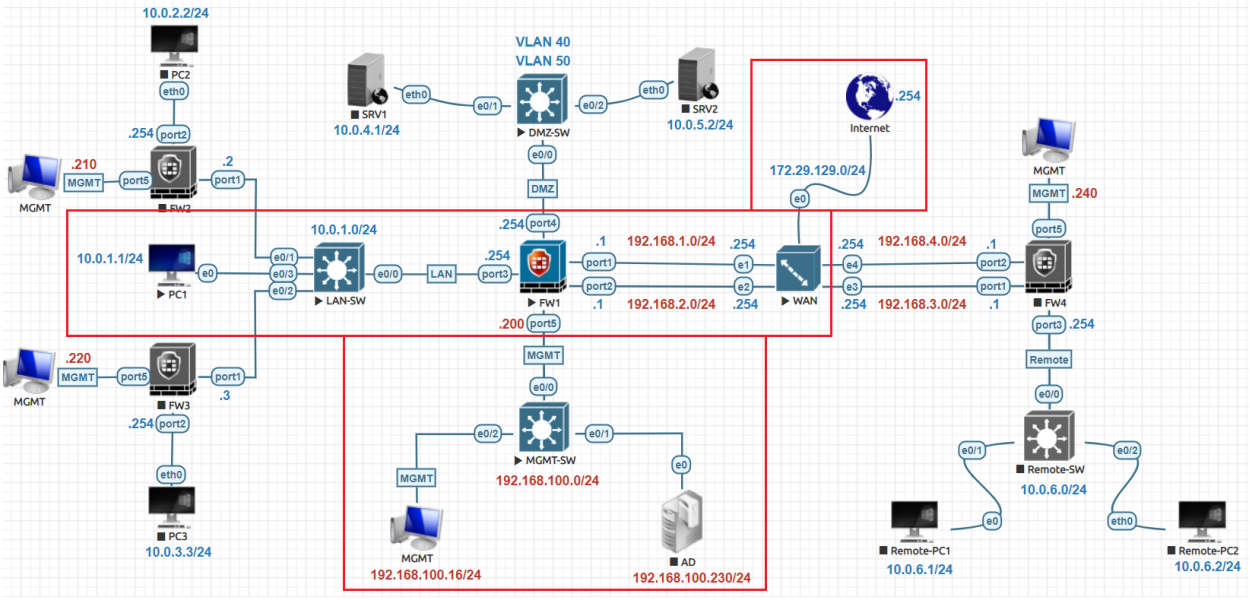
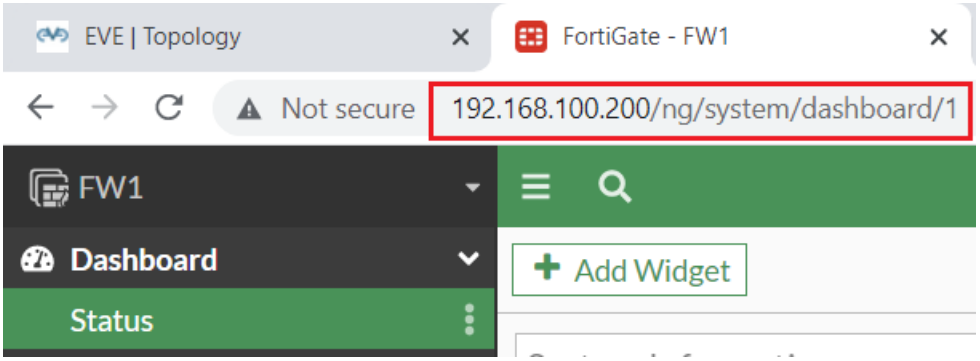
Initial Working Lab:



Change Hostname
FortiGate-VM64-KVM # config system global FortiGate-VM64-KVM (global) # set hostname FW1 FortiGate-VM64-KVM (global) # end

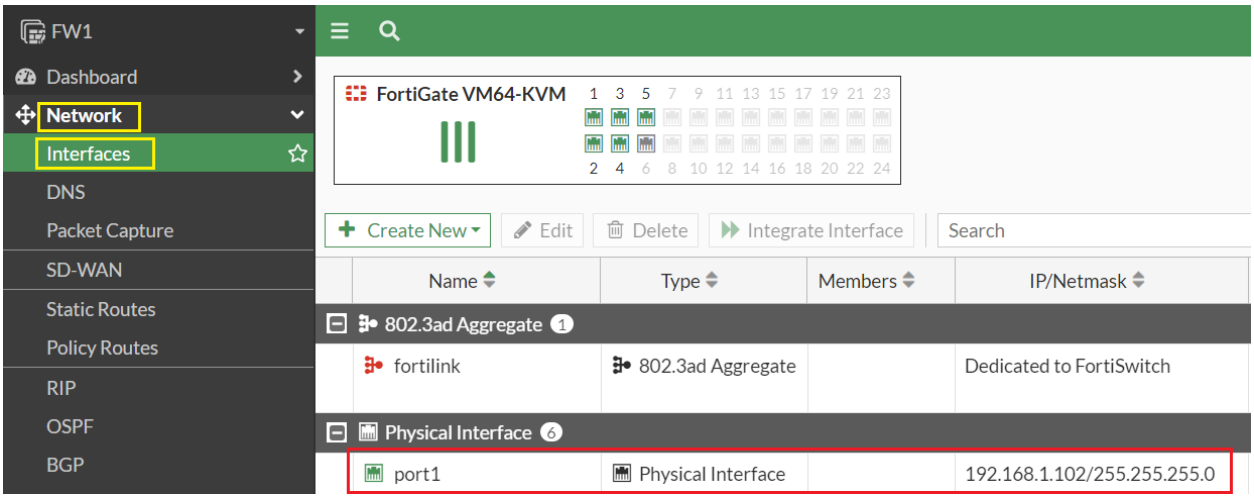
Configure Management Interface
FW1 # config system interface FW1 (interface) # edit port5 FW1 (port4) # set mode static FW1 (port4) # set ip 192.168.100.200/24 FW1 (port4) # set allowaccess https http ssh telnet ping FW1 (port4) # end

Login to FortiGate Firewall type http://192.168.100.200 in any browser.

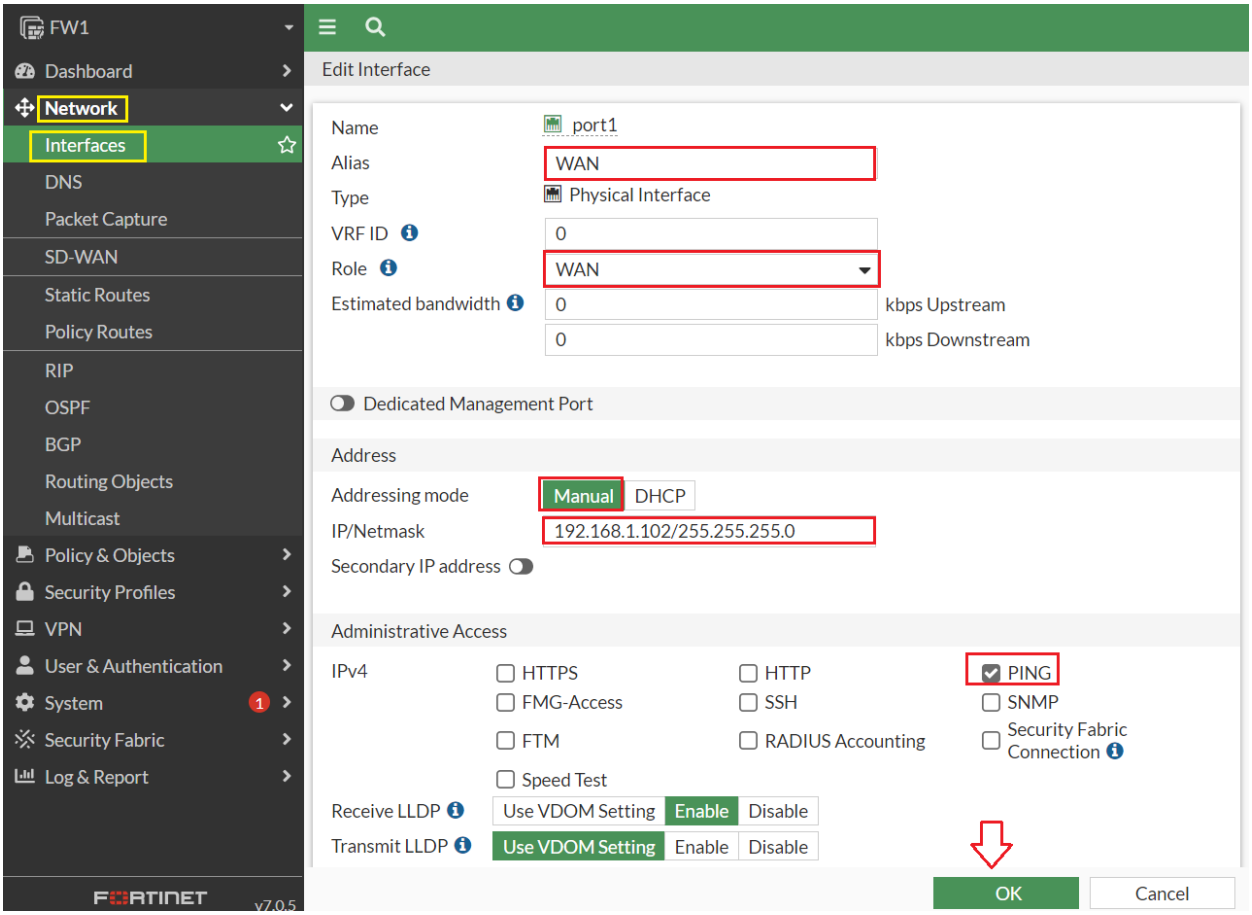


Configure Interfaces:

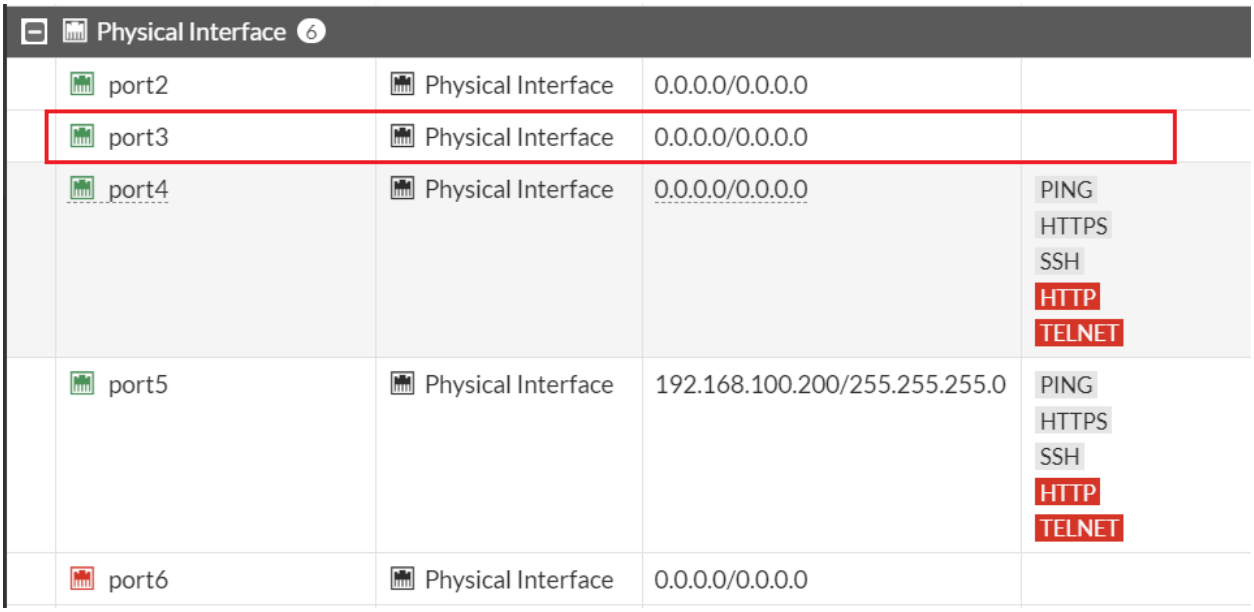
Go to Network>Interfaces select port1 Click Edit



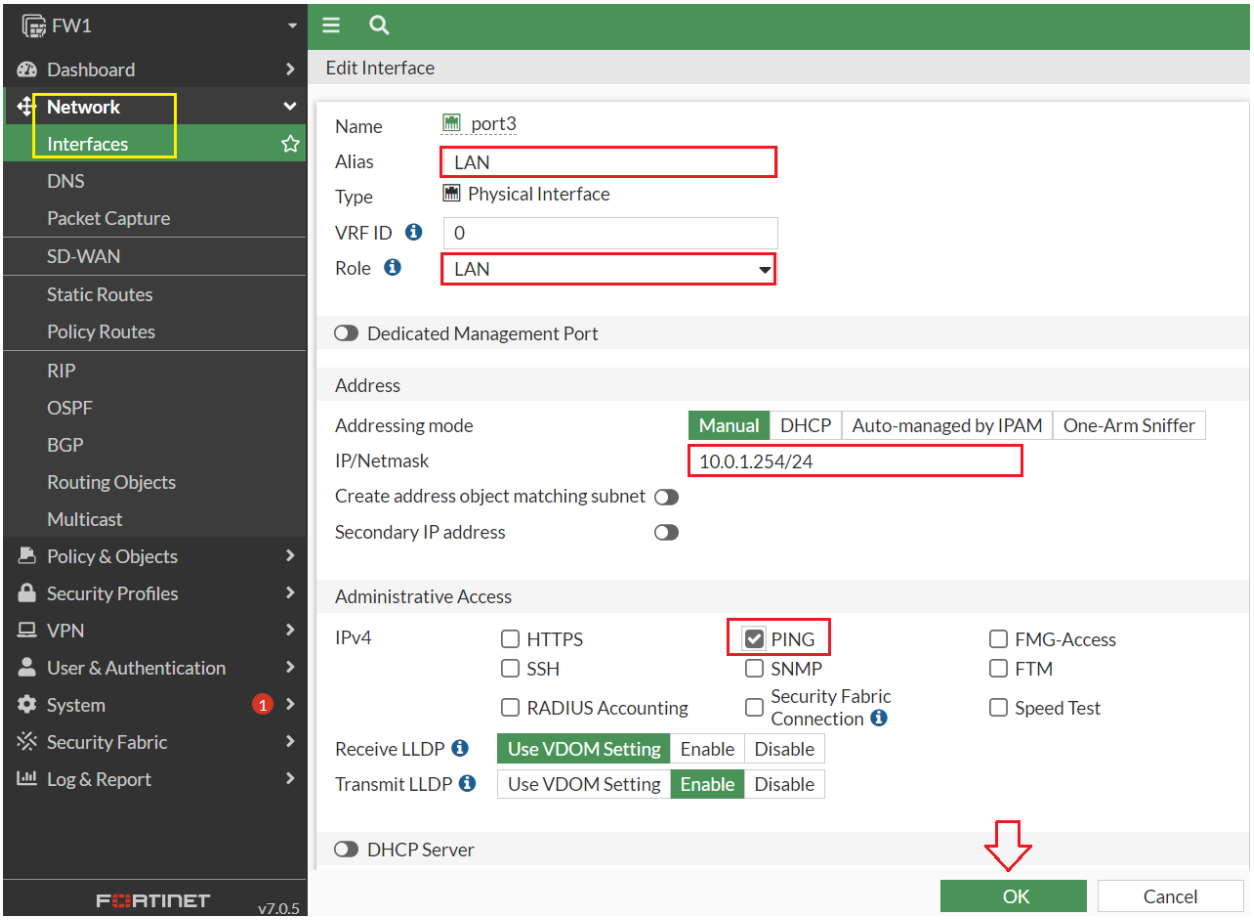
In Alias type WAN, change the Address Mode to Manual type IP/Netmask 192.168.1.102/24, in Administrative access uncheck everything only checked PING leave all the rest of configuration default and press OK button.



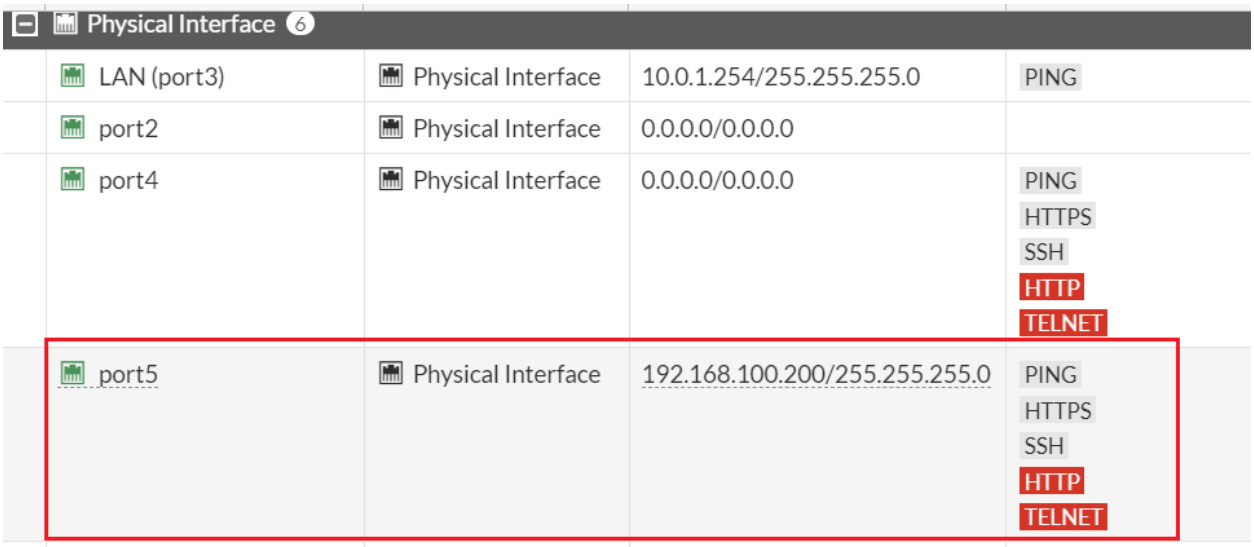
Go to Network>Interfaces select port3 Click Edit



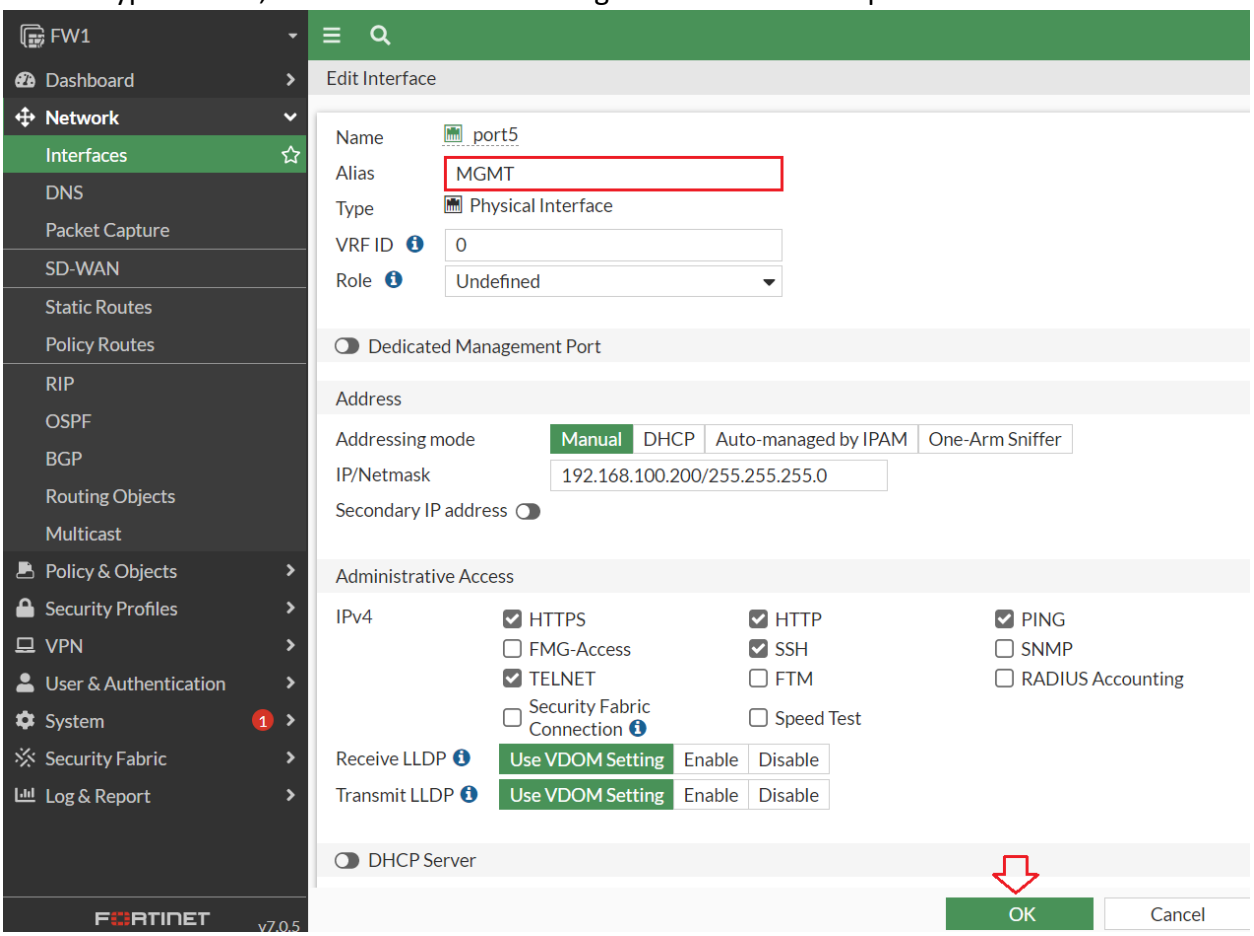
In Alias type LAN, change the Address Mode to Manual type IP/Netmask 10.0.1.254/24, in Administrative access only checked PING leave all the rest of configuration default & press OK.



Go to Network>Interfaces select port5 Click Edit

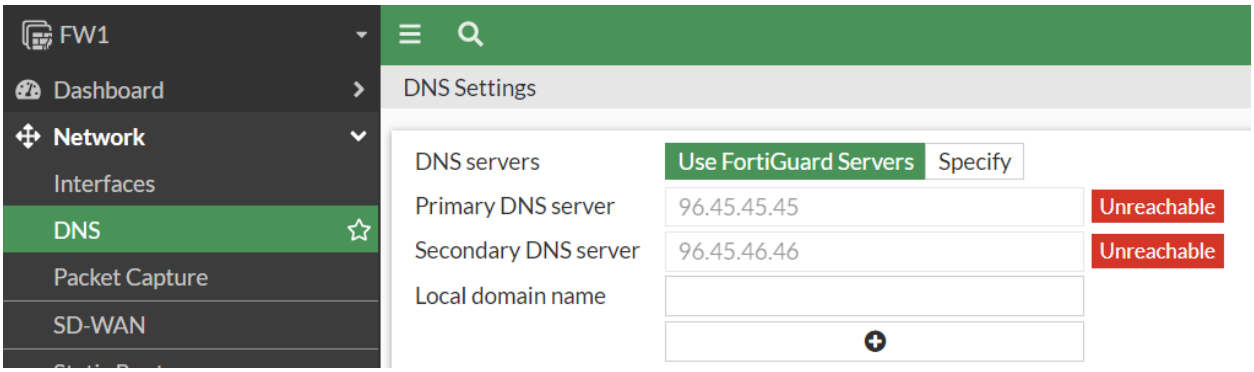


In Alias type MGMT, leave all the rest of configuration default and press OK button.

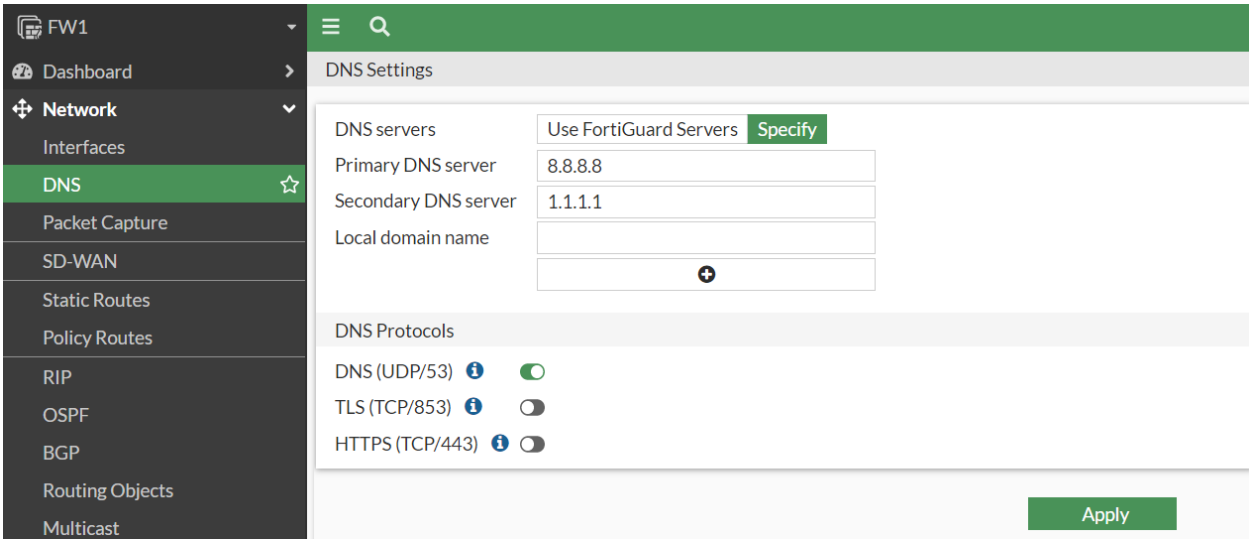


DNS Configuration:

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

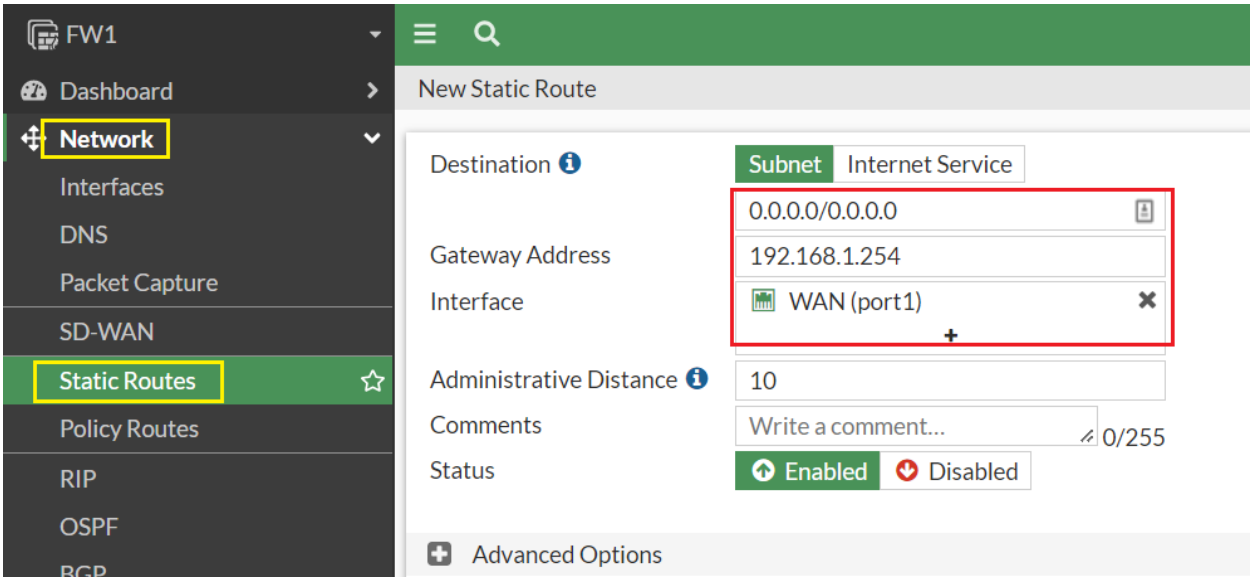


It is possible to specify using different DNS server, click on Specify and enter in primary / secondary DNS servers. In Primary DNS Server, type the IP address of the primary DNS server 8.8.8.8. In Secondary DNS Server, type the IP address of the secondary DNS server 1.1.1.1. Click Apply button to save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

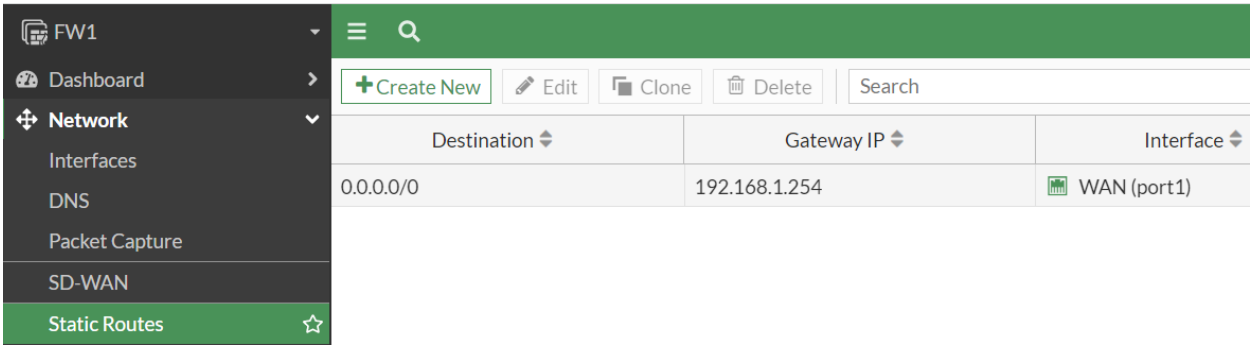


Default Route Configuration:

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 192.168.1.254 which the Gateway. Set the Interface to the WAN interface. Press OK to Save the changes.

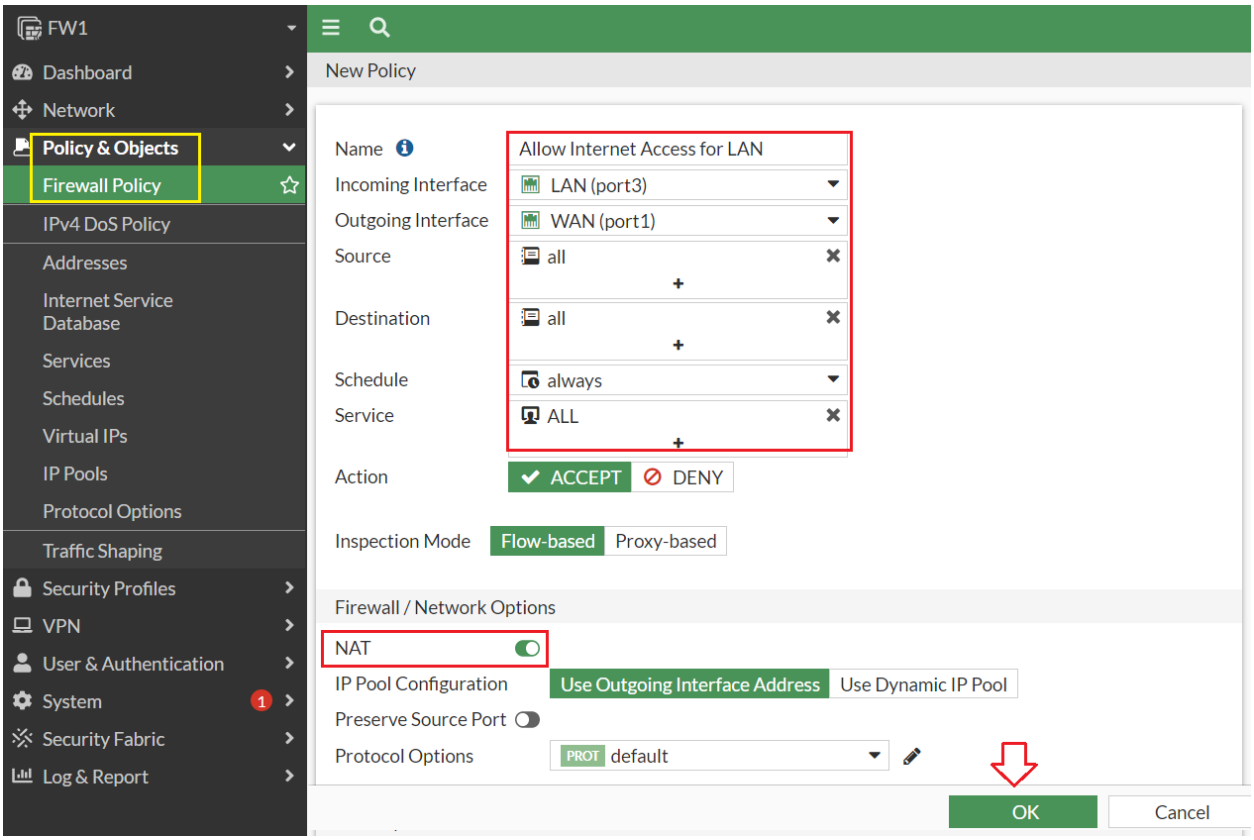


Go back to Network> Static Routes to see the configure routes, Finally, look like below.

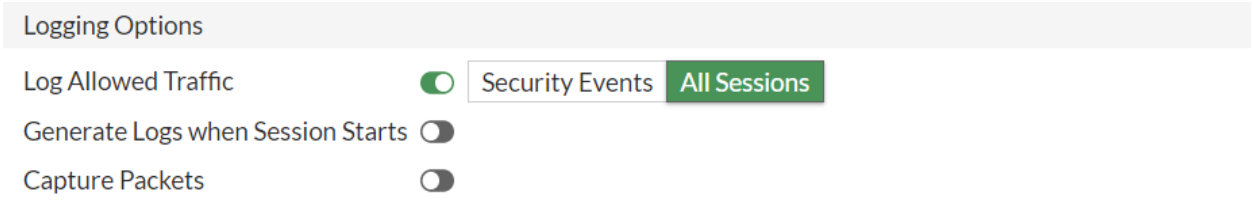


Creating a Policy:

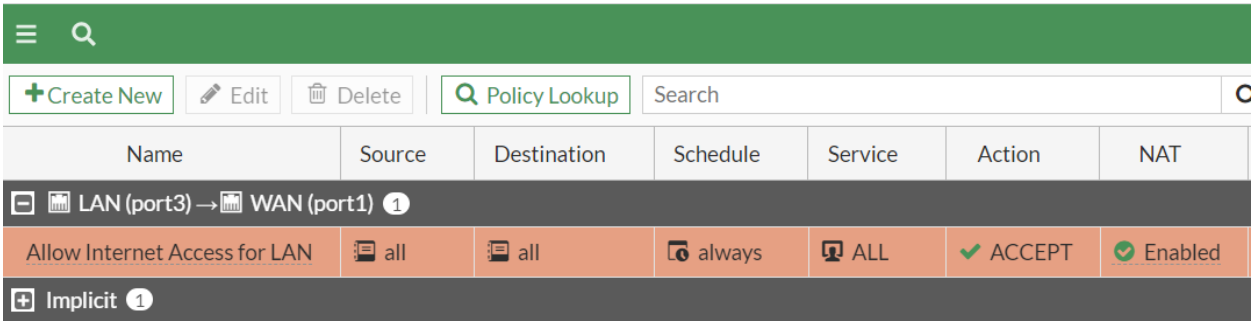
To create a new policy, go to Policy & Objects > Firewall Policy. Give the policy a Name that indicates that the policy will be for traffic to the Internet in my case it is Allow-All. Set the Incoming Interface to LAN and the Outgoing Interface to WAN. Set Source, Destination Address, Schedule, and Services, 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.

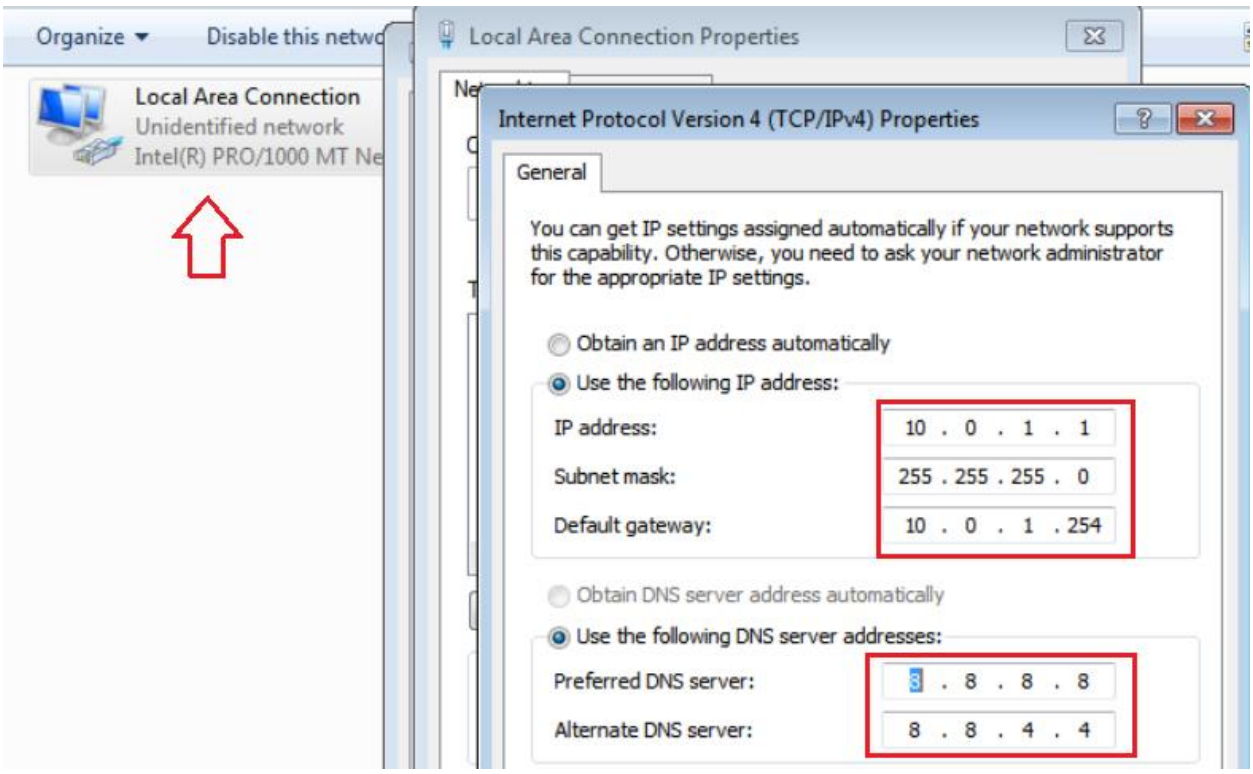


Go back to Policy & Objects > Firewall Policy to see the configure Policy, Finally, look like below.

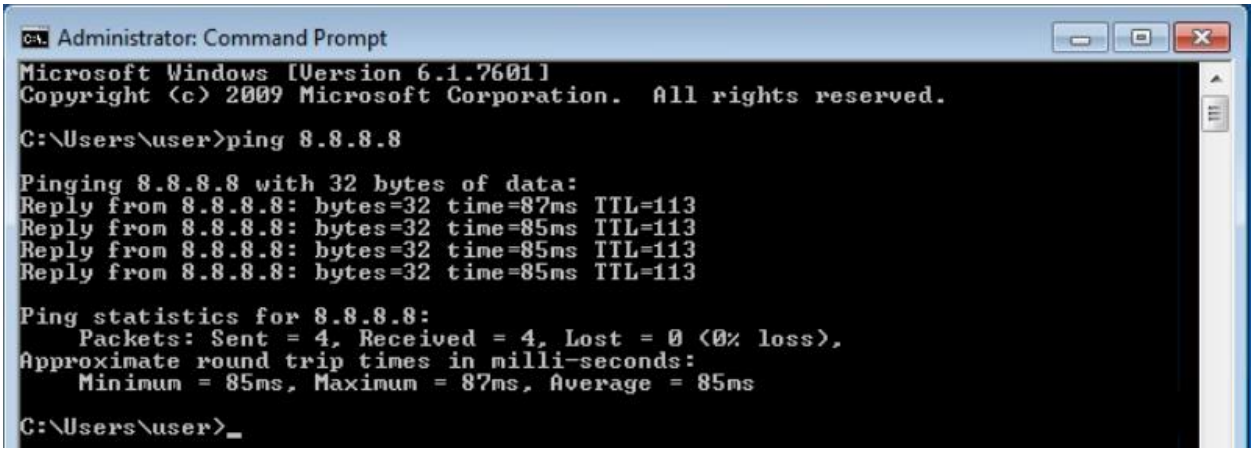


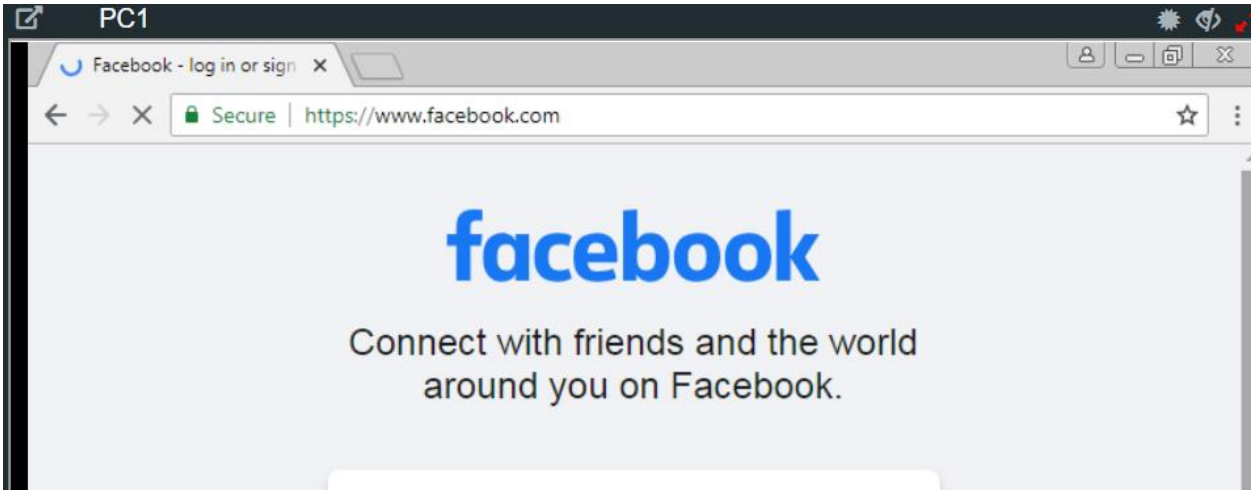
Configure LAN PC:

assign static IP and details.

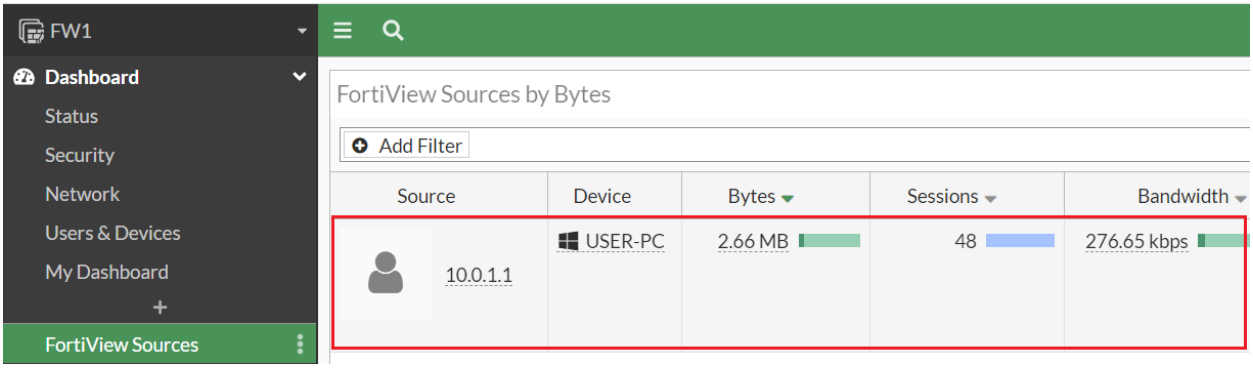


Browse the Internet using the PC on the internal network.

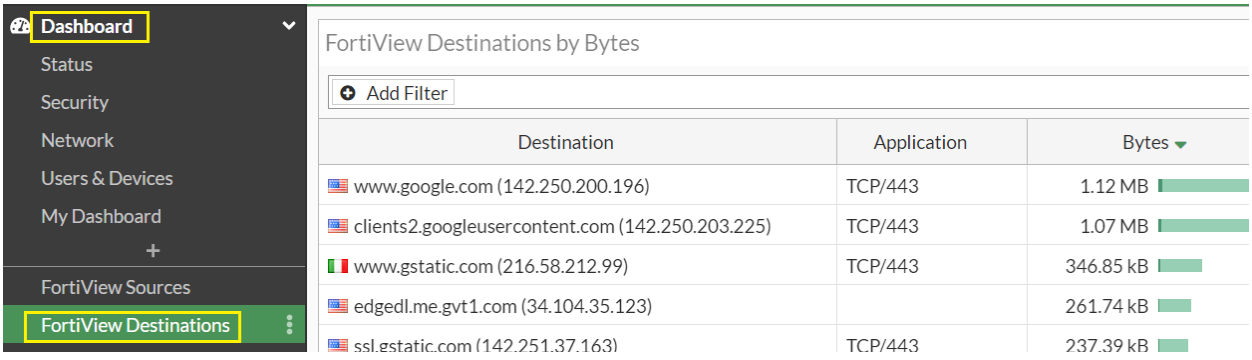




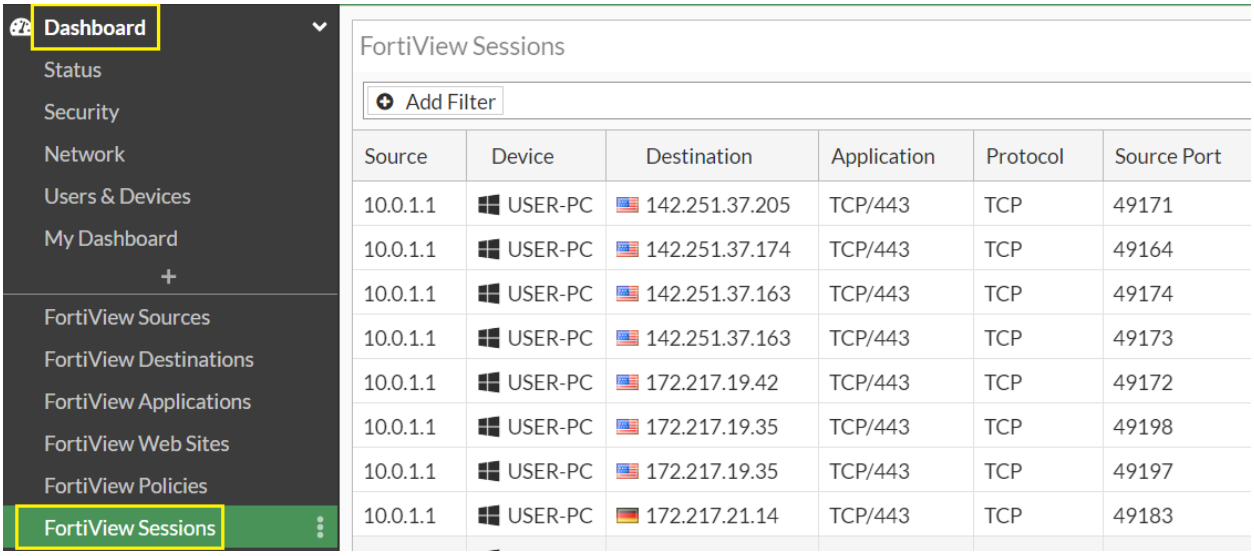
To view information about FortiGate traffic, go to Dashboard >FortiView Sources. The PC appears on the list of sources.



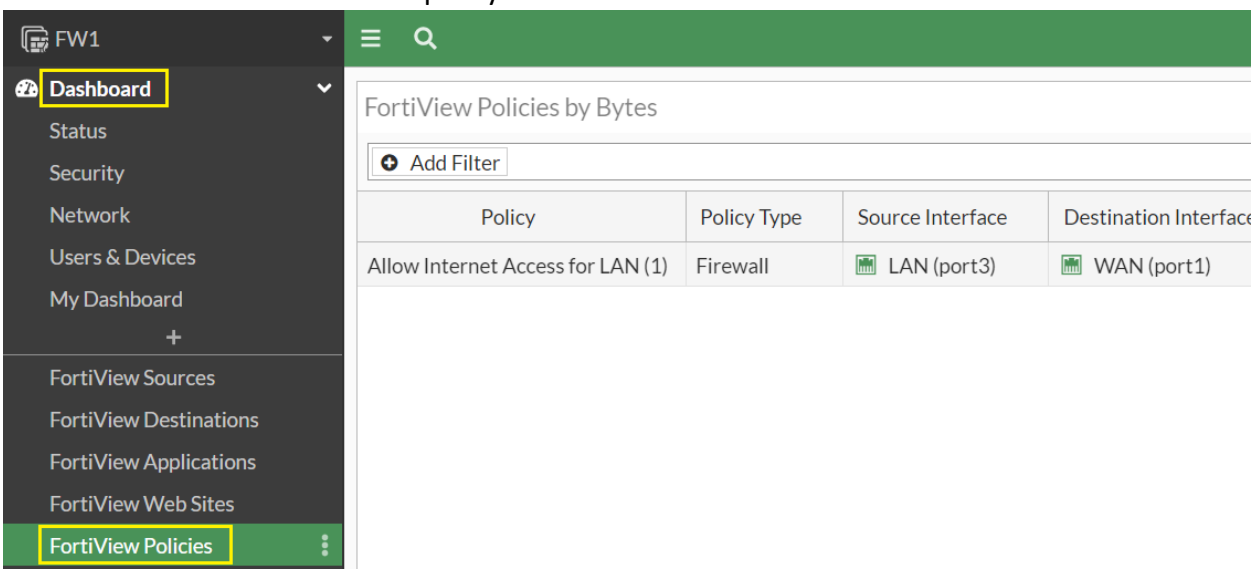
To view information about FortiGate traffic, go to Dashboard > FortiView Destinations. The appears on the list of Destinations.



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.