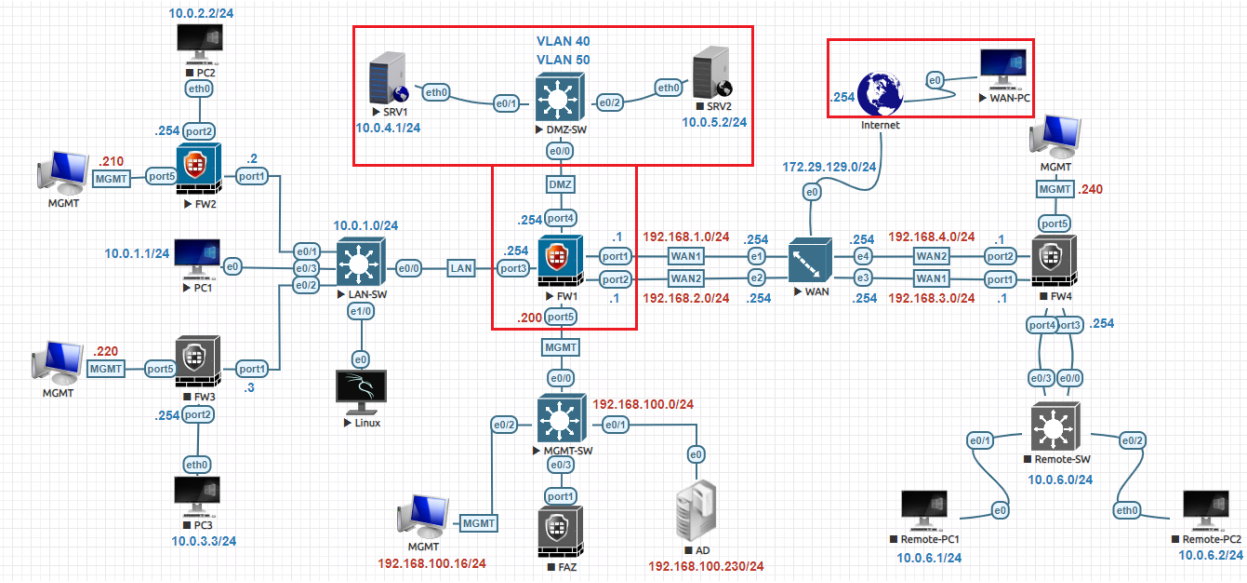
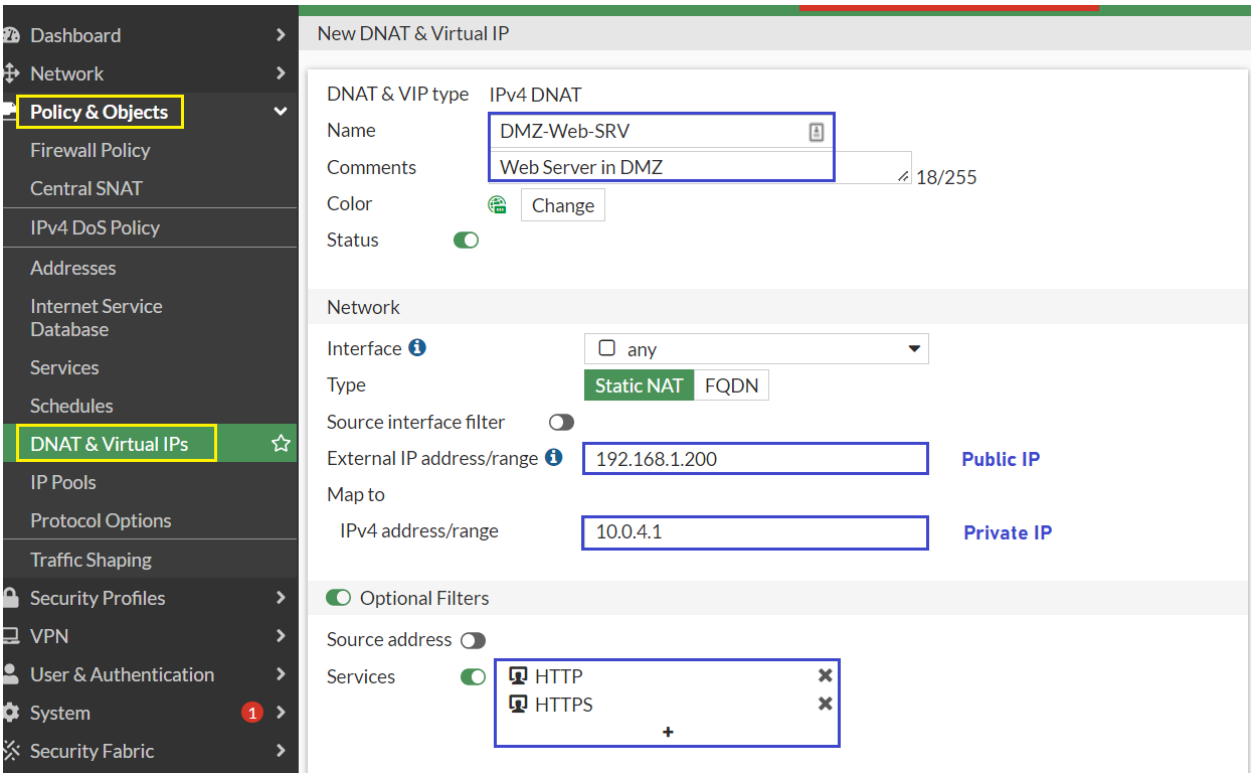
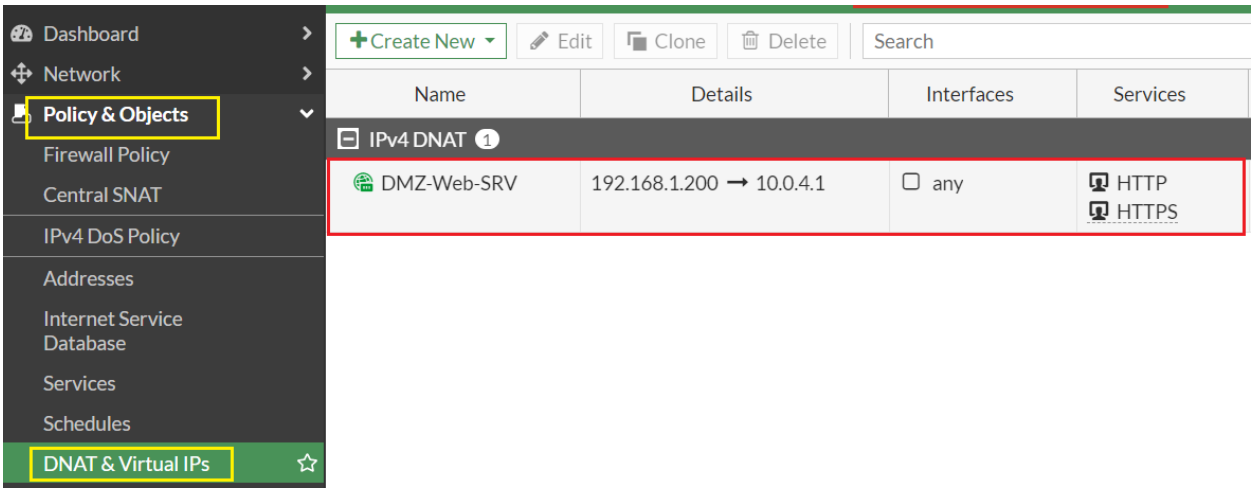
Destination NAT Lab:



VIP with Services:

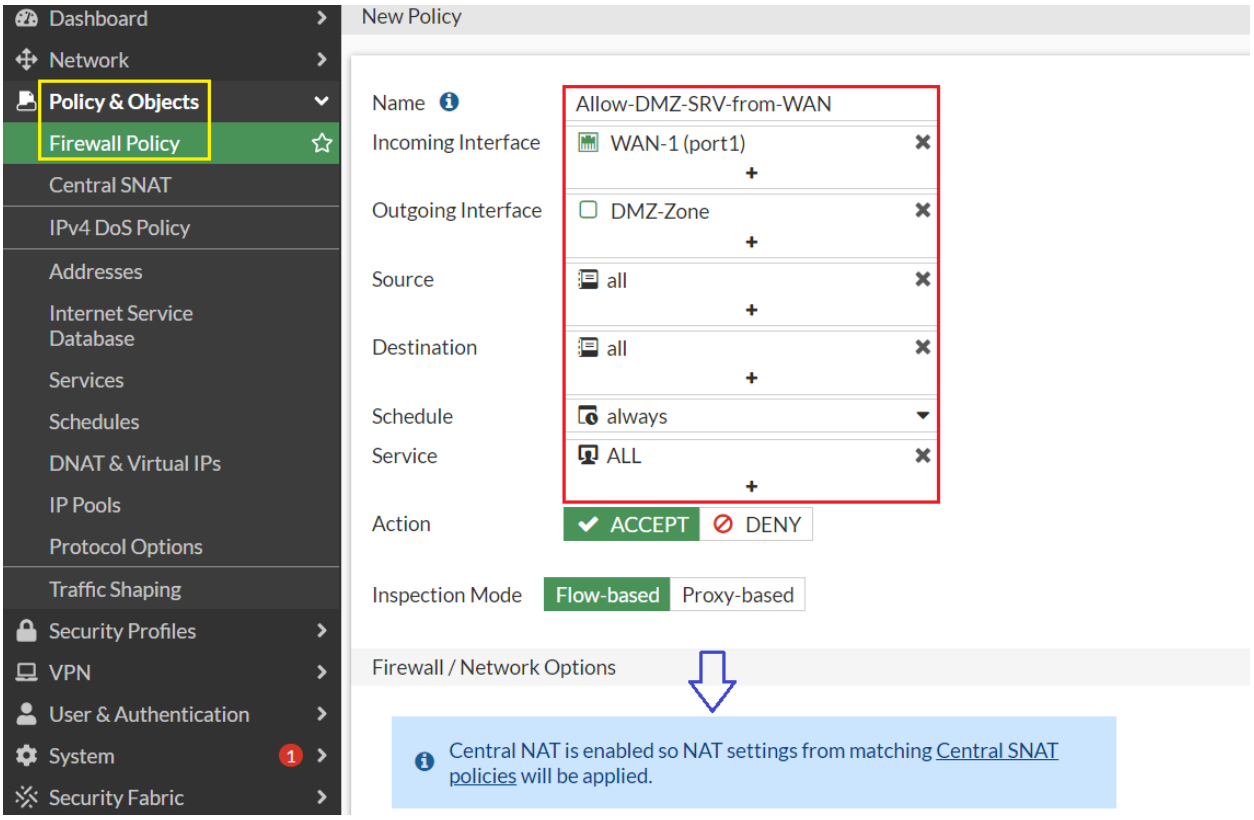
To create a virtual IP, go to Policy & Objects > DNAT & Virtual IPs Click Create New and select DNAT & Virtual IP. Enter a unique name for the virtual IP and fill in the other fields. Click OK.





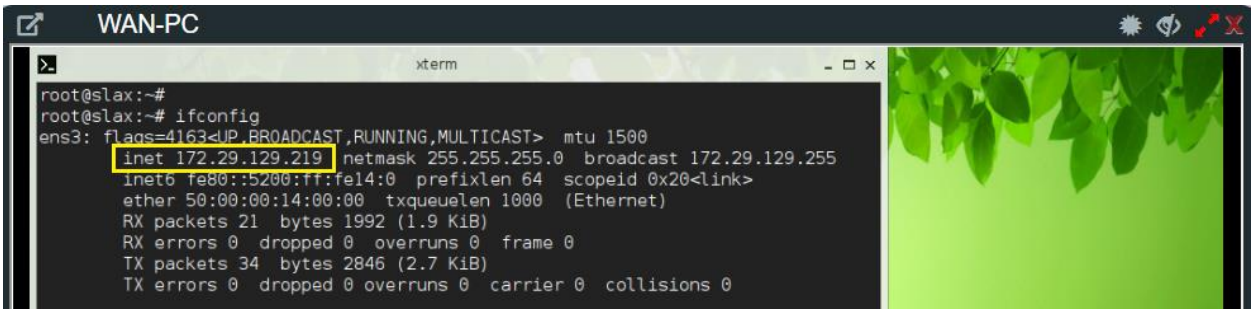
Creating Security Policy:

After finishing create the Virtual IP then Create the Policy. Go to Policy & Objects > Firewall Policy and create a security policy allowing access to a server behind the firewall. Set Incoming Interface to your Internet-facing interface, Outgoing Interface to interface connected to server.

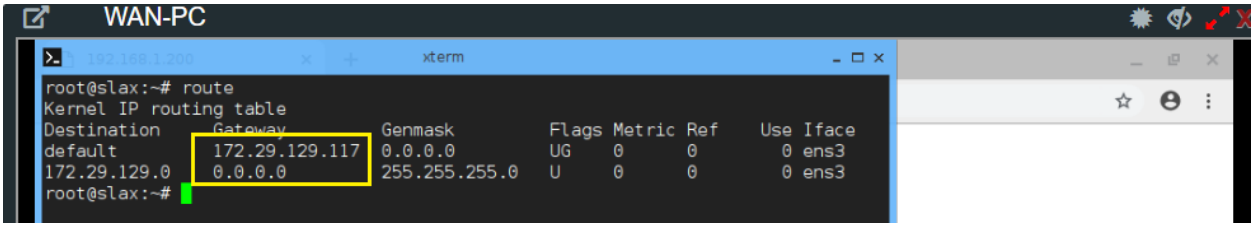


Verification & Testing:

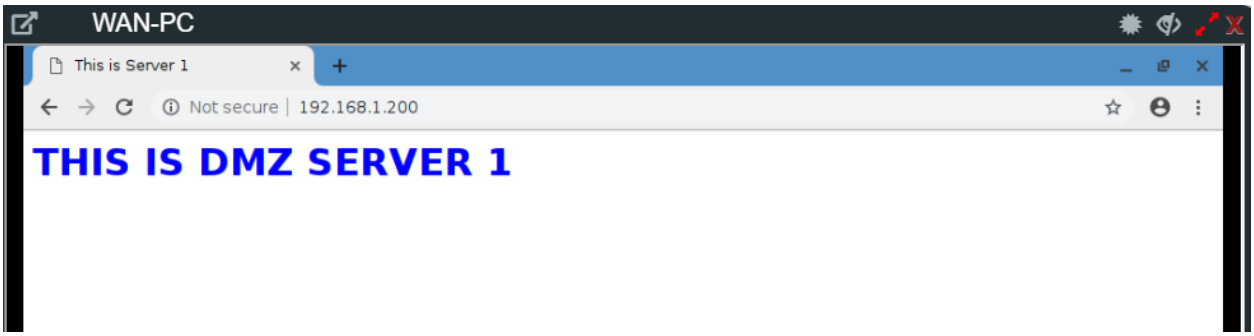
Let's verify External WAN PC IP address connected to Internet Cloud.

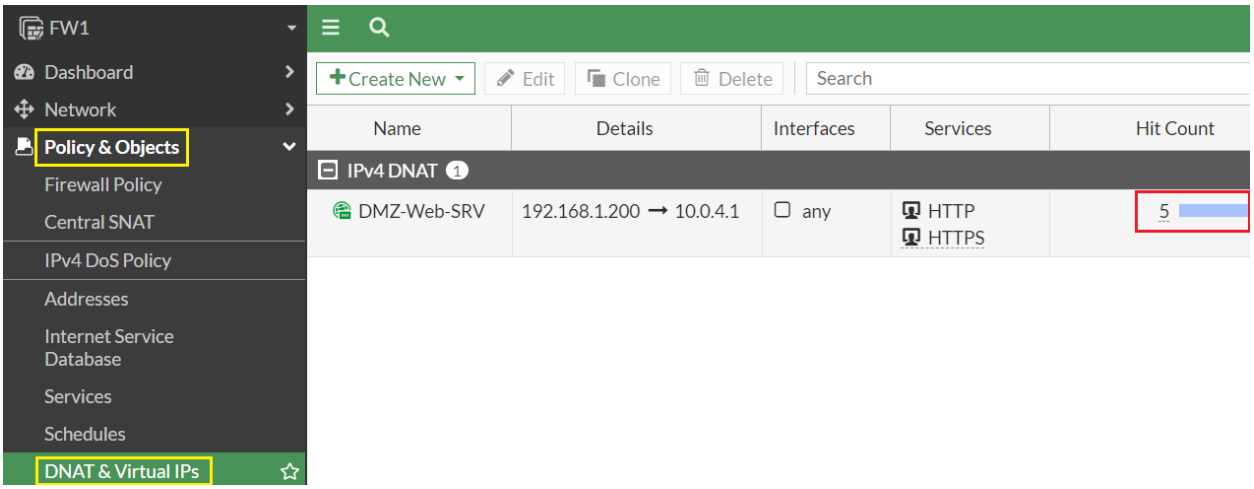


Let's verify External WAN PC Default Gateway in this case it should be your WAN public IP.

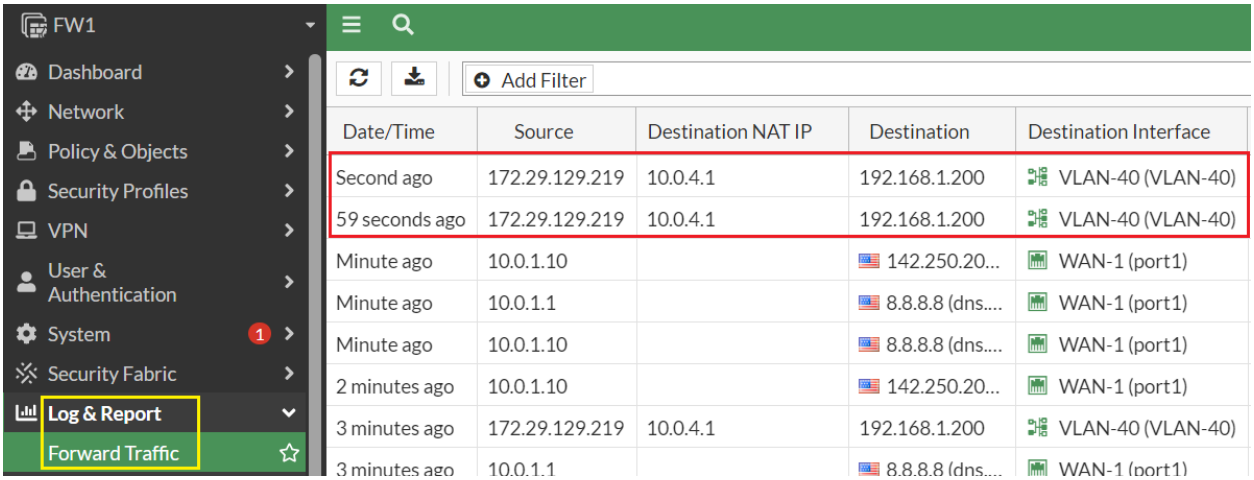


To ensure that TCP port 80 is open, connect to the web server from a remote connection on the other side of the firewall hit public IP of the Firewall 192.168.1.200.

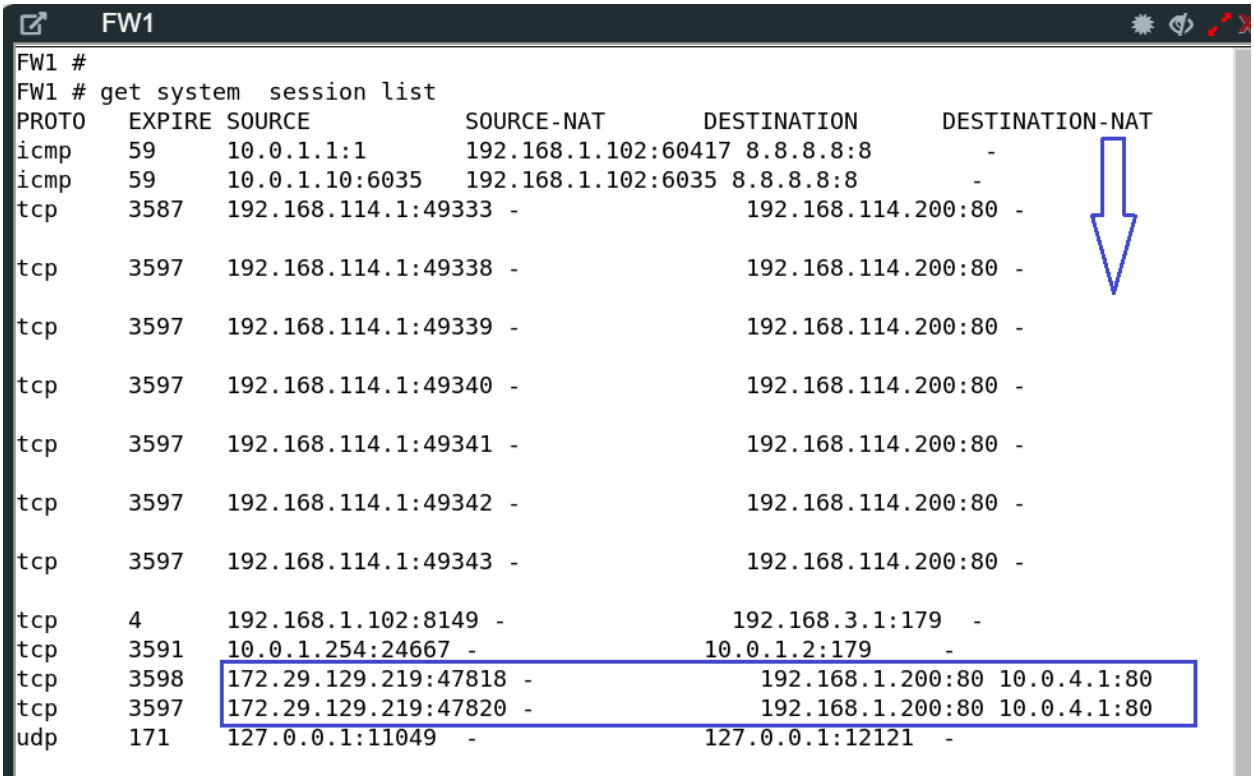




Let's go to Logs & Report> Forward Traffic to see Destination NAT Address Translation.



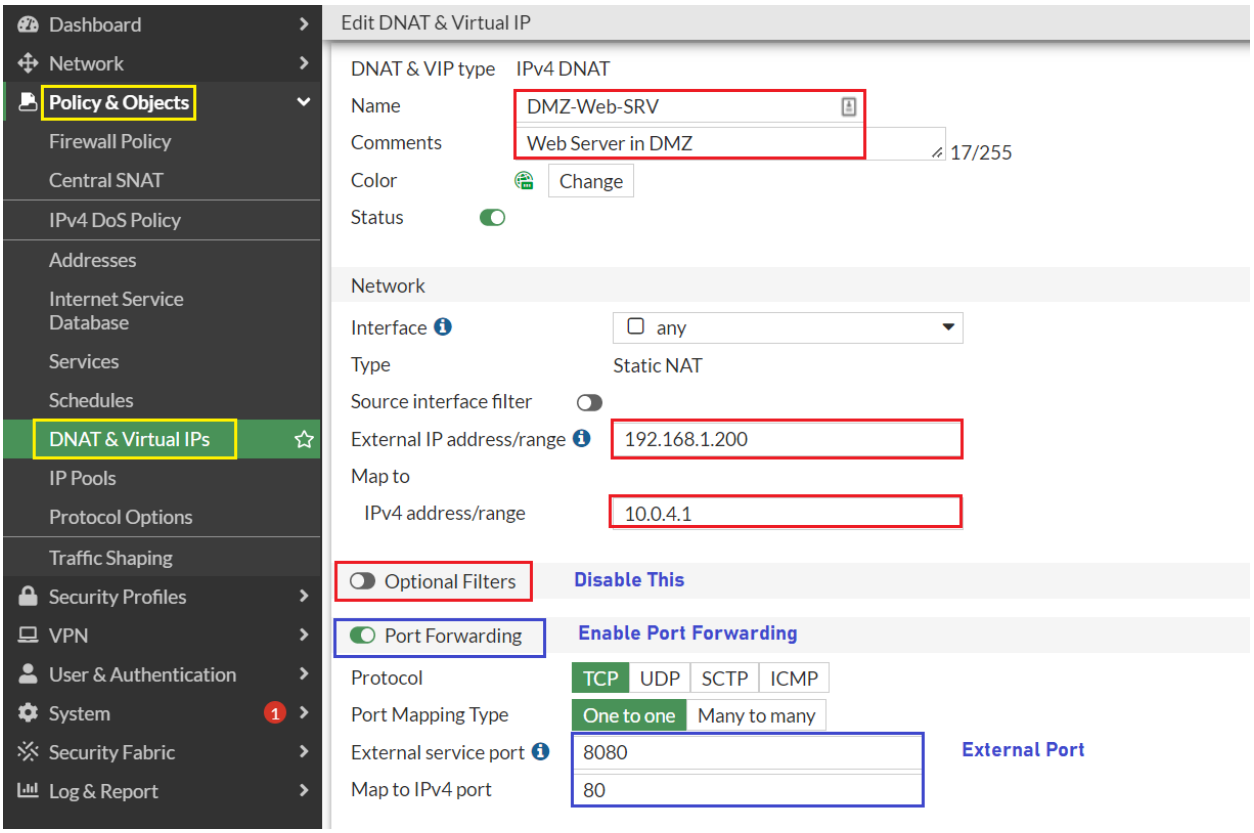
Let's verify through FortiGate Firewall CLI command get system session list.



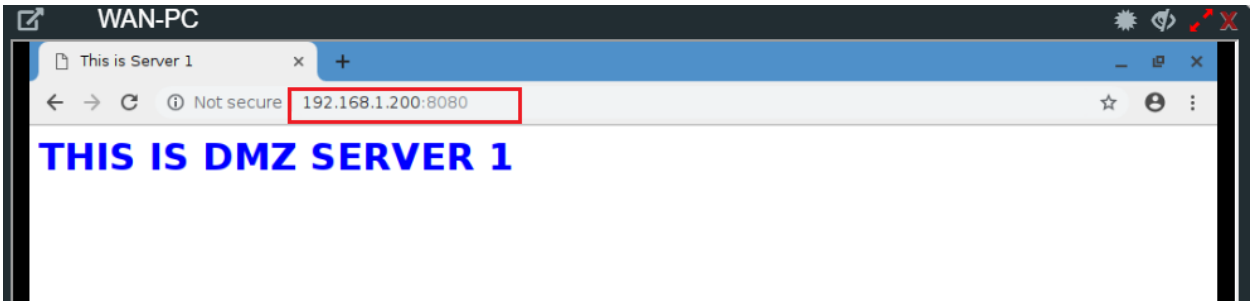
VIP with Port Forwarding:

To create a virtual IP, go to Policy & Objects > DNAT & Virtual IPs Click Create New and select DNAT & Virtual IP. Enter a unique name for the virtual IP and fill in the other fields.

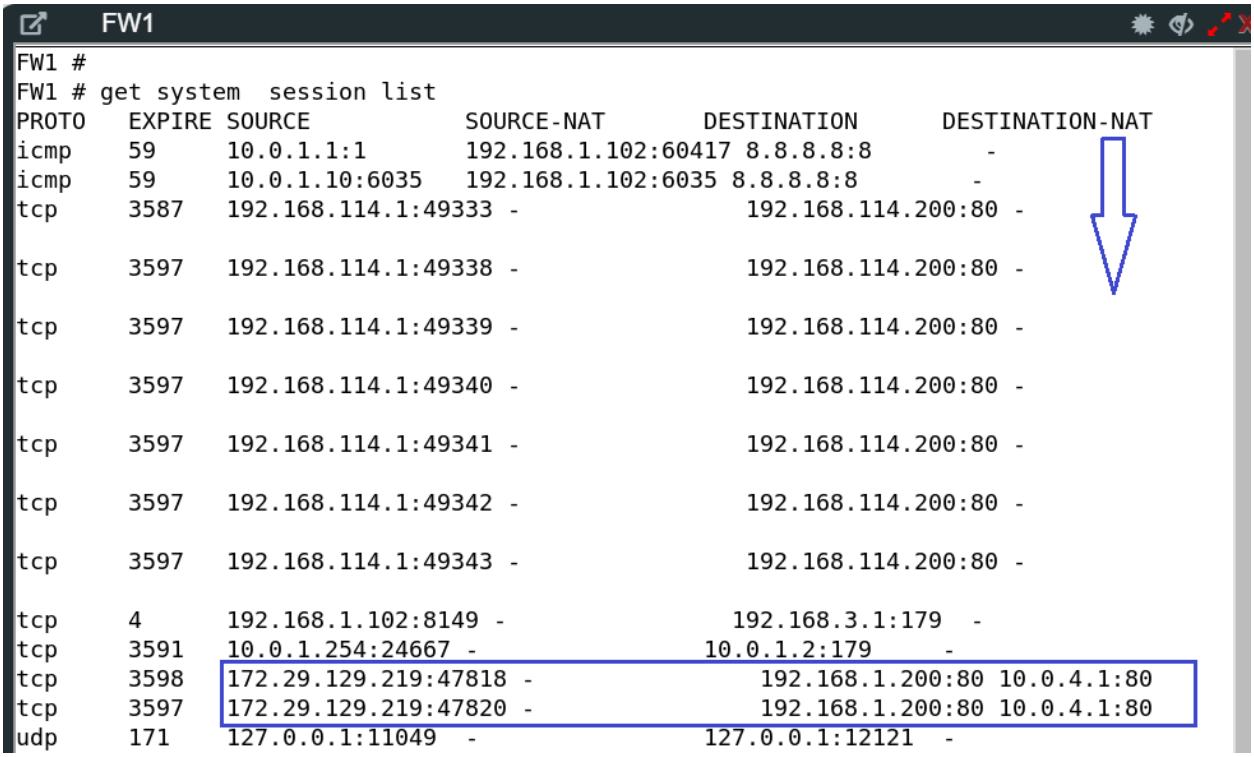
Field	Value
VIP Type	IPV4 DNAT
Name	DMZ-Web-SRV
Comments	Web Server in DMZ
Color	Choose any color you like in this case green
Interface	any
Type	Static NAT (Default Setting)
External IP Address/Range	192.168.1.200 (External IP of Firewall)
Mapped IP Address/Range	10.0.4.1 (Internal IP Address of DMZ Server)
Enable Port Forwarding	Slide to enable
External Service port	8080
Map to IPv4 port	80



Verification & Testing:



Also, can be verify from CLI type command: get system session list



Let's go to Logs & Report> Forward Traffic to see Destination NAT Address Translation.