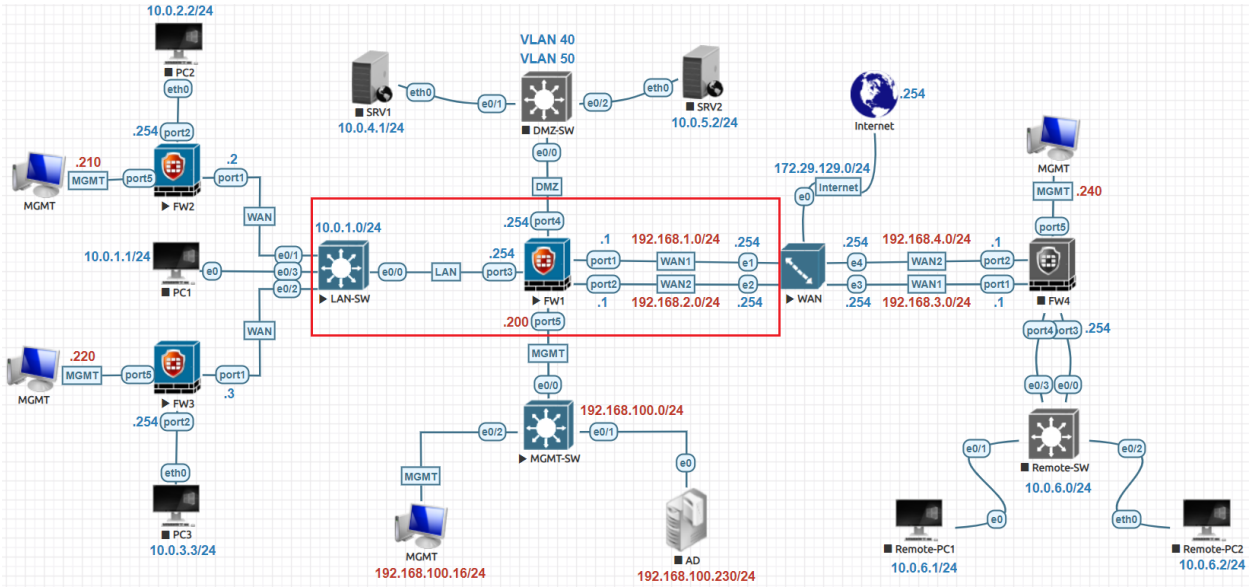
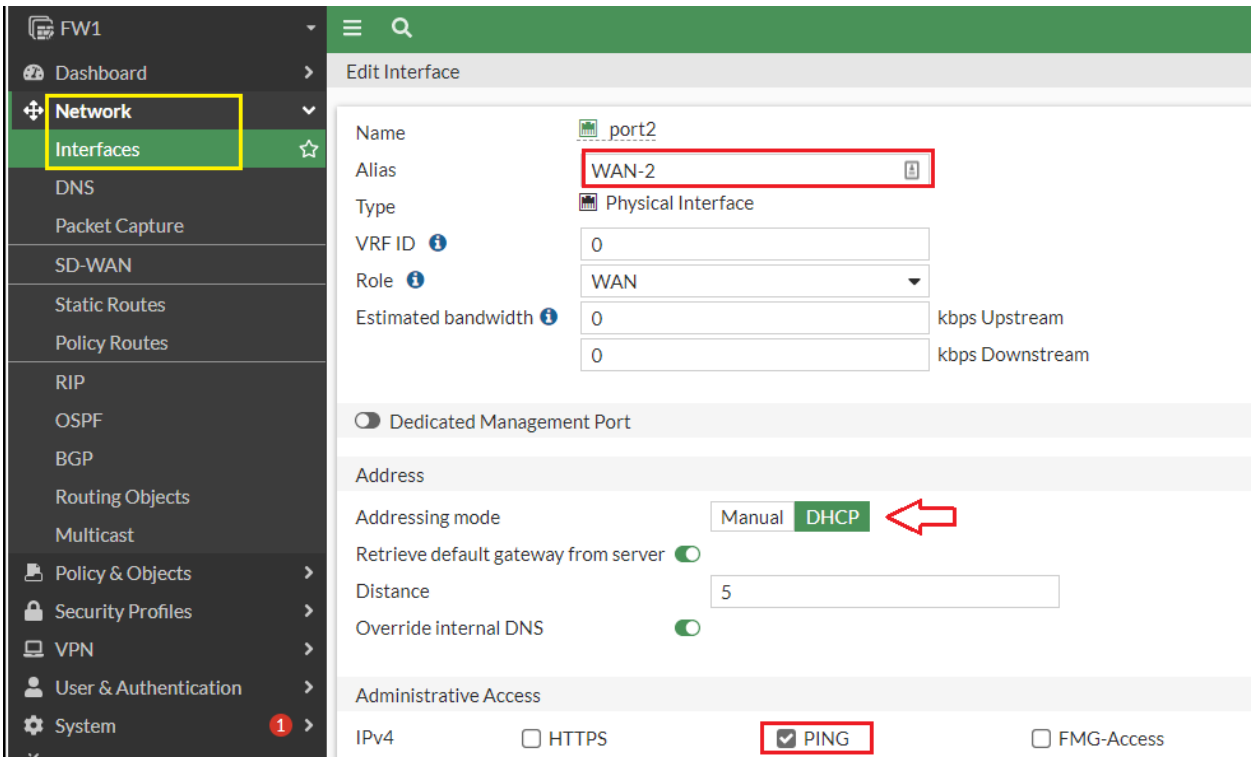
Policy Routing Lab:



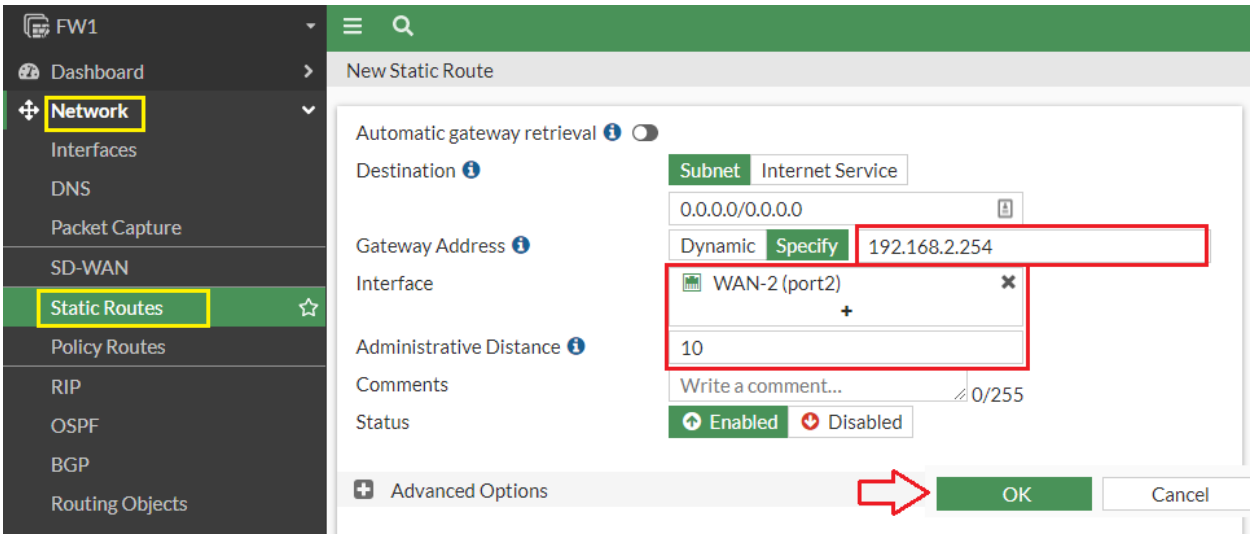
Configure Interface:

Go to Network>Interfaces select port2 Click Edit in Alias type WAN-2, change the Address Mode to Manual type IP/Netmask 192.168.2.102/24, in Administrative access uncheck everything only checked PING leave all the rest of configuration default and press OK button.

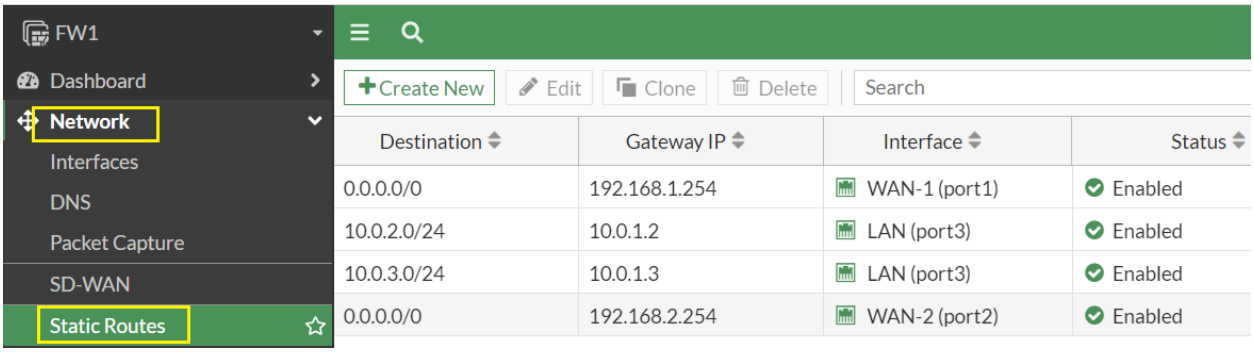


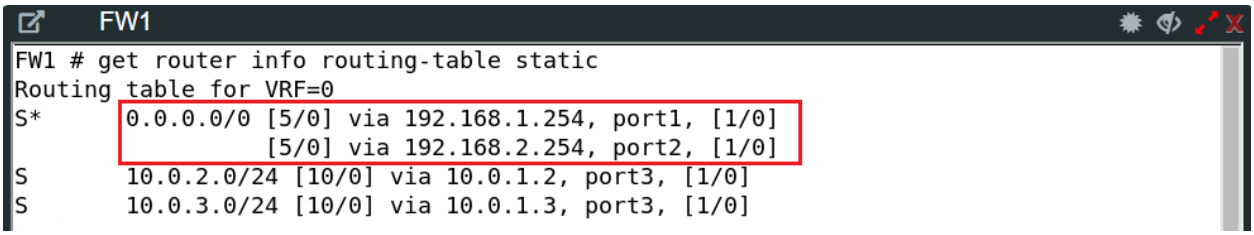
Default Route Configuration:

To create a new default route, go to Network > Static Routes and create a static route for ISP-2. 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 192.168.2.254 which the Gateway. Set the Interface to the WAN-2 interface. Press OK to Save the changes.



Finally, now we have two default Route for equal Cost Multi-Path available.

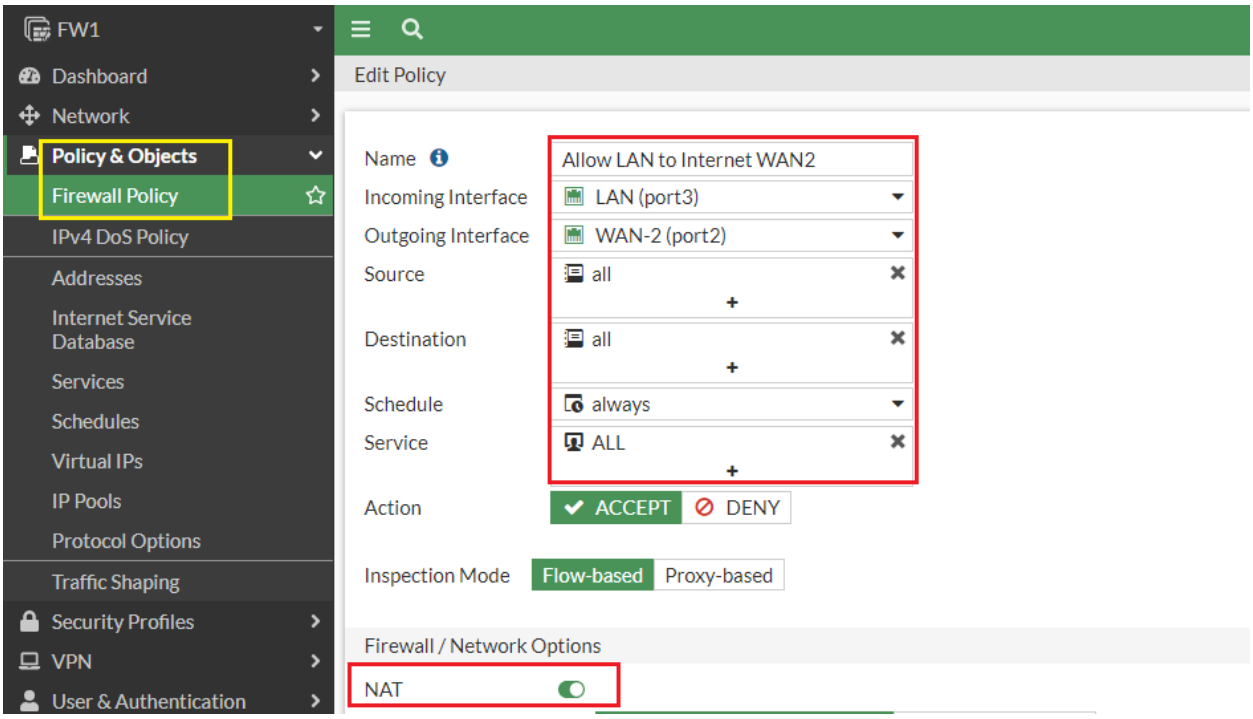




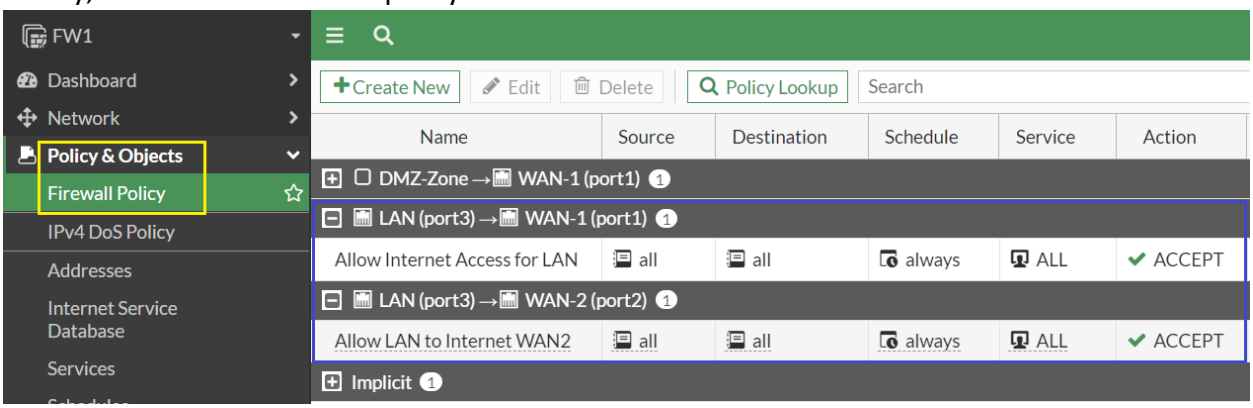
Change Equal Cost Multi-Path Mode
FW1 # config system settings FW1 (settings) # set v4-ecmp-mode weight-based FW1 (settings) # end

Creating a 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-2. 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.

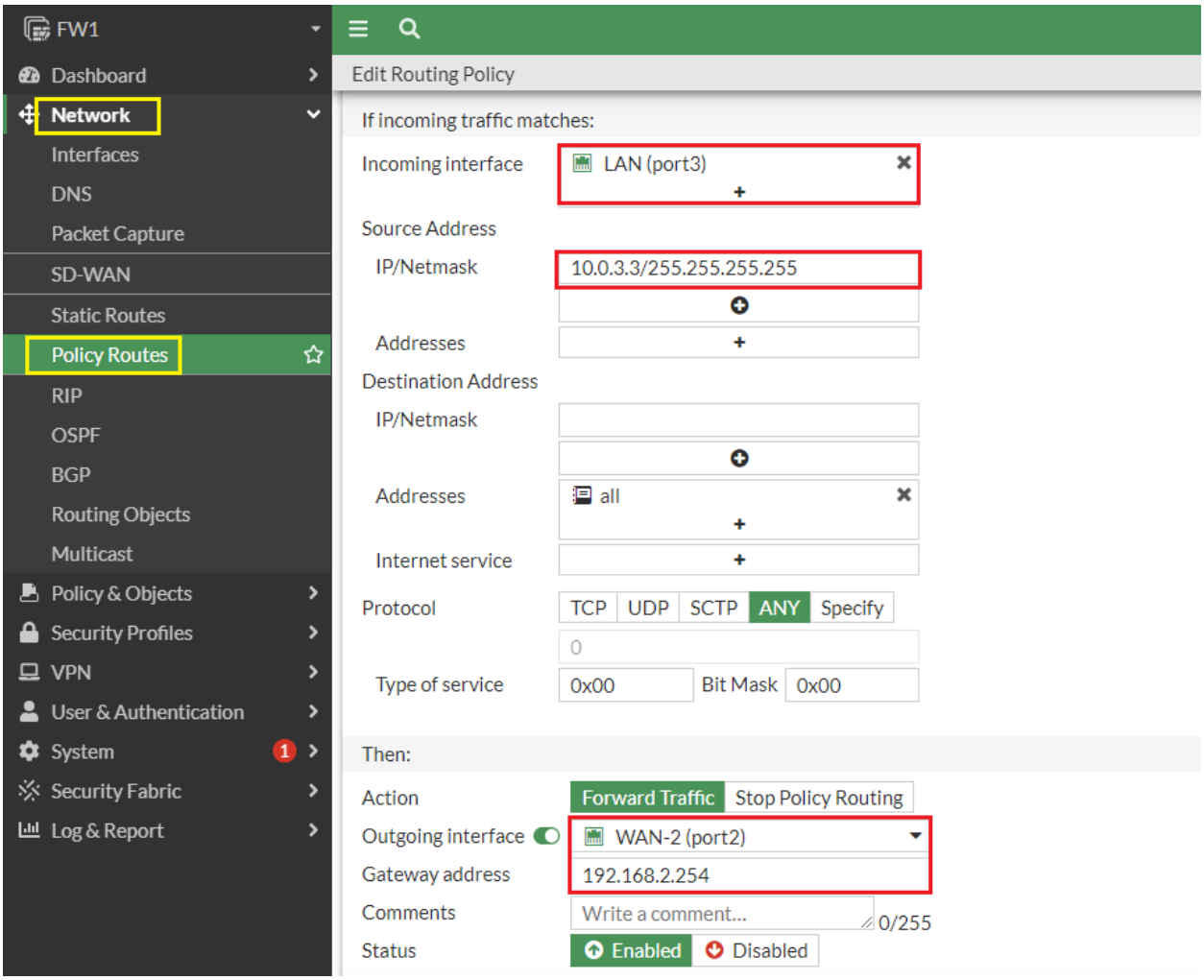


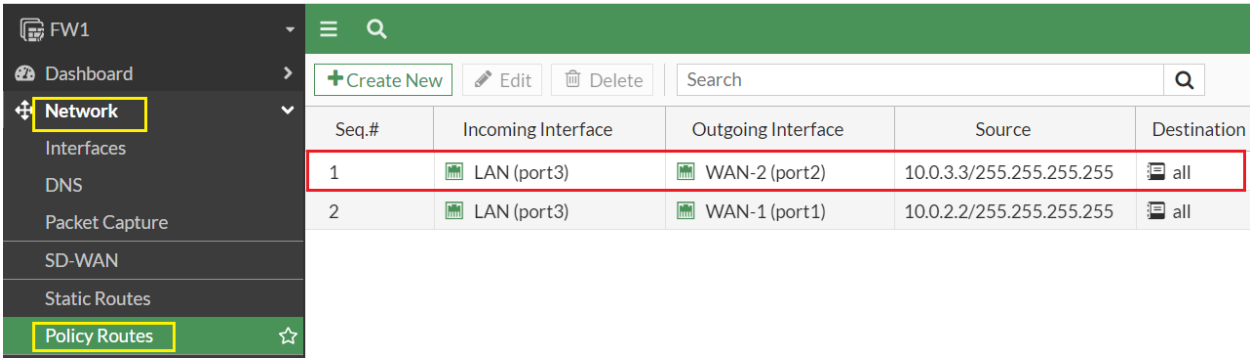
Finally, we have two Firewall policy one for LAN to WAN-1 and second for LAN to WAN-2.



Policy Routes:

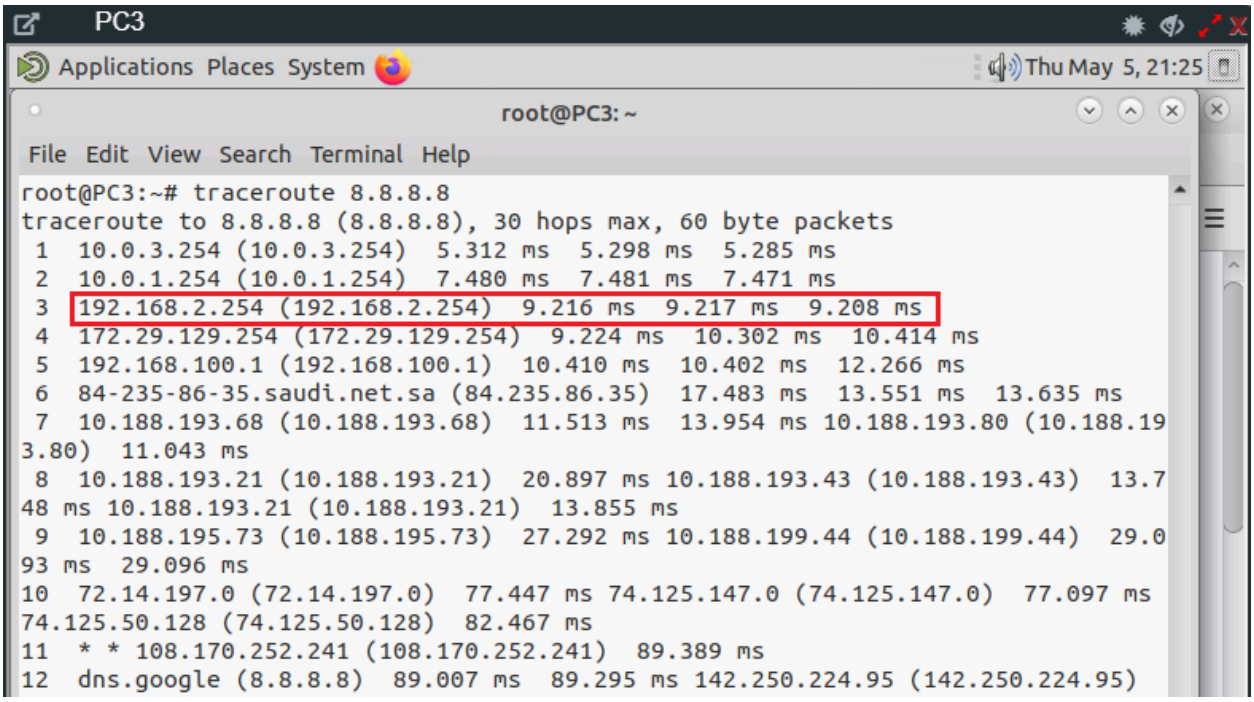
Navigate to Network>Policy Routes > Create New let's create a policy route to send PC3 as a source 10.0.3.3 all traffic to next hop or gateway 192.168.2.254 which is WAN-2.



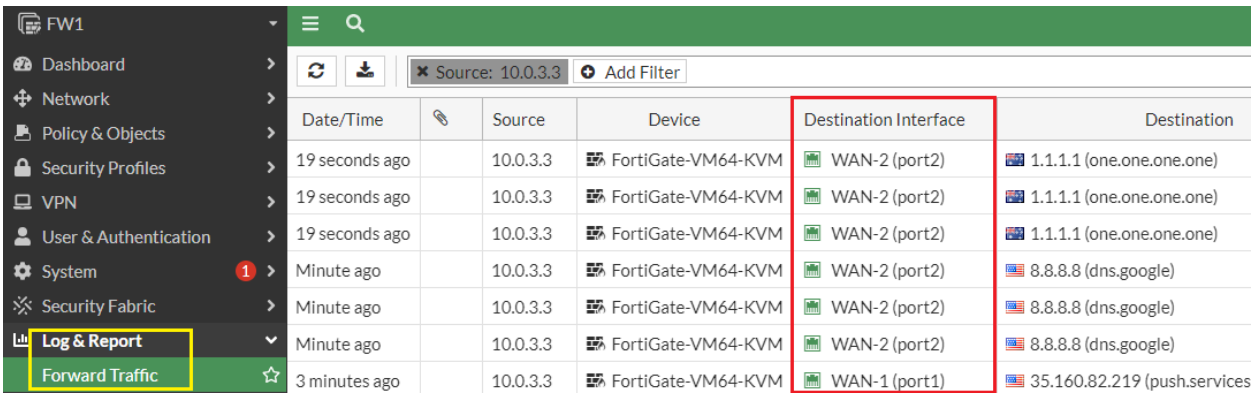


Verification and Testing:

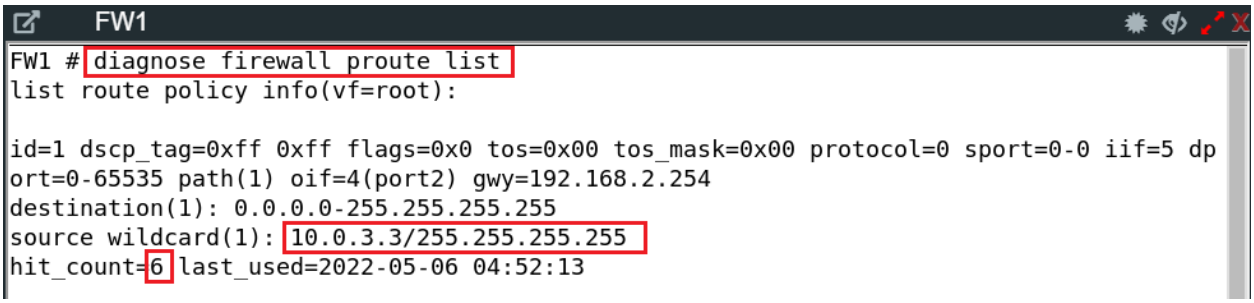
Let's traceroute from PC3 as you can see the traffic is passing through WAN-2 gateway.



Let's check Forward Traffic for the given Source 10.0.3.3 Destination Interface is WAN-2.

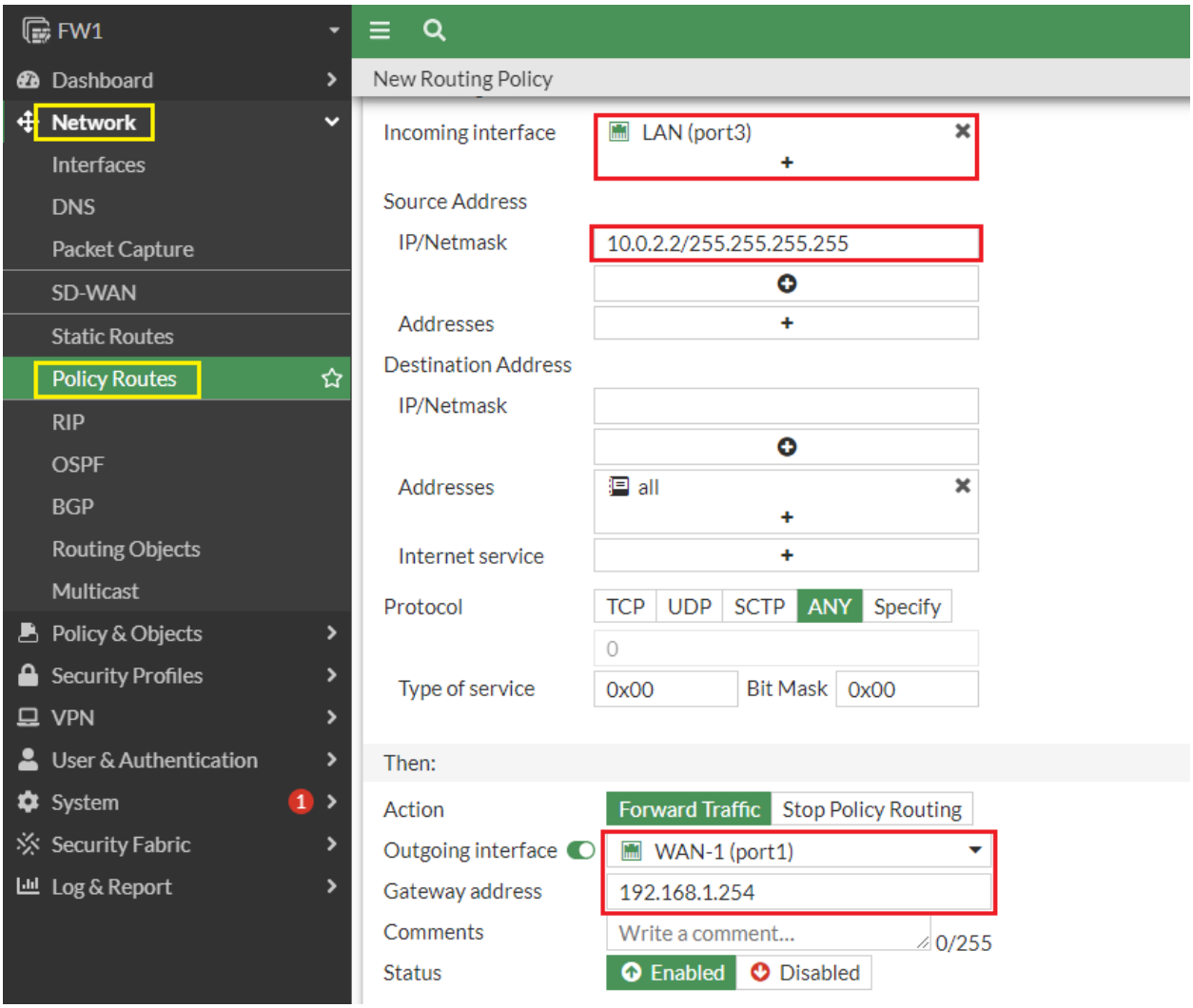


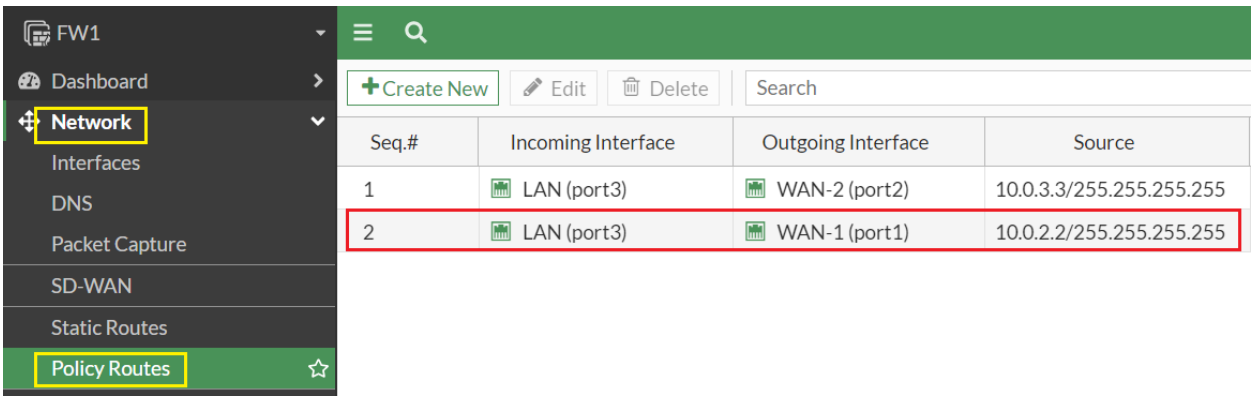
Verify through Fortigate Firewall FW1 CLI there is hit counts for ID=1 which is first policy.



Policy Routes:

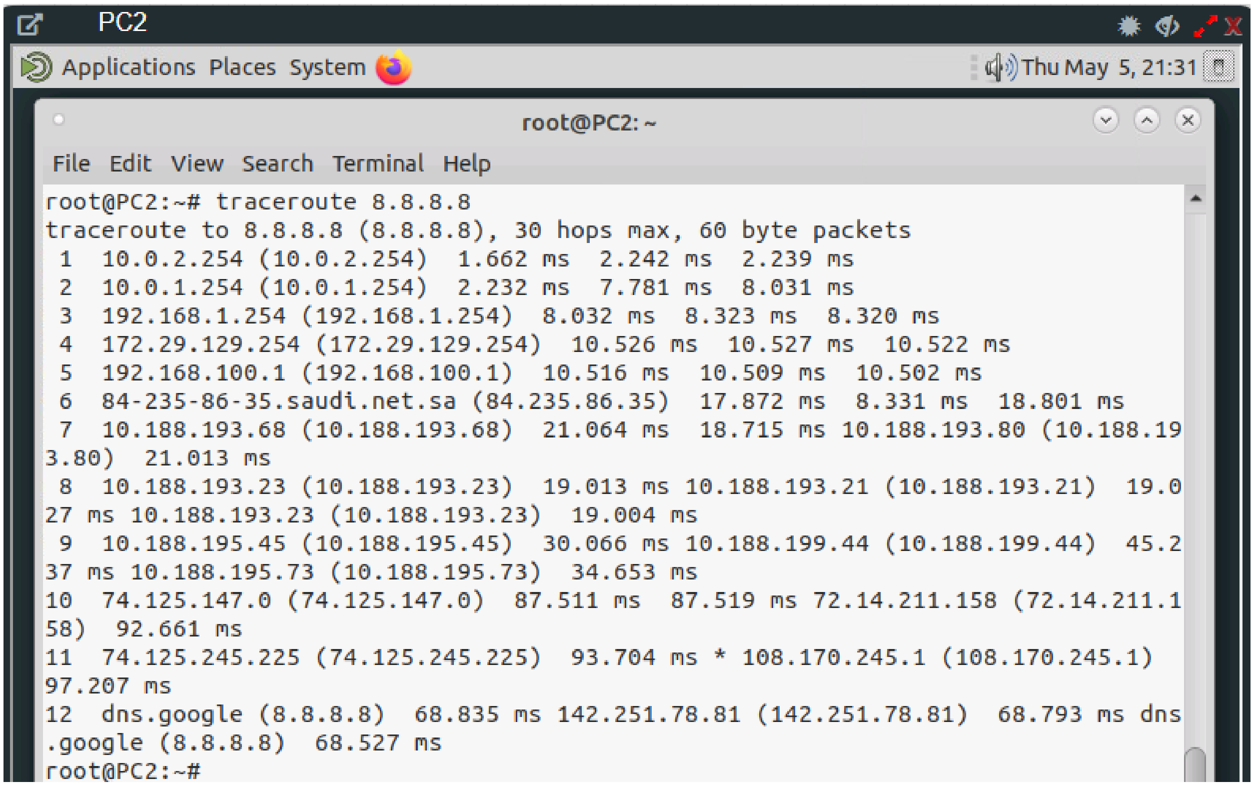
Navigate to Network>Policy Routes > Create New let's create a policy route to send PC2 as a source 10.0.2.2 all traffic to next hop or gateway 192.168.1.254 which is WAN-1.

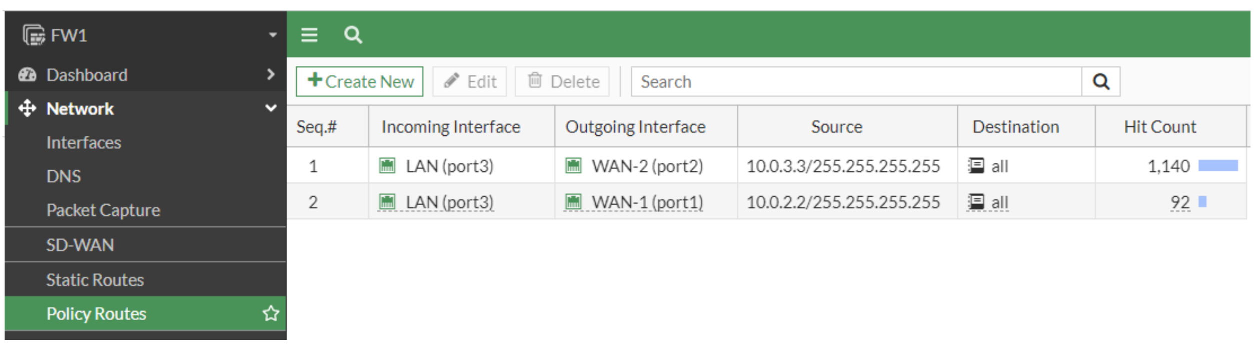


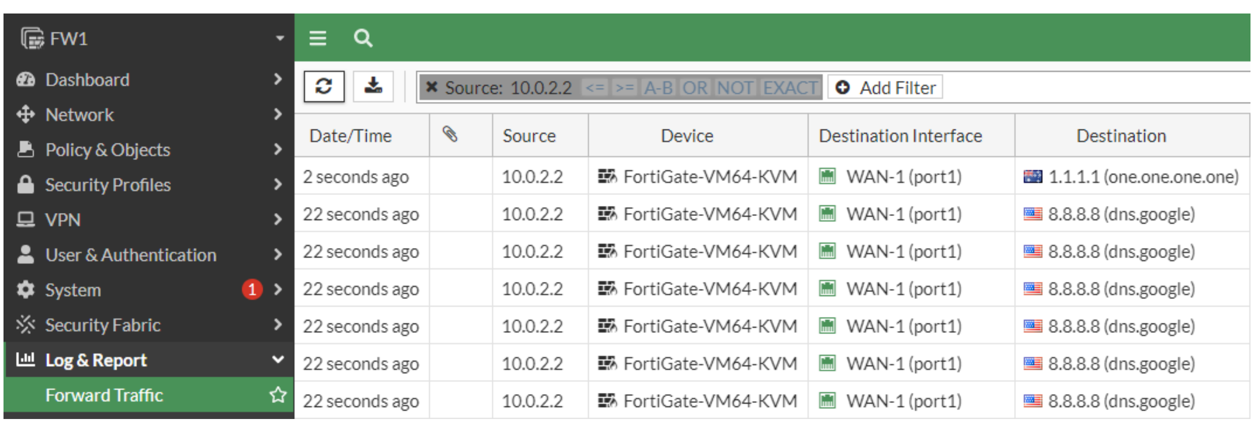


Verification and Testing:

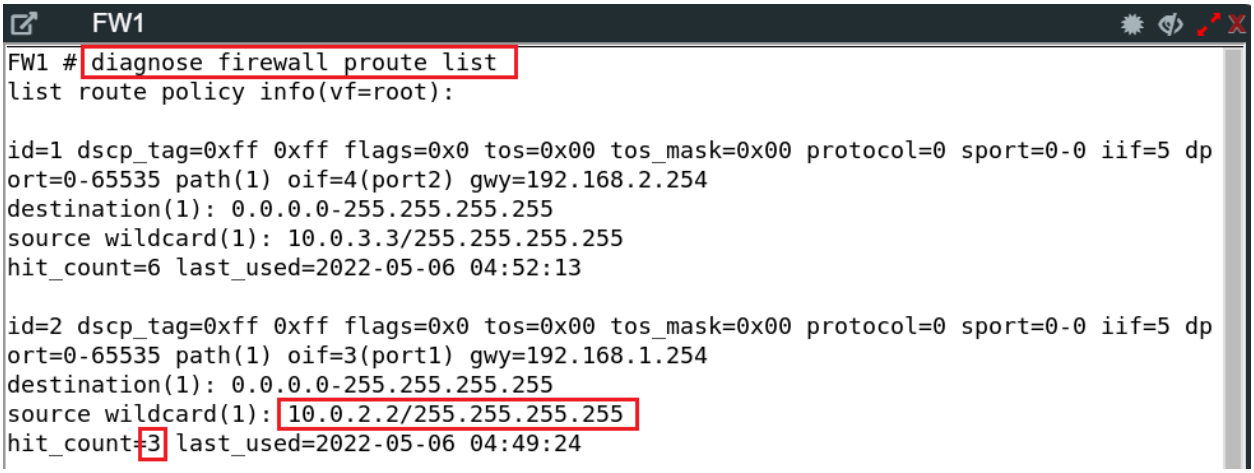
Let's traceroute from PC2 as you can see the traffic is passing through WAN-1 gateway.



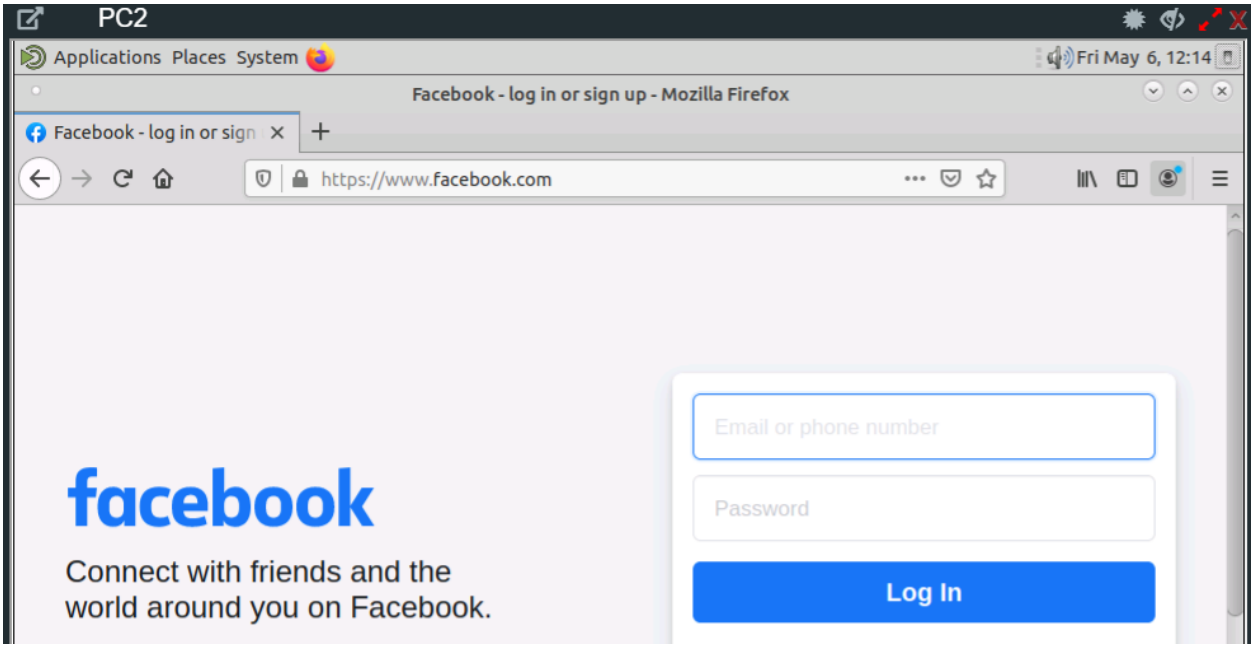




Verify through Fortigate Firewall FW1 CLI there is hit counts for ID=2 which is second policy.



Let's generate some traffic from Internal LAN PC2 open a browser open any website.



After generate the traffic the hit count increase for policy number 2 which is ID=2.