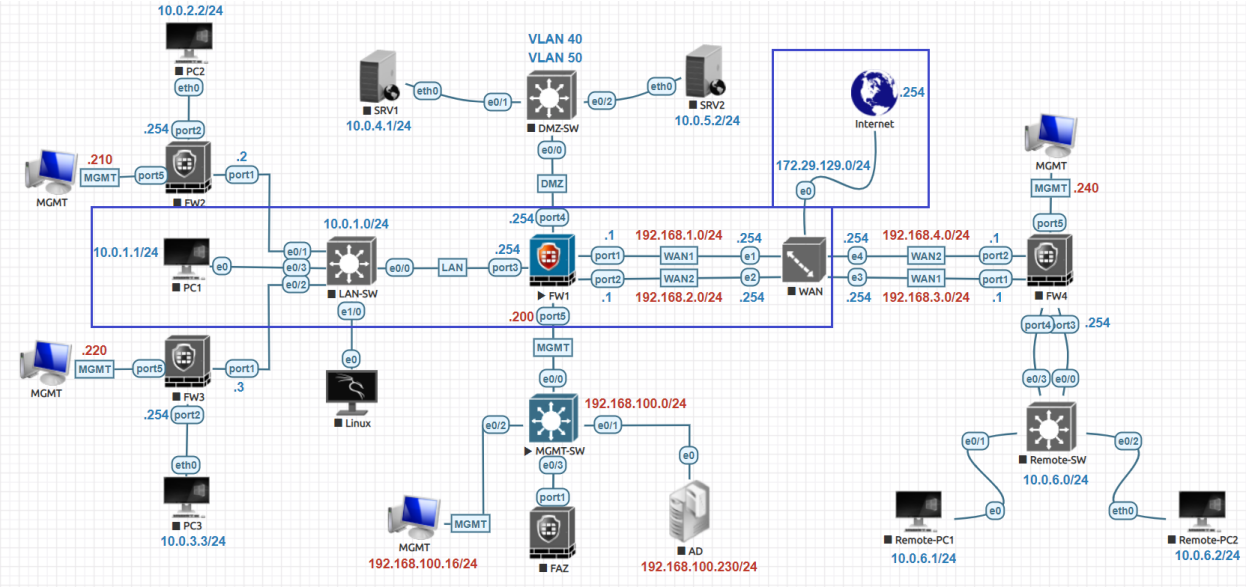
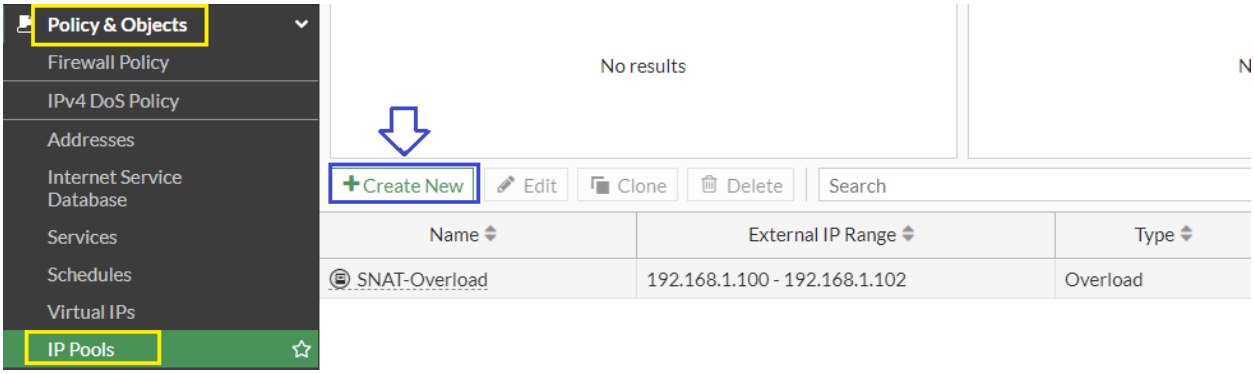
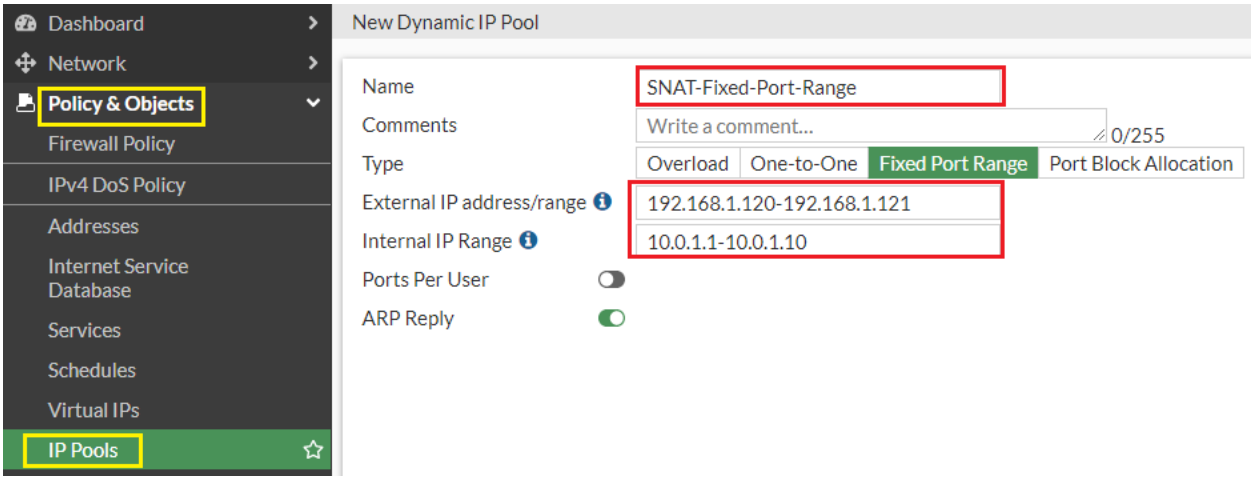
Policy Source Fixed Port Range NAT Lab:

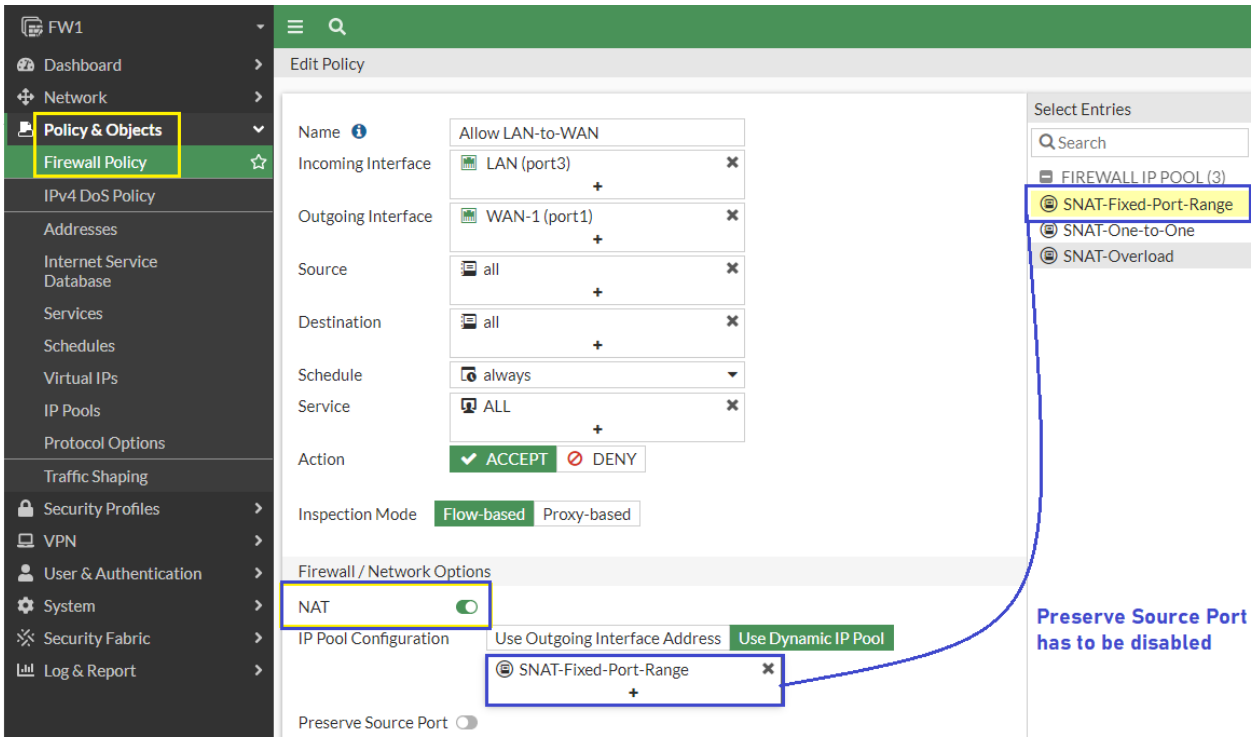


First, to create the IP Pool, or Fixed Port Range NAT pool. Navigate to Policy & Objects > IP Pools and click Create New Enter a descriptive name, click Fixed Port Range and enter the external IP address want applied for this pool in this case (192.168.1.120-192.168.1.121).



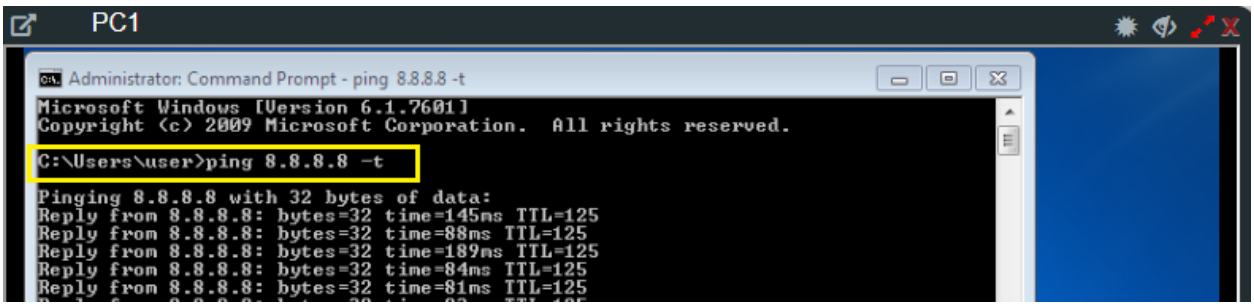


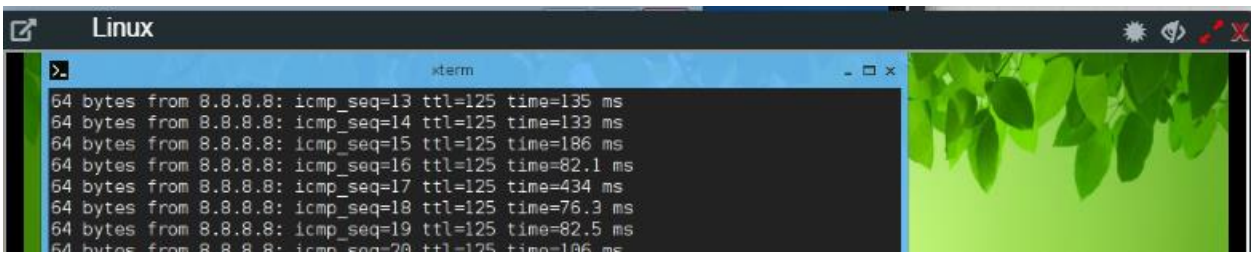
Let's go back to Policy & Objects > Firewall Policy Enable NAT and Change the IP Pool Configuration to Use Dynamic IP Pool & select IP Pool created earlier (SNAT-Fixed-Port-Range).



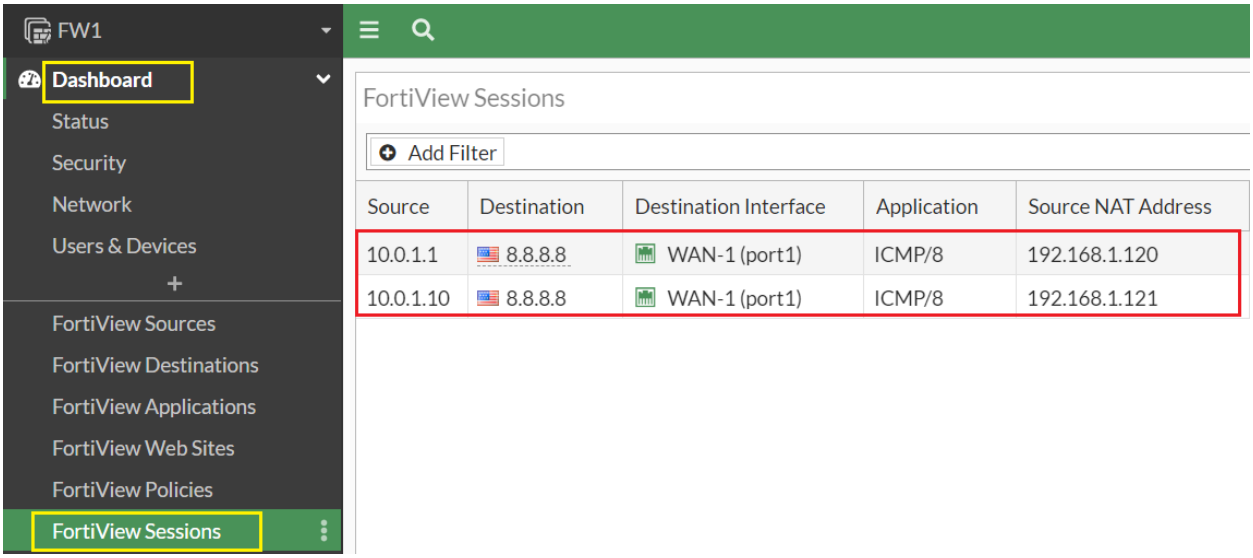
Verification & Testing:

When the clients in internal network need to access servers in external network, we need to translate IP addresses from 10.0.1.0/24 to IP address 192.168.1.120 – 192.168.1.121. For packets that match this policy, its source IP address is translated to the IP address of the outgoing range 192.168.1.120 – 192.168.1.121. Let's visit from internal PCs to external.

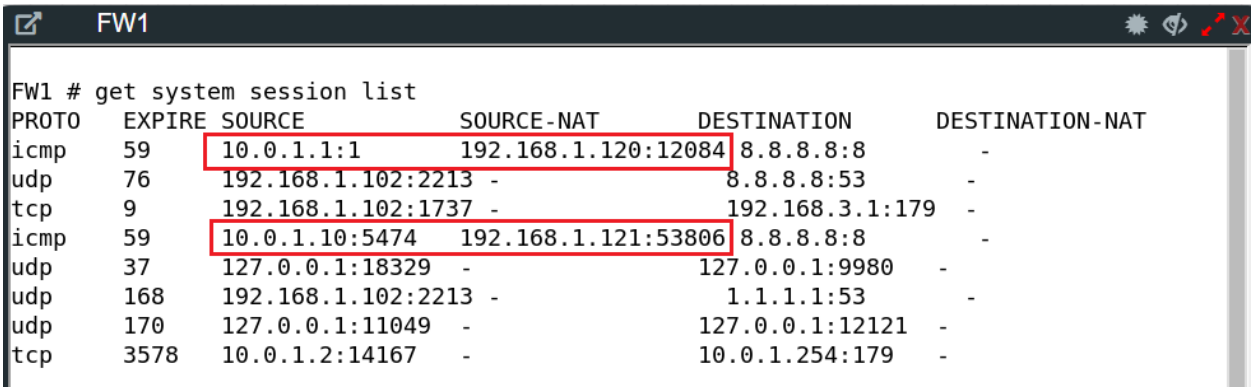




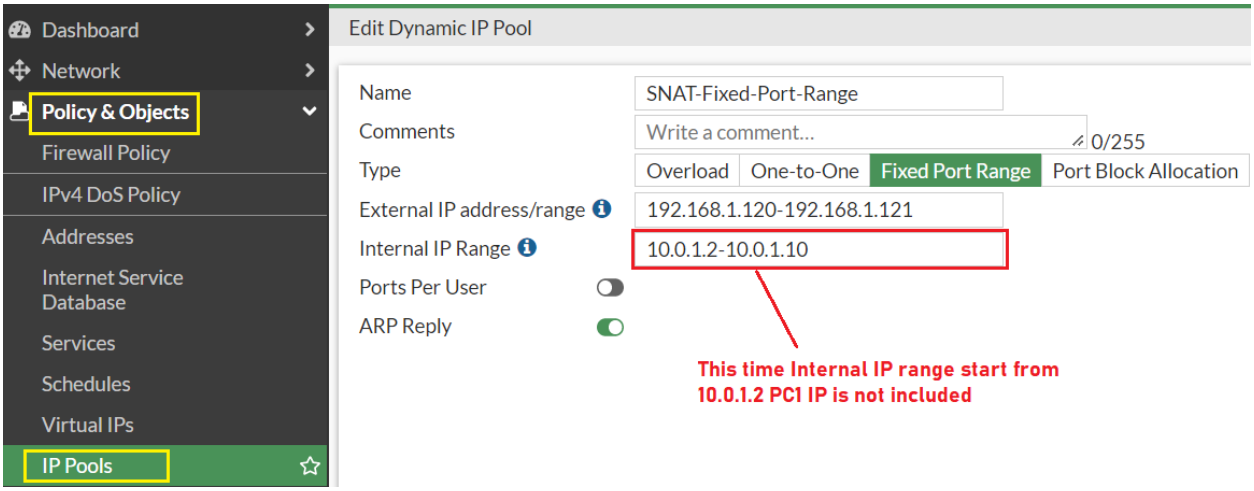
Let's go to Dashboard>FortiView Session better to Apply Filter for best view.



Let's verify through FortiGate Firewall CLI command get system session list.



Let's go back to Policy & Objects > IP Pools and edit Fixed Port Range entries and change the Internal IP Range to 192.168.1.1-192.168.1.3 this time 192.168.1.4 is not included.



Communication is not working anymore from PC1 IP 10.0.1.1 because it's not included in Internal IP Range of Fixed Port Range.