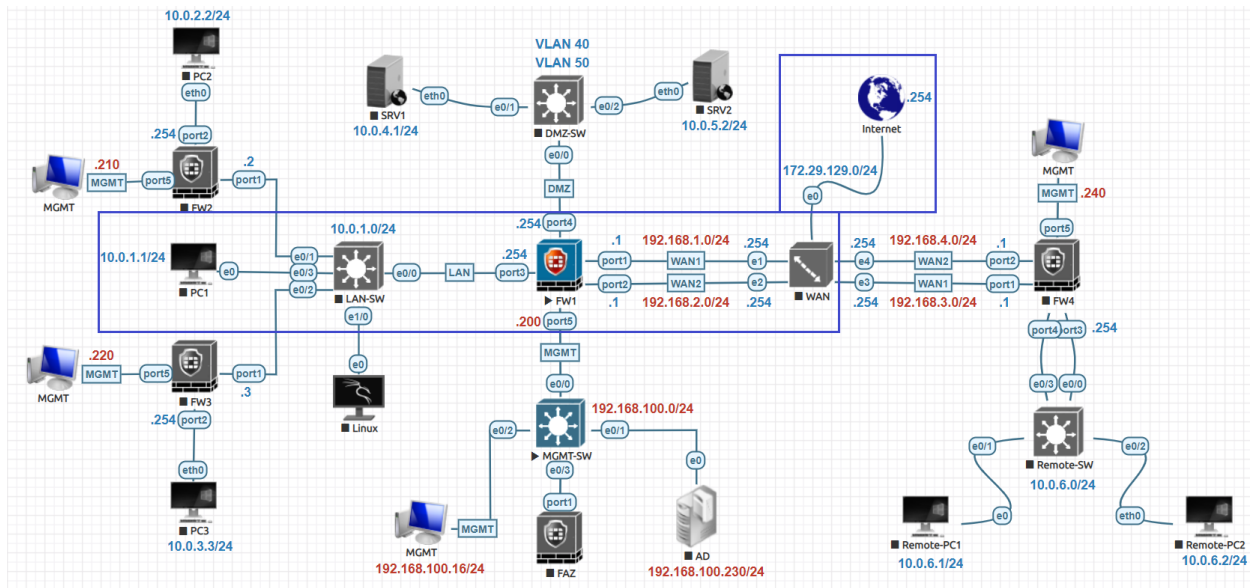


Policy Source Port Block Allocation NAT Lab:



First, to create the IP Pool, **Port Block Allocation** NAT pool. Navigate to **Policy & Objects > IP Pools** and click **Create New**. Enter a descriptive name, click **Port Block Allocation** and enter the external IP address range you want applied for this pool in this case (**192.168.1.130-192.168.1.132**).

Name	External IP Range	Type
SNAT-Overload	192.168.1.100 - 192.168.1.102	Overload

New Dynamic IP Pool

Name: SNAT-Port-Block-Allocation

Comments: Write a comment... 0/255

Type: Overload One-to-One Fixed Port Range **Port Block Allocation**

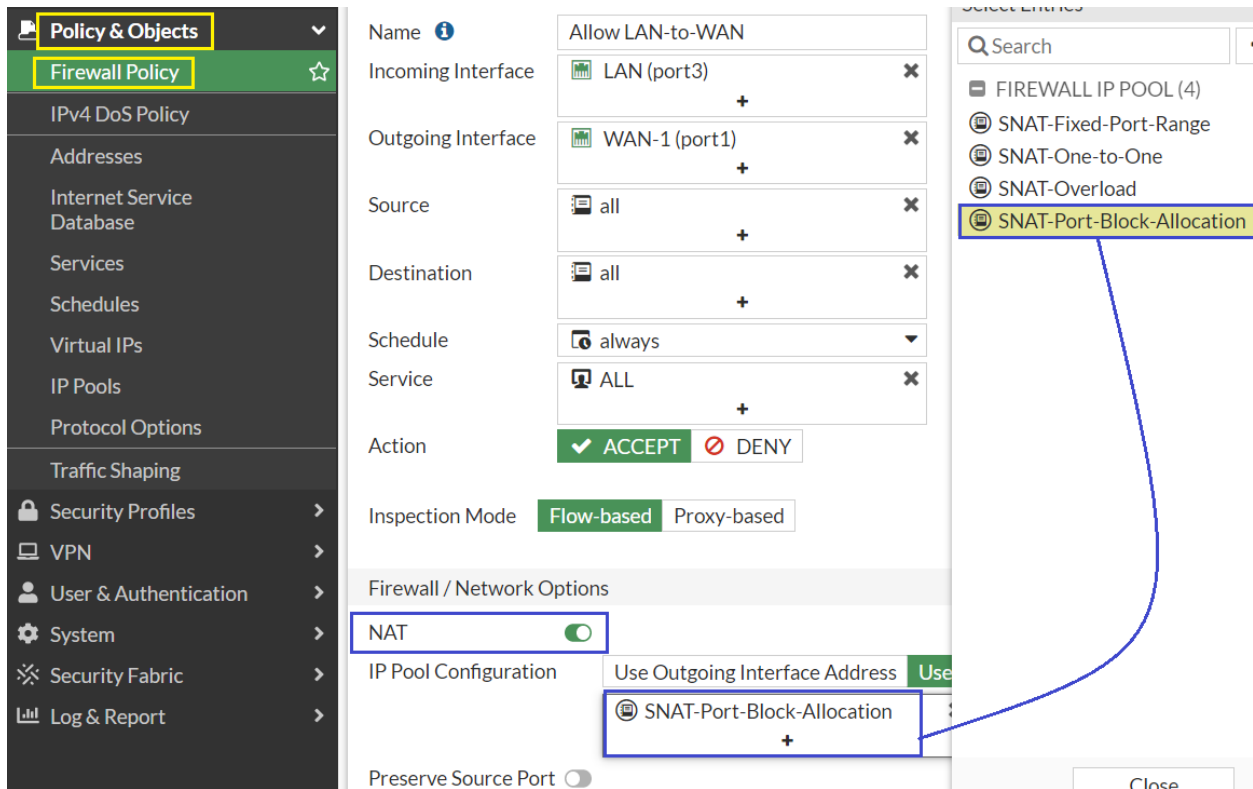
External IP address/range: 192.168.1.130-192.168.1.132

Block Size: 128

Blocks Per User: 8

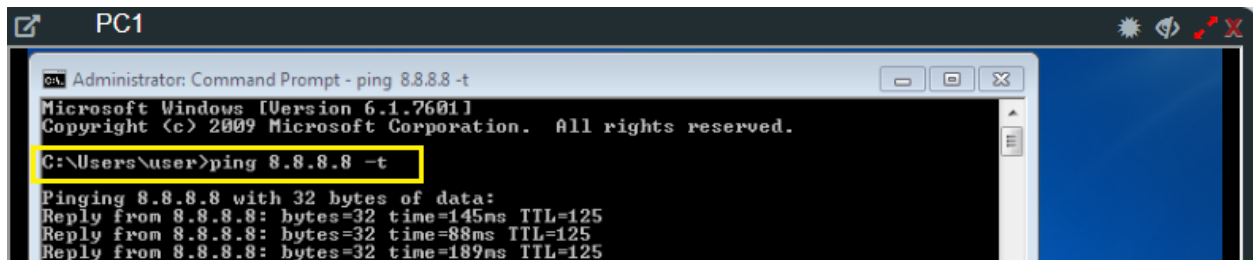
ARP Reply:

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 which is (**SNAT-Port-Block-Allocation**). Click **OK**.



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 **192.168.1.130 – 192.168.1.132**. For packets that match this policy, its source IP address is translated to the IP address of the outgoing range **192.168.1.130 – 192.168.1.132**. Let's visit from internal PCs to external.



```

Linux
>
64 bytes from 8.8.8.8: icmp_seq=13 ttl=125 time=135 ms
64 bytes from 8.8.8.8: icmp_seq=14 ttl=125 time=133 ms
64 bytes from 8.8.8.8: icmp_seq=15 ttl=125 time=186 ms
64 bytes from 8.8.8.8: icmp_seq=16 ttl=125 time=82.1 ms
64 bytes from 8.8.8.8: icmp_seq=17 ttl=125 time=434 ms
64 bytes from 8.8.8.8: icmp_seq=18 ttl=125 time=76.3 ms
64 bytes from 8.8.8.8: icmp_seq=19 ttl=125 time=82.5 ms
64 bytes from 8.8.8.8: icmp_seq=20 ttl=125 time=186 ms

```

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

The screenshot shows the FortiView Sessions dashboard. The left sidebar has 'Dashboard' and 'FortiView Sessions' highlighted. The main area displays a table of sessions with the following data:

Source	Destination	Destination Interface	Application	Source NAT Address
10.0.1.1	8.8.8.8	WAN-1 (port1)	ICMP/8	192.168.1.130
10.0.1.10	8.8.8.8	WAN-1 (port1)	ICMP/8	192.168.1.130
10.0.1.10	1.1.1.1	WAN-1 (port1)	UDP/53	192.168.1.102
10.0.1.10	142.250.180.4	WAN-1 (port1)	TCP/443	192.168.1.130
10.0.1.10	142.250.180.4	WAN-1 (port1)	TCP/443	192.168.1.130

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     192.168.1.130:5249  8.8.8.8:8       -
udp     127     192.168.1.102:2943 -                8.8.8.8:53      -
udp     77       192.168.1.102:2943 -                192.168.1.254:53 -
udp     46       127.0.0.1:22357 -                127.0.0.1:9980  -
icmp    59       10.0.1.10:6035 192.168.1.130:5139  8.8.8.8:8       -
tcp     3598    192.168.114.1:62844 -                192.168.114.200:80 -
udp     77       10.0.1.10:46462 192.168.1.102:46462 1.1.1.1:53      -
udp     126     10.0.1.1:57465 192.168.1.102:57465 8.8.8.8:53      -
udp     91       192.168.1.102:2943 -                1.1.1.1:53      -
tcp     3590    10.0.1.10:58484 192.168.1.130:5236 142.250.180.4:443 -
tcp     118     10.0.1.10:58486 192.168.1.130:5238 142.250.180.4:443 -
--More--

```