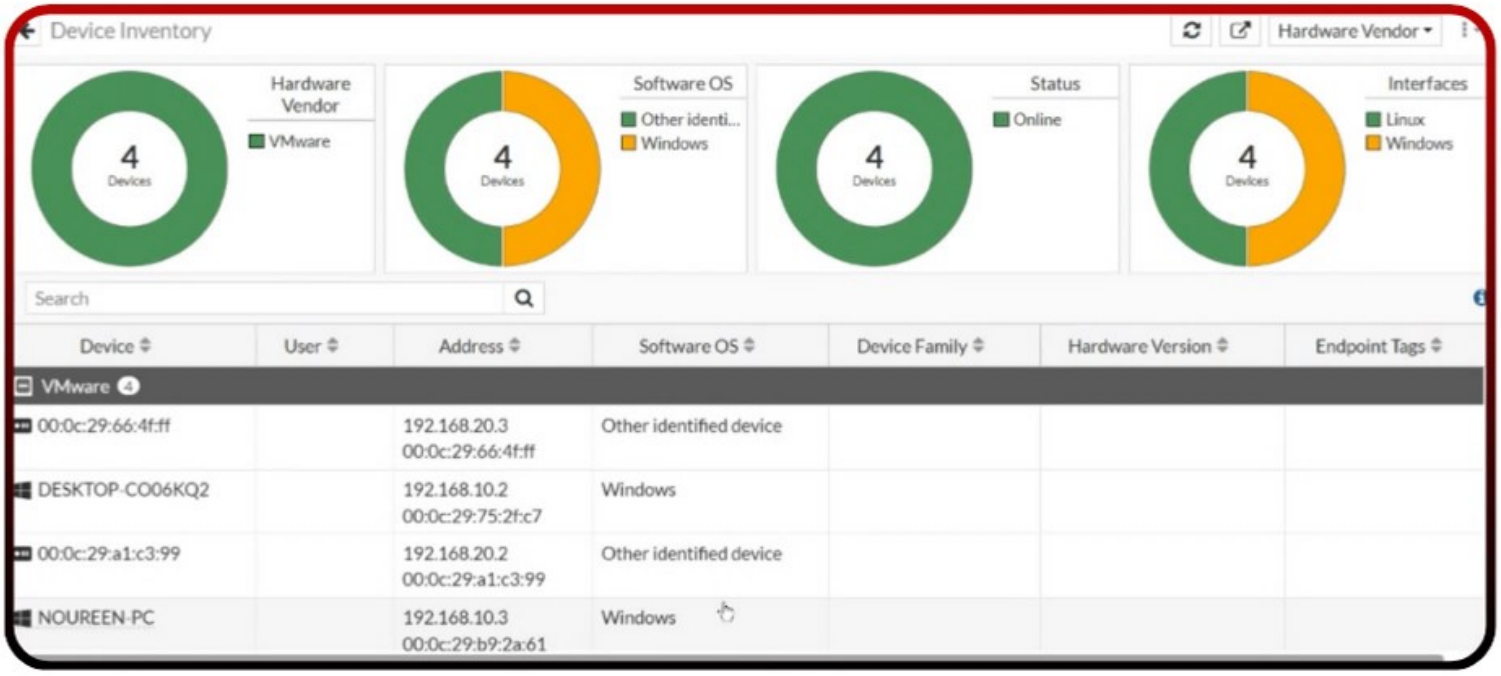
VLAN 20

We do as mentioned before but with our second VLAN for Linux



Physical interfaces after adding VLANs' subinterfaces

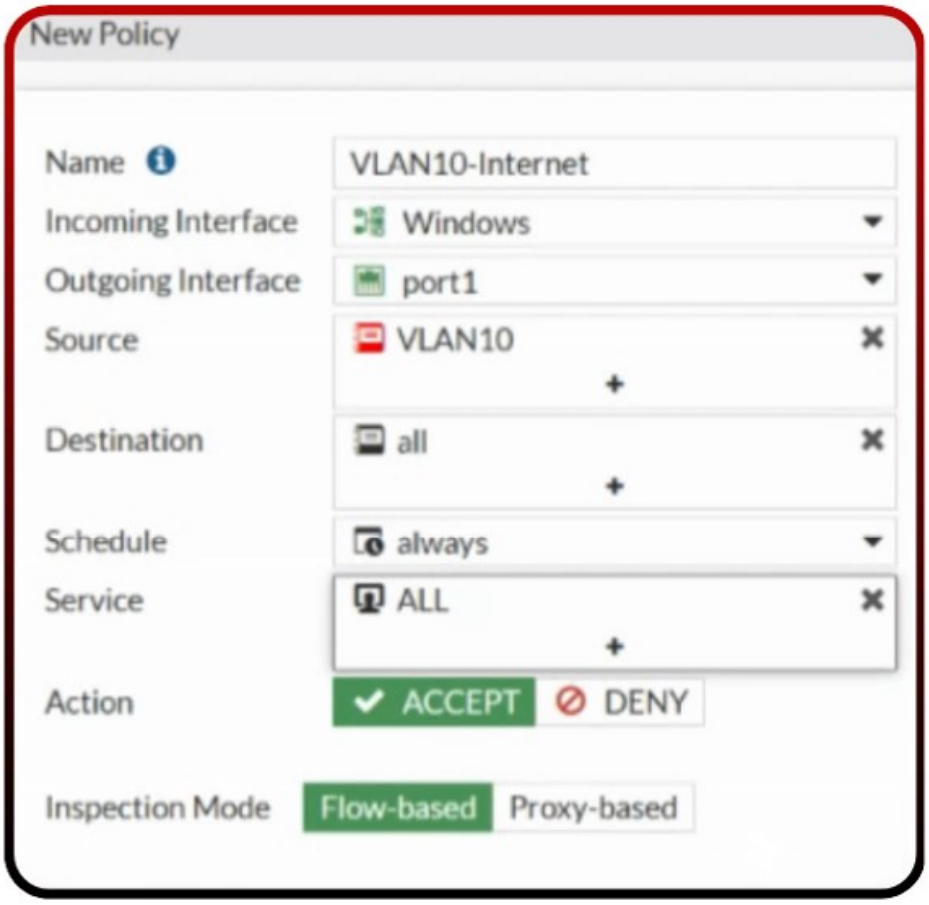
The corresponding dashboard shows all our connected Virtual Machines, alongside their IP addresses, and some other statistics



04 FortiGate Policies

Now that both VLANs are created, it's only convenient that they have access with the outside world, the Internet. That can be achieved through policies set on our FortiGate.

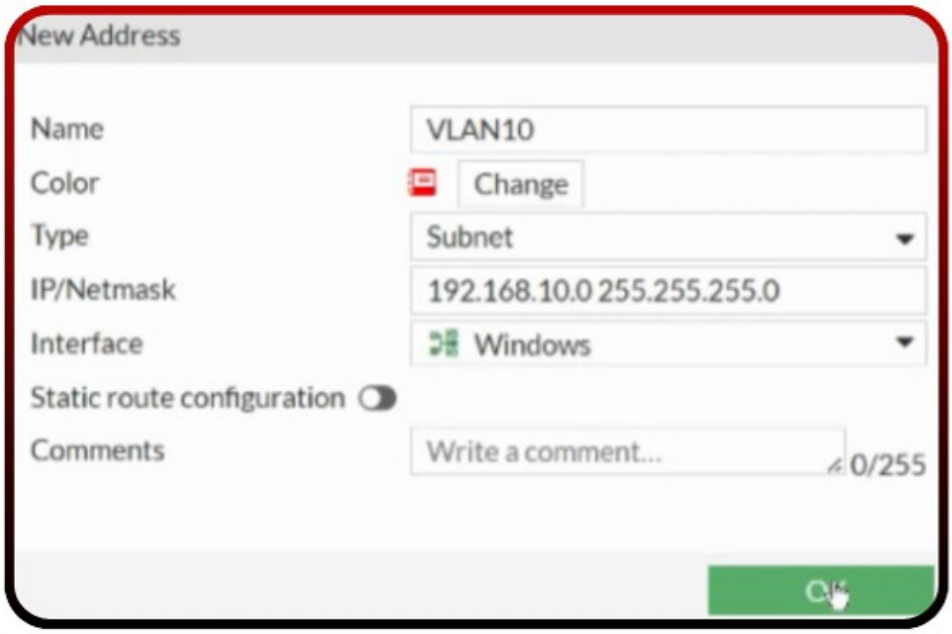
VLAN 10 Policy



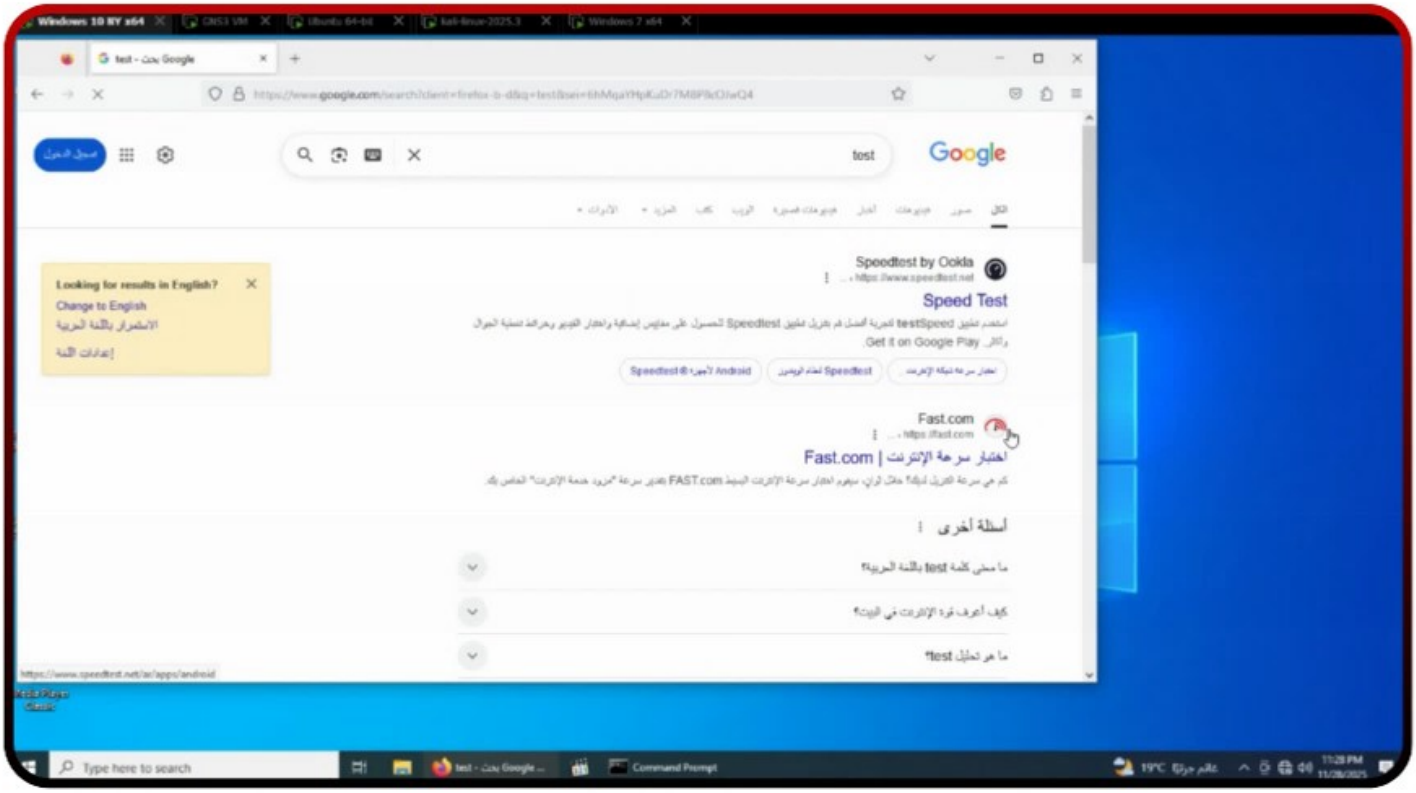
The policy that is to be created can be broken down into:

- **Name**: The name of the policy
- **Incoming Interface**: The interface where traffic *enters* the firewall.
- **Outcoming Interface**: The interface where traffic *leaves* the firewall.
- **Source**: The addresses/networks are allowed by this policy
- **Destination**: The allowed destination addresses.
- **Schedule**: When the policy is active.
- **Service**: The protocols/ports allowed

When defining the ‘Source’ address/networks, we add our VLAN to make it the source on our current policy



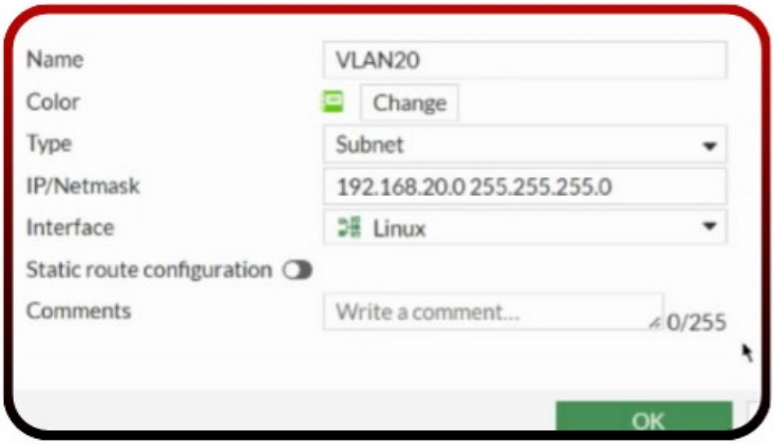
Testing our policy:



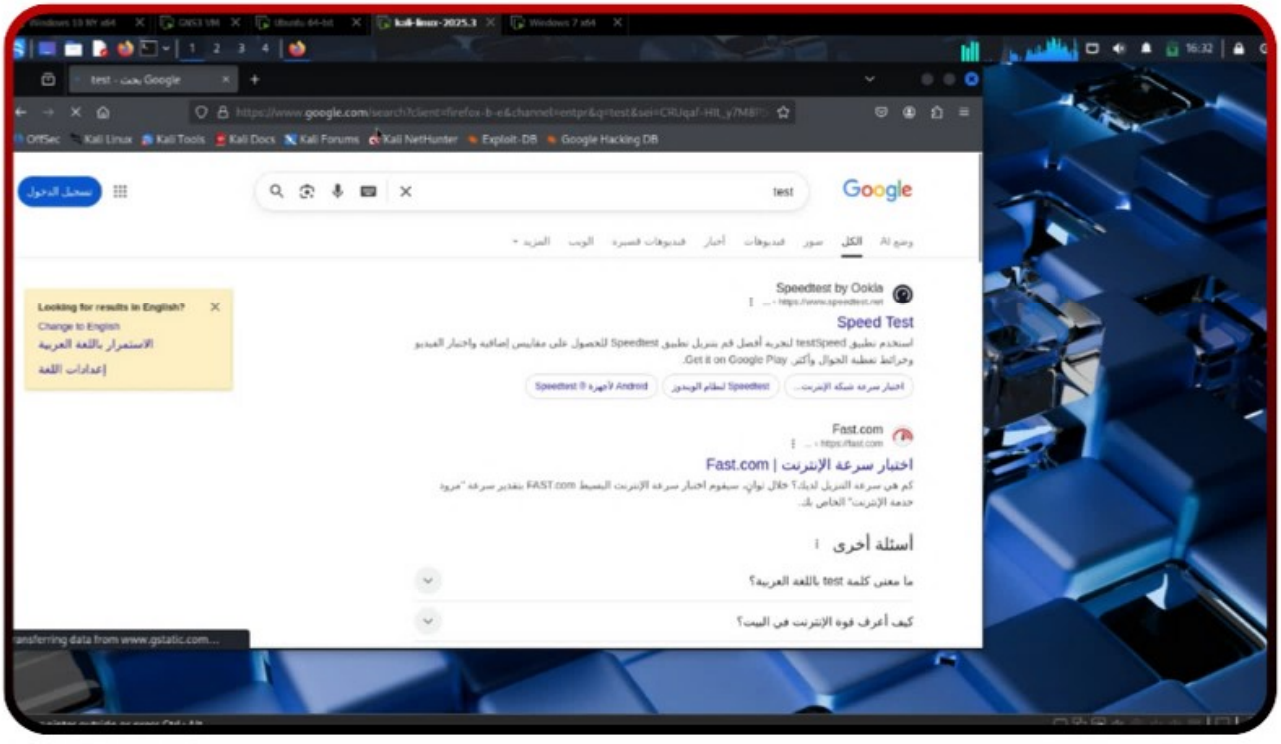
After Testing on one of the VLAN 10 devices, we are given internet access

VLAN 20 Policy

After successfully creating the VLAN 10 policy, we'll do the same for the second VLAN



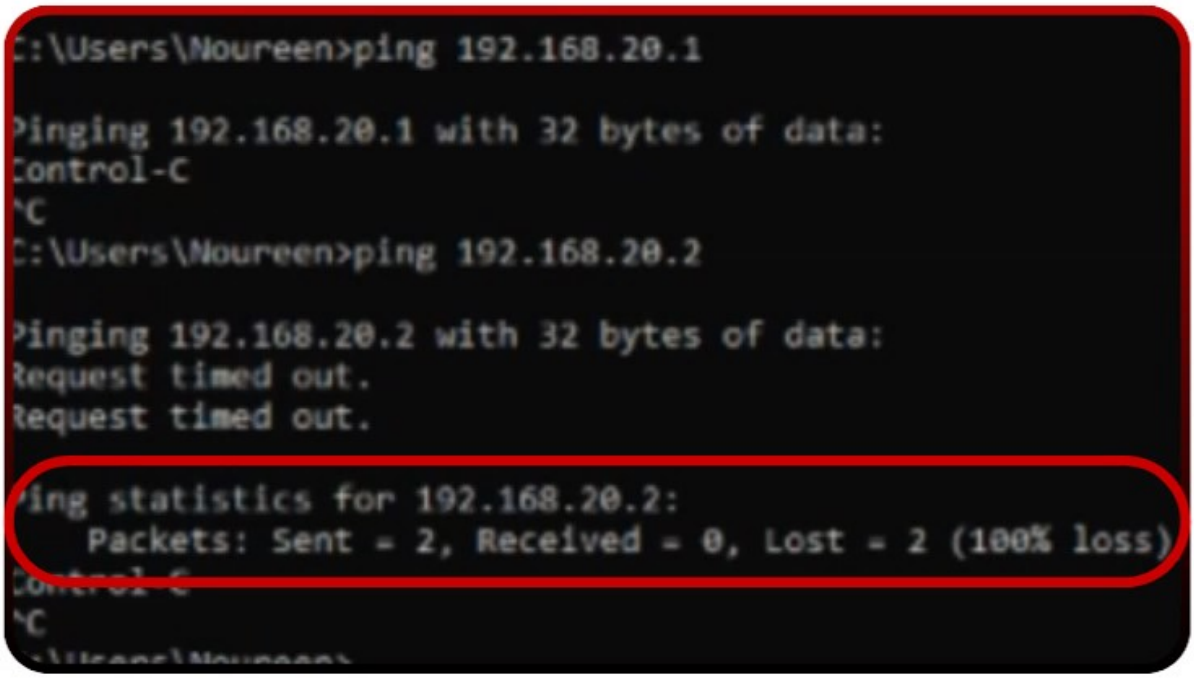
Testing our policy:



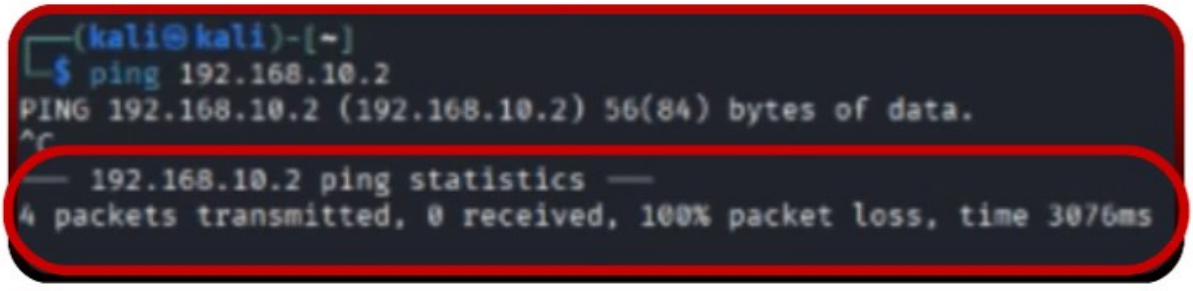
05 Inter-VLAN routing on FortiGate

After successfully surfing the internet, our VLANs will need to communicate and exchange traffic

Pinging from:
VLAN 10
to
VLAN 20

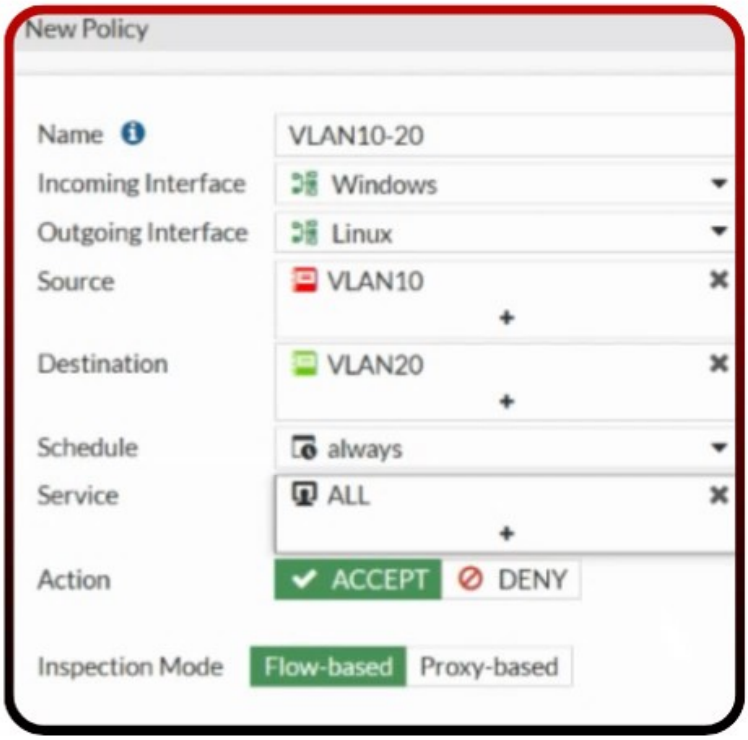


Pinging from:
VLAN 20
to
VLAN 10



It's clear that it's impossible to PING from one VLAN to another without explicitly setting up INTER-VLAN Routing using **Router-on-a-Stick** with FortiGate policies.

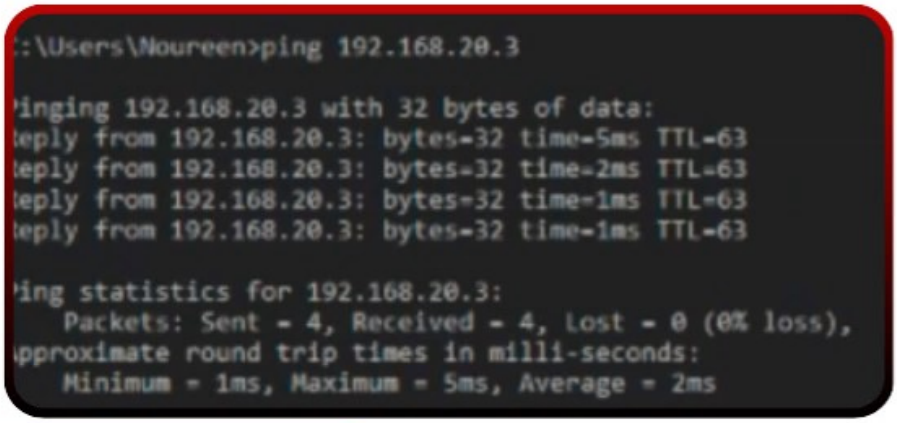
VLAN 10 → VLAN 20

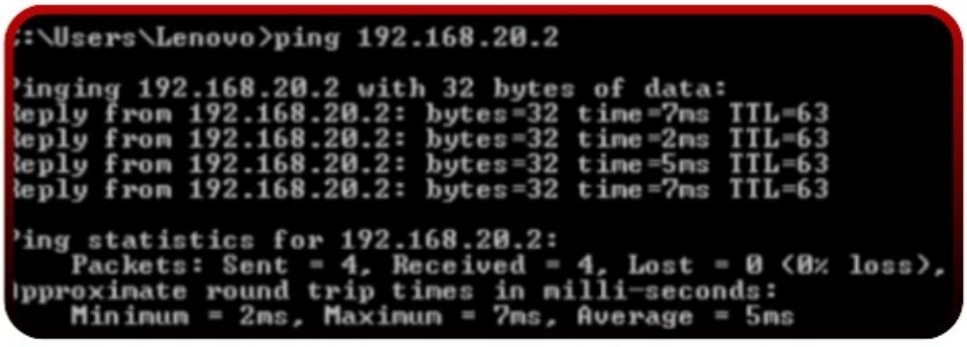


The following policy allows ANY type of traffic to be directed from VLAN 10 (Source) to VLAN 20 (Destination), but NOT the other way around

Testing Policy

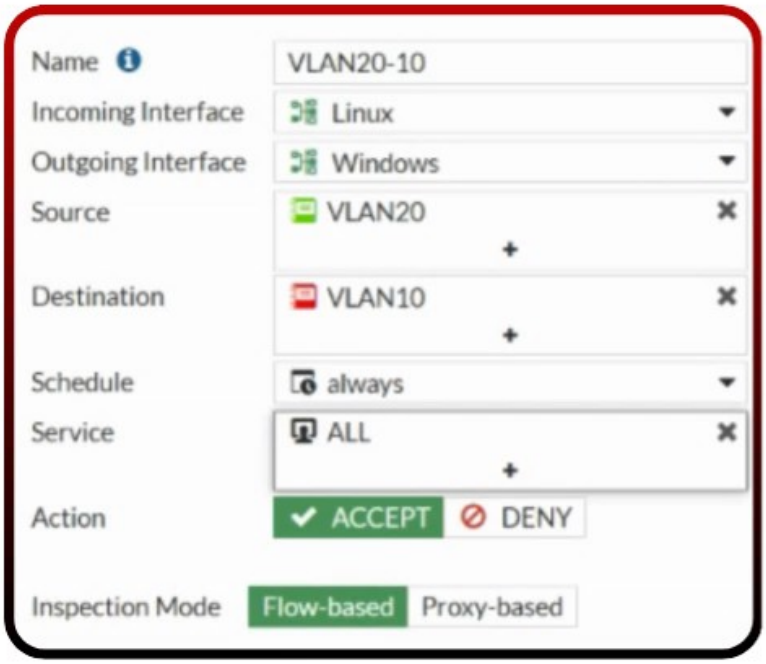
Both devices on VLAN 10 can ping devices on VLAN 20 but not the other way.





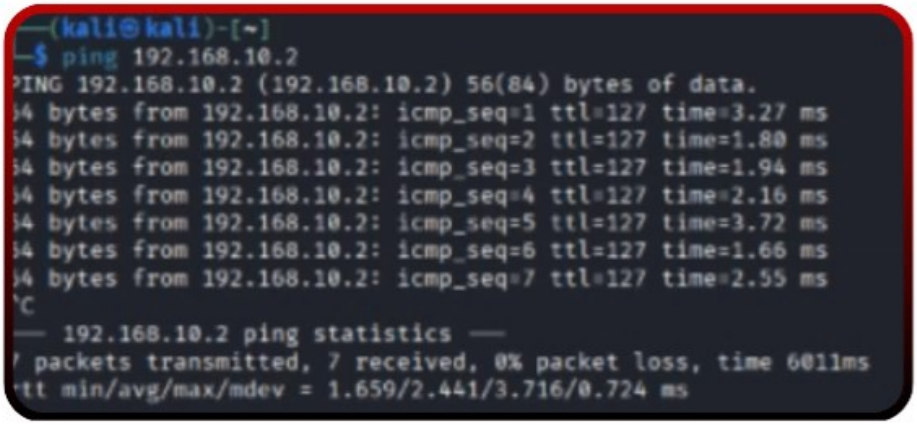
VLAN 20 → VLAN 10

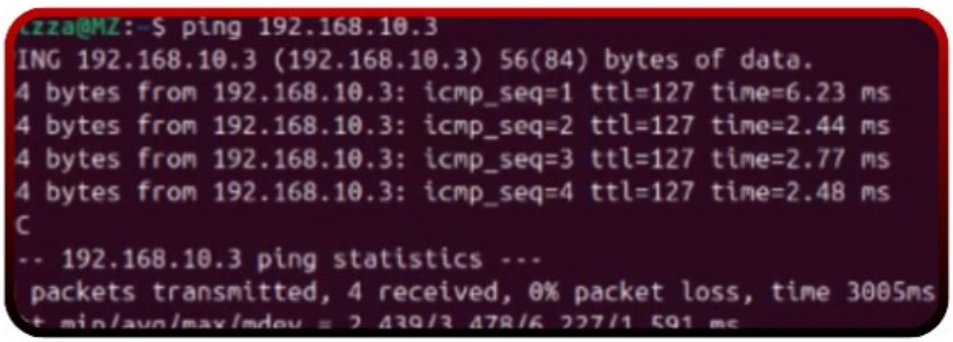
The following policy allows ANY type of traffic to be directed from VLAN 20 (Source) to VLAN 10 (Destination), so communication is bidirectional



Testing Policy

Both devices on VLAN 20 can ping devices on VLAN 10 and vice versa.





Traffic Monitoring

Date/Time		Source	Device	Destination	Application Name	Result	Policy ID
21 seconds ago		192.168.20.3	00:0c:29:66:4f:ff	192.168.10.3		✔ 336 B / 336 B	VLAN20-10 (4)
26 seconds ago		192.168.20.3	00:0c:29:66:4f:ff	192.168.10.2		✔ 252 B / 252 B	VLAN20-10 (4)
45 seconds ago		192.168.20.2	00:0c:29:a1:c3:99	192.168.10.2		✔ 588 B / 588 B	VLAN20-10 (4)
2 minutes ago		192.168.10.3	WIN-HEDD8RLH058	192.168.20.3		✔ 240 B / 240 B	VLAN10-20 (3)
3 minutes ago		192.168.10.3	WIN-HEDD8RLH058	192.168.20.2		✔ 240 B / 240 B	VLAN10-20 (3)
3 minutes ago		192.168.10.2	DESKTOP-CO06KQ2	192.168.20.3		✔ 240 B / 240 B	VLAN10-20 (3)
minutes ago		192.168.10.2	DESKTOP-CO06KQ2	192.168.20.2		✔ 240 B / 240 B	VLAN10-20 (3)

All Policies

Linux → port1 1									
VLAN20-Internet	VLAN20	all	always	ALL	✔ ACCEPT	Enabled	no-inspection	UTM	107.97 MB
Linux → Windows 1									
VLAN20-10	VLAN20	VLAN10	always	ALL	✔ ACCEPT	Enabled	no-inspection	All	2.35 kB
Windows → Linux 1									
VLAN10-20	VLAN10	VLAN20	always	ALL	✔ ACCEPT	Enabled	no-inspection	All	3.36 kB
Windows → port1 1									
VLAN10-Internet	VLAN10	all	always	ALL	✔ ACCEPT	Enabled	no-inspection	UTM	46.80 MB
Implicit 1									
plicit Deny	all	all	always	ALL	⊘ DENY			Disabled	200.06 kB