



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

1

Topology

2

VLANs on Switch

3

VLANs on FortiGate

4

FortiGate Policies

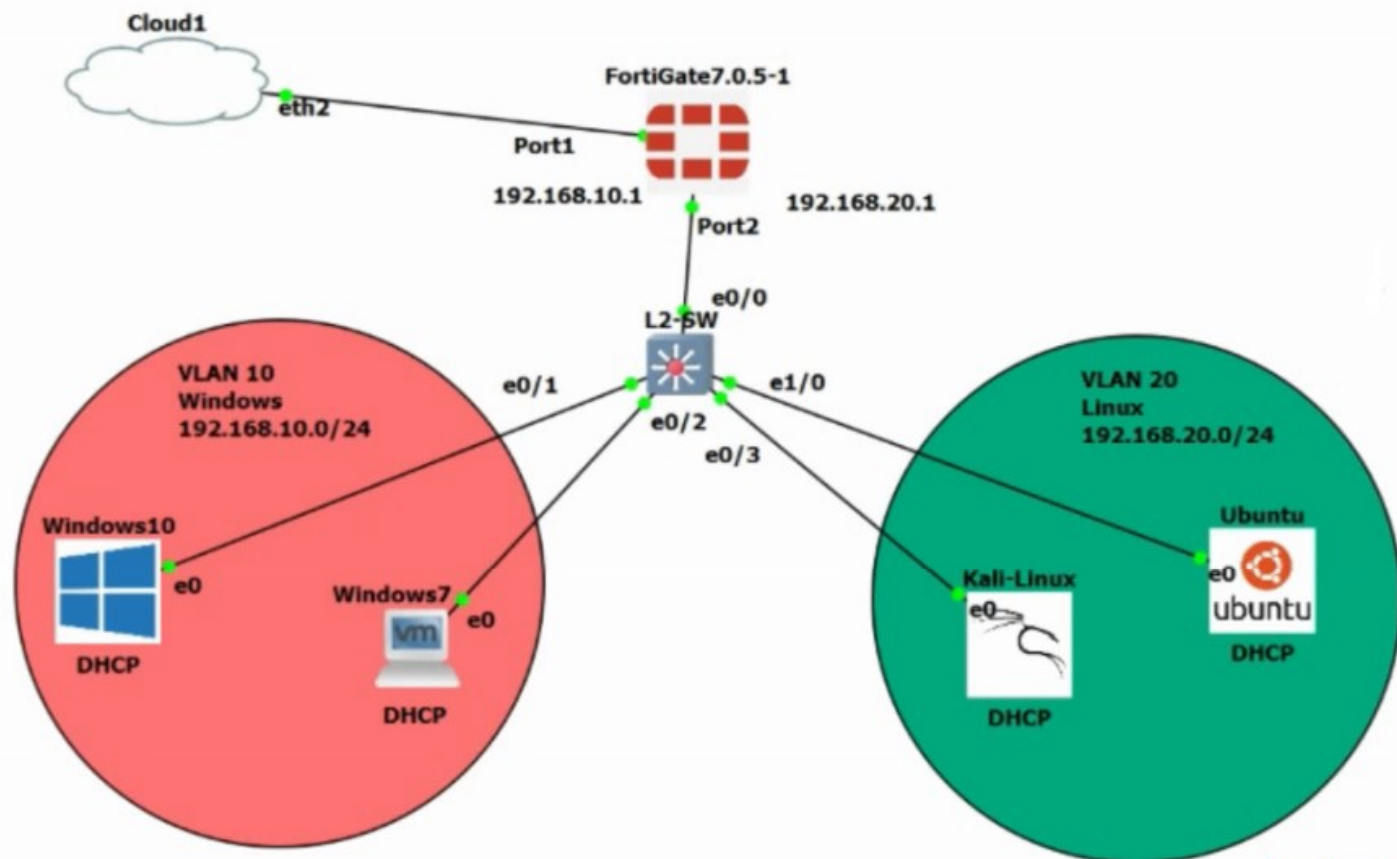
5

**Inter-VLAN routing
on FortiGate**

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

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

2) Double Checking VLANs creation.

Enter 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

Setting ports:

- o e0/1
- o e0/2
- o e0/3
- o 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
```



```

SW(config)#int e0/0
SW(config-if)#swi
SW(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode.
SW(config-if)#swi
SW(config-if)#switchport trunk en
SW(config-if)#switchport trunk encapsulation dot1
SW(config-if)#switchport trunk encapsulation dot1q
SW(config-if)#switchport mode trunk
SW(config-if)#
Nov 28 20:48:00.776: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
SW(config-if)#
Nov 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     10,20

```

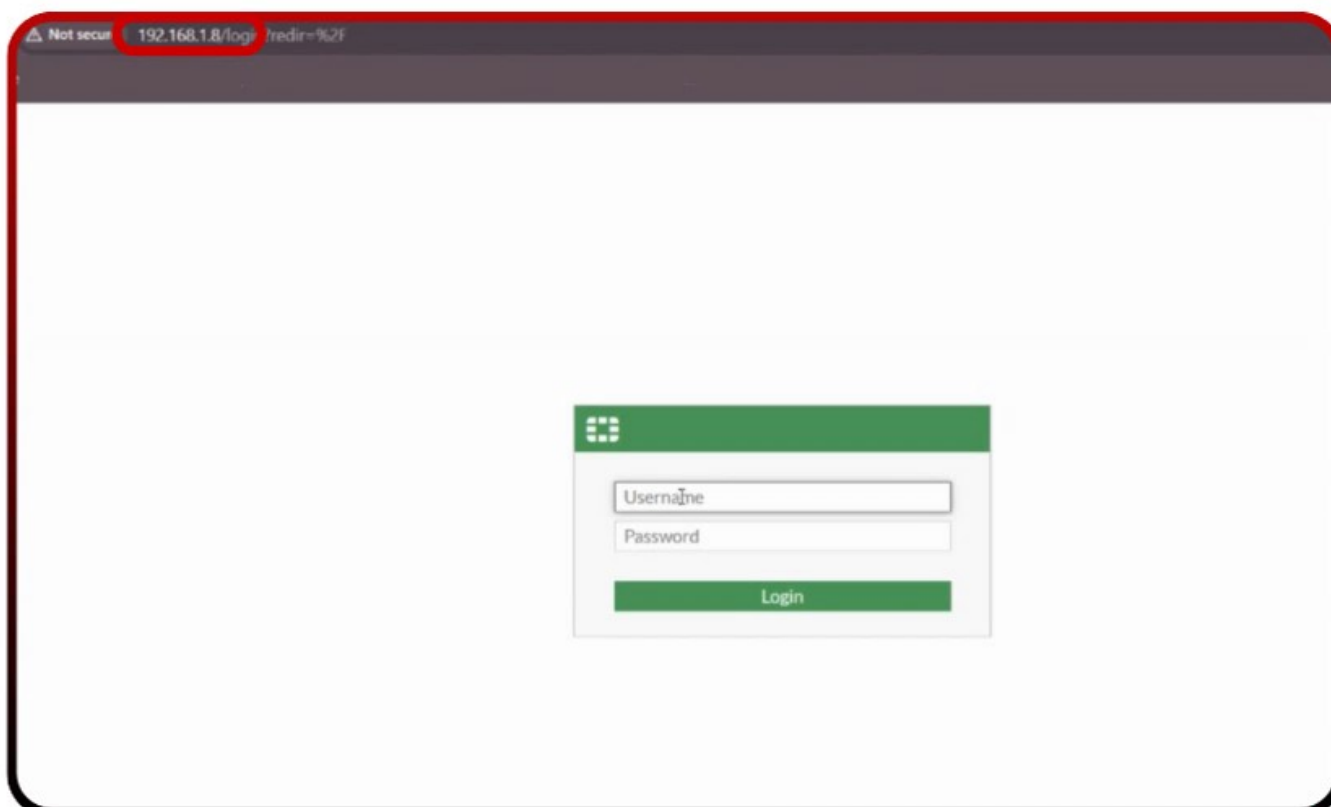
Allowing only VLAN 10 and VLAN 20 to pass through the Trunk port for security purposes

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.

```
fortiGate-VM64-KVM login: admin
Password:
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Welcome!

fortiGate-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

Physical Interface 3				
port1	Physical Interface	192.168.1.8/255.255.255.0	PING HTTPS SSH HTTP FMG-Access	
port2	Physical Interface	0.0.0.0/0.0.0.0		
port3	Physical Interface	0.0.0.0/0.0.0.0		

Our physical interfaces on the FortiGate firewall prior to VLAN configuration

Creating both VLANs:

VLAN 10

New Interface

Name	Windows
Alias	
Type	VLAN
VLAN protocol	802.1Q 802.1AD
Interface	port2
VLAN ID	10
VRF ID	0
Role	LAN

Address

Addressing mode: Manual DHCP Auto-managed by IPAM

IP/Netmask: 192.168.10.1/24

Create address object matching subnet: ☒

Name: Windows address

Destination: 192.168.10.1/24

Secondary IP address: ☐

Administrative Access

IPv4	<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> PING	<input type="checkbox"/> FMG-Access
	<input type="checkbox"/> SSH	<input type="checkbox"/> SNMP	<input type="checkbox"/> FTM
	<input type="checkbox"/> RADIUS Accounting	<input type="checkbox"/> Security Fabric Connection	<input type="checkbox"/> Speed Test

DHCP Server

DHCP status: ☒ Enabled ☐ Disabled

Address range: 192.168.10.2-192.168.10.254

Netmask: 255.255.255.0

Default gateway: Same as Interface IP Specify

DNS server: Same as System DNS Same as Interface IP Specify

Lease time: 604800 second(s)

Advanced

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

New Interface

Name	Linux
Alias	
Type	VLAN
VLAN protocol	802.1Q 802.1AD
Interface	port2
VLAN ID	20
VRF ID	0
Role	LAN

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

DHCP Server

DHCP status: Enabled Disabled

Address range: 192.168.20.2-192.168.20.254

Netmask: 255.255.255.0

Default gateway: Same as Interface IP Specify

DNS server: Same as System DNS Same as Interface IP Specify

Lease time: 604800 second(s)

Advanced

Address

Addressing mode: Manual DHCP Auto-managed by IPAM

IP/Netmask: 192.168.20.1/24

Create address object matching subnet: On

Name: Linux address

Destination: 192.168.20.1/24

Secondary IP address: Off

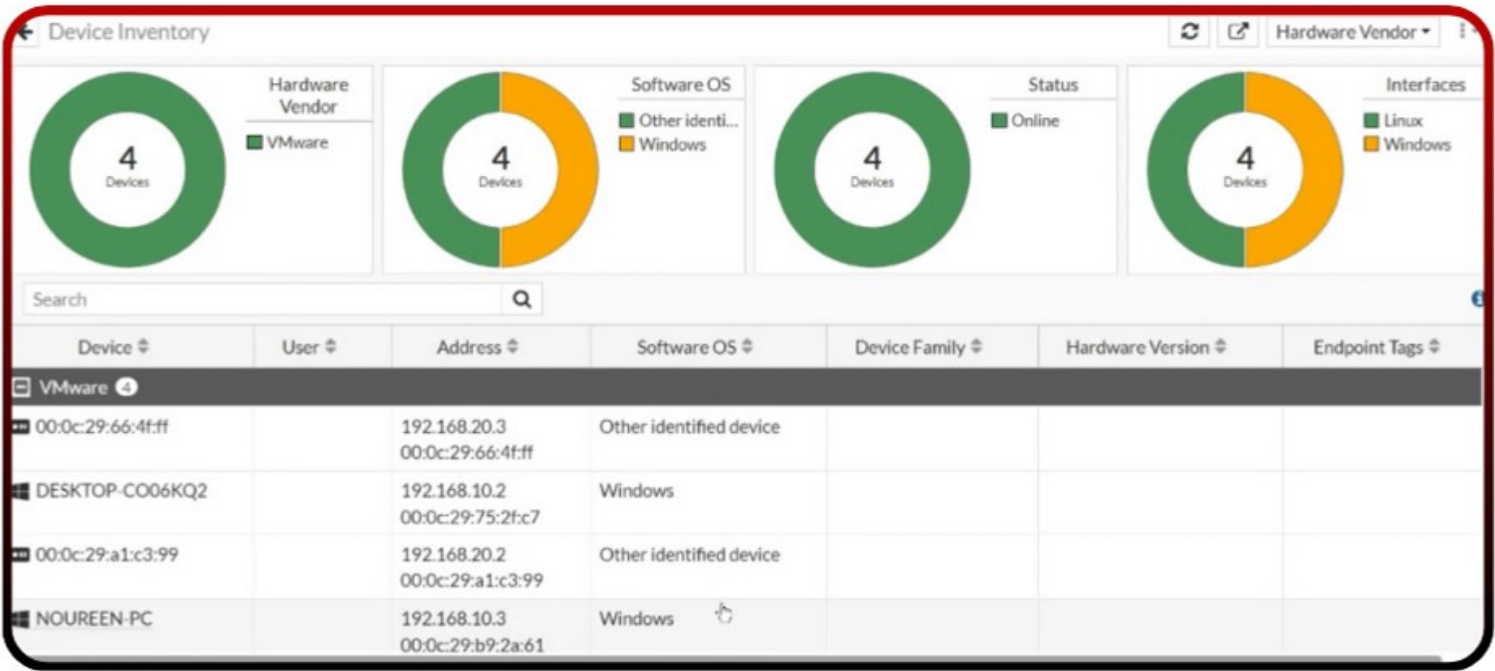
Administrative Access

IPv4	<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> PING	<input type="checkbox"/> FMG Access
	<input type="checkbox"/> SSH	<input type="checkbox"/> SNMP	<input type="checkbox"/> FTM
	<input type="checkbox"/> RADIUS Accounting	<input type="checkbox"/> Security Fabric Connection	<input type="checkbox"/> Speed Test

Physical interfaces after adding VLANs' subinterfaces

Physical Interface				
port1	Physical Interface	192.168.1.8/255.255.255.0	PING	HTTPS
			SSH	HTTP
			FMG Access	
port2	Physical Interface	0.0.0.0/0.0.0.0		
• Linux	VLAN	192.168.20.1/255.255.255.0	PING	HTTPS
• Windows	VLAN	192.168.10.1/255.255.255.0	PING	HTTPS
port3	Physical Interface	0.0.0.0/0.0.0.0		

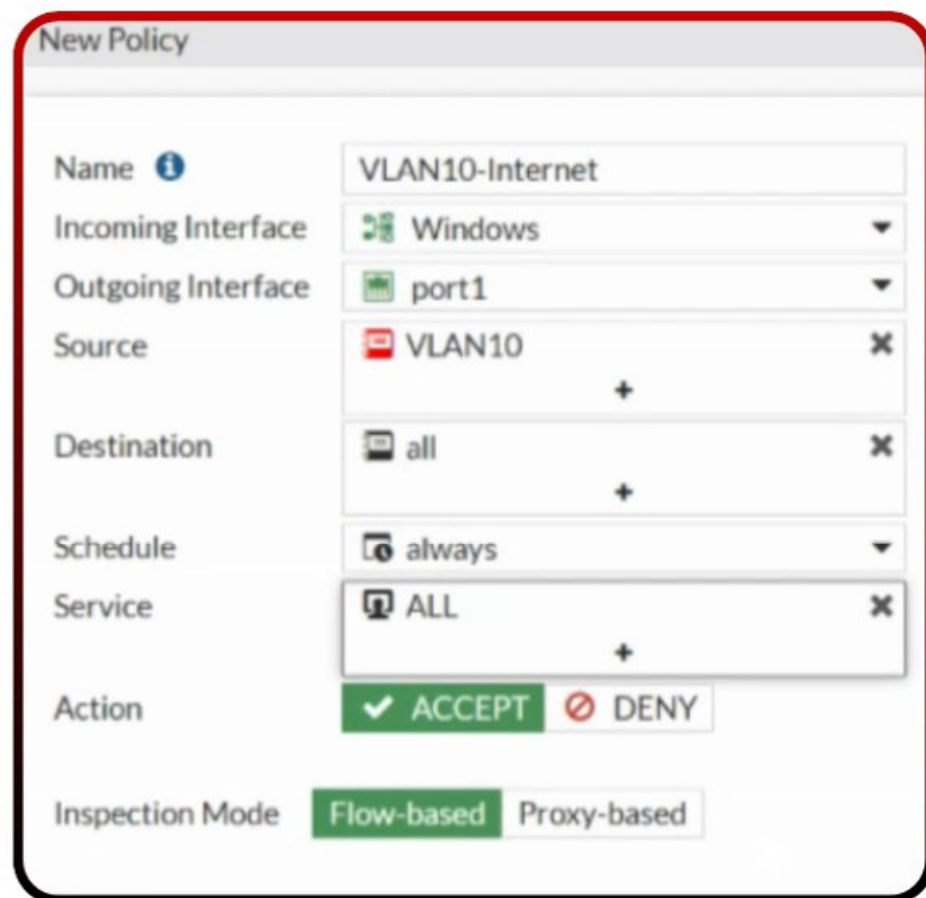
The corresponding dashboard shows all our connected Virtual Machines, alongside their IP addresses, and some other statistics



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 screenshot shows the 'New Policy' configuration window in FortiGate. The fields are as follows:

Field	Value
Name	VLAN10-Internet
Incoming Interface	Windows
Outgoing Interface	port1
Source	VLAN10
Destination	all
Schedule	always
Service	ALL
Action	ACCEPT
Inspection Mode	Flow-based

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

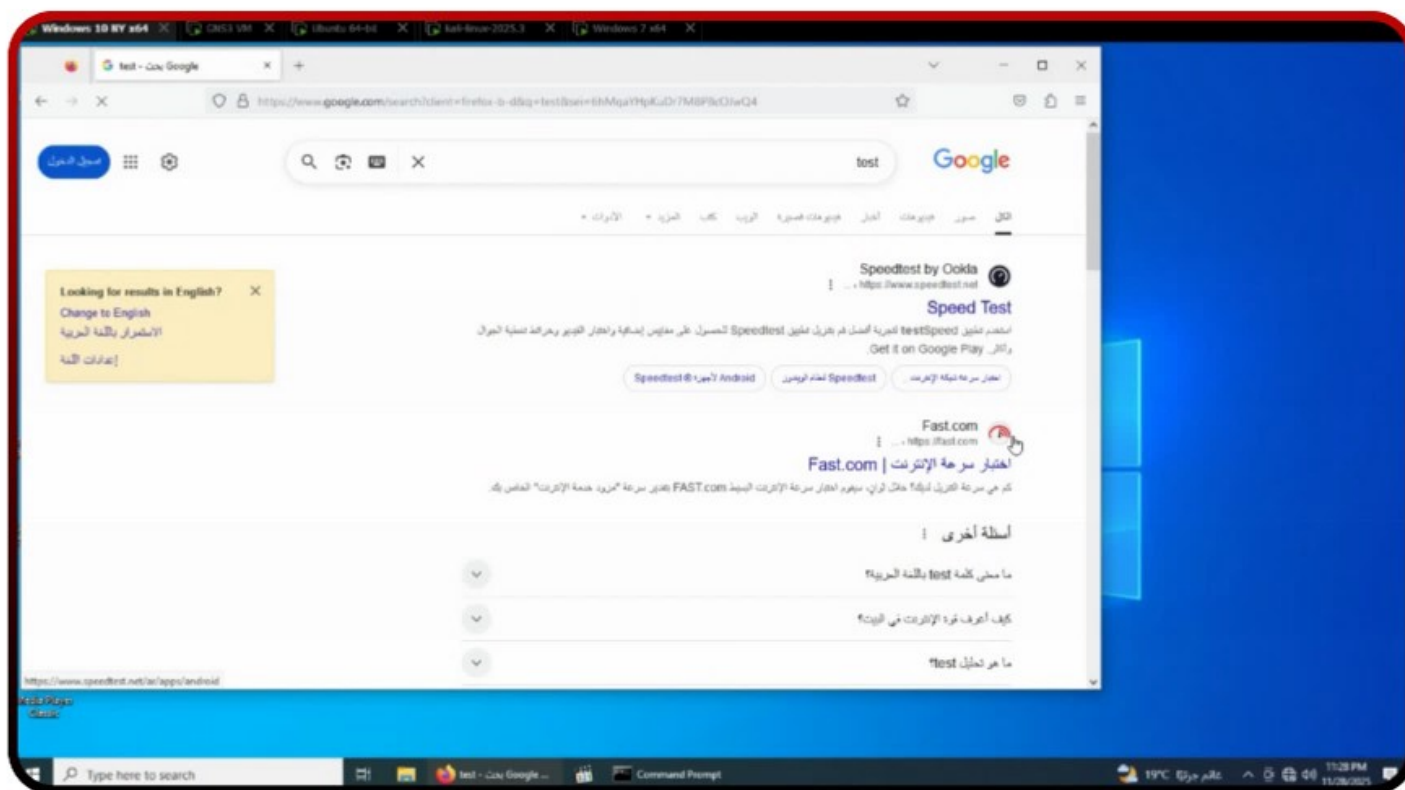
When defining the 'Source' address/networks, we add our VLAN to make it the source on our current policy

The 'New Address' window shows the following configuration:

- Name: VLAN10
- Color: (Red icon) Change
- Type: Subnet
- IP/Netmask: 192.168.10.0 255.255.255.0
- Interface: Windows
- Static route configuration: ☐
- Comments: Write a comment... 0/255

A green 'OK' button is at the bottom right.

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

New Policy

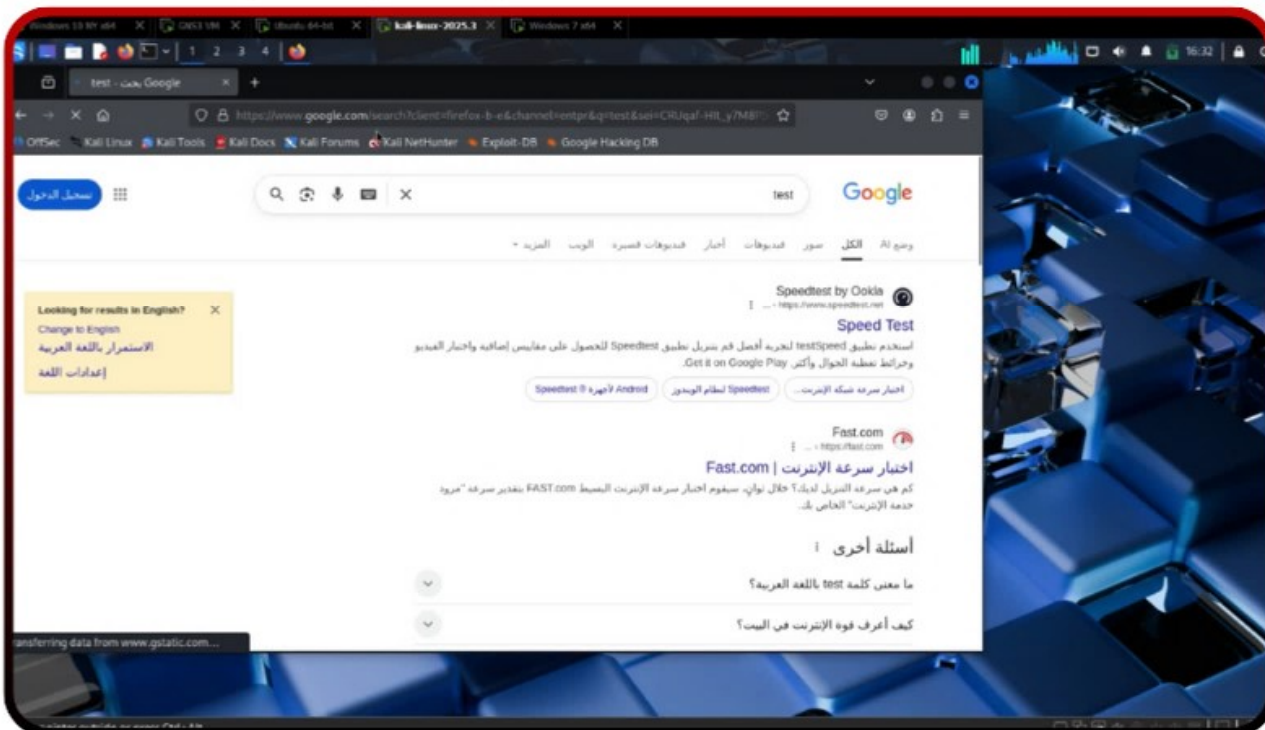
Name	VLAN20-Internet
Incoming Interface	Linux
Outgoing Interface	port1
Source	VLAN20
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based

VLAN20

Name	VLAN20
Color	<input checked="" type="checkbox"/> Change
Type	Subnet
IP/Netmask	192.168.20.0 255.255.255.0
Interface	Linux
Static route configuration	<input type="checkbox"/>
Comments	Write a comment... 0/255

OK

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

```
C:\Users\Noureen>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:
Control-C
^C
C:\Users\Noureen>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 192.168.20.2:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss)
```

Pinging from:
VLAN 20
to
VLAN 10

```
(kali@kali)-[~]
$ ping 192.168.10.2
PING 192.168.10.2 (192.168.10.2) 56(84) bytes of data.
^C
--- 192.168.10.2 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3076ms
```

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

New Policy

Name	VLAN10-20
Incoming Interface	Windows
Outgoing Interface	Linux
Source	VLAN10
Destination	VLAN20
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based

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.

```
C:\Users\Noureen>ping 192.168.20.3
```

```
Pinging 192.168.20.3 with 32 bytes of data:
Reply from 192.168.20.3: bytes=32 time=5ms TTL=63
Reply from 192.168.20.3: bytes=32 time=2ms TTL=63
Reply from 192.168.20.3: bytes=32 time=1ms TTL=63
Reply from 192.168.20.3: bytes=32 time=1ms TTL=63
```

```
Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 5ms, Average = 2ms
```

```
C:\Users\Lenovo>ping 192.168.20.2
```

```
Pinging 192.168.20.2 with 32 bytes of data:
Reply from 192.168.20.2: bytes=32 time=7ms TTL=63
Reply from 192.168.20.2: bytes=32 time=2ms TTL=63
Reply from 192.168.20.2: bytes=32 time=5ms TTL=63
Reply from 192.168.20.2: bytes=32 time=7ms TTL=63
```

```
Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 7ms, Average = 5ms
```

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

Name	VLAN20-10
Incoming Interface	Linux
Outgoing Interface	Windows
Source	VLAN20
Destination	VLAN10
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	<input checked="" type="checkbox"/> Flow-based <input type="checkbox"/> Proxy-based

Testing Policy

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

```
(kali@kali)-[~]
$ ping 192.168.10.2
PING 192.168.10.2 (192.168.10.2) 56(84) bytes of data:
64 bytes from 192.168.10.2: icmp_seq=1 ttl=127 time=3.27 ms
64 bytes from 192.168.10.2: icmp_seq=2 ttl=127 time=1.80 ms
64 bytes from 192.168.10.2: icmp_seq=3 ttl=127 time=1.94 ms
64 bytes from 192.168.10.2: icmp_seq=4 ttl=127 time=2.16 ms
64 bytes from 192.168.10.2: icmp_seq=5 ttl=127 time=3.72 ms
64 bytes from 192.168.10.2: icmp_seq=6 ttl=127 time=1.66 ms
64 bytes from 192.168.10.2: icmp_seq=7 ttl=127 time=2.55 ms
^C
-- 192.168.10.2 ping statistics --
7 packets transmitted, 7 received, 0% packet loss, time 6011ms
rtt min/avg/max/mdev = 1.659/2.441/3.716/0.724 ms
```

```
lzza@MZ:~$ ping 192.168.10.3
PING 192.168.10.3 (192.168.10.3) 56(84) bytes of data:
4 bytes from 192.168.10.3: icmp_seq=1 ttl=127 time=6.23 ms
4 bytes from 192.168.10.3: icmp_seq=2 ttl=127 time=2.44 ms
4 bytes from 192.168.10.3: icmp_seq=3 ttl=127 time=2.77 ms
4 bytes from 192.168.10.3: icmp_seq=4 ttl=127 time=2.48 ms
^C
-- 192.168.10.3 ping statistics --
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 2.430/3.478/6.227/1.501 ms
```

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)
3 minutes ago		192.168.10.2	DESKTOP-CO06KQ2	192.168.20.2		✓ 240 B / 240 B	VLAN10-20 (3)

All Policies

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