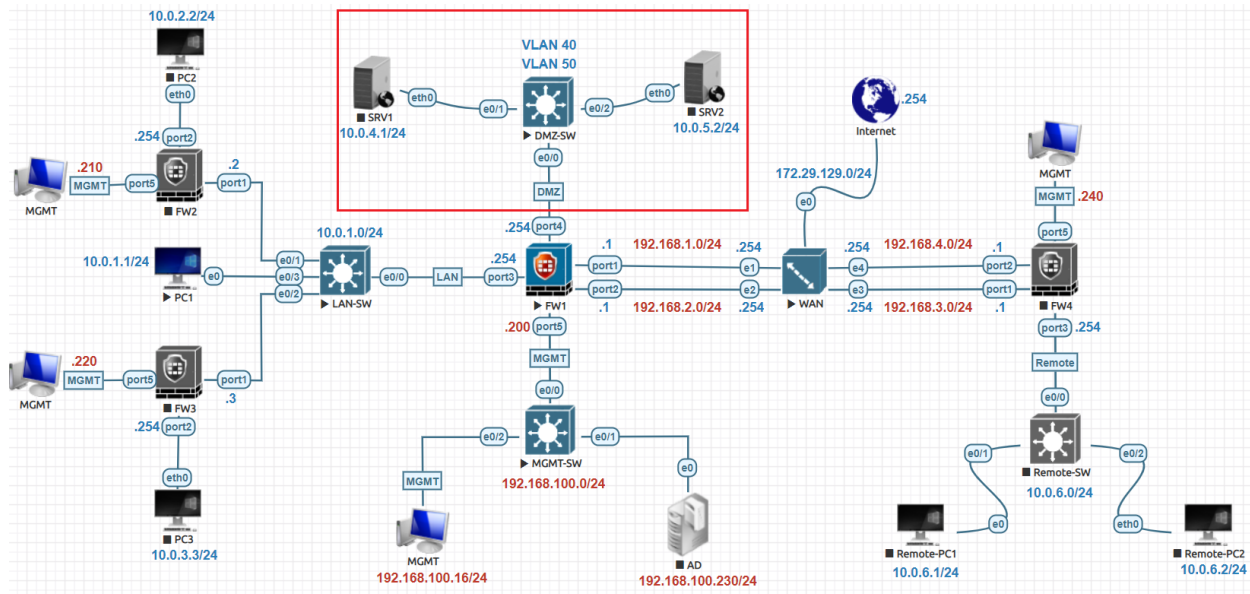


VLAN LAB:



Cisco Switch Configuration

```
Switch(config)#hostname DMZ-SW
```

```
DMZ-SW(config)#VLAN 40
```

```
DMZ-SW(config-vlan)#name SRV1
```

```
DMZ-SW(config-vlan)#exit
```

```
DMZ-SW(config-vlan)#VLAN 50
```

```
DMZ-SW(config-vlan)#name SRV2
```

```
DMZ-SW(config)#interface ethernet 0/1
```

```
DMZ-SW(config-if)#switchport access vlan 40
```

```
DMZ-SW(config-if)#description Connected to SRV1
```

```
DMZ-SW(config-if)# exit
```

```
DMZ-SW(config)#interface ethernet 0/2
```

```
DMZ-SW(config-if)#switchport access vlan 50
```

```
DMZ-SW(config-if)#description Connected to SRV2
```

```
DMZ-SW(config-if)# exit
```

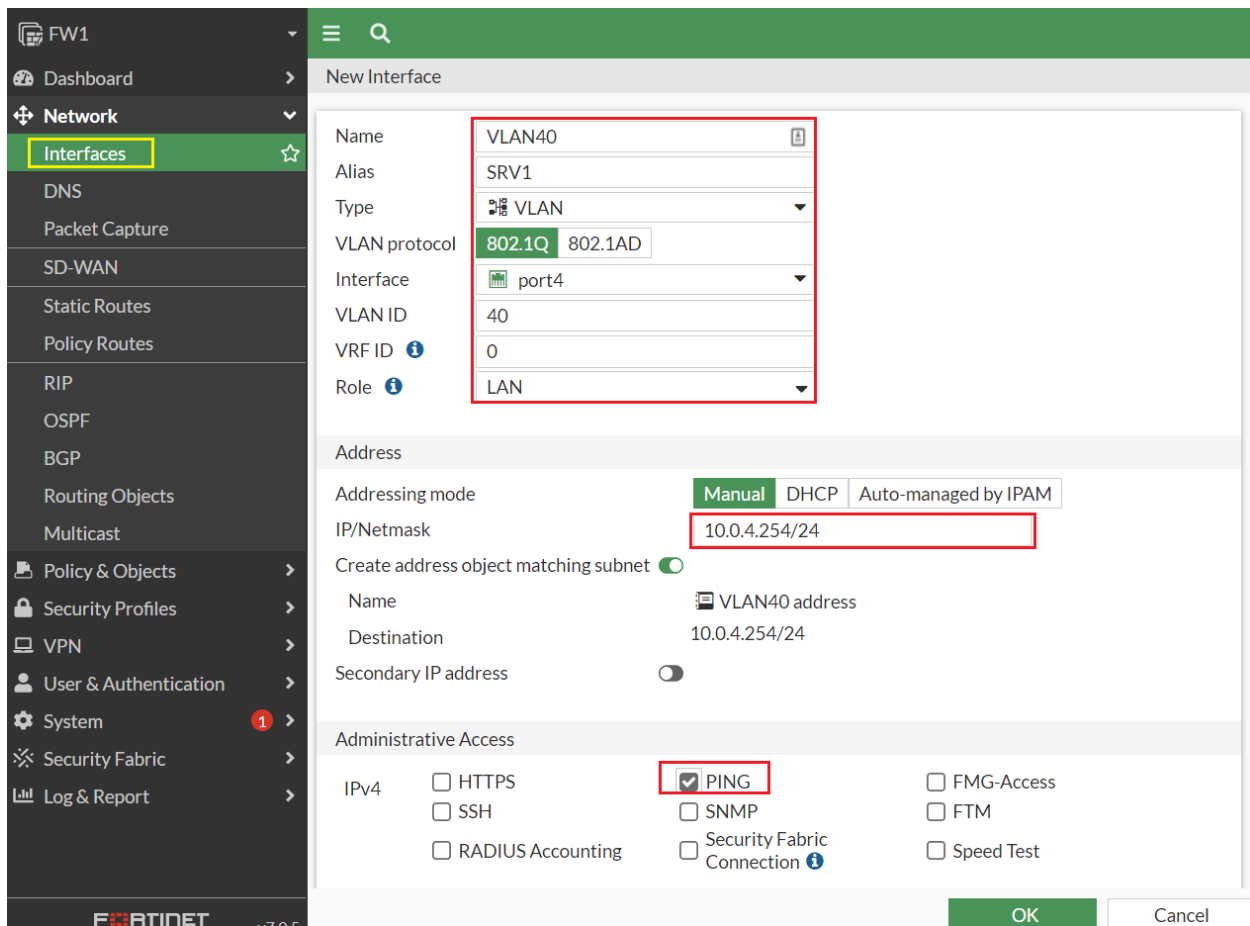
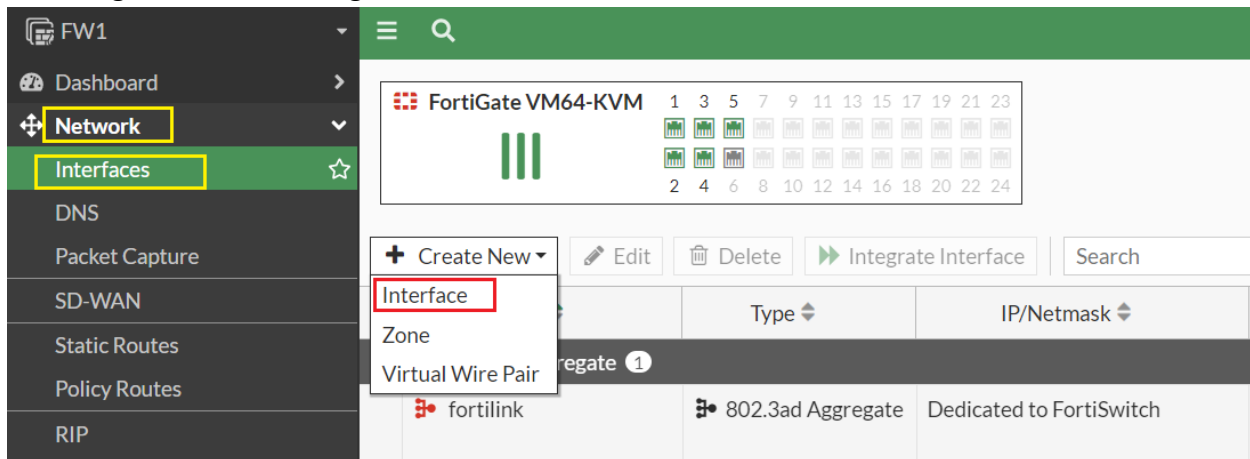
```
DMZ-SW(config)#interface ethernet 0/0
```

```
DMZ-SW(config-if)#switchport trunk encapsulation dot1q
```

```
DMZ-SW(config-if)#switchport mode trunk
```

```
DMZ-SW(config-if)#description TRUNK Interface connected to FW
```

To configure an interface, go to **Network > Interfaces** Click **Create New > Interface**.



Configure other interface, go to **Network > Interfaces** Click **Create New > Interface**.

New Interface

Name: VLAN50
 Alias: SRV2
 Type: VLAN
 VLAN protocol: 802.1Q 802.1AD
 Interface: port4
 VLAN ID: 50
 VRF ID: 0
 Role: LAN

Address

Addressing mode: Manual DHCP Auto-managed by IPAM
 IP/Netmask: 10.0.5.254/24
 Create address object matching subnet: ☒
 Name: VLAN50 address
 Destination: 10.0.5.254/24
 Secondary IP address: ☐

Administrative Access

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

OK Cancel

Finally, two created interfaces display below under port 4 VLAN40 and VLAN50.

+ Create New Edit Delete Integrate Interface <input type="text" value="Search"/>				
	Name	Type	IP/Netmask	Administrative Access
802.3ad Aggregate 1				
	fortilink	802.3ad Aggregate	Dedicated to FortiSwitch	PING Security Fabric Connection
Physical Interface 8				
	DMZ (port4)	Physical Interface	0.0.0.0/0.0.0.0	PING
	SRV1 (VLAN40)	VLAN	10.0.4.254/255.255.255.0	PING
	SRV2 (VLAN50)	VLAN	10.0.5.254/255.255.255.0	PING

Go to **Network > DNS** Set DNS Servers to **Specify**, Configure the primary and secondary DNS servers as needed. Configure additional DNS settings as needed Click Apply.

DNS Settings

DNS servers: Use FortiGuard Servers **Specify**

Primary DNS server: 8.8.8.8 90 ms

Secondary DNS server: 8.8.4.4 70 ms

Local domain name:

DNS Protocols

DNS (UDP/53) ☒

TLS (TCP/853) ☐

HTTPS (TCP/443) ☐

Create a new default route, go to **Network > Static Routes**.

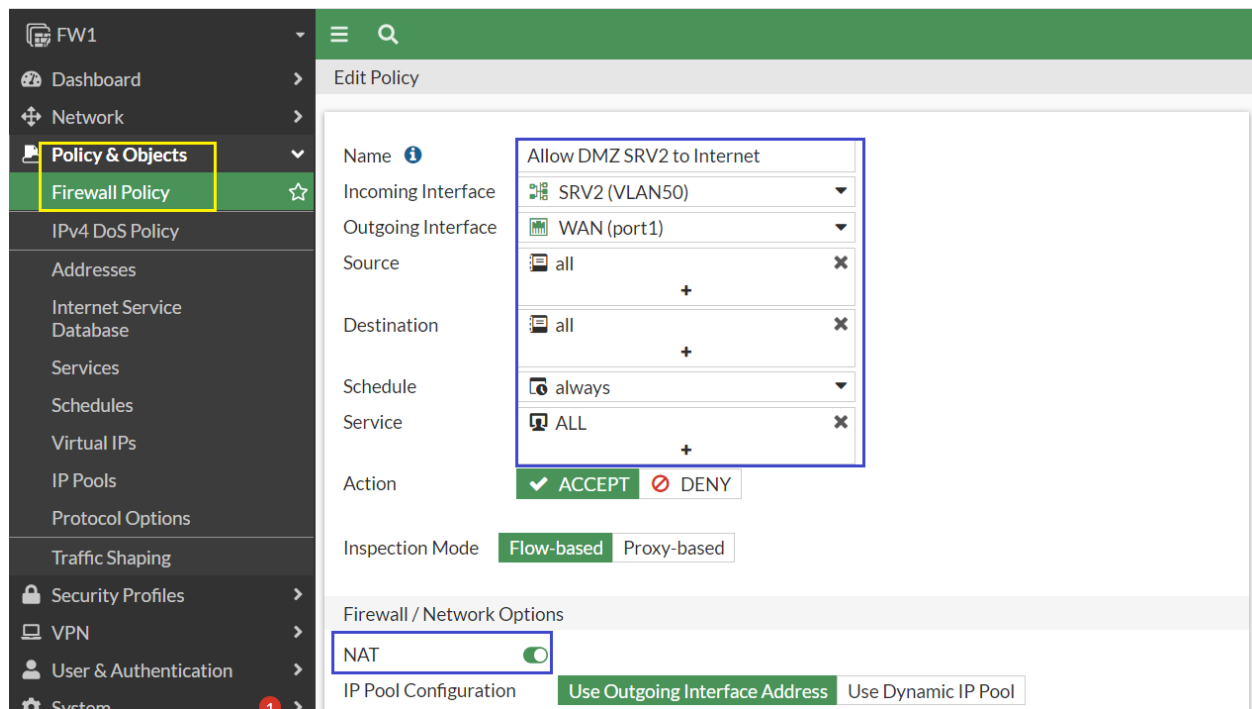
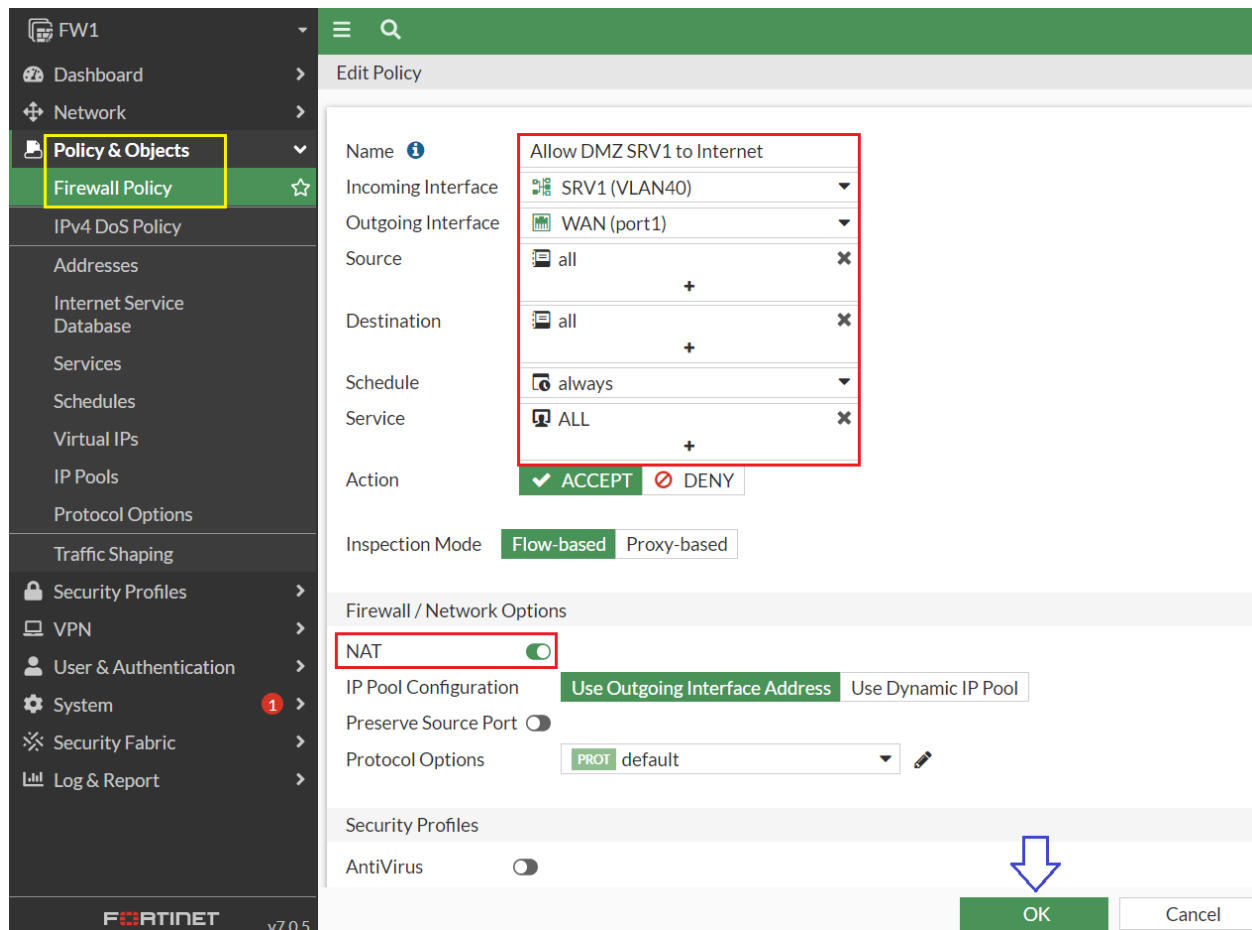
Static Routes

Destination	Gateway IP	Interface
0.0.0.0/0	192.168.1.254	WAN (port1)

Create a firewall policy, go to **Policy & Objects > Firewall Policy**, and click **Create New**.

Firewall Policy

Name	Source	Destination	Schedule	Service
DMZ (port4) → WAN (port1) 1				
Allow DMZ to Internet	all	all	always	ALL
LAN (port3) → WAN (port1) 1				
Allow Internet Access for LAN	all	all	always	ALL
Implicit 1				

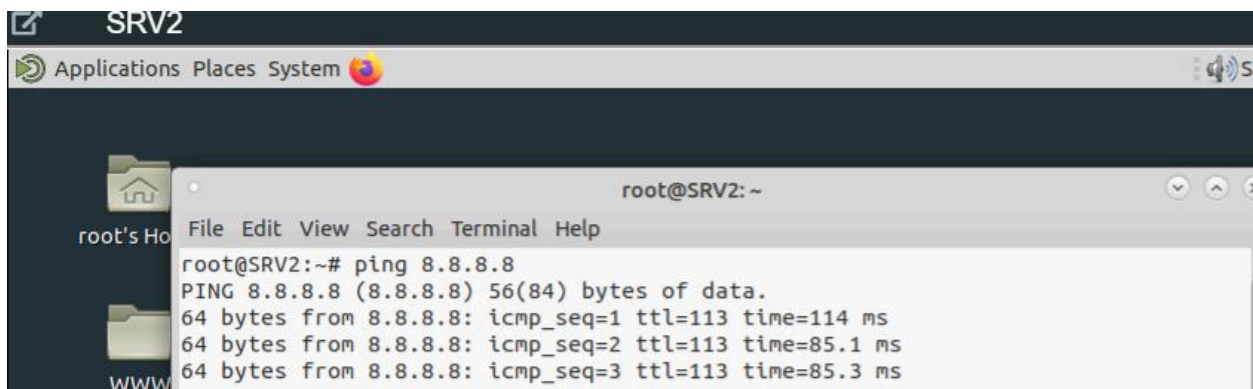
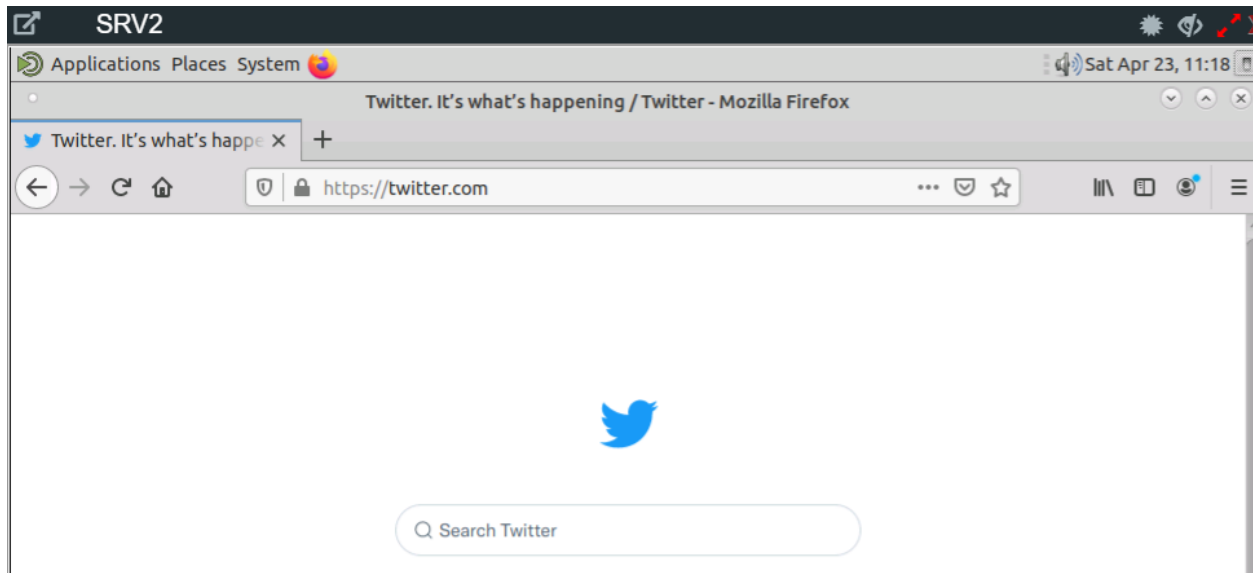


Test and Verification:

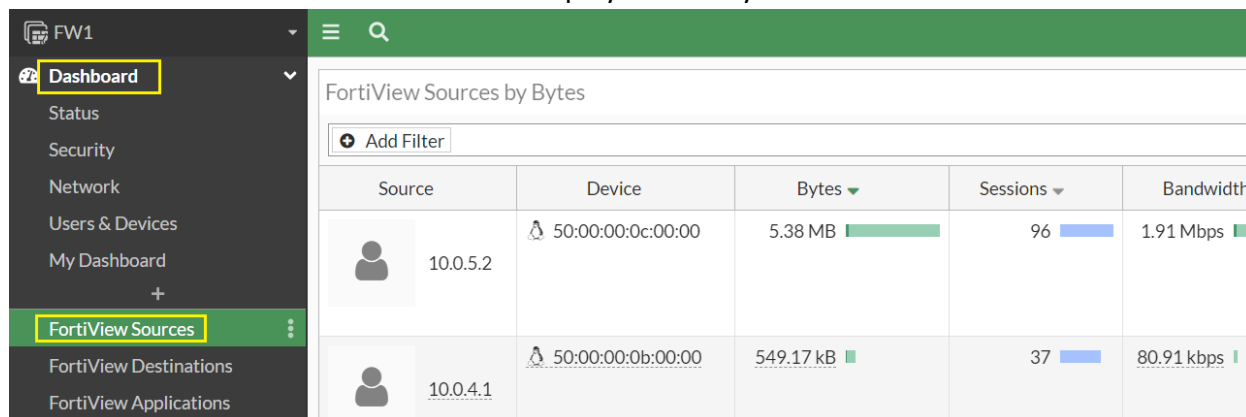
Try to access any website from SRV1 in this case facebook.com it's working.



Now, try to access any website from SRV2 in this case twitter.com it's working.

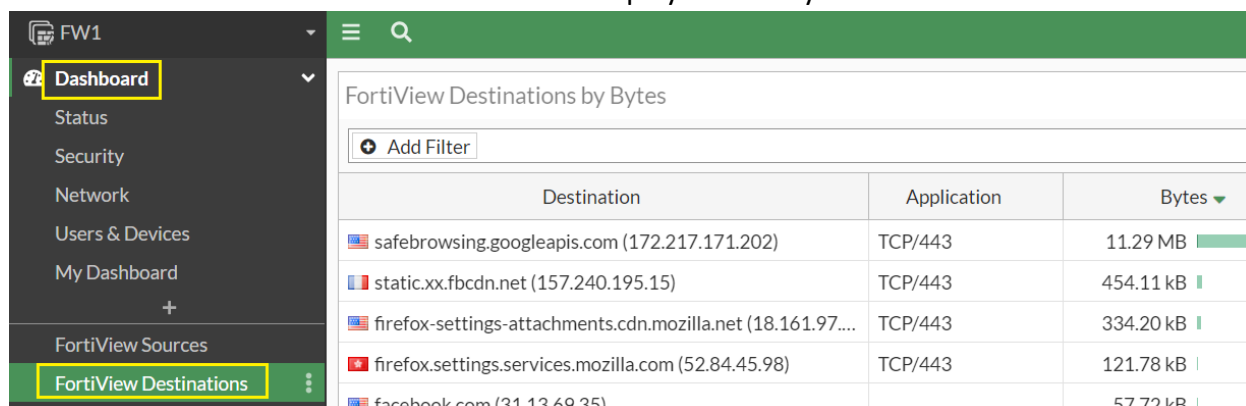


Go to **Dashboard > FortiView Sources** to display and verify VLAN40 & VLAN50 source IP.



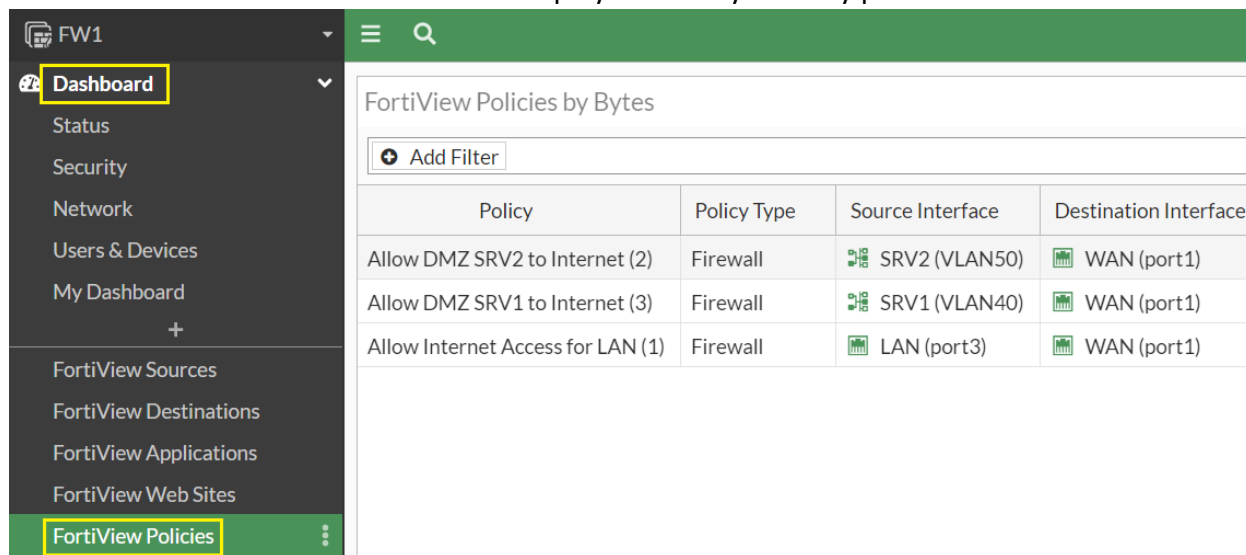
Source	Device	Bytes	Sessions	Bandwidth
10.0.5.2	50:00:00:0c:00:00	5.38 MB	96	1.91 Mbps
10.0.4.1	50:00:00:0b:00:00	549.17 kB	37	80.91 kbps

Go to **Dashboard > FortiView Destinations** to display and verify the destinations domains & IP.



Destination	Application	Bytes
safebrowsing.googleapis.com (172.217.171.202)	TCP/443	11.29 MB
static.xx.fbcdn.net (157.240.195.15)	TCP/443	454.11 kB
firefox-settings-attachments.cdn.mozilla.net (18.161.97...)	TCP/443	334.20 kB
firefox.settings.services.mozilla.com (52.84.45.98)	TCP/443	121.78 kB
facebook.com (31.13.69.35)		57.72 kB

Go to **Dashboard > FortiView Policies** to display and verify security policies has been hits & used.



Policy	Policy Type	Source Interface	Destination Interface
Allow DMZ SRV2 to Internet (2)	Firewall	SRV2 (VLAN50)	WAN (port1)
Allow DMZ SRV1 to Internet (3)	Firewall	SRV1 (VLAN40)	WAN (port1)
Allow Internet Access for LAN (1)	Firewall	LAN (port3)	WAN (port1)

Go to **Dashboard > FortiView Sessions** to display and verify all VLANs visited links sessions.

FortiView Sessions

+ Add Filter

Source	Device	Destination	Application	Protocol	Source Port
10.0.4.1	50:00:00:0b:00:00	44.241.107.50	TCP/443	TCP	59336
10.0.1.1	USER-PC	8.8.8.8	UDP/53	UDP	49710
10.0.5.2	50:00:00:0c:00:00	35.82.112.36	TCP/443	TCP	57532

Go to **Log & Report > Forward Traffic** to display and verify all VLANs visited links sessions.

Forward Traffic

+ Add Filter

Date/Time	Source	Device	Destination
18 seconds ago	10.0.5.2	50:00:00:0c:00:00	35.82.112.36 (push.services.mozilla.com)
39 seconds ago	10.0.4.1	50:00:00:0b:00:00	44.241.107.50 (push.services.mozilla.com)
Minute ago	10.0.4.1	50:00:00:0b:00:00	8.8.8.8 (dns.google)
Minute ago	10.0.4.1	50:00:00:0b:00:00	31.13.69.35 (facebook.com)
Minute ago	10.0.5.2	50:00:00:0c:00:00	8.8.8.8 (dns.google)
Minute ago	10.0.5.2	50:00:00:0c:00:00	8.8.8.8 (dns.google)
Minute ago	10.0.5.2	50:00:00:0c:00:00	8.8.8.8 (dns.google)
Minute ago	10.0.5.2	50:00:00:0c:00:00	8.8.8.8 (dns.google)