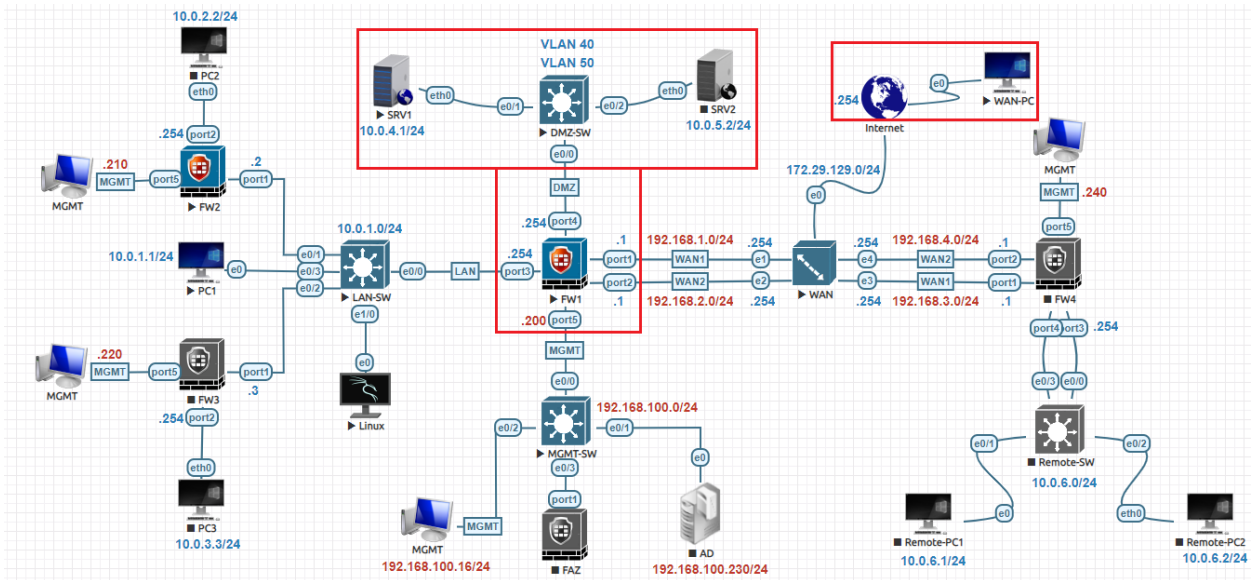
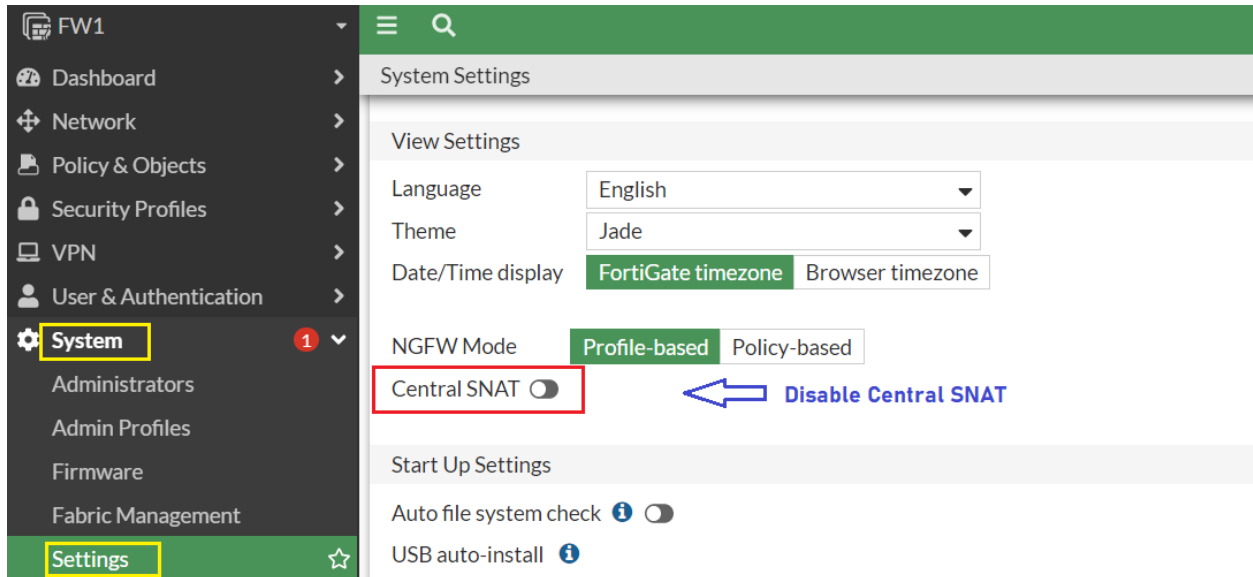


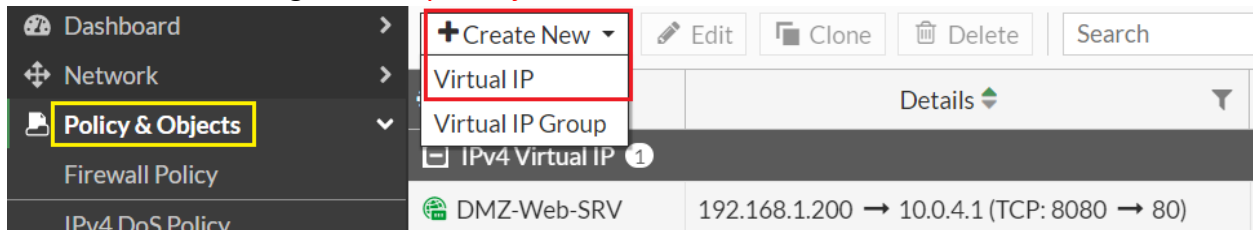
Create VIP Without Central SNAT:



Let's Disable Central SNAT first navigate to **System>Settings >View Settings** click **OK**.



To create a virtual IP, go to **Policy & Objects > Virtual IPs** Click **Create New** and select **Virtual IP**.



Enter a unique name for the virtual IP and fill in the other fields.

Field	Value
VIP Type	IPV4
Name	DMZ-Web-SRV2
Comments	Web Server 2 in DMZ
Color	Choose any color you like.
Interface	any
Type	Static NAT (Default Setting)
External IP Address/Range	192.168.1.201 (External IP address of Firewall)
Mapped IP Address/Range	10.0.5.2 (Internal IP Address of FTP Server)
Services	HTTP and HTTPS

Configuration details for the Virtual IP:

- VIP type: IPv4
- Name: DMZ-Web-SRV2
- Comments: Web Server 2 in DMZ
- Color: (Change button)
- Interface: any
- Type: Static NAT
- External IP address/range: 192.168.1.201
- Map to IPv4 address/range: 10.0.5.2
- Optional Filters:
 - Source address: (Off)
 - Services: HTTP, HTTPS
- Port Forwarding: (Off)

Name	Details	Interfaces
DMZ-Web-SRV	192.168.1.200 → 10.0.4.1 (TCP: 8080 → 80)	<input type="checkbox"/> any
DMZ-Web-SRV2	192.168.1.201 → 10.0.5.2	<input type="checkbox"/> any

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.

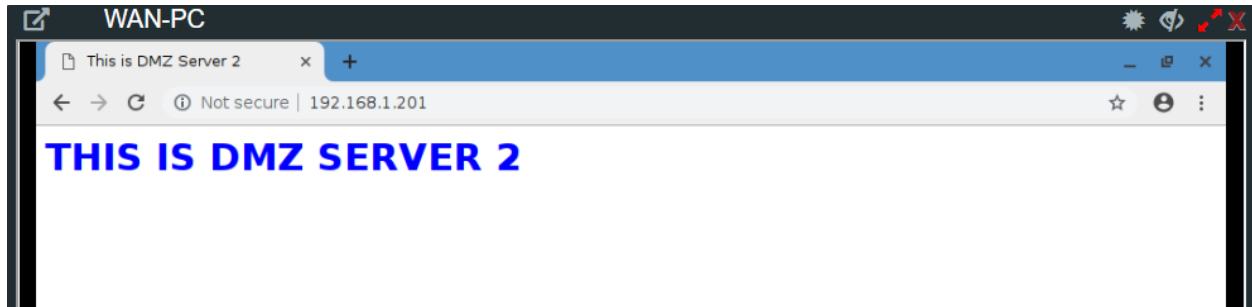
The screenshot shows the 'Edit Policy' configuration for a firewall policy. The policy name is 'Allow-DMZ-SRV-from-WAN'. The incoming interface is 'WAN-1 (port1)' and the outgoing interface is 'DMZ-Zone'. The source is 'all' and the destination is 'DMZ-Web-SRV2'. The schedule is 'always' and the service is 'ALL'. The action is 'ACCEPT'. The inspection mode is 'Flow-based'. The NAT option is checked. The protocol options are set to 'default'. A 'Select Entries' dialog is open, showing a list of entries with 'DMZ-Web-SRV2' selected.

Already created Virtual IP, go to **Policy & Objects > Virtual IPs** to verify.

Name	Details	Interfaces
DMZ-Web-SRV	192.168.1.200 → 10.0.4.1 (TCP: 8080 → 80)	<input type="checkbox"/> any
DMZ-Web-SRV2	192.168.1.201 → 10.0.5.2	<input type="checkbox"/> any

Verification & Testing:

To ensure that TCP port 80 is open, connect to the DMZ Web Server from a remote connection on the other side of the firewall hit public IP of the Firewall **192.168.1.201**



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

A screenshot of the firewall's 'Log & Report' interface, specifically the 'Forward Traffic' view. The interface shows a table with columns: Source, Destination NAT IP, Destination, Destination NAT Po..., and Destination Port. Two rows are highlighted with a red border, showing traffic from source 172.29.129.219 to destination NAT IP 10.0.5.2, which is translated to destination 192.168.1.201 on port 80.

Source	Destination NAT IP	Destination	Destination NAT Po...	Destination Port
172.29.129.219	10.0.5.2	192.168.1.201	80	80
172.29.129.219	10.0.5.2	192.168.1.201	80	80
10.0.1.1		8.8.8.8 (dns.go...		
10.0.1.10		8.8.8.8 (dns.go...		
10.0.1.1		172.217.171....		443
10.0.1.1		8.8.8.8 (dns.go...		443
10.0.1.10		147.78.237.1...		123
10.0.1.1		8.8.8.8 (dns.go...		

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

```
FW1 # get system session list
PROTO  EXPIRE  SOURCE          SOURCE-NAT      DESTINATION     DESTINATION-NAT
icmp   59      10.0.1.1:1     192.168.1.102:60417  8.8.8.8:8      -
icmp   59      10.0.1.10:6035 192.168.1.102:6035  8.8.8.8:8      -
udp    118     192.168.1.102:4221 -                192.168.1.254:53 -
udp    141     192.168.1.102:4197 -                8.8.8.8:53     -
udp    108     192.168.1.102:4221 -                8.8.8.8:53     -
udp    104     10.0.1.10:40599 192.168.1.102:40599 1.1.1.1:53     -
tcp    3561    192.168.114.1:49333 -                192.168.114.200:80 -
tcp    3596    192.168.114.1:50807 -                192.168.114.200:80 -
tcp    3588    10.0.1.254:24667 -                10.0.1.2:179   -
udp    119     192.168.1.102:4221 -                1.1.1.1:53     -
tcp    3594    172.29.129.219:53676 -                192.168.1.201:80 10.0.5.2:80
tcp    119     172.29.129.219:53674 -                192.168.1.201:80 10.0.5.2:80
tcp    3571    10.0.1.10:47682 192.168.1.102:47682 142.250.178.14:443 -
```