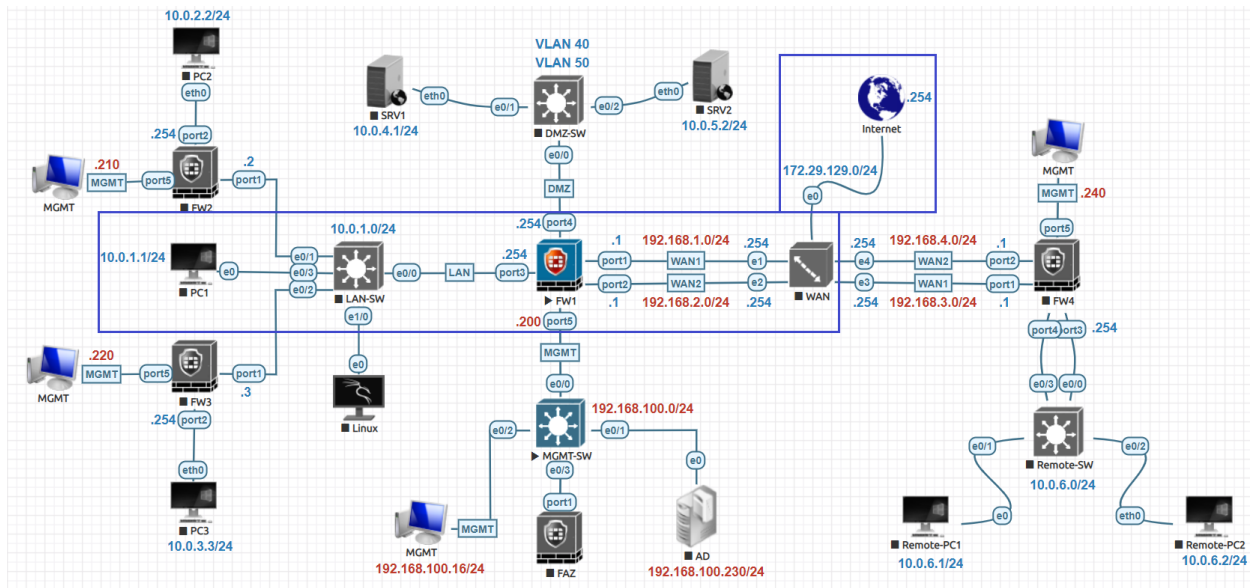


Policy Source One-To-One NAT Lab:



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**).

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

New Dynamic IP Pool

Name: SNAT-One-to-One

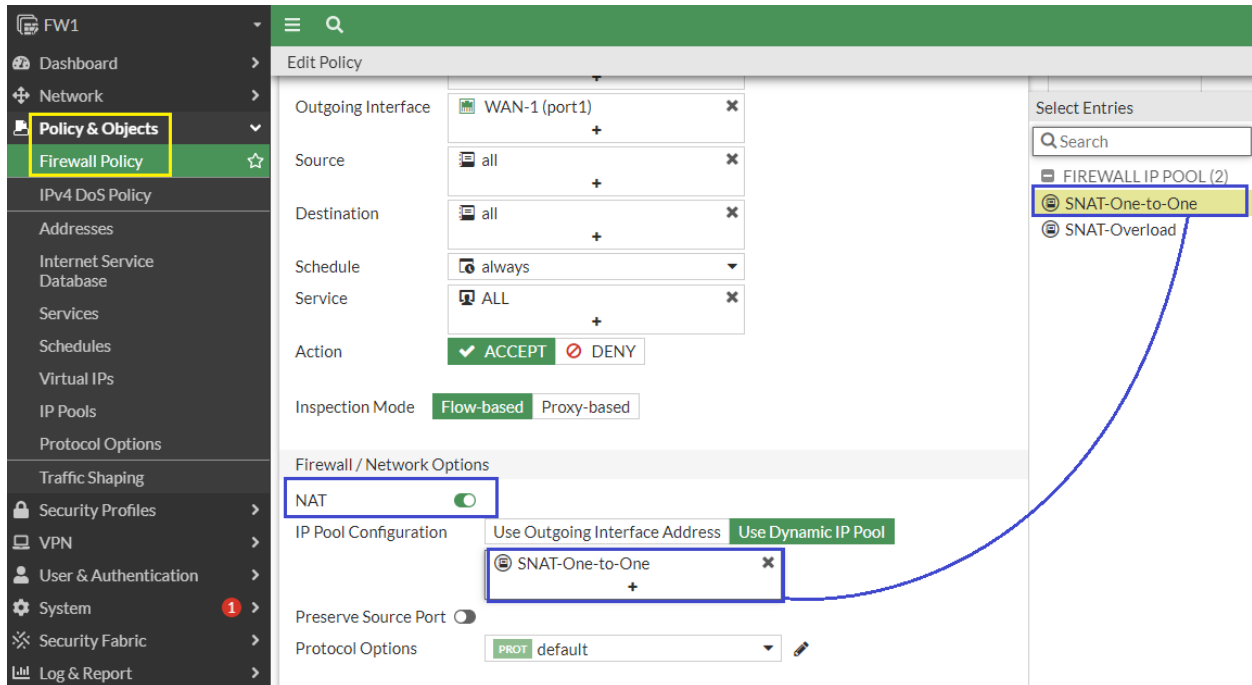
Comments: Write a comment... /0/255

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

External IP address/range: 192.168.1.110-192.168.1.111

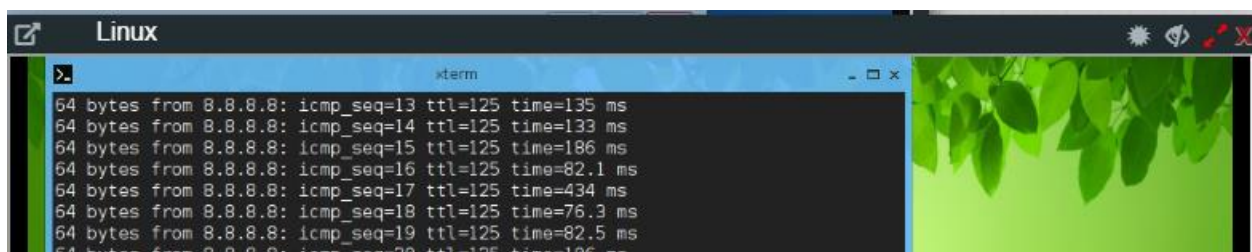
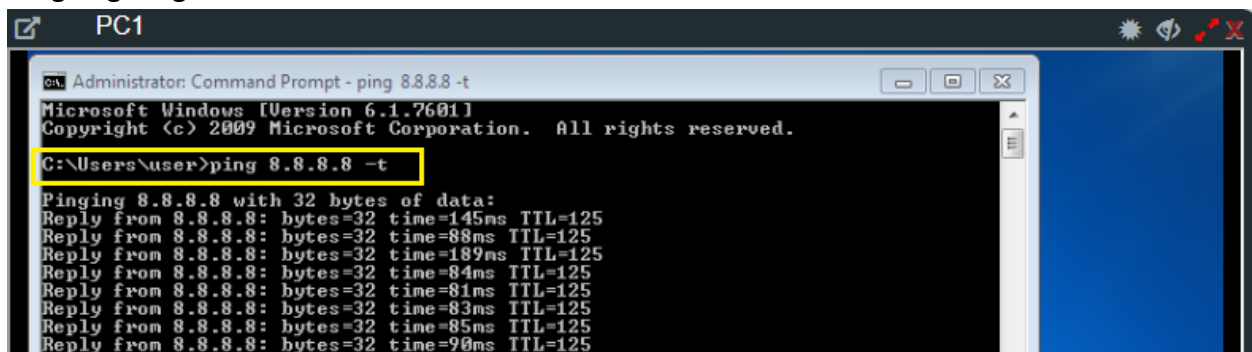
ARP Reply:

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 (**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.

Source	Destination	Destination Interface	Application	Source NAT Address
10.0.1.1	8.8.8.8	WAN-1 (port1)	ICMP/8	192.168.1.110
10.0.1.10	8.8.8.8	WAN-1 (port1)	ICMP/8	192.168.1.111
10.0.1.10	34.104.35.123	WAN-1 (port1)	TCP/80	192.168.1.100

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

```
FW1 # get system session list
PROTO  EXPIRE  SOURCE          SOURCE-NAT      DESTINATION      DESTINATION-NAT
udp     86      127.0.0.1:5465  -               127.0.0.1:9980  -
icmp    59      10.0.1.1:1     192.168.1.110:1 8.8.8.8:8       -
icmp    59      10.0.1.10:3572 192.168.1.111:3572 8.8.8.8:8       -
udp     58      192.168.1.102:3797 -                8.8.8.8:53      -
udp     179     192.168.1.102:3797 -                192.168.1.254:53 -
tcp     0       127.0.0.1:12770 -                127.0.0.1:9980  -
tcp     3589    192.168.114.1:53880 -                192.168.114.200:80 -
tcp     3599    192.168.114.1:54240 -                192.168.114.200:80 -
tcp     0       192.168.114.1:54234 -                192.168.114.200:80 -
tcp     0       192.168.114.1:54235 -                192.168.114.200:80 -
tcp     0       192.168.114.1:54236 -                192.168.114.200:80 -
```

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.

ID	Name	From	To	Source	Hit Count
9	Allow-DNS	LAN (port3)	WAN-1 (port1)	all	54
8	Local-User Policy		port1	local-user	0
7	MAC-Based-Policy		port1	PC1-Win-7-MAC	0
1	Allow LAN-to-WAN	LAN (port3)	WAN-1 (port1)	all	57

Policy ID 1

Policy Name Allow LAN-to-WAN

This policy has the following issues:

- It is using an exhausted IP Pool