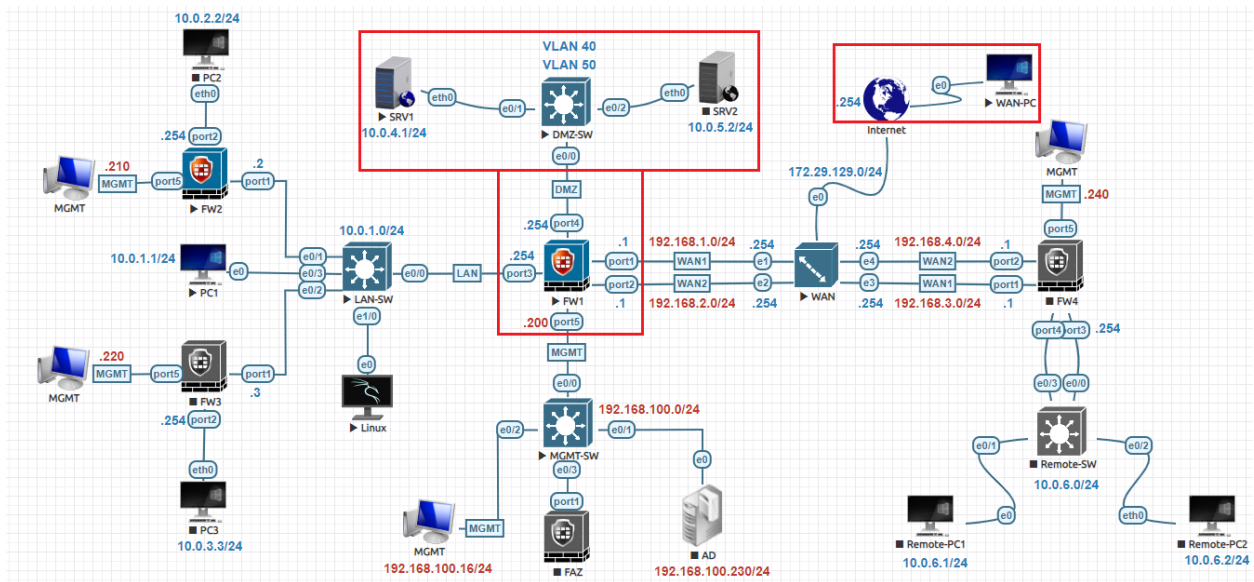


## Destination NAT Lab:



## 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**.

**Policy & Objects**

- Dashboard
- Network
- Policy & Objects**
  - Firewall Policy
  - Central SNAT
  - IPv4 DoS Policy
  - Addresses
  - Internet Service Database
  - Services
  - Schedules
  - DNAT & Virtual IPs**
  - IP Pools
  - Protocol Options
  - Traffic Shaping
- Security Profiles
- VPN
- User & Authentication
- System
- Security Fabric

**New DNAT & Virtual IP**

DNAT & VIP type: IPv4 DNAT

Name: DMZ-Web-SRV

Comments: Web Server in DMZ

Color:

Status:

**Network**

Interface:  any

Type:  Static NAT  FQDN

Source interface filter:

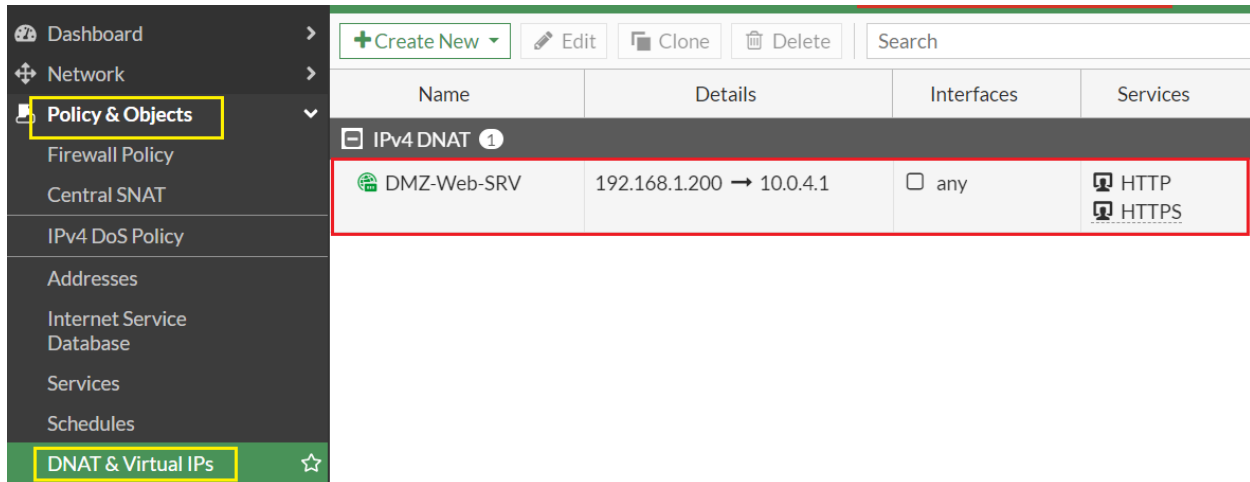
External IP address/range: 192.168.1.200 **Public IP**

Map to: IPv4 address/range: 10.0.4.1 **Private IP**

**Optional Filters**

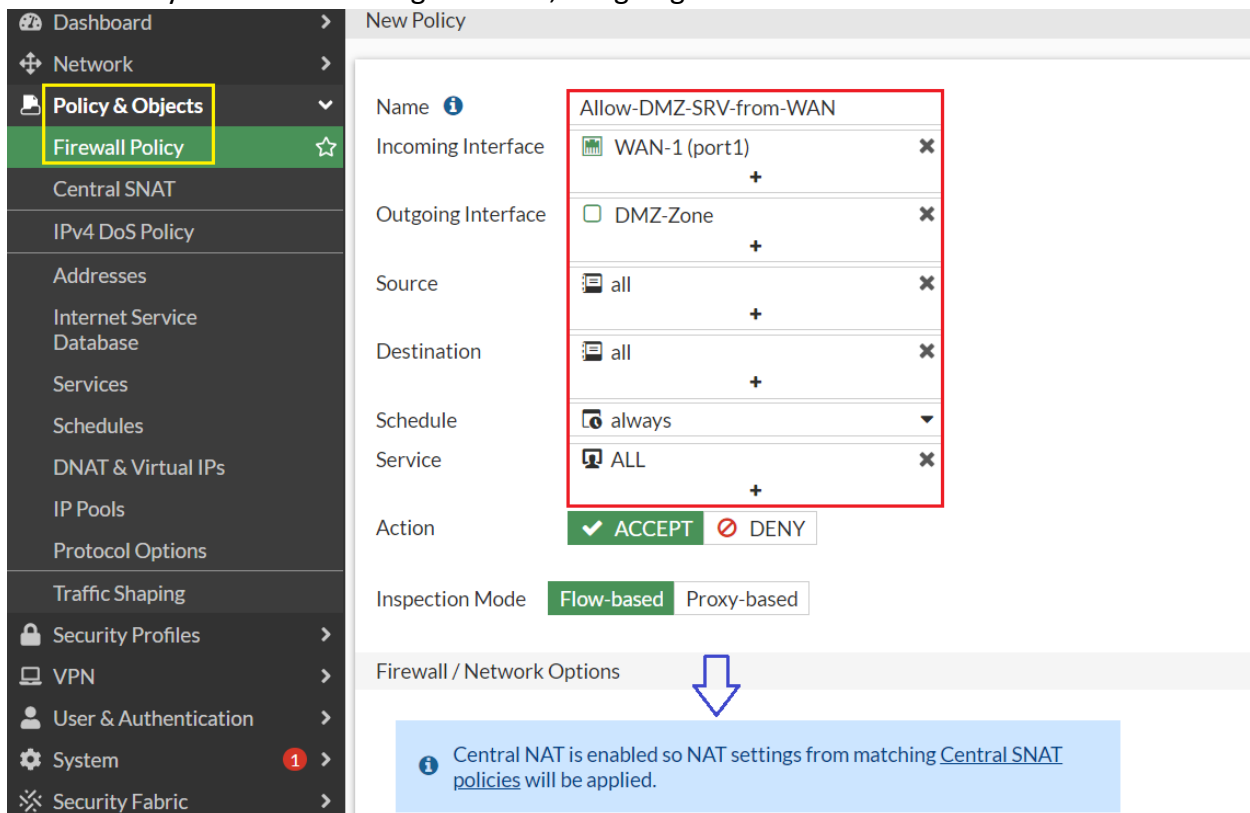
Source address:

Services:  HTTP  HTTPS



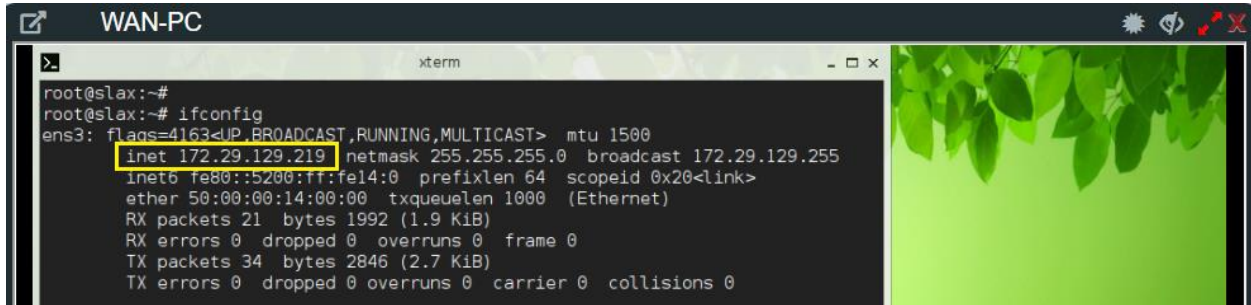
### Creating Security Policy:

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.



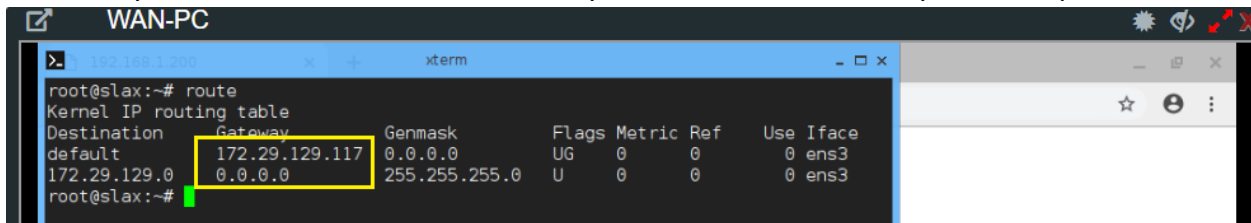
## Verification & Testing:

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



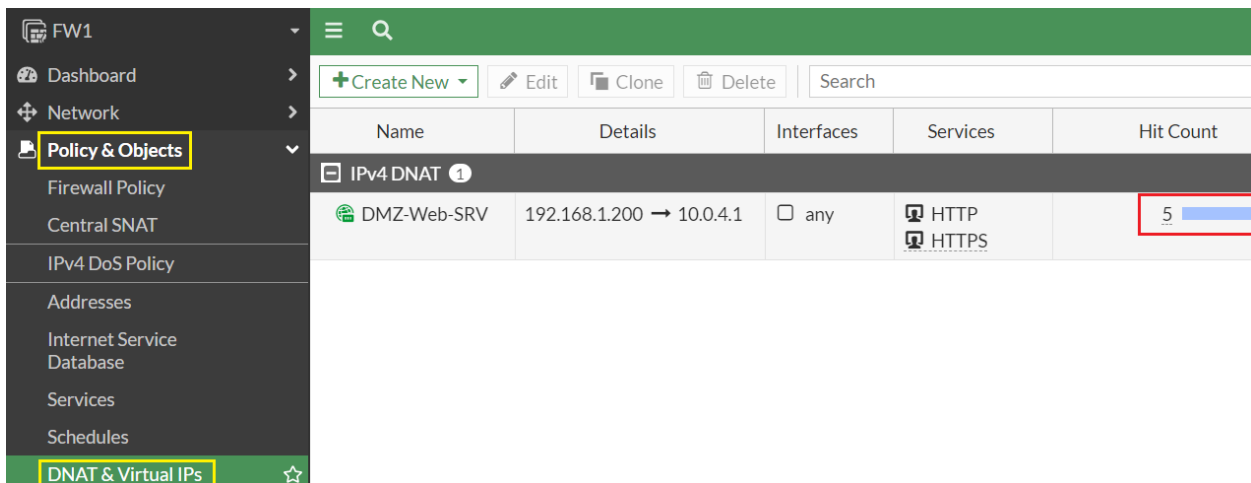
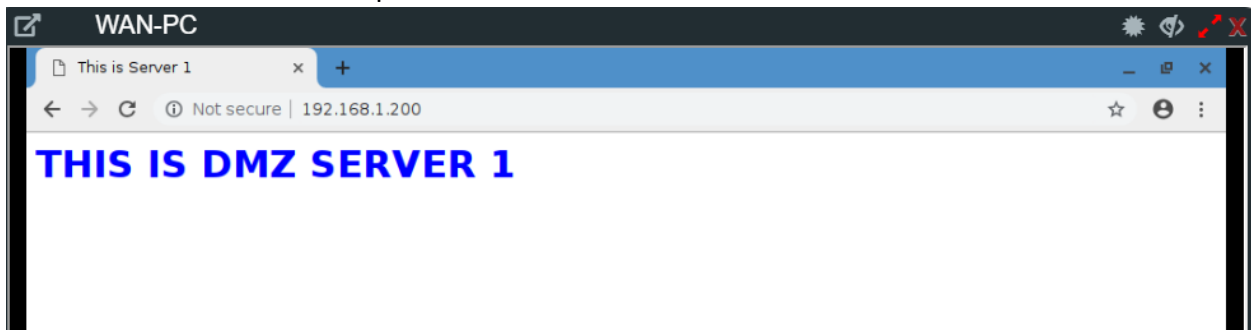
```
root@slax:~# ifconfig
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.29.129.219 netmask 255.255.255.0 broadcast 172.29.129.255
    inet6 fe80::5200:ff:fe14:0 prefixlen 64 scopeid 0x20<link>
    ether 50:00:00:14:00:00 txqueuelen 1000 (Ethernet)
    RX packets 21 bytes 1992 (1.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 34 bytes 2846 (2.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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



```
root@slax:~# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default 172.29.129.117 0.0.0.0 UG 0 0 0 ens3
172.29.129.0 0.0.0.0 255.255.255.0 U 0 0 0 ens3
```

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.

Date/Time	Source	Destination NAT IP	Destination	Destination Interface
Second ago	172.29.129.219	10.0.4.1	192.168.1.200	VLAN-40 (VLAN-40)
59 seconds ago	172.29.129.219	10.0.4.1	192.168.1.200	VLAN-40 (VLAN-40)
Minute ago	10.0.1.10		142.250.20...	WAN-1 (port1)
Minute ago	10.0.1.1		8.8.8.8 (dns...	WAN-1 (port1)
Minute ago	10.0.1.10		8.8.8.8 (dns...	WAN-1 (port1)
2 minutes ago	10.0.1.10		142.250.20...	WAN-1 (port1)
3 minutes ago	172.29.129.219	10.0.4.1	192.168.1.200	VLAN-40 (VLAN-40)
3 minutes ago	10.0.1.1		8.8.8.8 (dns...	WAN-1 (port1)

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

```
FW1 #
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        -
tcp     3587     192.168.114.1:49333 -                192.168.114.200:80 -
tcp     3597     192.168.114.1:49338 -                192.168.114.200:80 -
tcp     3597     192.168.114.1:49339 -                192.168.114.200:80 -
tcp     3597     192.168.114.1:49340 -                192.168.114.200:80 -
tcp     3597     192.168.114.1:49341 -                192.168.114.200:80 -
tcp     3597     192.168.114.1:49342 -                192.168.114.200:80 -
tcp     3597     192.168.114.1:49343 -                192.168.114.200:80 -
tcp     4        192.168.1.102:8149 -                192.168.3.1:179 -
tcp     3591     10.0.1.254:24667 -                10.0.1.2:179 -
tcp     3598     172.29.129.219:47818 -                192.168.1.200:80 10.0.4.1:80
tcp     3597     172.29.129.219:47820 -                192.168.1.200:80 10.0.4.1:80
udp     171     127.0.0.1:11049 -                127.0.0.1:12121 -
```

## VIP with Port Forwarding:

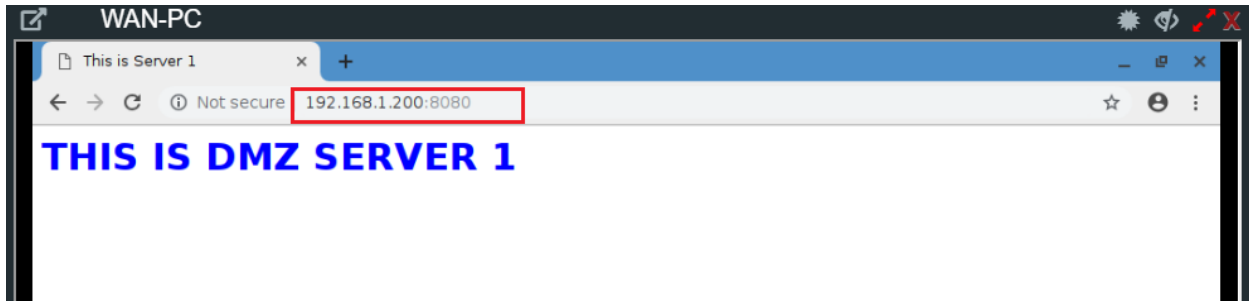
To create a virtual IP, go to **Policy & Objects > DNAT & Virtual IPs** Click **Create New** and select **DNAT & Virtual IP**. Enter a unique name for the virtual IP and fill in the other fields.

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

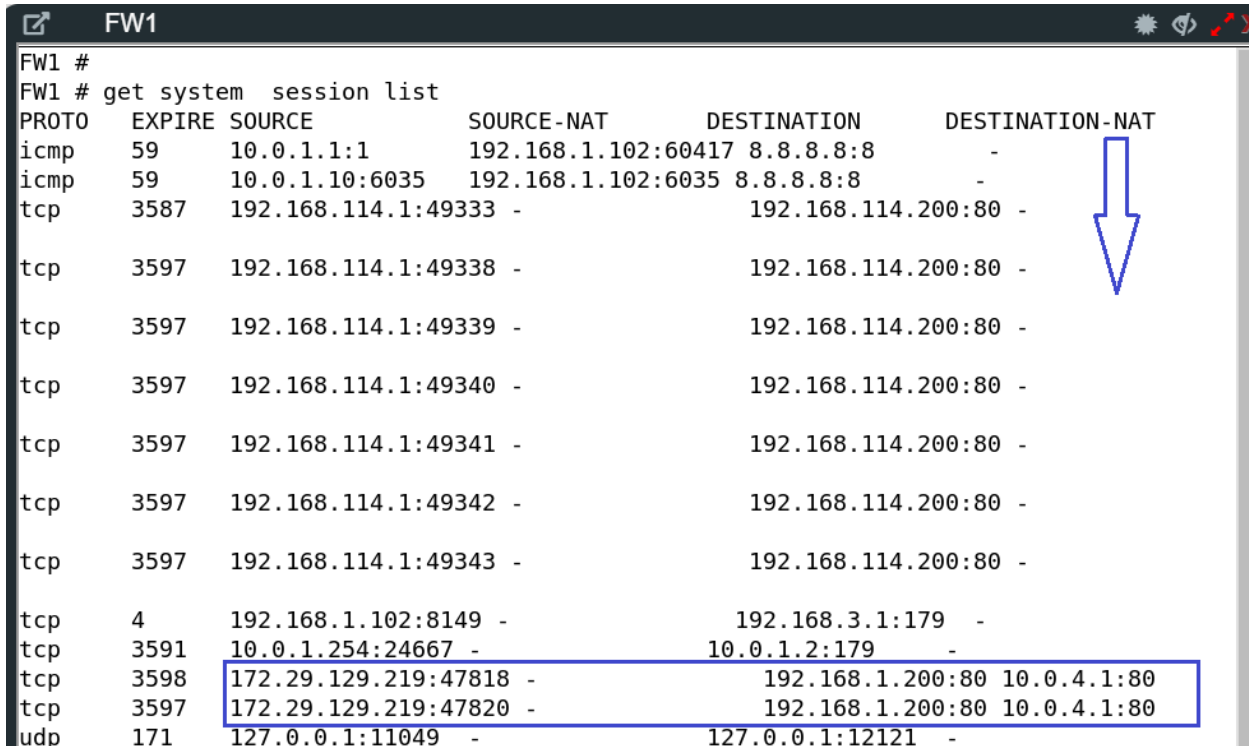
The screenshot displays the Mikrotik WinBox interface for configuring a DNAT & Virtual IP rule. The sidebar on the left shows the navigation menu with 'Policy & Objects' and 'DNAT & Virtual IPs' highlighted. The main configuration area is titled 'Edit DNAT & Virtual IP' and shows the following settings:

- DNAT & VIP type:** IPv4 DNAT
- Name:** DMZ-Web-SRV
- Comments:** Web Server in DMZ
- Color:** Green (with a 'Change' button)
- Status:** Enabled (toggle switch)
- Network:**
  - Interface:** any
  - Type:** Static NAT
  - Source interface filter:** Disabled
  - External IP address/range:** 192.168.1.200
  - Map to:**
    - IPv4 address/range:** 10.0.4.1
- Optional Filters:** Disabled (with a 'Disable This' button)
- Port Forwarding:** Enabled (with a 'Enable Port Forwarding' button)
- Protocol:** TCP (selected), UDP, SCTP, ICMP
- Port Mapping Type:** One to one (selected), Many to many
- External service port:** 8080 (labeled as 'External Port')
- 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.

