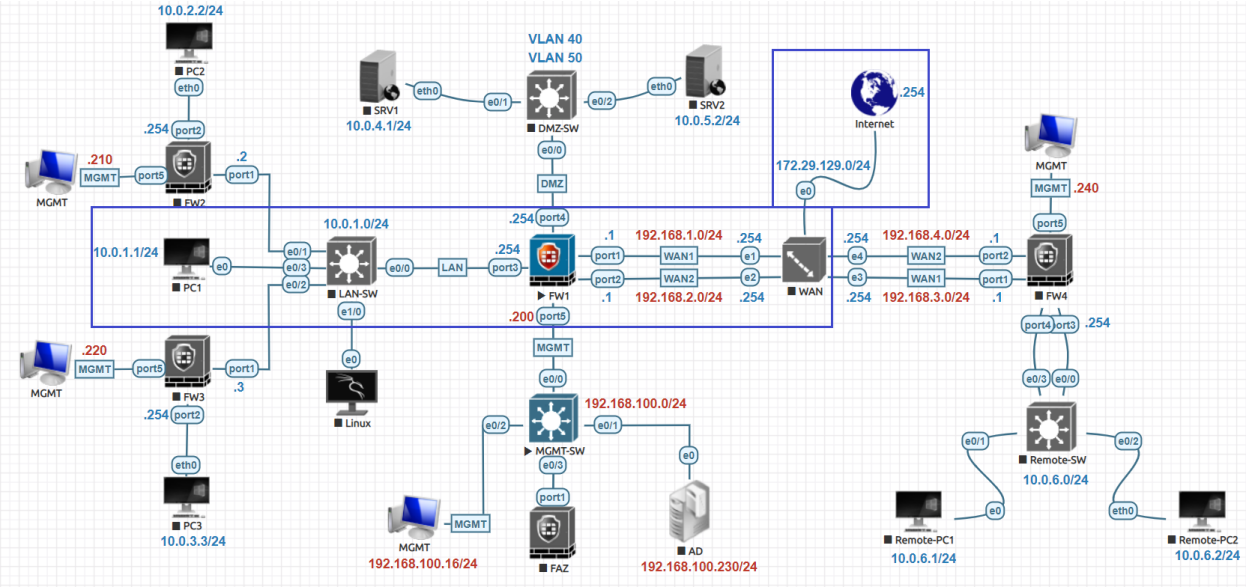
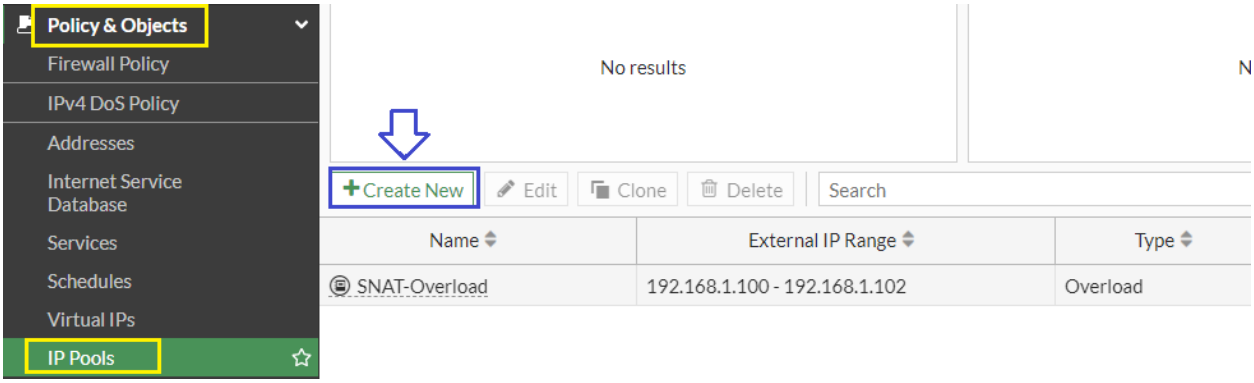
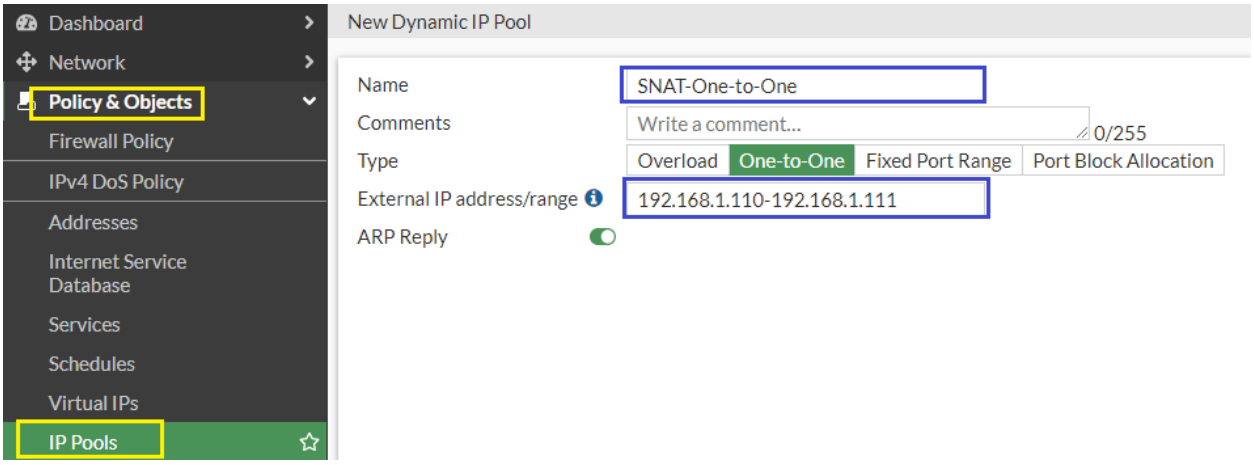
Policy Source One-To-One NAT Lab:

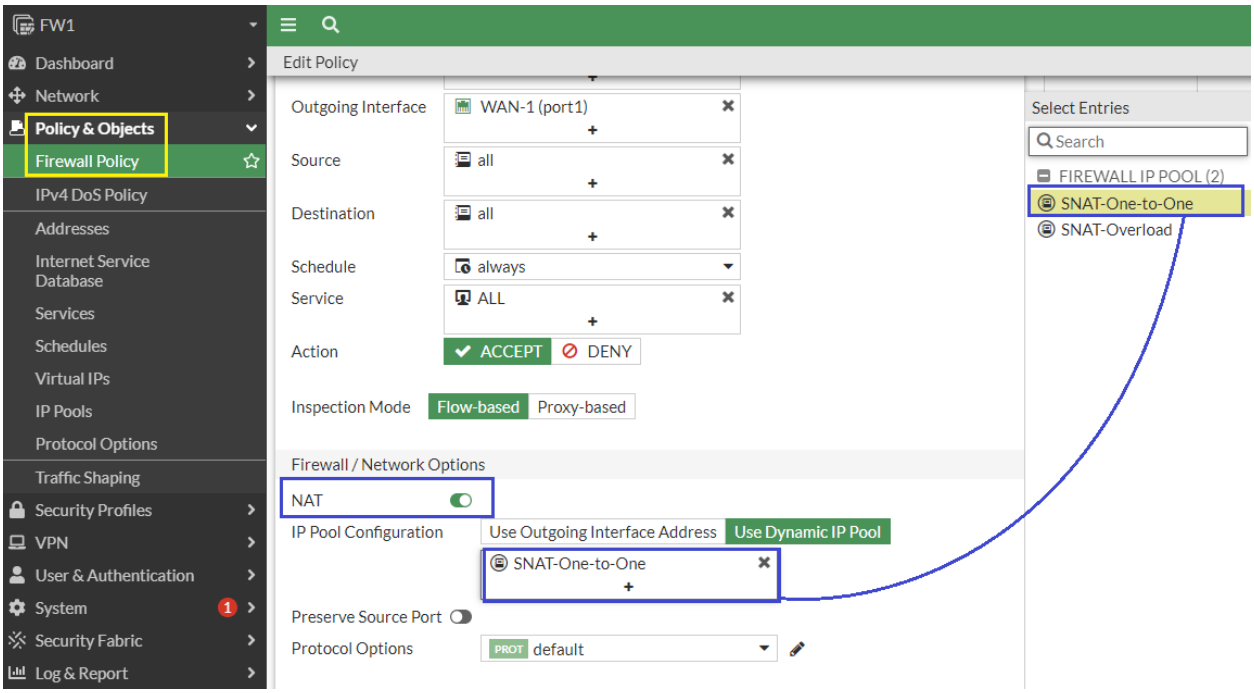


First, to create the IP Pool, or one-to-one NAT pool. Navigate to Policy & Objects > IP Pools and click Create New Enter a descriptive name, click One-to-One and enter the external IP address you want applied for this pool in this case (192.168.1.110-192.168.1.111).



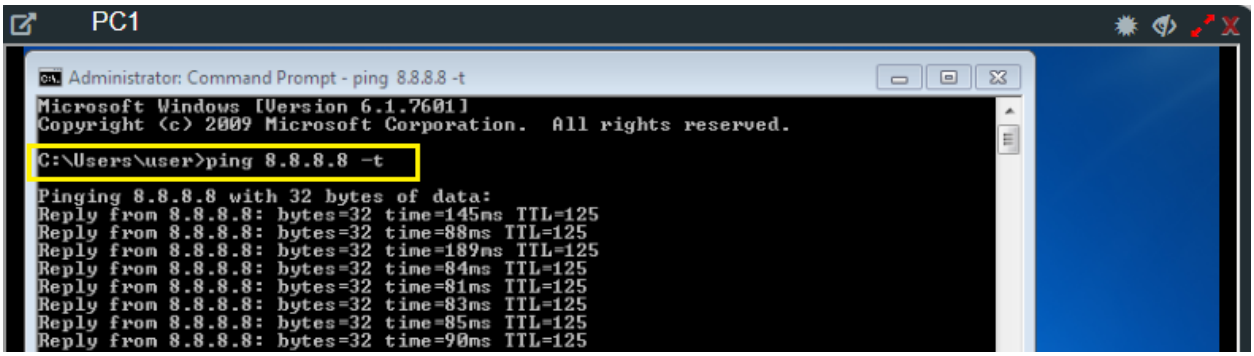


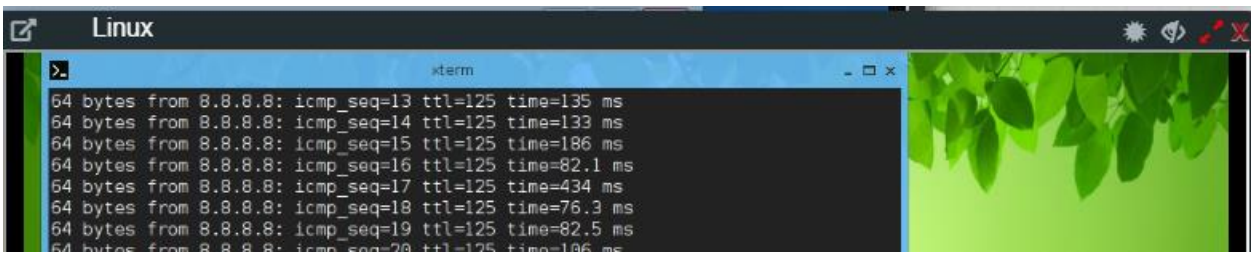
Let's go back to Policy & Objects > Firewall Policy Enable NAT and Change the IP Pool Configuration to Use Dynamic IP Pool and select the IP Pool created earlier (SNAT-One-to-One).



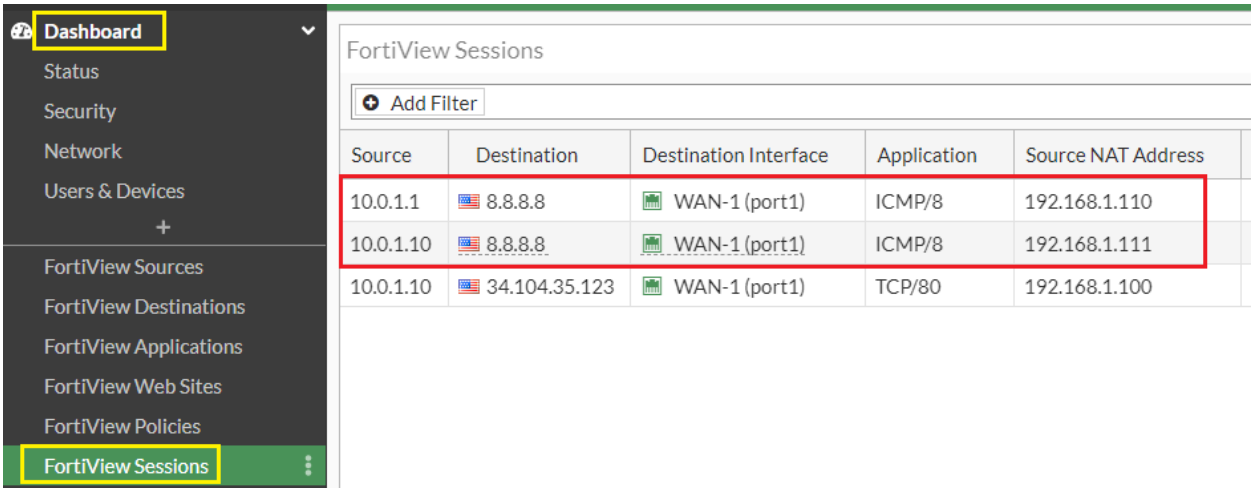
Verification & Testing:

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 192.168.1.110 – 192.168.1.111. For packets that match this policy, its source IP address is translated to the IP address of the outgoing range 192.168.1.110 – 192.168.1.111. Let's visit from Internal PCs to external.

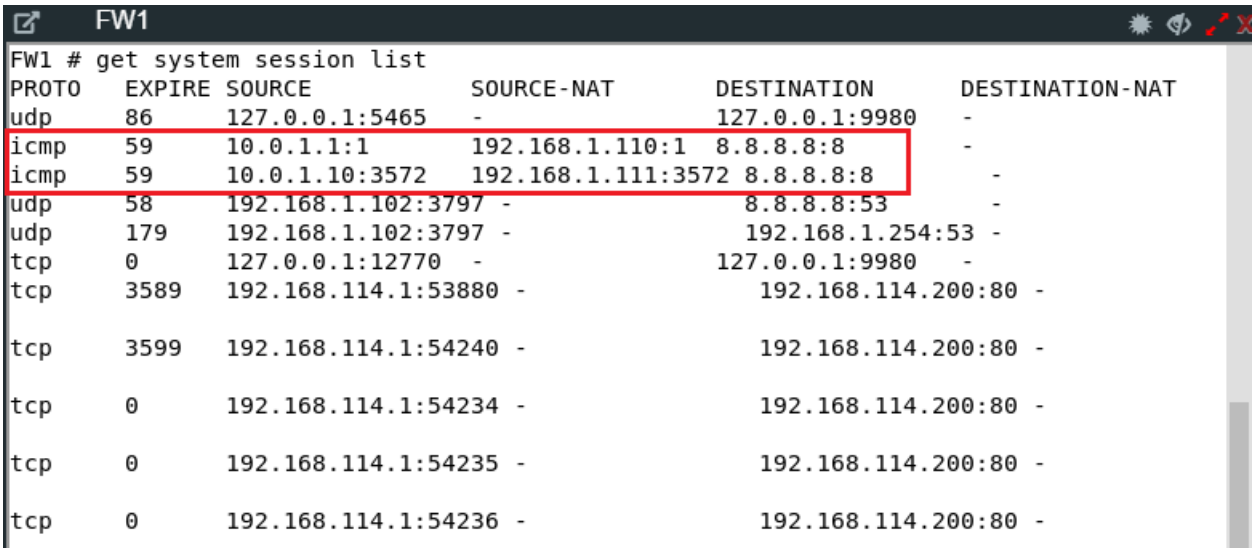




Let's go to Dashboard>FortiView Session better to Apply Filter for best view.



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



If you connect third system and try to access external network, it will not work because this one to one mapping and we have two IPs in the pool which is already used.