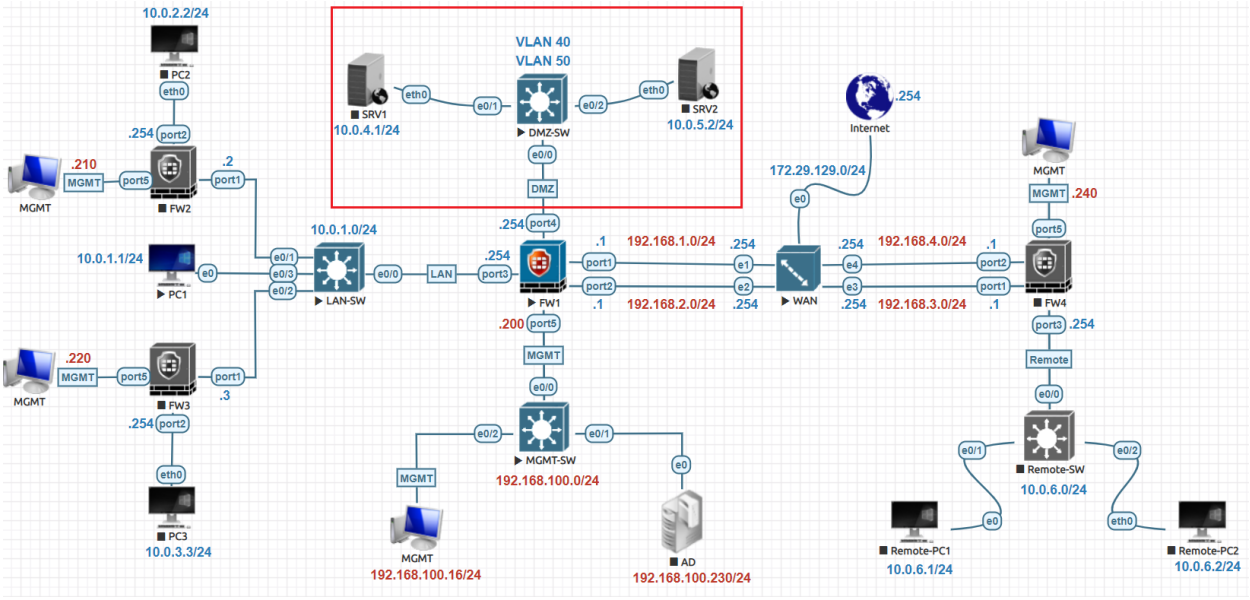
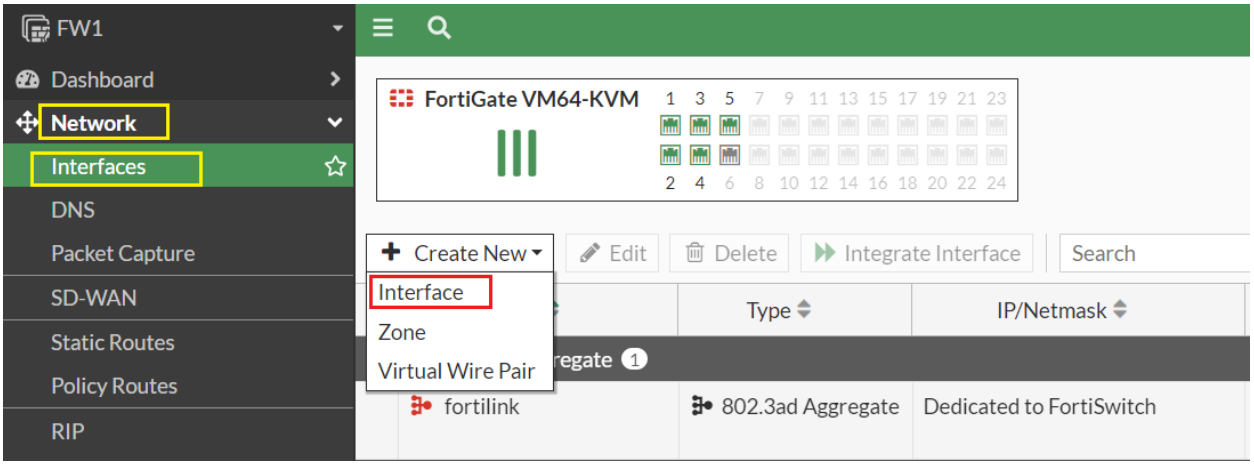
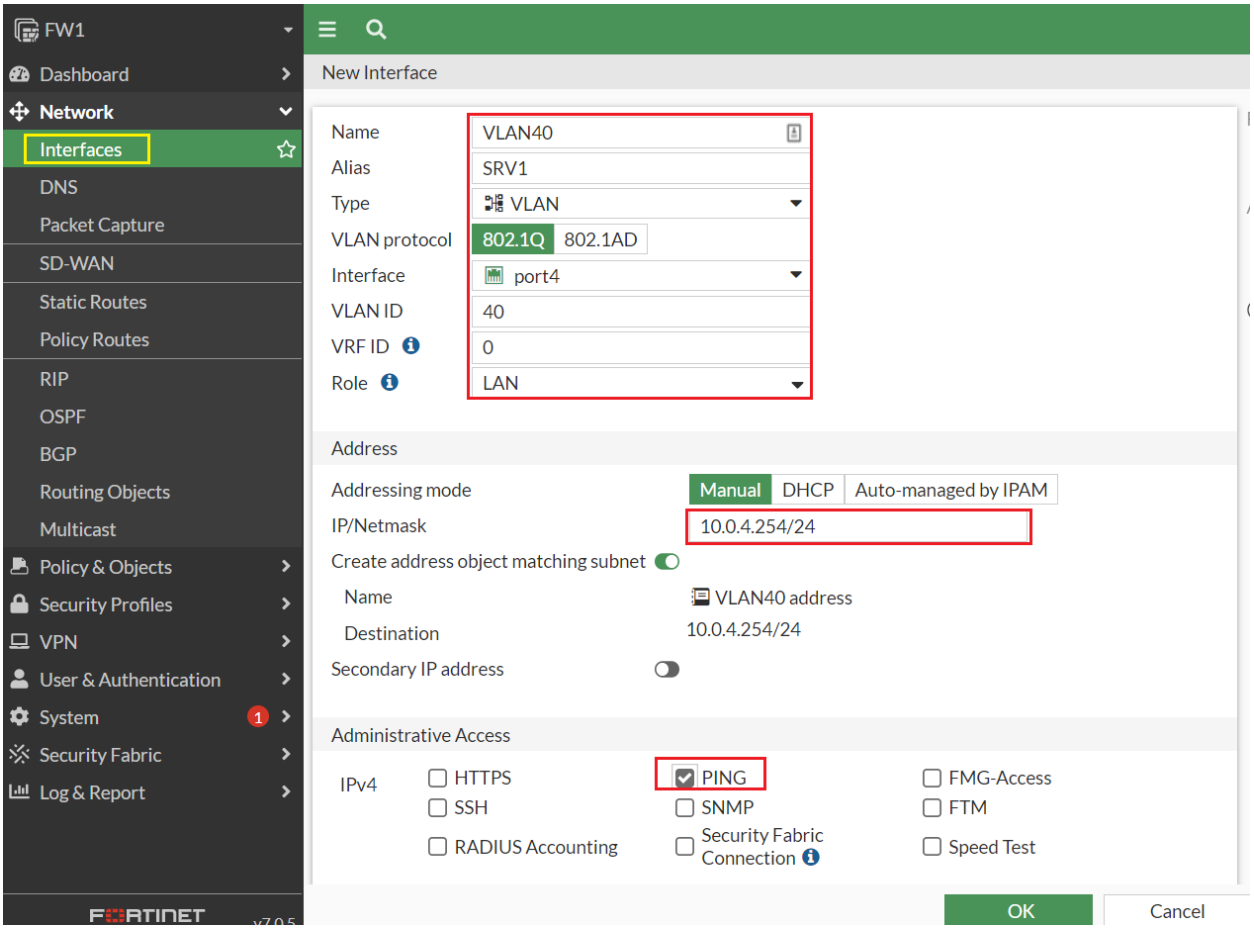
VLAN LAB:



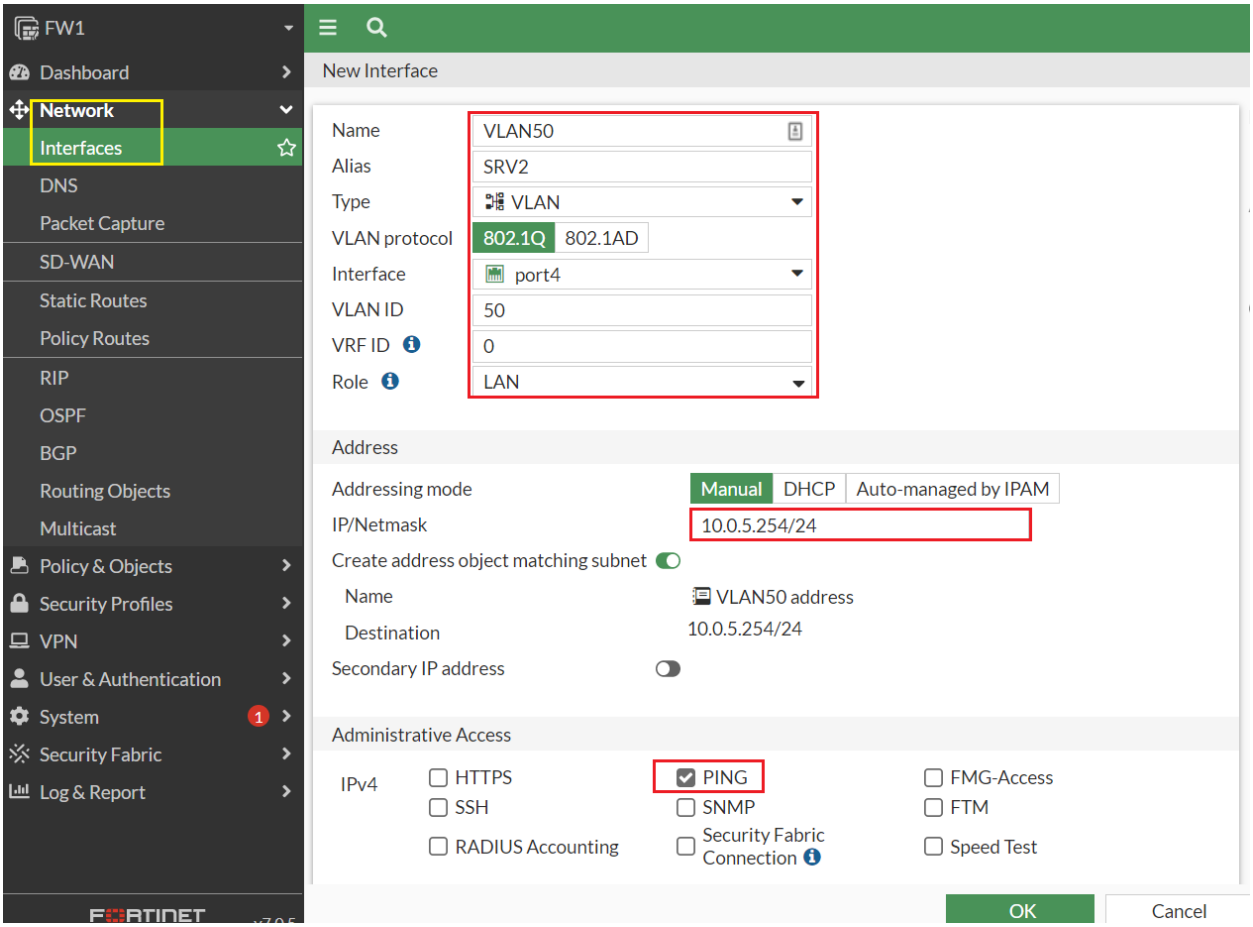
Cisco Switch Configuration
Switch(config)#hostname DMZ-SW DMZ-SW(config)#VLAN 40 DMZ-SW(config-vlan)#name SRV1 DMZ-SW(config-vlan)#exit DMZ-SW(config-vlan)#VLAN 50 DMZ-SW(config-vlan)#name SRV2
DMZ-SW(config)#interface ethernet 0/1 DMZ-SW(config-if)#switchport access vlan 40 DMZ-SW(config-if)#description 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.

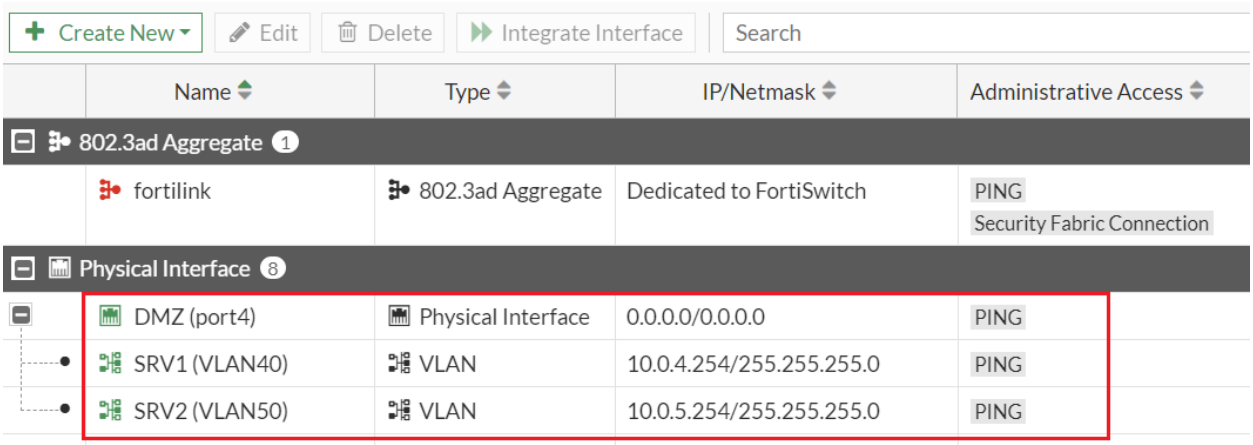




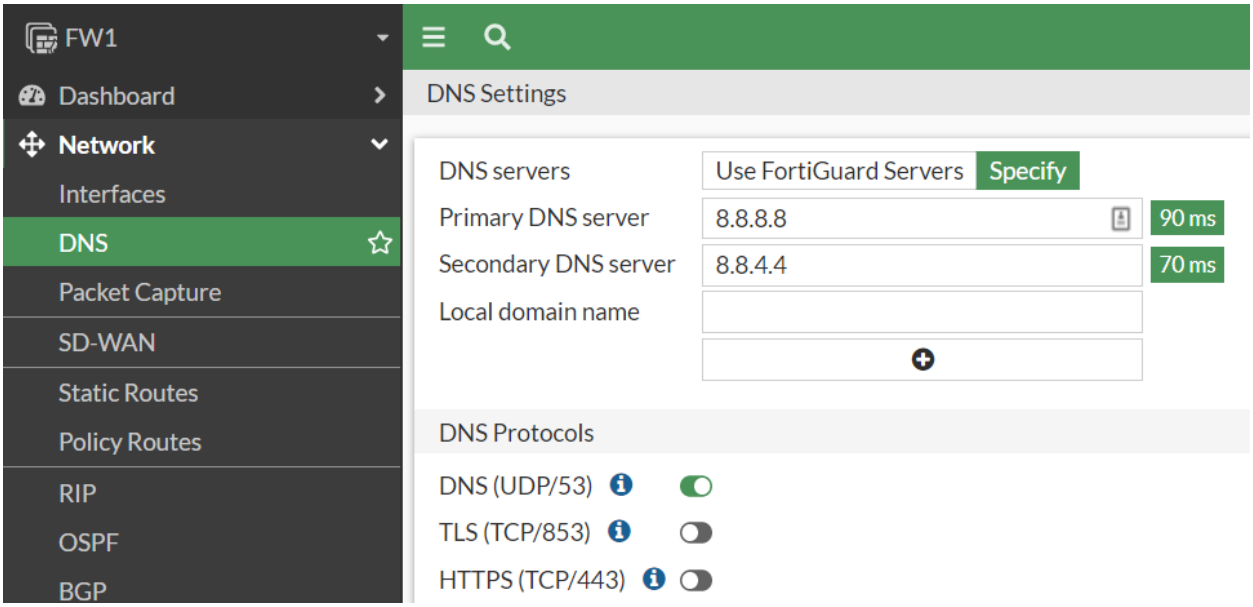
Configure other interface, go to Network > Interfaces Click Create New > Interface.



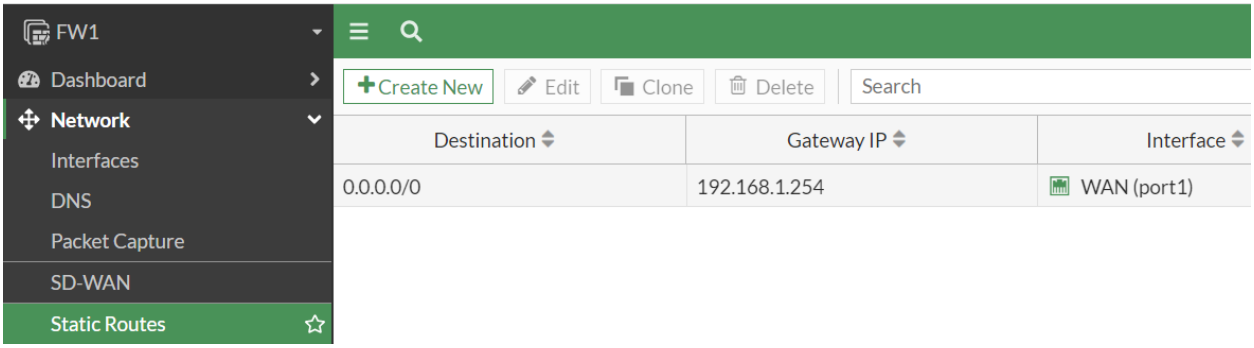
Finally, two created interfaces display below under port 4 VLAN40 and VLAN50.



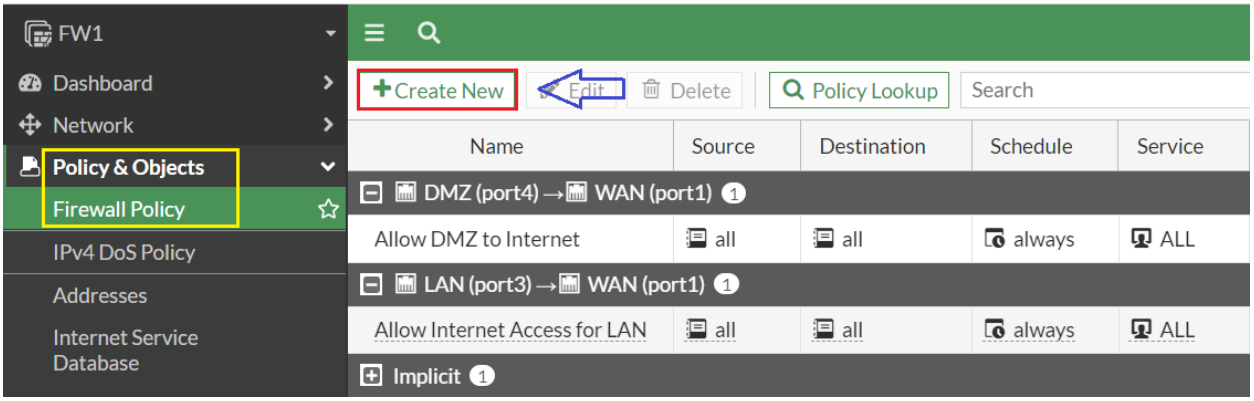
Go to Network > DNS Set DNS Servers to Specify, Configure the primary and secondary DNS servers as needed. Configure additional DNS settings as needed Click Apply.

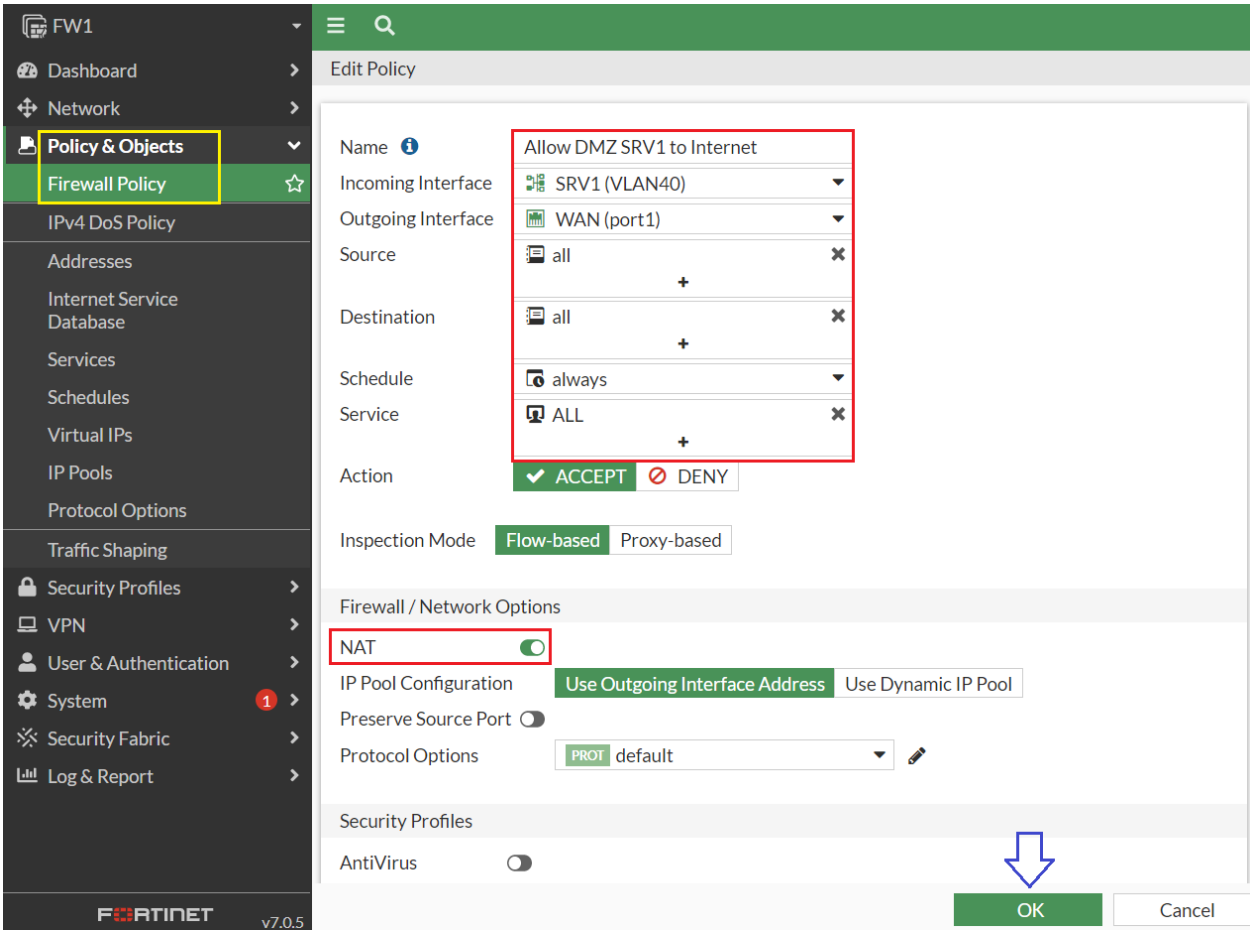


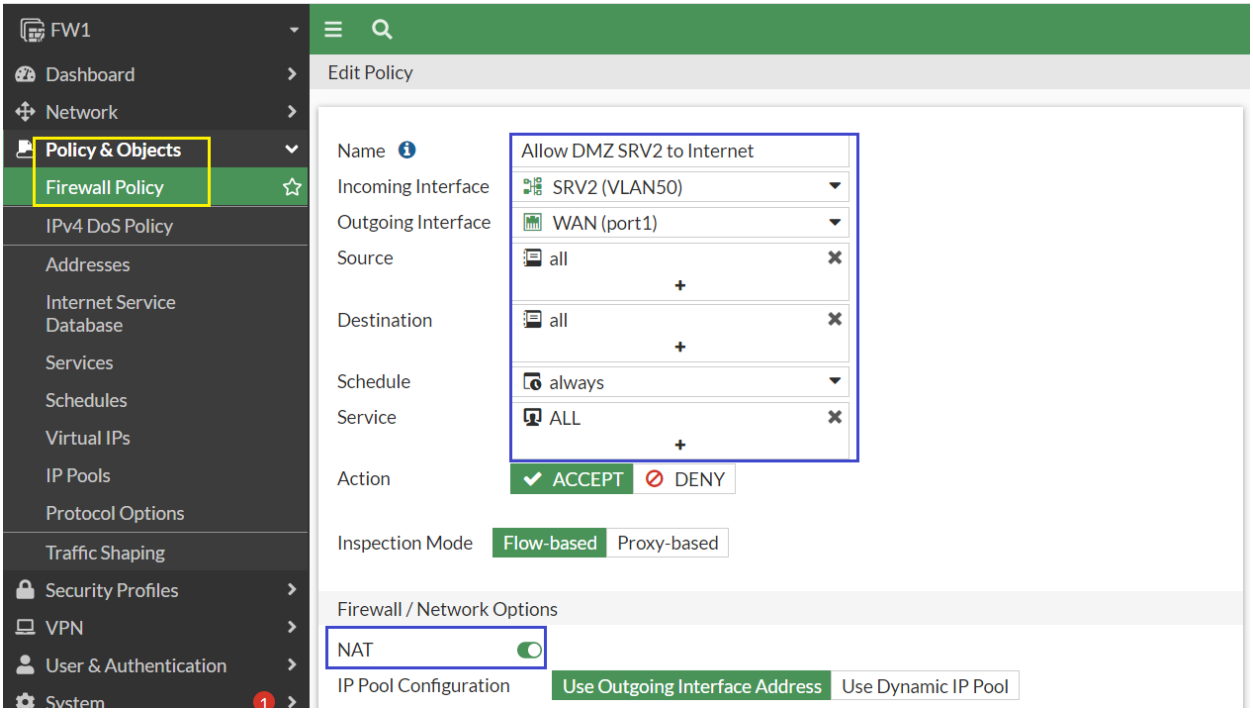
Create a new default route, go to Network > Static Routes.



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



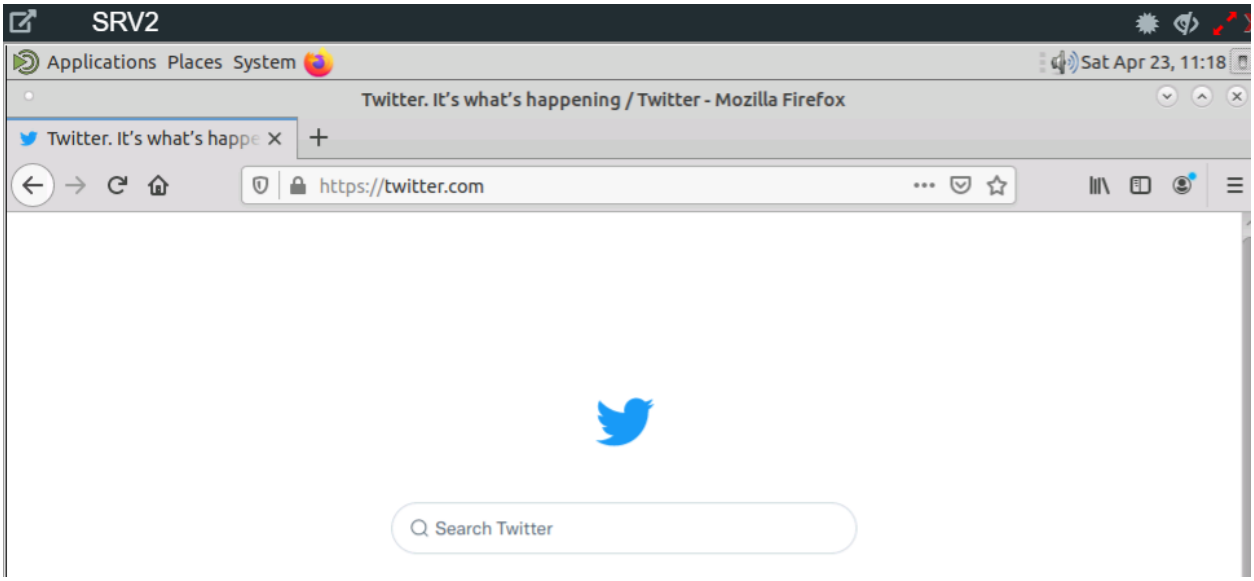

FW1
Dashboard
Network
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
System
Security Fabric
Log & Report
FORTINET
v7.0.5
Edit Policy
Name
Allow DMZ SRV1 to Internet
Incoming Interface
SRV1 (VLAN40)
Outgoing Interface
WAN (port1)
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
OK
Cancel

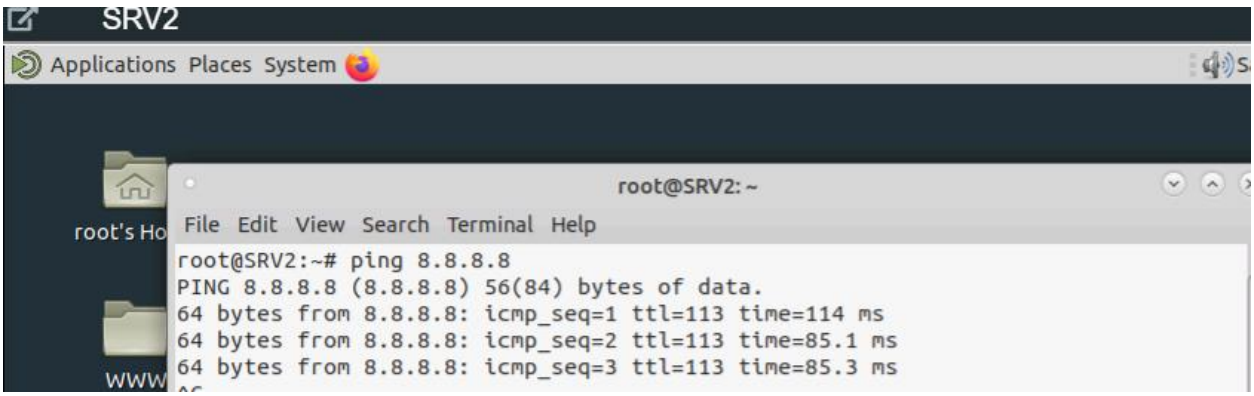

FW1
Dashboard
Network
Policy & Objects
Firewall Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
System
Edit Policy
Name
Allow DMZ SRV2 to Internet
Incoming Interface
SRV2 (VLAN50)
Outgoing Interface
WAN (port1)
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

Test and Verification:

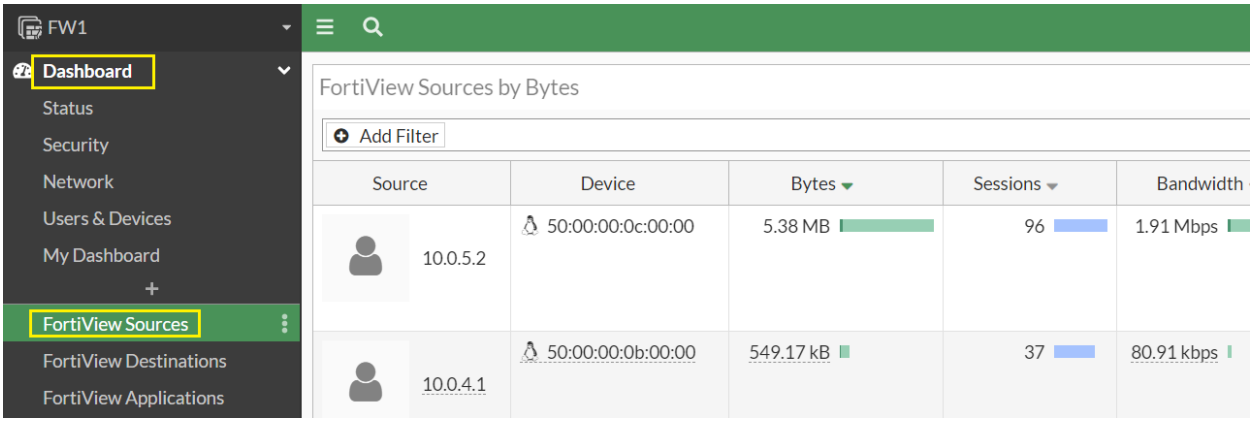
Try to access any website from SRV1 in this case facebook.com it's working.

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

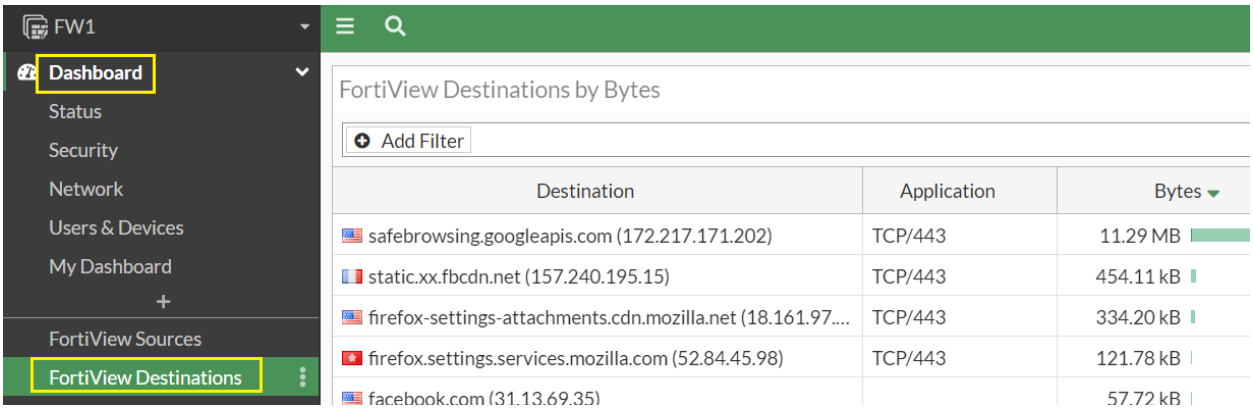




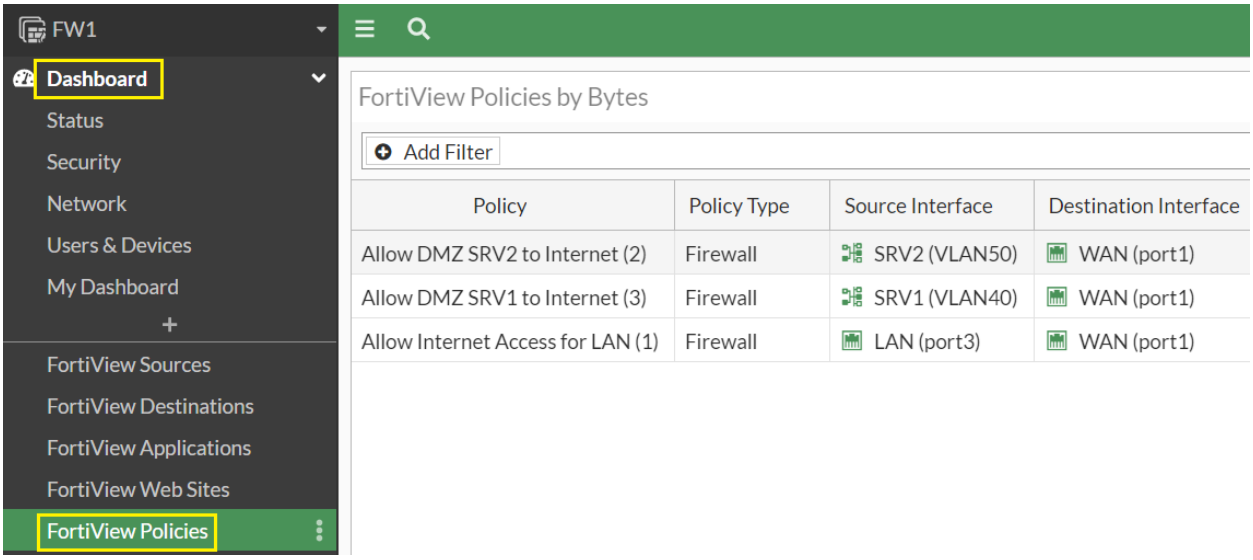
Go to Dashboard> FortiView Sources to display and verify VLAN40 & VLAN50 source IP.



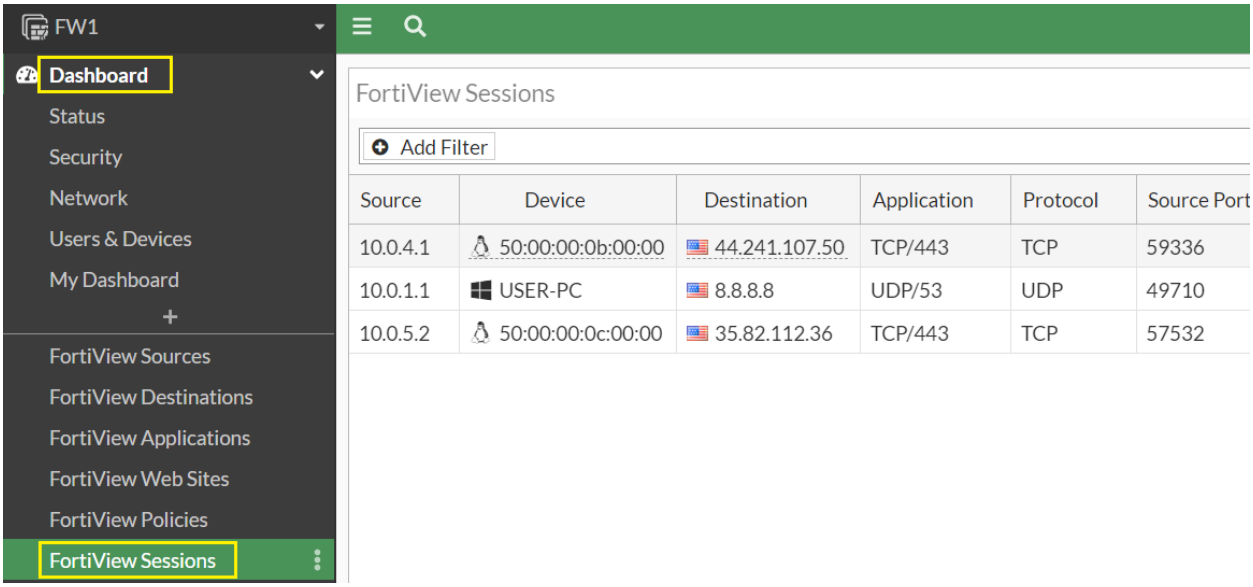
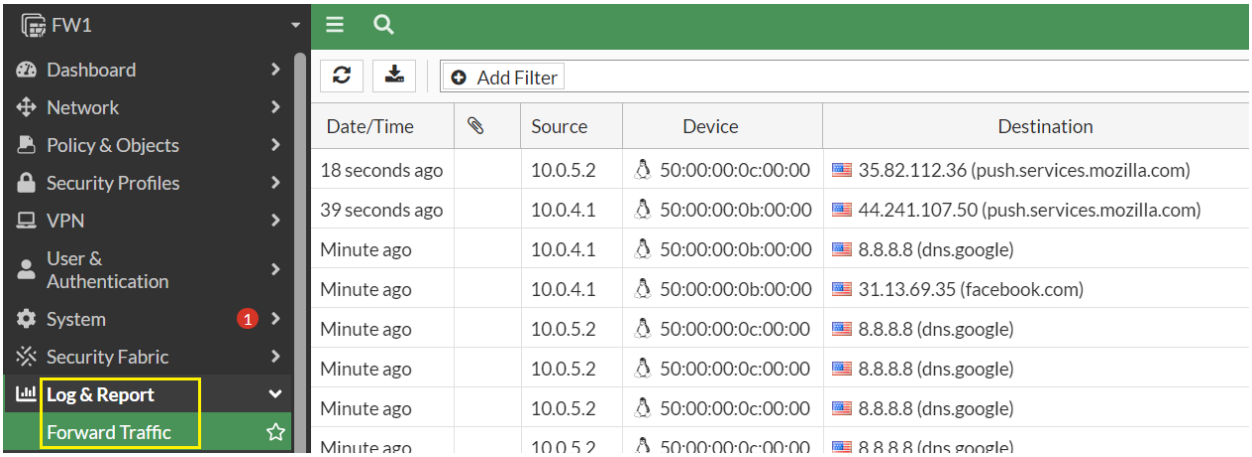
Go to Dashboard> FortiView Destinations to display and verify the destinations domains & IP.



Go to Dashboard> FortiView Polices to display and verify security polices has been hits & used.



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



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