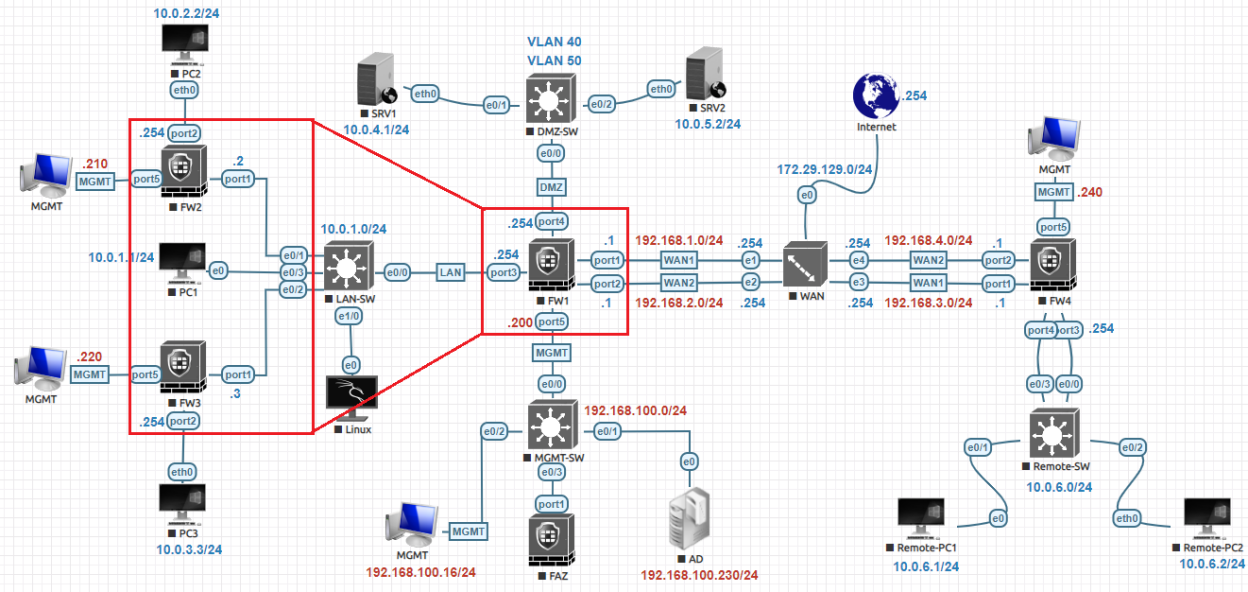
Static & Default Route Lab:



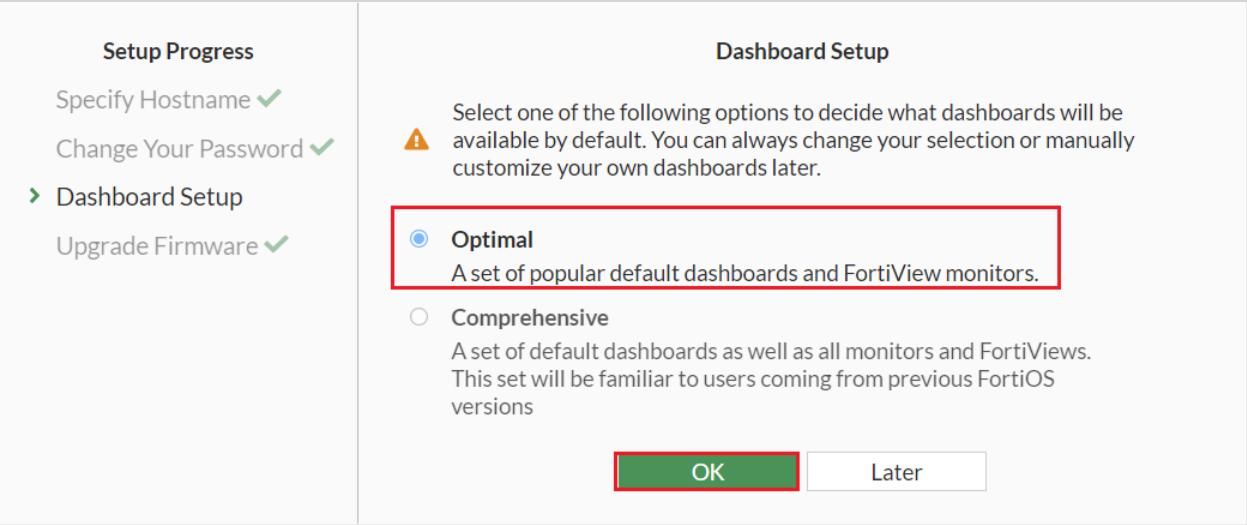
Change Hostname FW2
FortiGate-VM64-KVM # config system global FortiGate-VM64-KVM (global) # set hostname FW2 FortiGate-VM64-KVM (global) # end

Configure Management Interface FW2
FW2 # config system interface FW2 (interface) # edit port5 FW2 (port4) # set mode static FW2 (port4) # set ip 192.168.100.210/24 FW2 (port4) # set allowaccess https http ssh telnet ping FW2 (port4) # end

Change Hostname FW3
FortiGate-VM64-KVM # config system global FortiGate-VM64-KVM (global) # set hostname FW3 FortiGate-VM64-KVM (global) # end

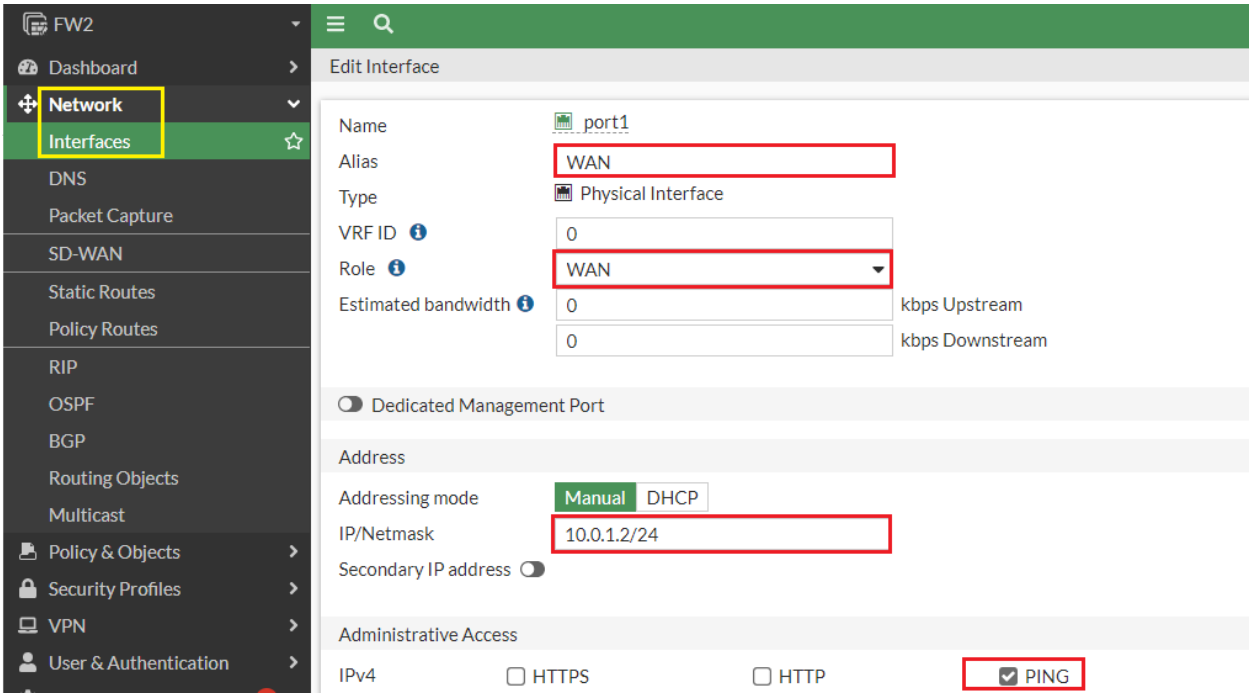
Configure Management Interface FW3
FW3 # config system interface FW3 (interface) # edit port5 FW3 (port4) # set mode static FW3 (port4) # set ip 192.168.100.220/24 FW3 (port4) # set allowaccess https http ssh telnet ping FW3 (port4) # end

Login to FortiGate Firewall type http://192.168.100.210 in any browser. Select Optimal and click OK to continue log in to Fortigate Firewall dashboard.

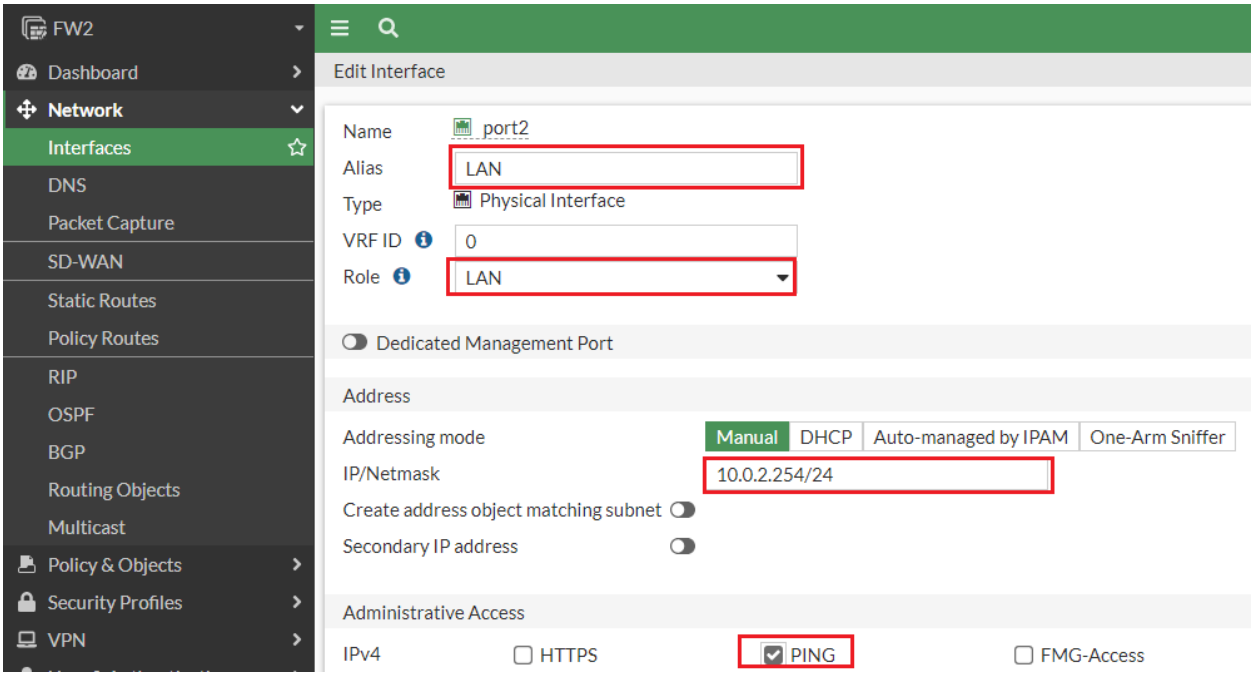


FW2 Configure Interfaces:

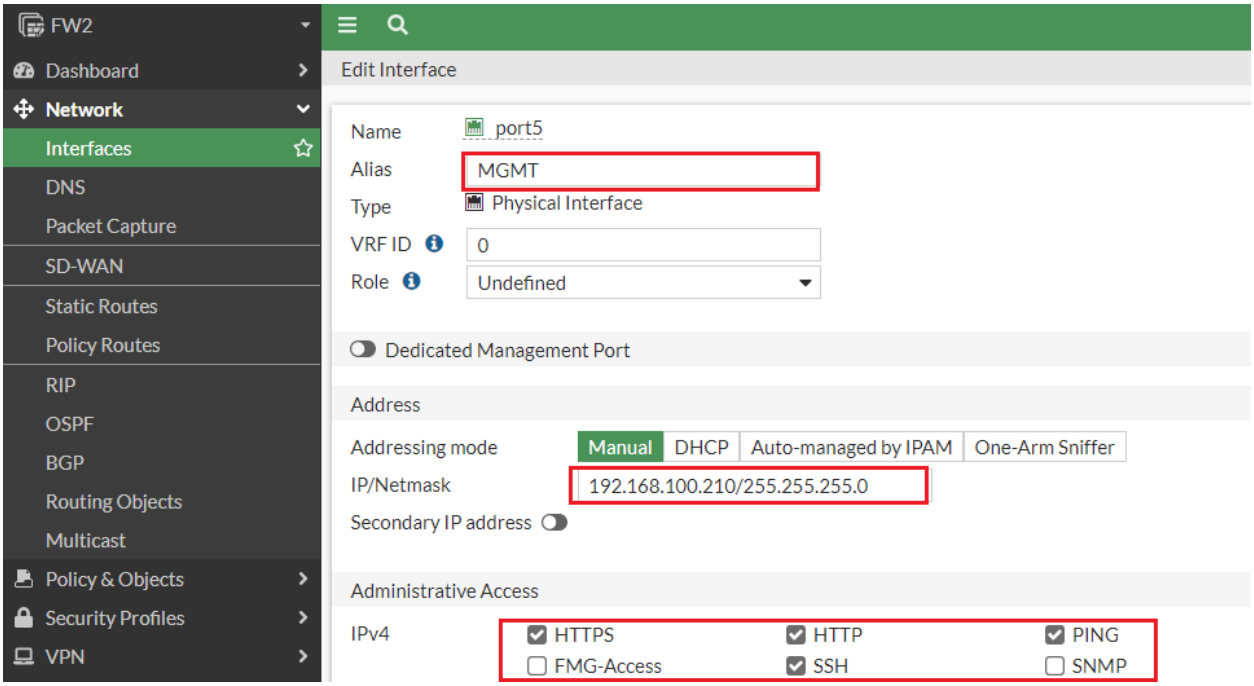
Go to Network>Interfaces select port1 Click Edit in Alias type WAN, change the Address Mode to Manual type IP/Netmask 10.0.1.2/24, in Administrative access uncheck everything only checked PING leave all the rest of configuration default and press OK button.



Go to Network>Interfaces select port2 Click Edit in Alias type LAN, change the Address Mode to Manual type IP/Netmask 10.0.2.254/24, in Administrative access only checked PING leave all the rest of configuration default & press OK.

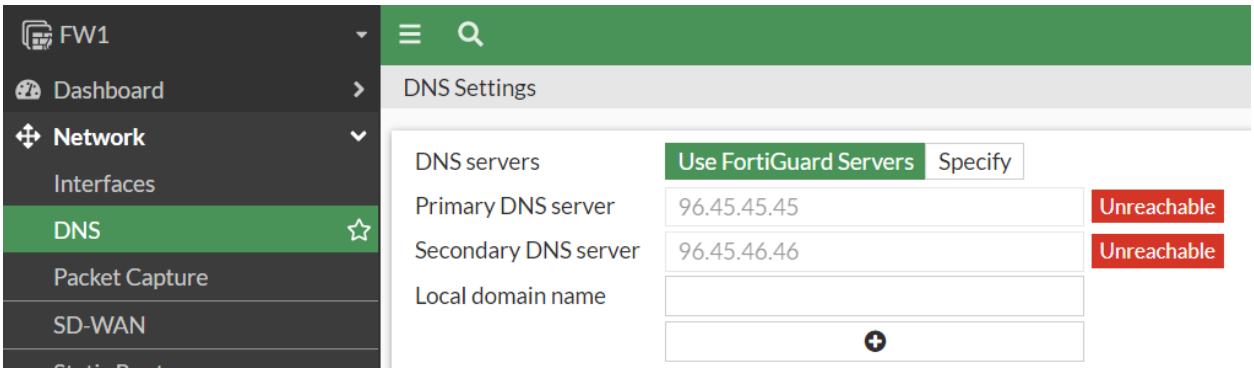


Go to Network>Interfaces select port5 Click Edit in Alias type MGMT, leave all the rest of configuration default and press OK button.

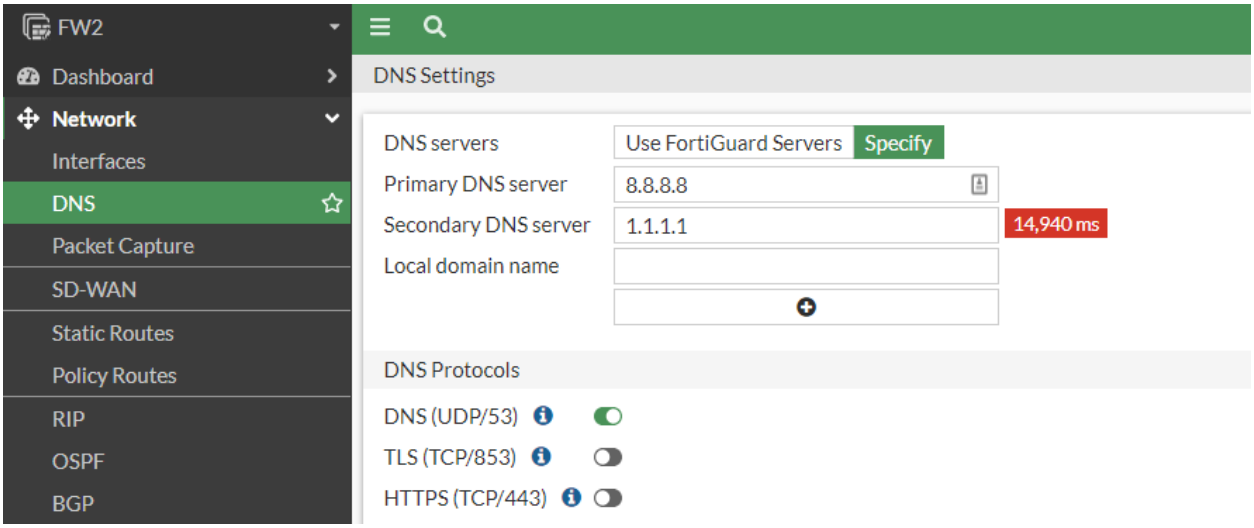


FW2 DNS Configuration:

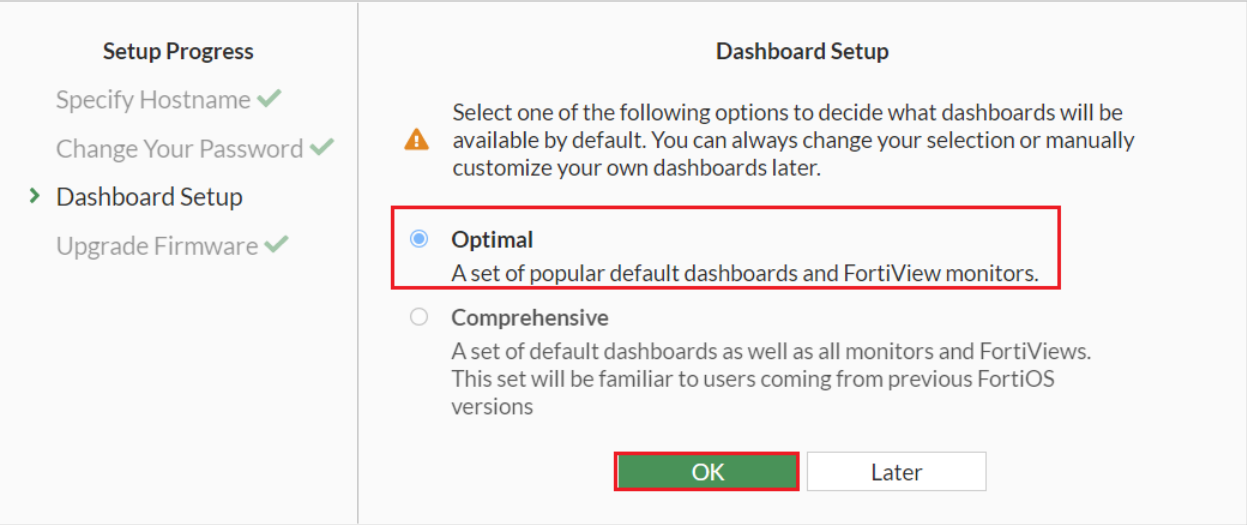
Go to Network > DNS by default, using Fortinet's FortiGuard severs are select.



It is possible to specify using different DNS server, click on Specify and enter in primary / secondary DNS servers. In Primary DNS Server, type the IP address of the primary DNS server 8.8.8.8. In Secondary DNS Server, type the IP address of the secondary DNS server 1.1.1.1. Click Apply button to save the changes.

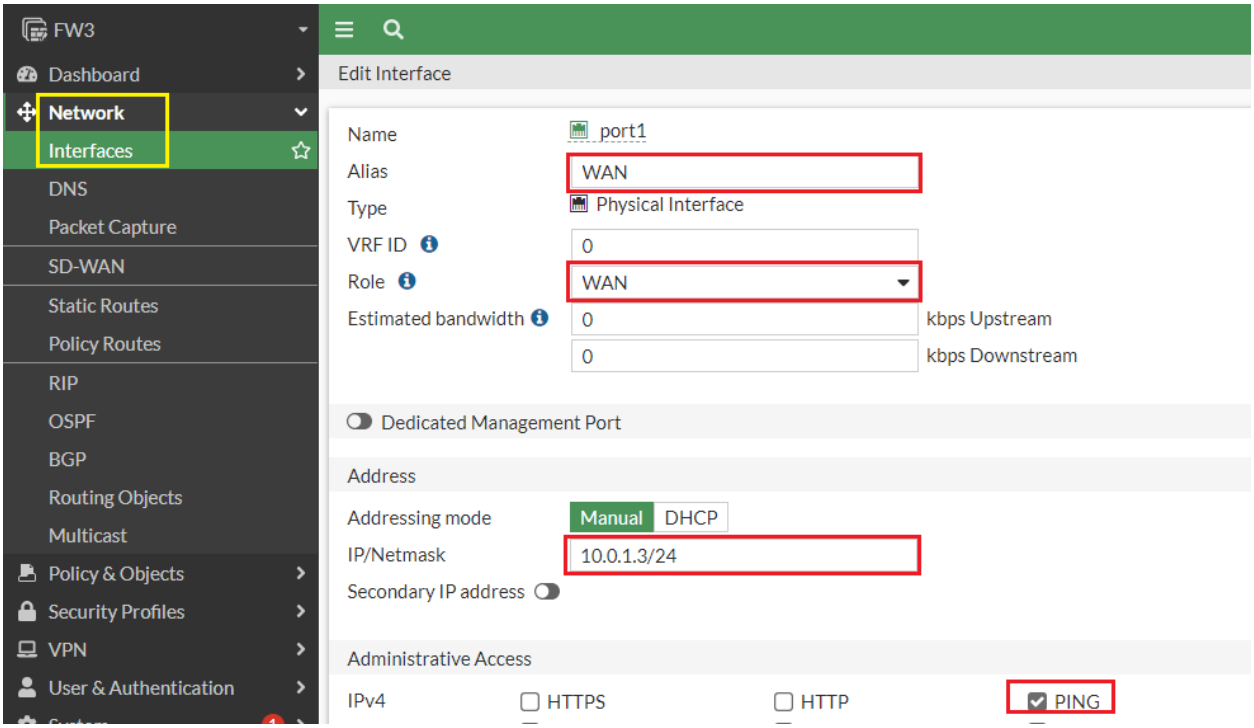


Login to FortiGate Firewall type http://192.168.100.220 in any browser. Select Optimal and click OK to continue log in to Fortigate Firewall dashboard.

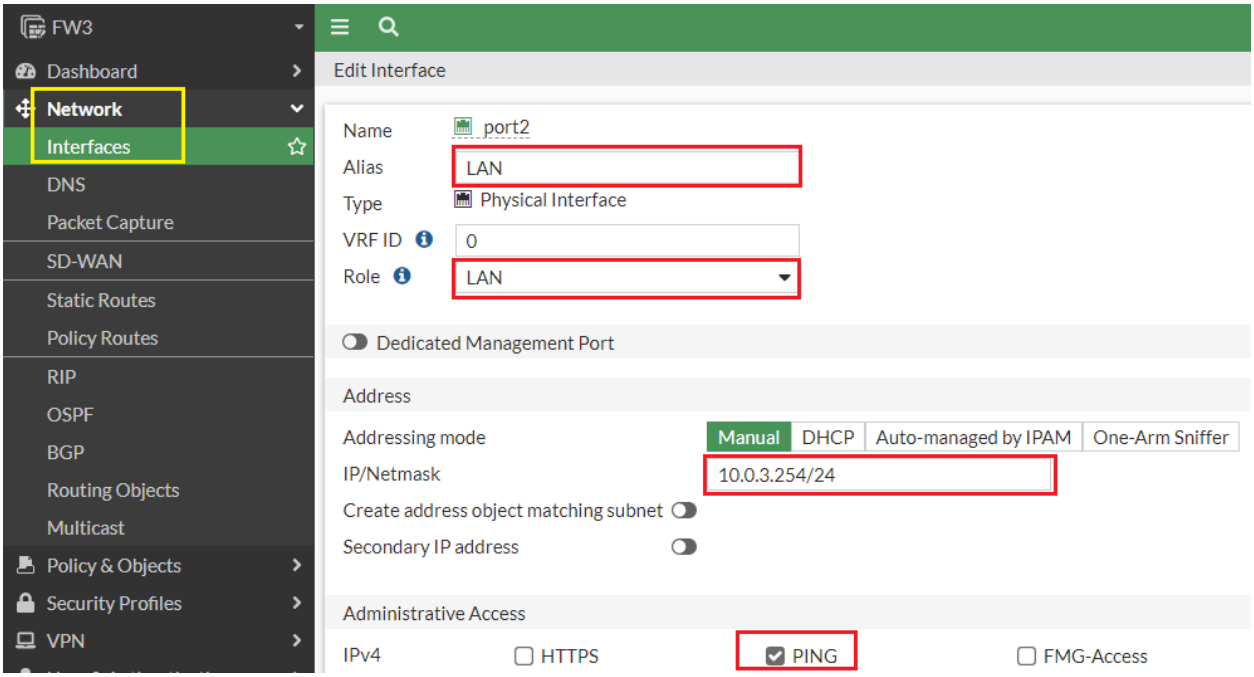


FW3 Configure Interfaces:

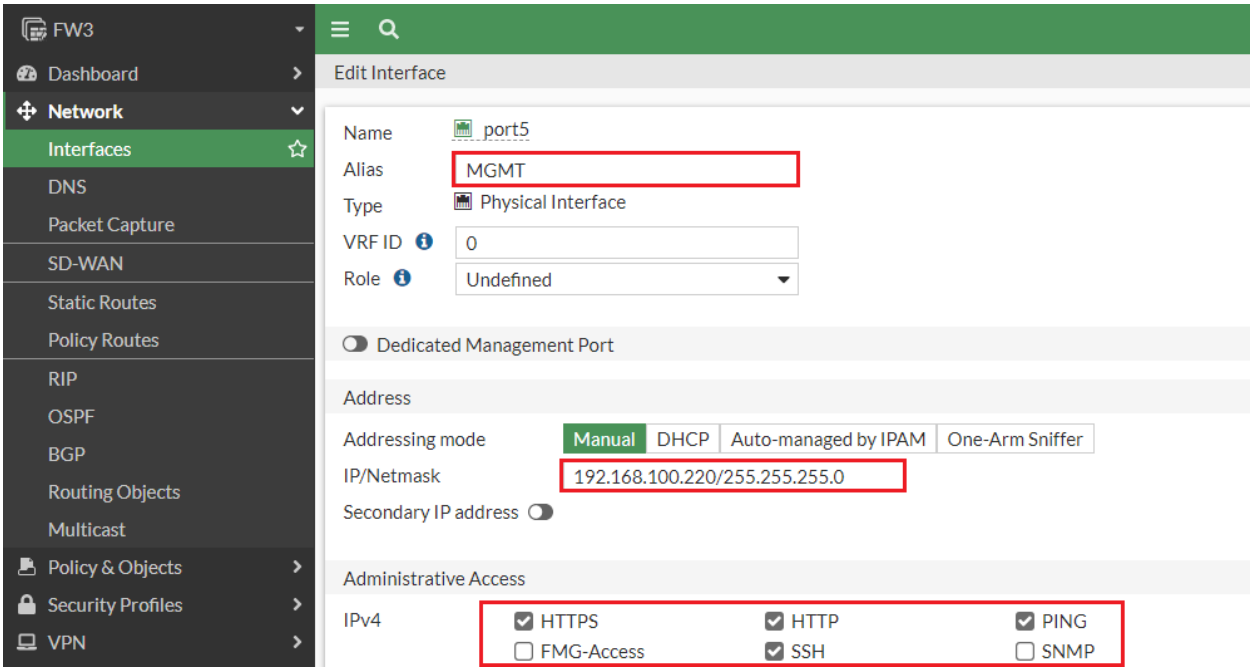
Go to Network>Interfaces select port1 Click Edit in Alias type WAN, change the Address Mode to Manual type IP/Netmask 10.0.1.3/24, in Administrative access uncheck everything only checked PING leave all the rest of configuration default and press OK button.



Go to Network>Interfaces select port2 Click Edit in Alias type LAN, change the Address Mode to Manual type IP/Netmask 10.0.3.254/24, in Administrative access only checked PING leave all the rest of configuration default & press OK.

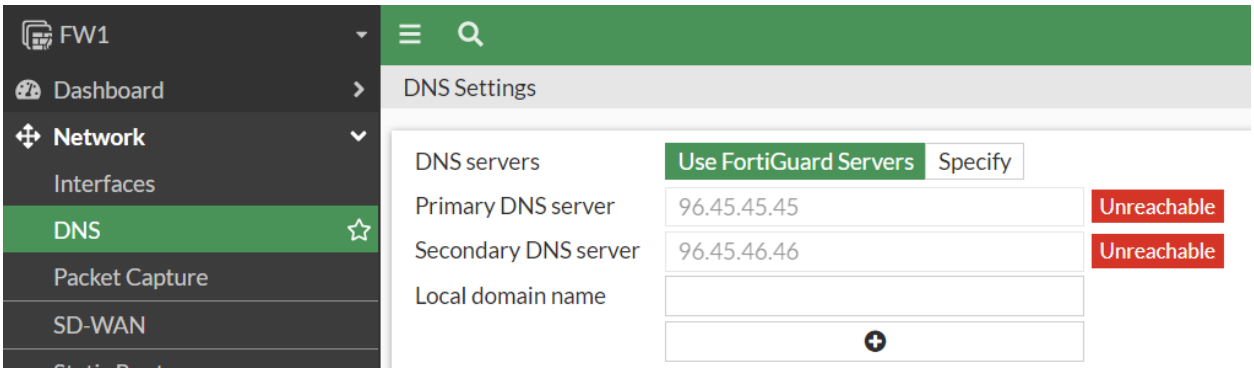


Go to Network>Interfaces select port5 Click Edit in Alias type MGMT, leave all the rest of configuration default and press OK button.

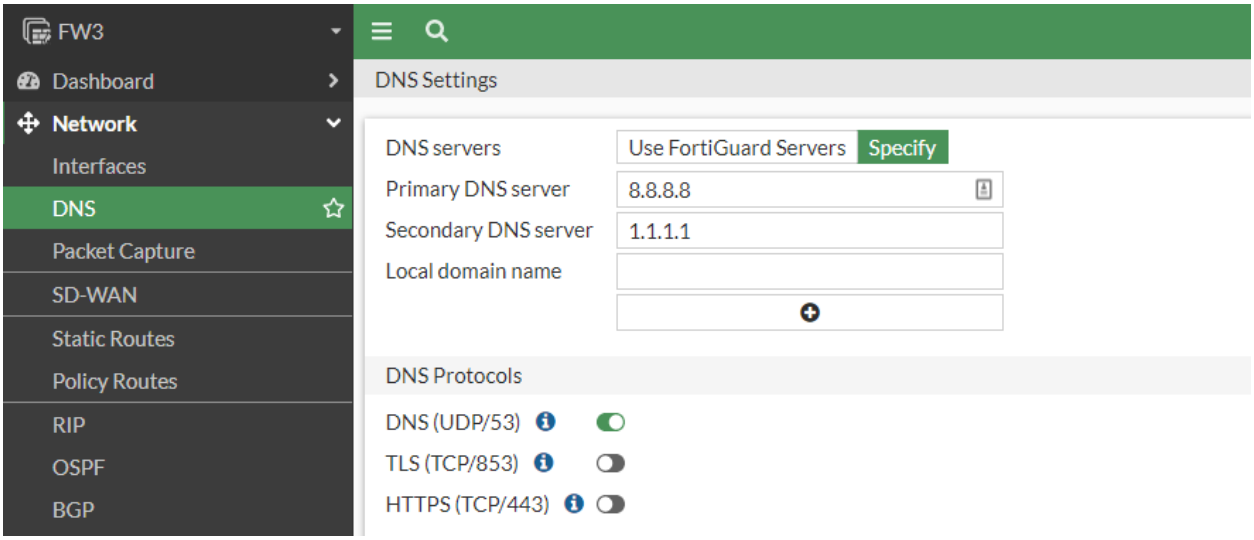


FW3 DNS Configuration:

Go to Network > DNS by default, using Fortinet's FortiGuard severs are select.

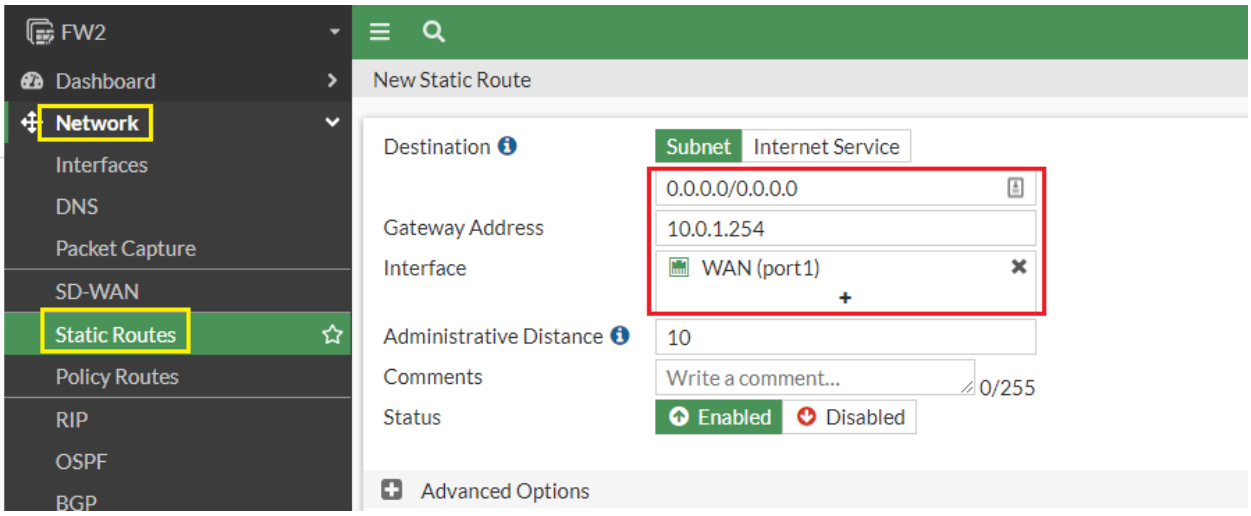


It is possible to specify using different DNS server, click on Specify and enter in primary / secondary DNS servers. In Primary DNS Server, type the IP address of the primary DNS server 8.8.8.8. In Secondary DNS Server, type the IP address of the secondary DNS server 1.1.1.1. Click Apply button to save the changes.



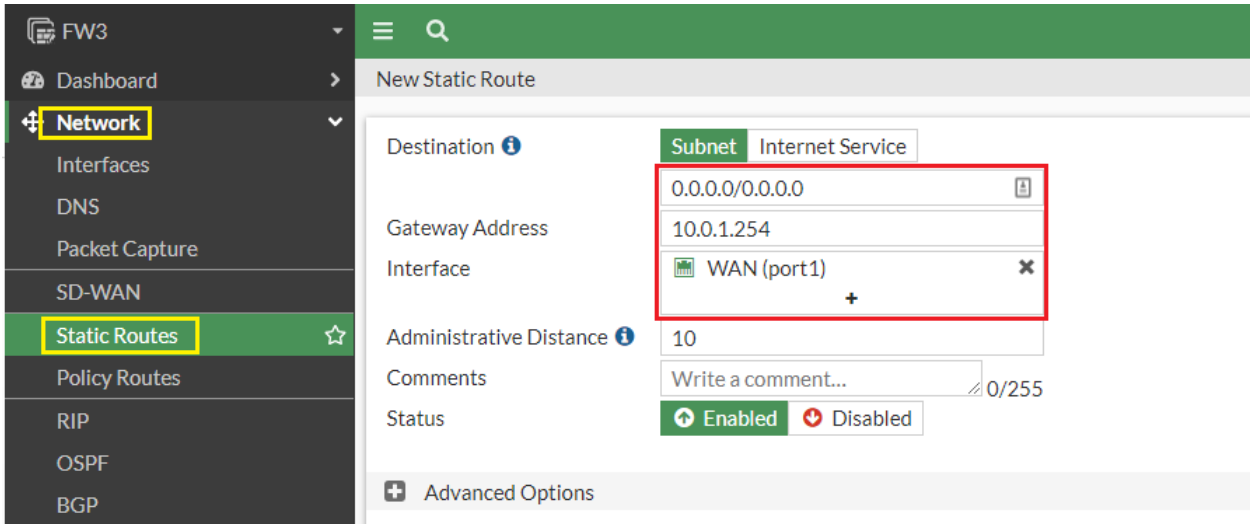
FW2 Default Route Configuration:

To create a new default route, go to Network > Static Routes and create a static route for ISP. Set Destination to Subnet and leave the destination IP address set to 0.0.0.0/0.0.0.0. Set Gateway to the IP address provided by your ISP and Interface to the Internet-facing interface in my case 10.0.1.254 which the Gateway. Set the Interface to the WAN interface. Press OK to Save the changes.



FW3 Default Route Configuration:

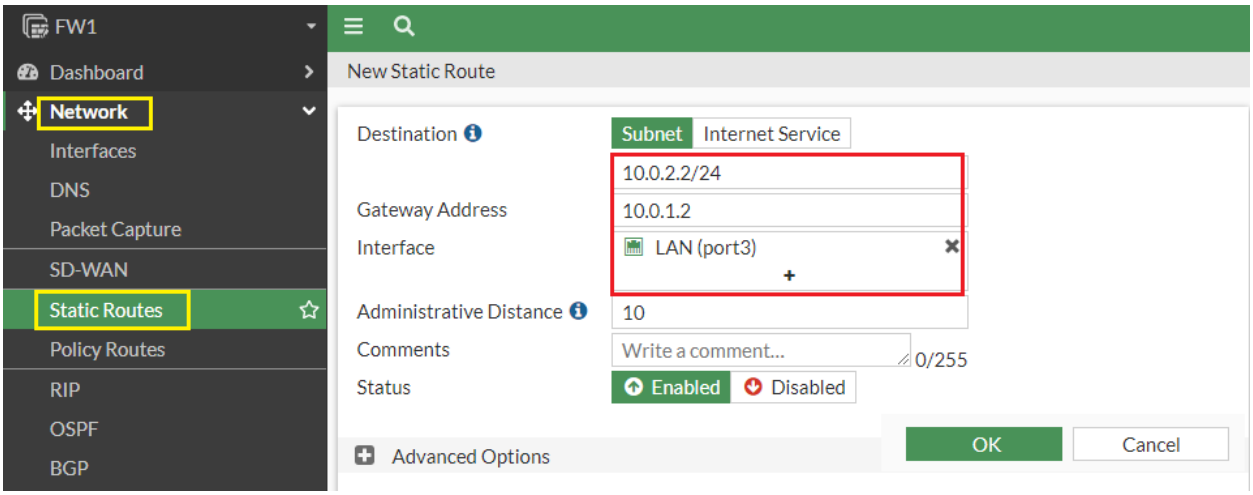
To create a new default route, go to Network > Static Routes and create a static route for ISP. Set Destination to Subnet and leave the destination IP address set to 0.0.0.0/0.0.0.0. Set Gateway to the IP address provided by your ISP and Interface to the Internet-facing interface in my case 10.0.1.254 which the Gateway. Set the Interface to the WAN interface. Press OK to Save the changes.



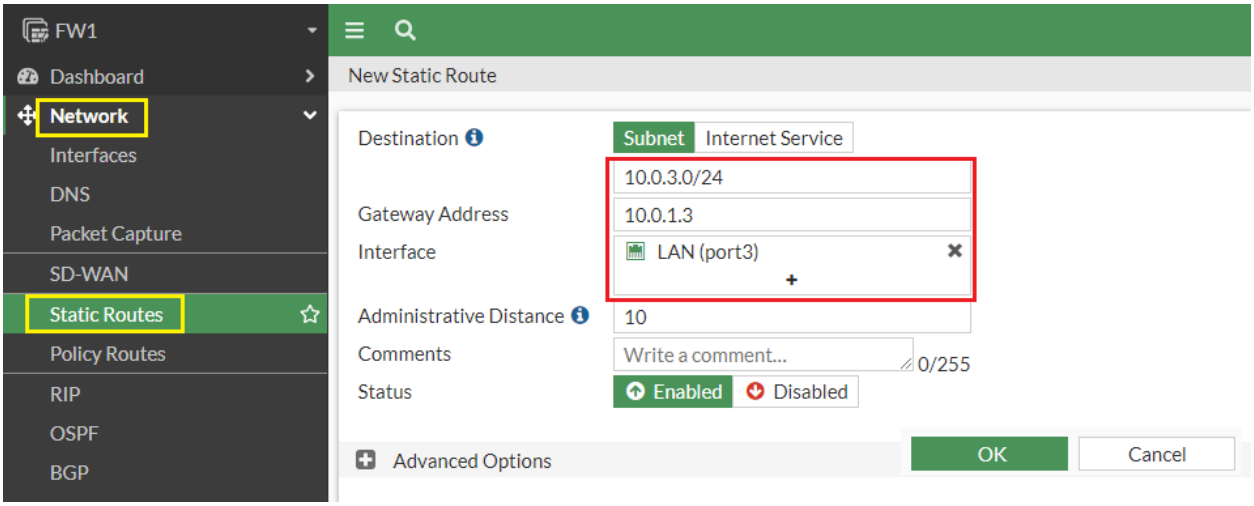
In FW1 we already configured Default route which gateway is 192.168.1.254.

FW1 Static Route Configuration:

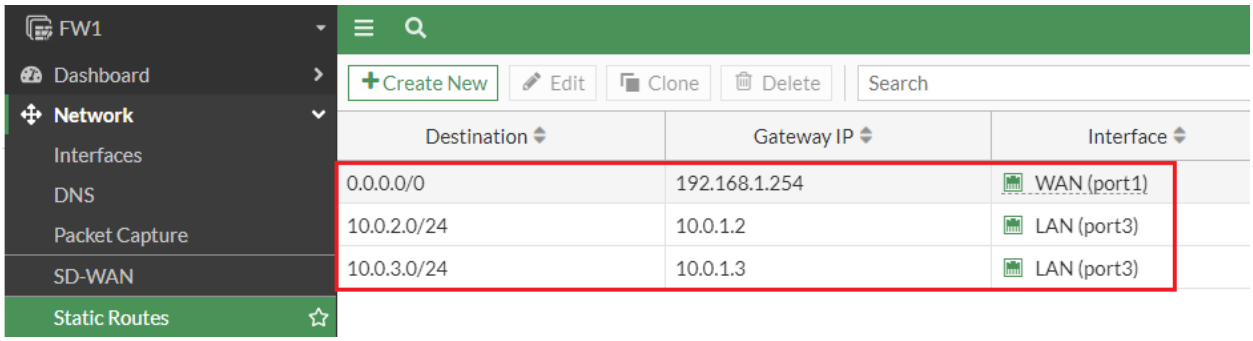
Let's create a static route for FW2 LAN Subnet while the gateway is FW2 IP address.



Let's create a static route for FW3 LAN Subnet while the gateway is FW3 IP address.

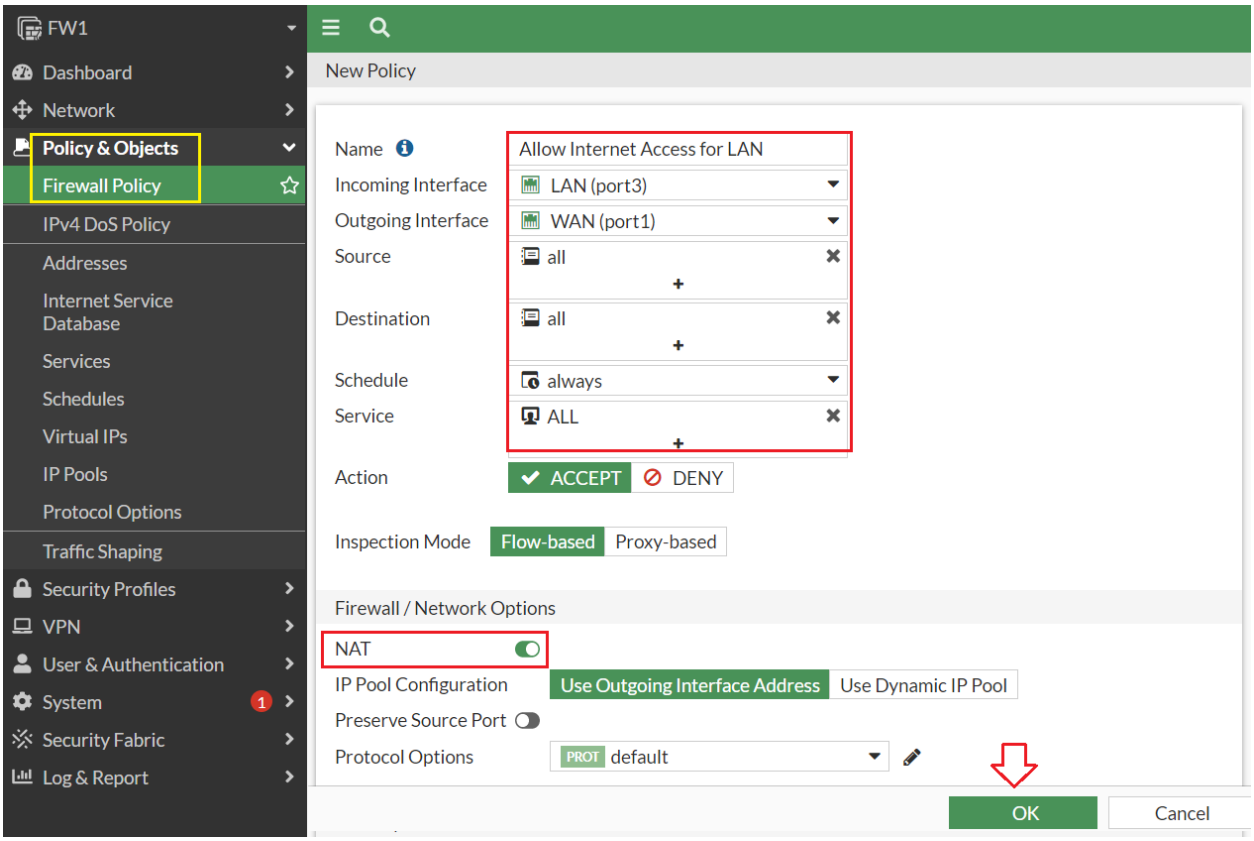


Finally, in FW1 we have three 3 routes one is default route going outside Internet while two 2 are static Routes for each firewall LAN Subnets.

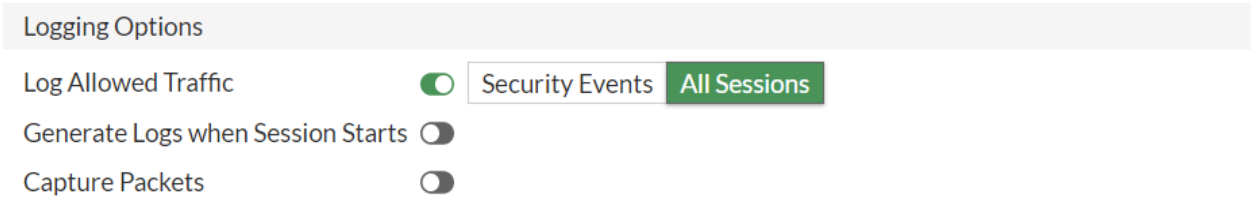


FW1 Firewall Policy:

To create a new policy, go to Policy & Objects > Firewall Policy. Give the policy a Name that indicates that the policy will be for traffic to the Internet in my case it is Allow-All. Set the Incoming Interface to LAN and the Outgoing Interface to WAN. Set Source, Destination Address, Schedule, and Services, as required in this case All. Ensure the Action is set to ACCEPT.
Turn on NAT and select Use Outgoing Interface Address.

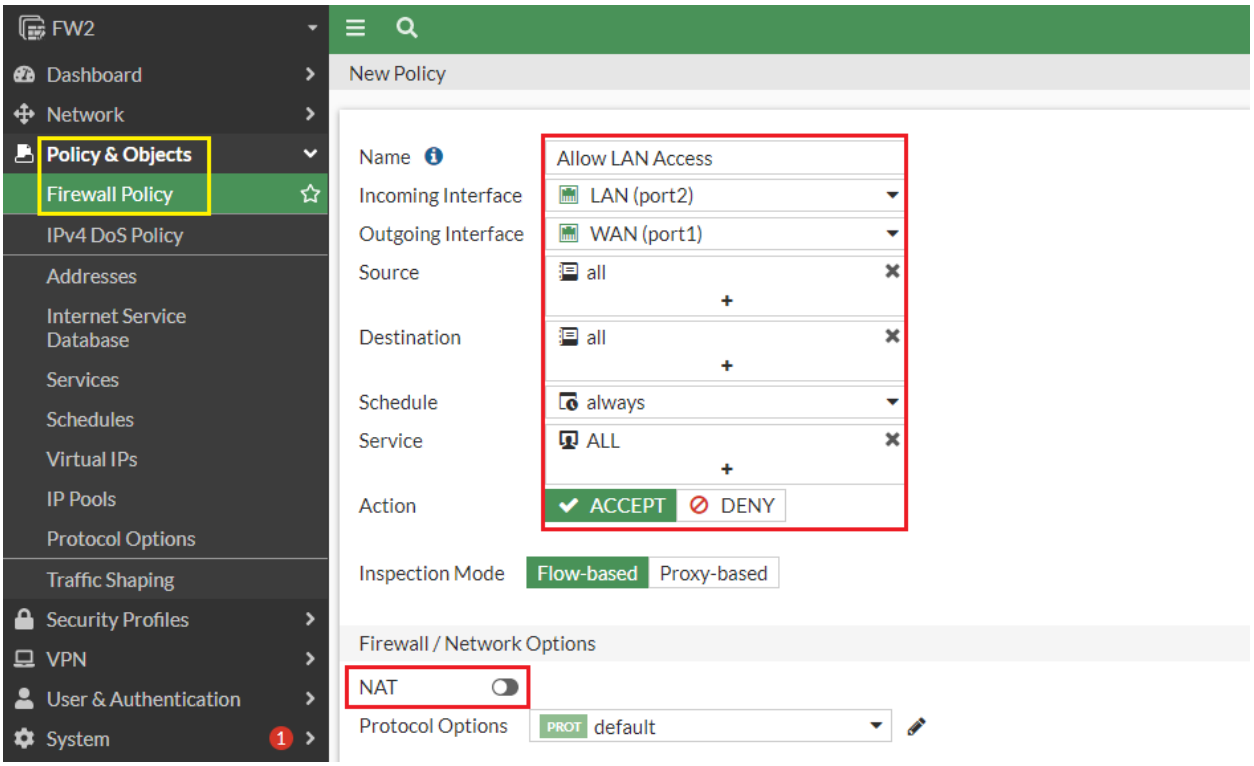


Scroll down to view the Logging Options. To view the results later, enable Log Allowed Traffic and select All Sessions.



FW2 Firewall Policy:

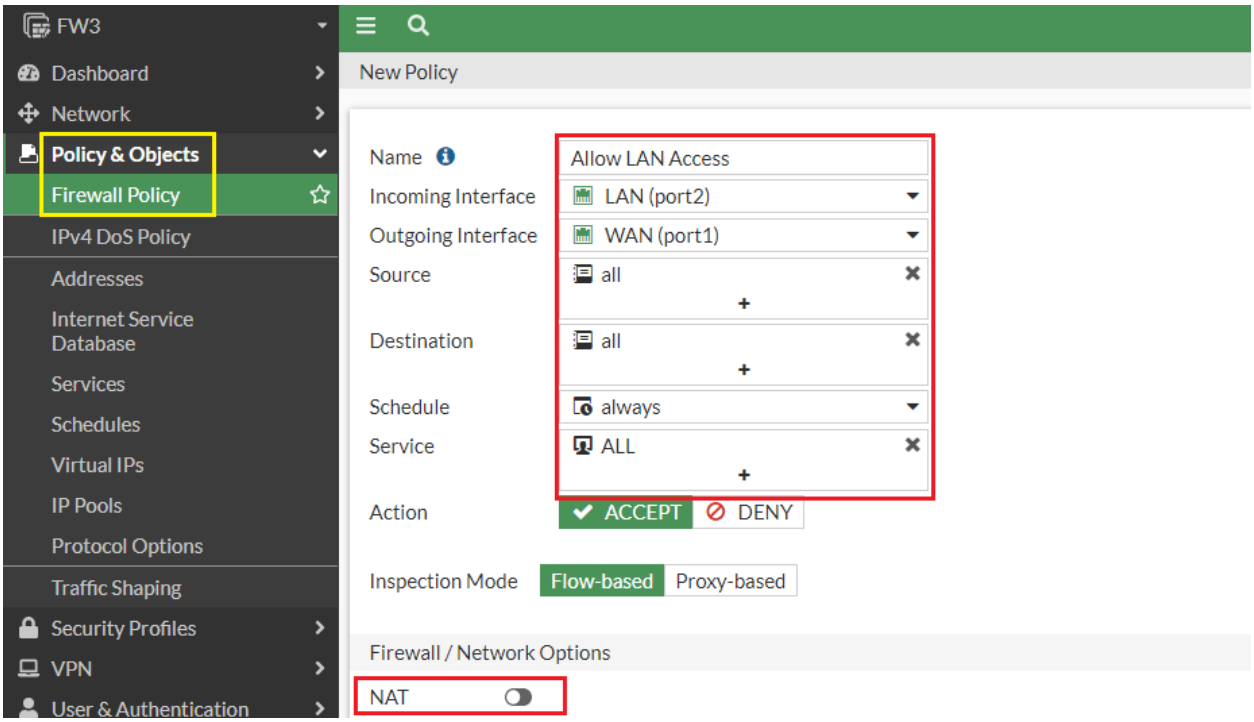
To create a new policy, go to Policy & Objects > Firewall Policy. Give the policy a Name that indicates that the policy will be for traffic to the Internet in my case it is Allow-All. Set the Incoming Interface to LAN and the Outgoing Interface to WAN. Set Source, Destination Address, Schedule, and Services, as required in this case All. Ensure the Action is set to ACCEPT.
Turn off NAT and select Use Outgoing Interface Address.



PC2 IP address configuration default gateway is FW2 IP Address.

FW3 Firewall Policy:

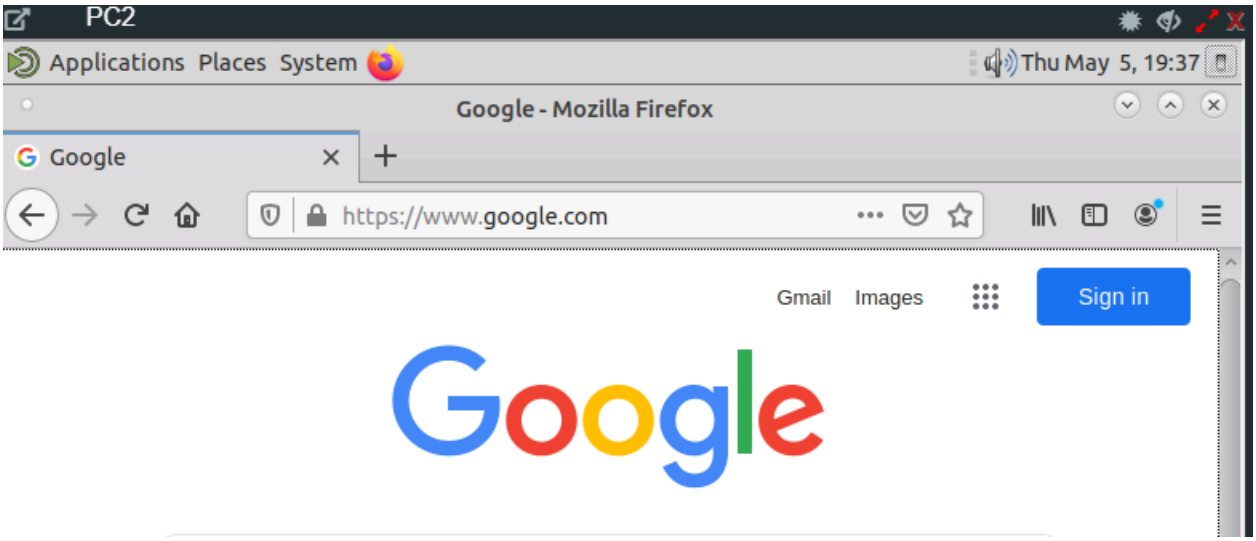
To create a new policy, go to Policy & Objects > Firewall Policy. Give the policy a Name that indicates that the policy will be for traffic to the Internet in my case it is Allow-All. Set the Incoming Interface to LAN and the Outgoing Interface to WAN. Set Source, Destination Address, Schedule, and Services, as required in this case All. Ensure the Action is set to ACCEPT.
Turn off NAT and select Use Outgoing Interface Address.



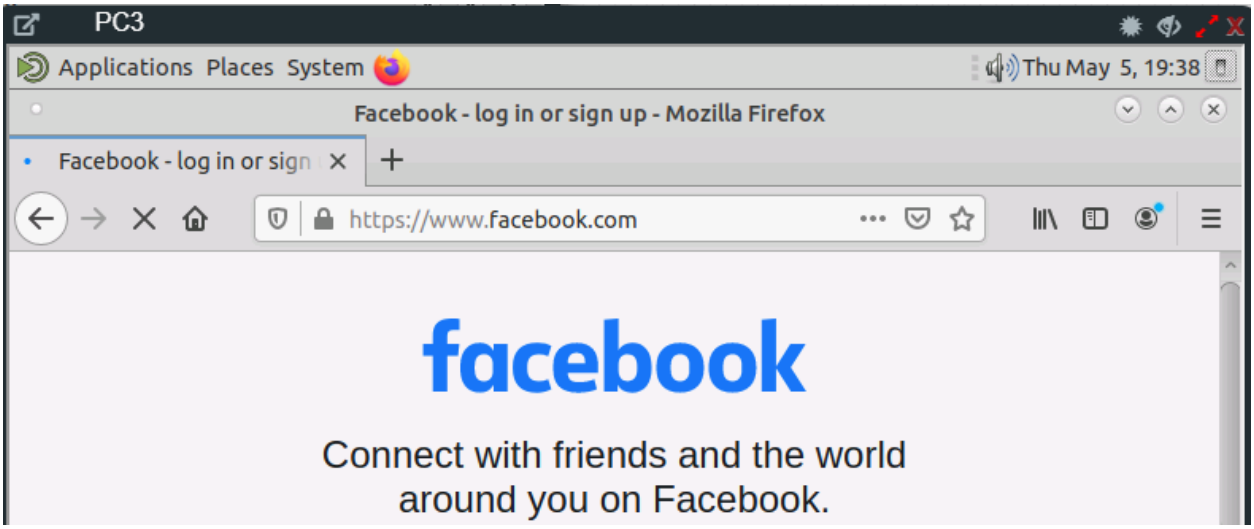
PC3 IP address configuration default gateway is FW3 IP Address.

Testing and Verification:

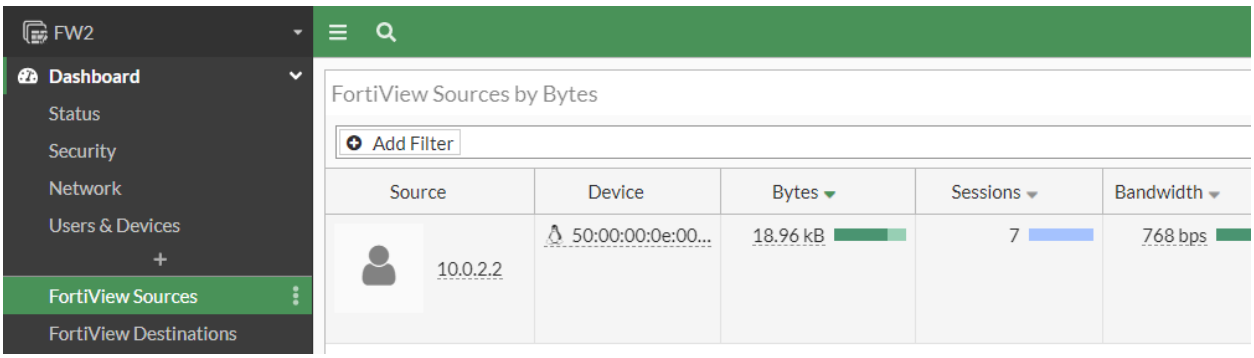
Browse the Internet using the PC2 on the internal LAN network of FW2.



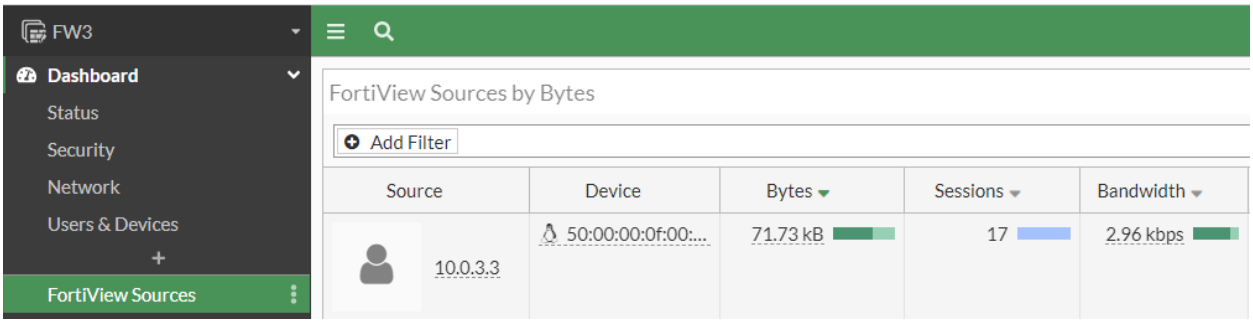
Browse the Internet using the PC3 on the internal LAN network of FW3.



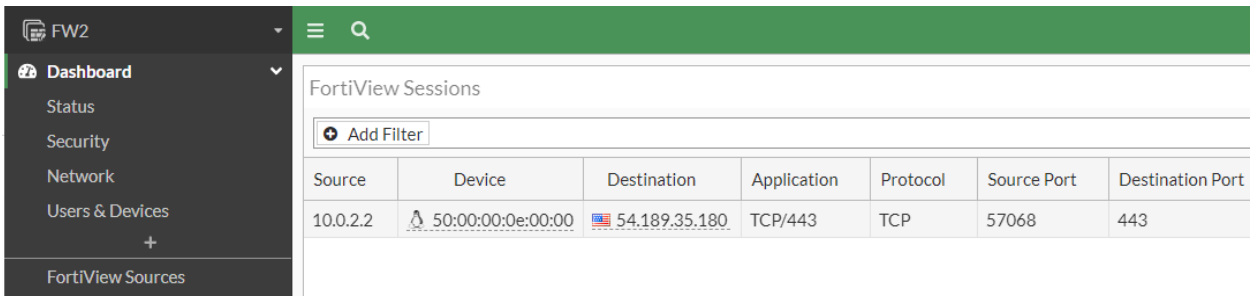
To view information about FortiGate traffic, go to Dashboard >FortiView Sources. The PC2 appears on the list of sources in FW2.



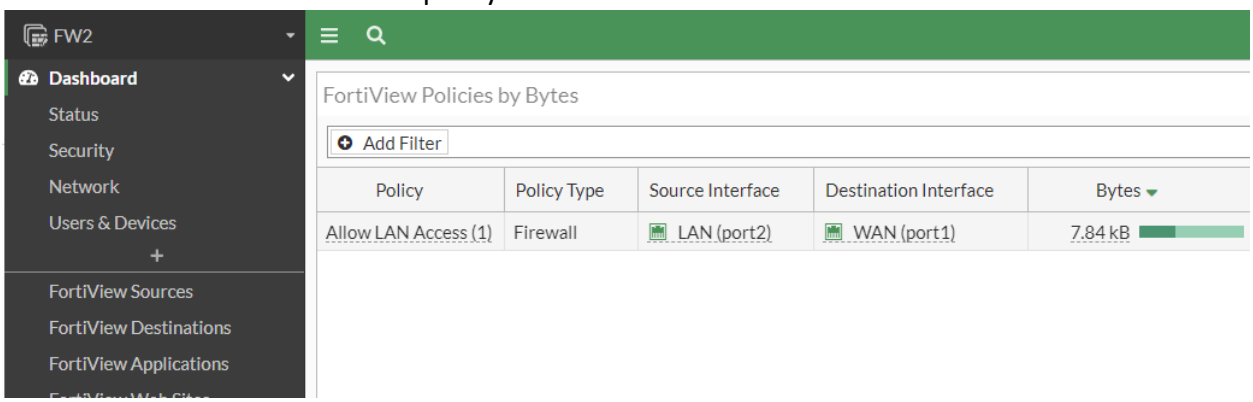
To view information about FortiGate traffic, go to Dashboard >FortiView Sources. The PC3 appears on the list of sources in FW3.



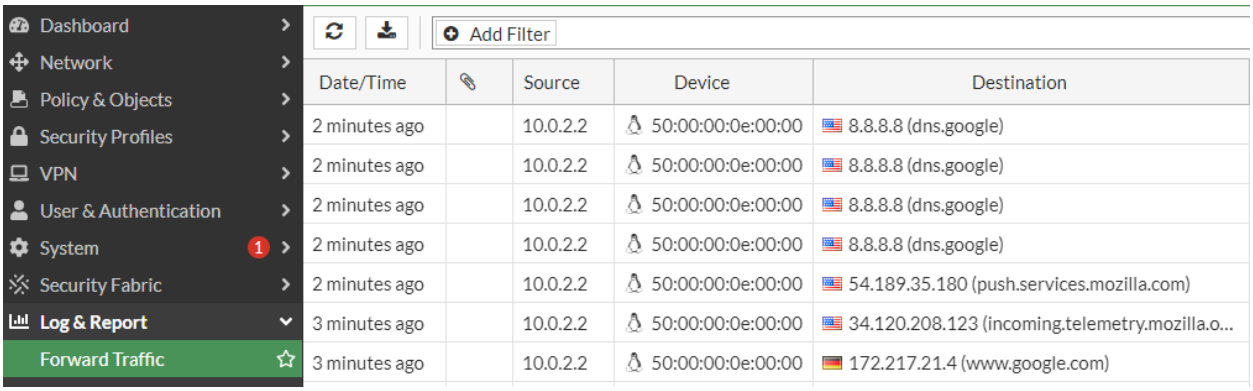
To view information about traffic, Go to Dashboard > FortiView Sessions.



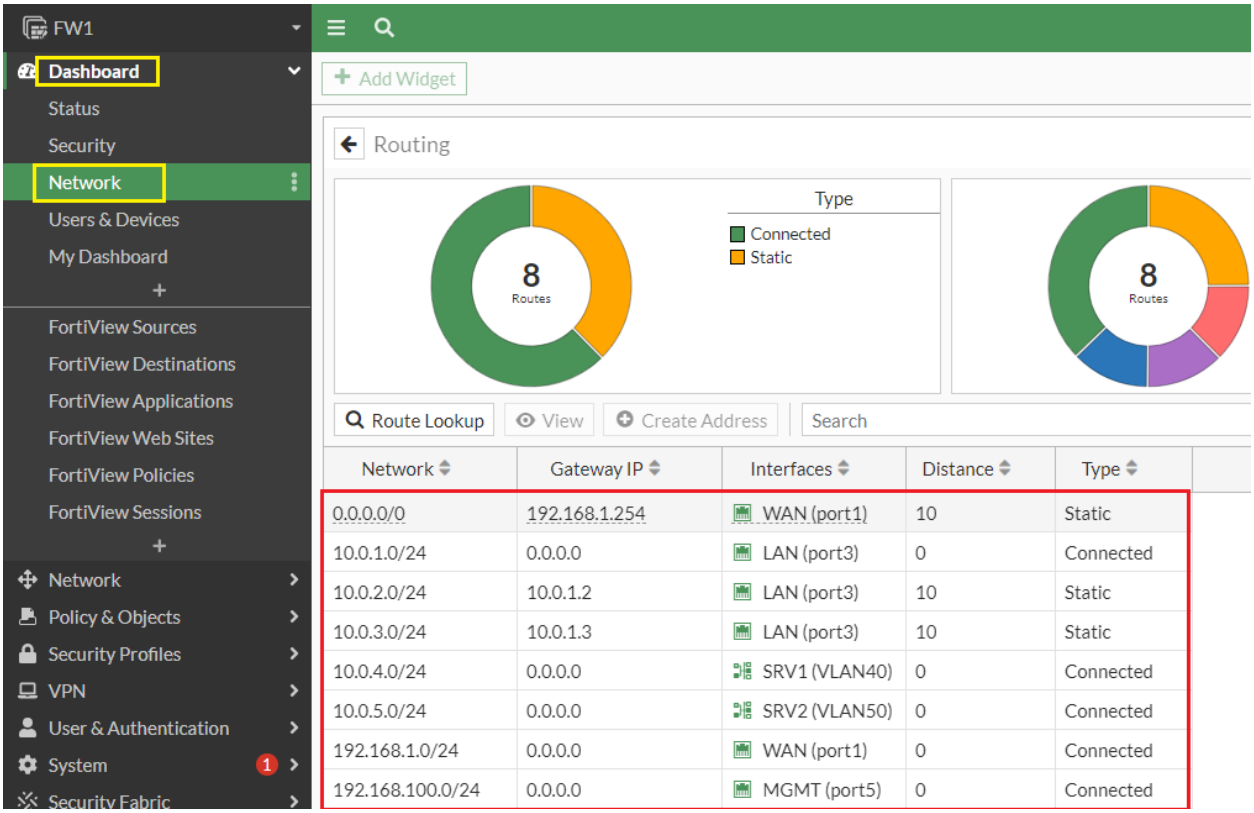
T view information about which policy has been used Go to Dashboard> FortiView Polices

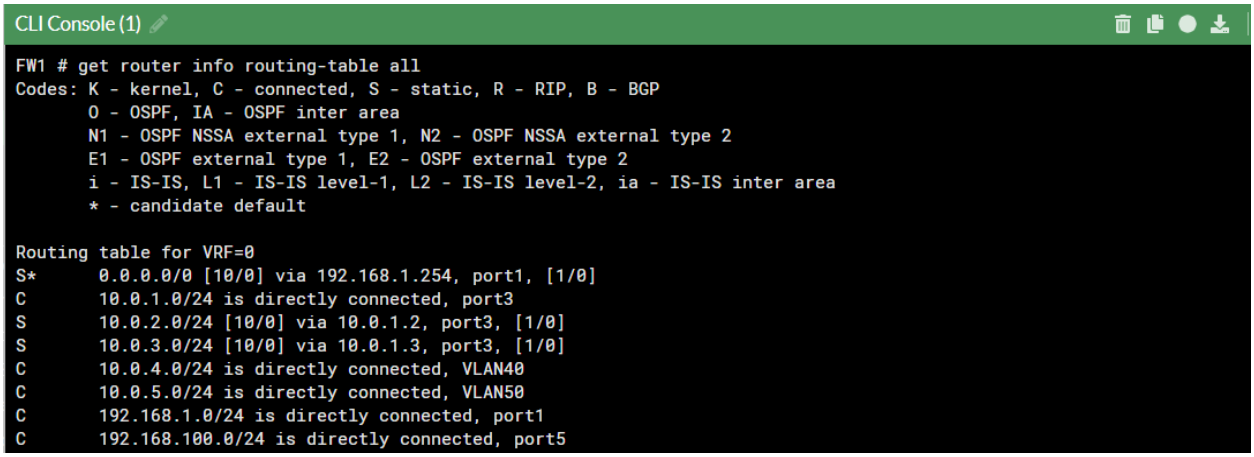


To view information about FortiGate traffic, go to Log & Report > Forward Traffic.



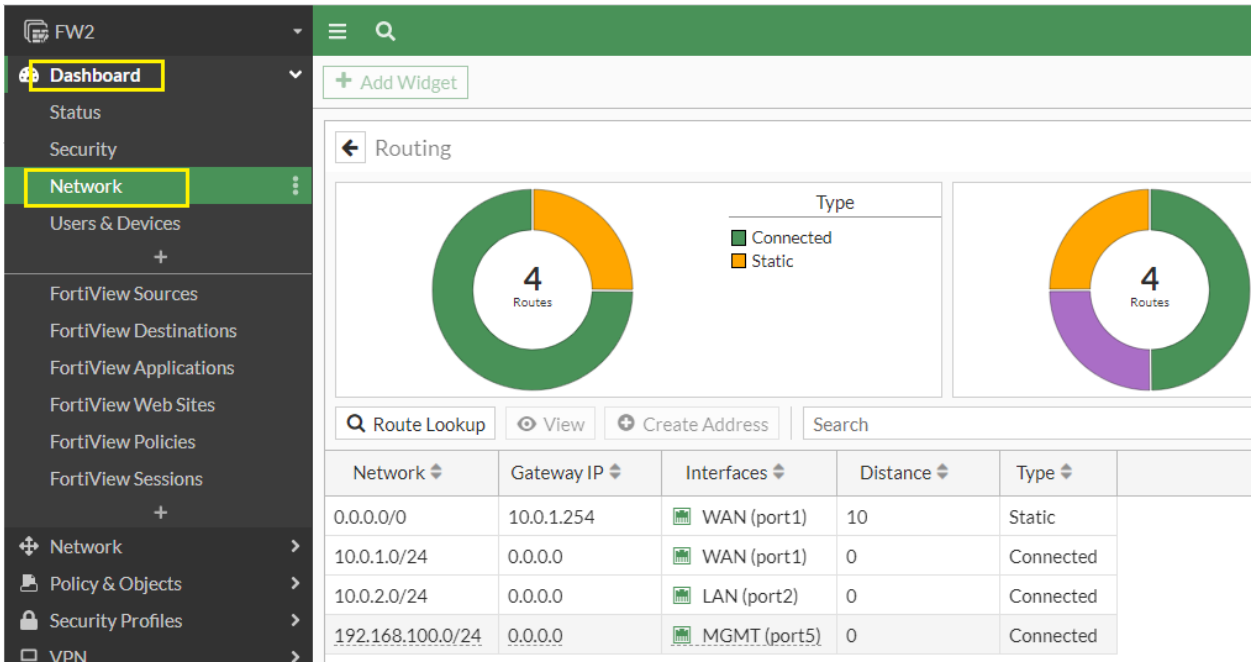
Let’s Verify the routing table of Firewall FW1.

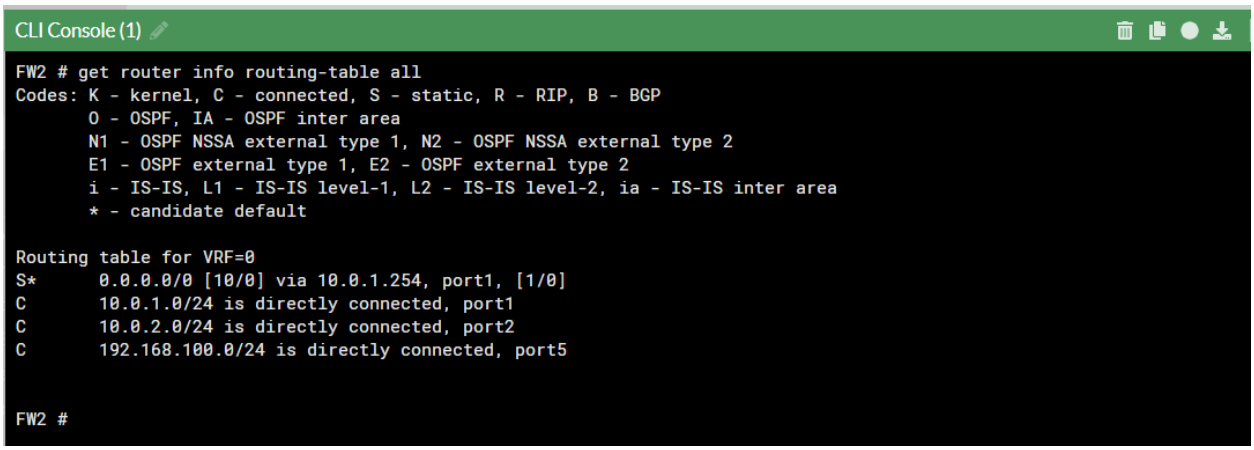


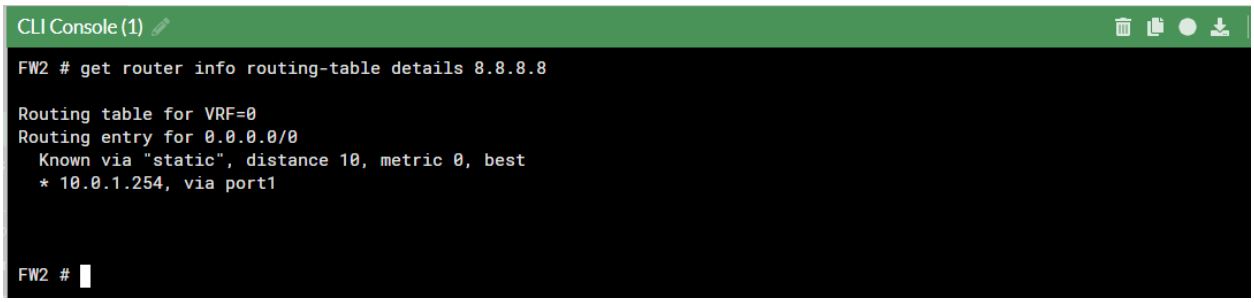



```
FW1 # get router info routing-table details 10.0.2.0

Routing table for VRF=0
Routing entry for 10.0.2.0/24
  Known via "static", distance 10, metric 0, best
  * 10.0.1.2, via port3

FW1 # get router info routing-table details 10.0.3.0

Routing table for VRF=0
Routing entry for 10.0.3.0/24
  Known via "static", distance 10, metric 0, best
  * 10.0.1.3, via port3
```

Let’s Verify the routing table of Firewall FW2.







Let’s Verify the routing table of Firewall FW3.