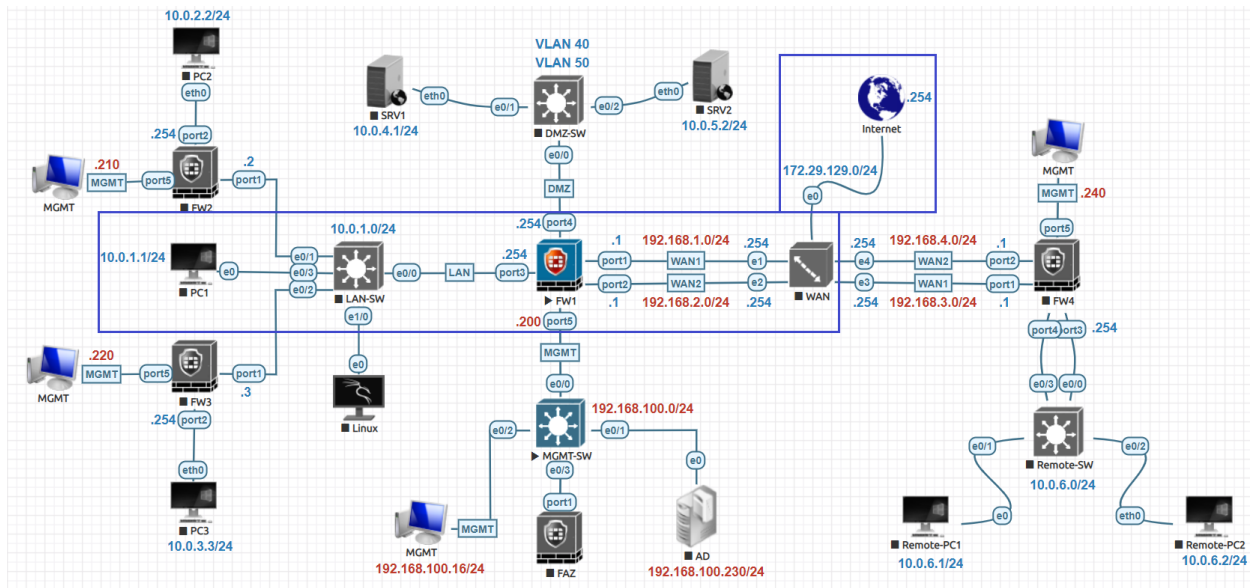


Policy Source Fixed Port Range NAT Lab:



First, to create the IP Pool, or **Fixed Port Range NAT** pool. Navigate to **Policy & Objects > IP Pools** and click **Create New**. Enter a descriptive name, click **Fixed Port Range** and enter the external IP address range you want applied for this pool in this case (**192.168.1.120-192.168.1.121**).

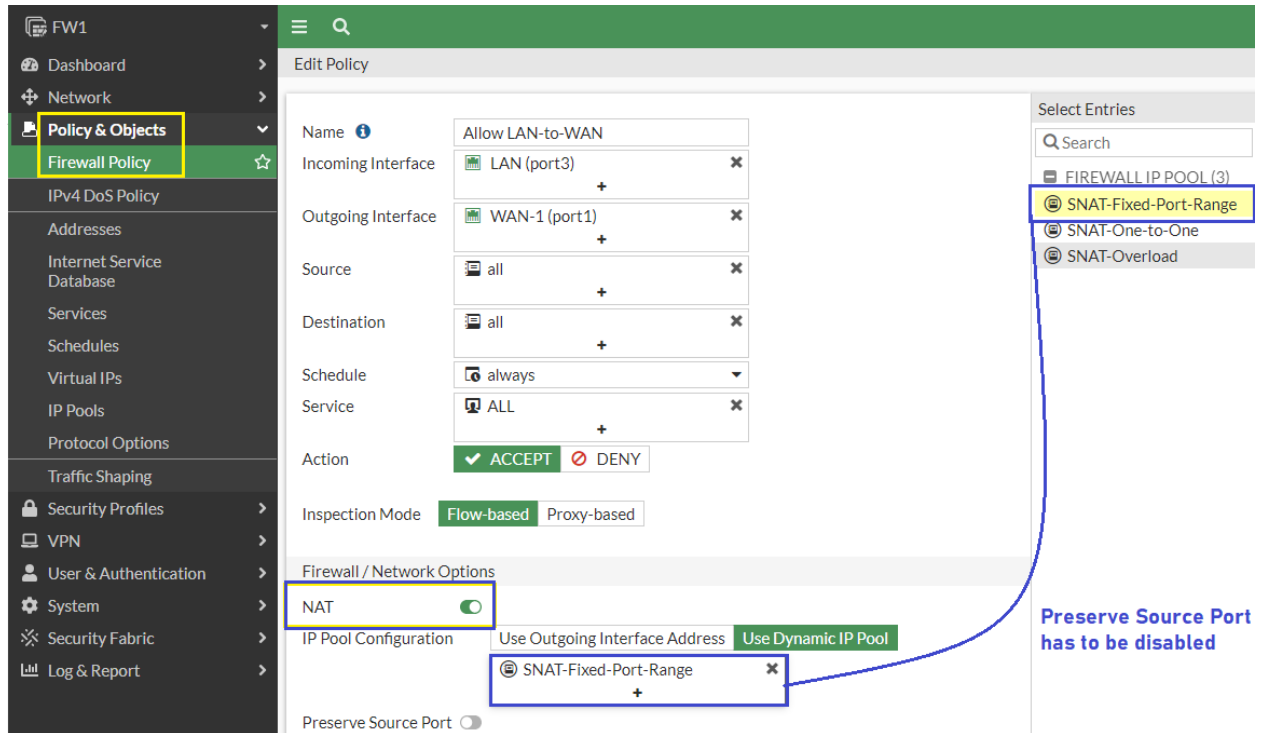
The screenshot shows the 'IP Pools' configuration page. A blue arrow points to the 'Create New' button. Below it, a table lists existing pools:

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

The screenshot shows the 'New Dynamic IP Pool' configuration form with the following details:

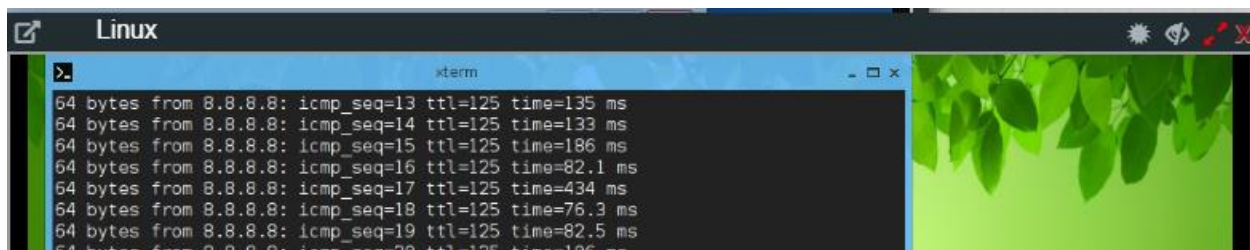
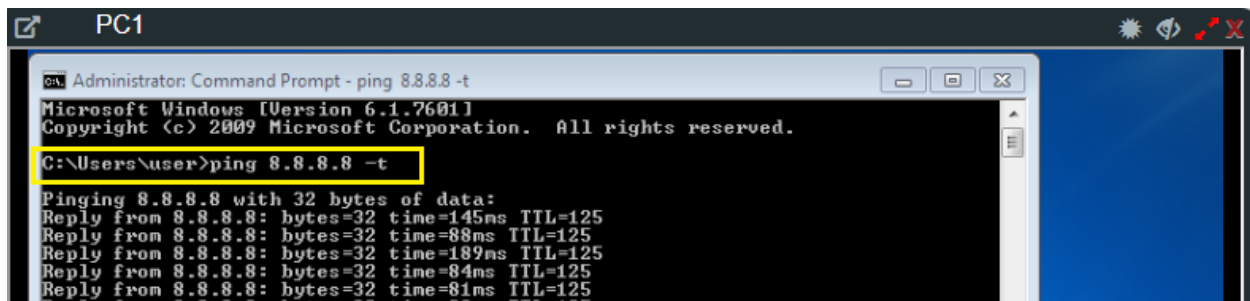
- Name:** SNAT-Fixed-Port-Range
- Comments:** Write a comment... (0/255)
- Type:** Overload, One-to-One, **Fixed Port Range**, Port Block Allocation
- External IP address/range:** 192.168.1.120-192.168.1.121
- Internal IP Range:** 10.0.1.1-10.0.1.10
- Ports Per User:**
- ARP Reply:**

Let's go back to **Policy & Objects > Firewall Policy** Enable **NAT** and Change the IP Pool Configuration to **Use Dynamic IP Pool** & select IP Pool created earlier (**SNAT-Fixed-Port-Range**).

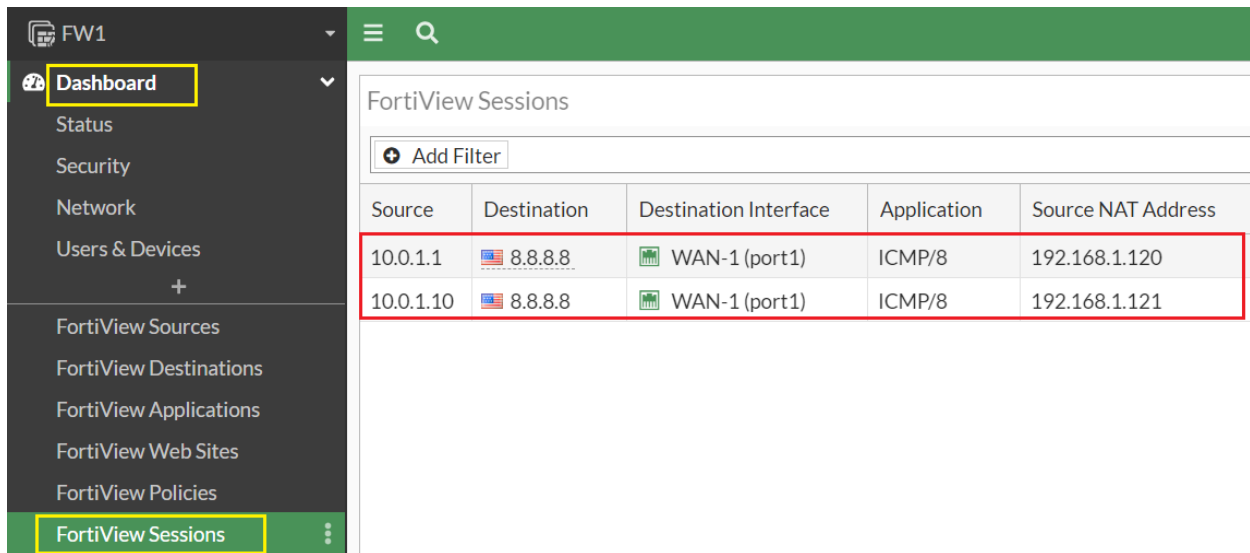


Verification & Testing:

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 **192.168.1.120 – 192.168.1.121**. For packets that match this policy, its source IP address is translated to the IP address of the outgoing range **192.168.1.120 – 192.168.1.121**. Let's visit from internal PCs to external.

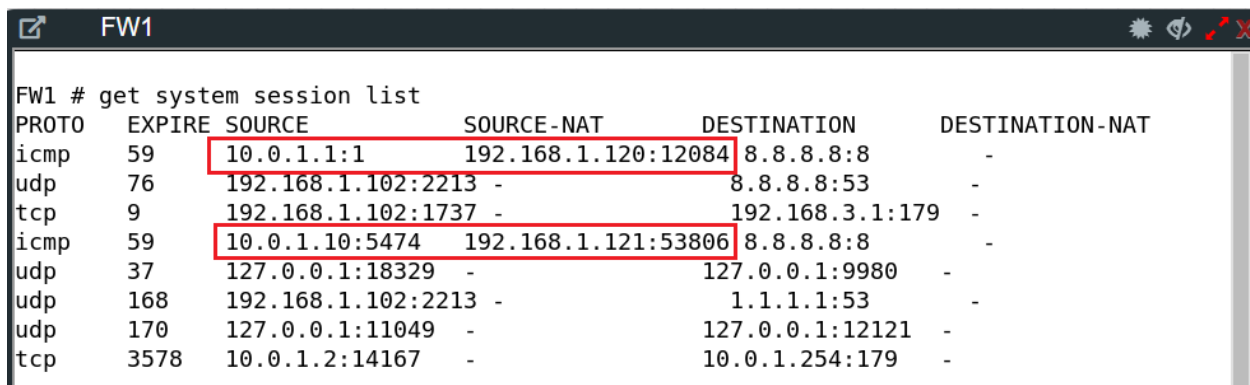


Let's go to **Dashboard > FortiView Session** better to Apply Filter for best view.



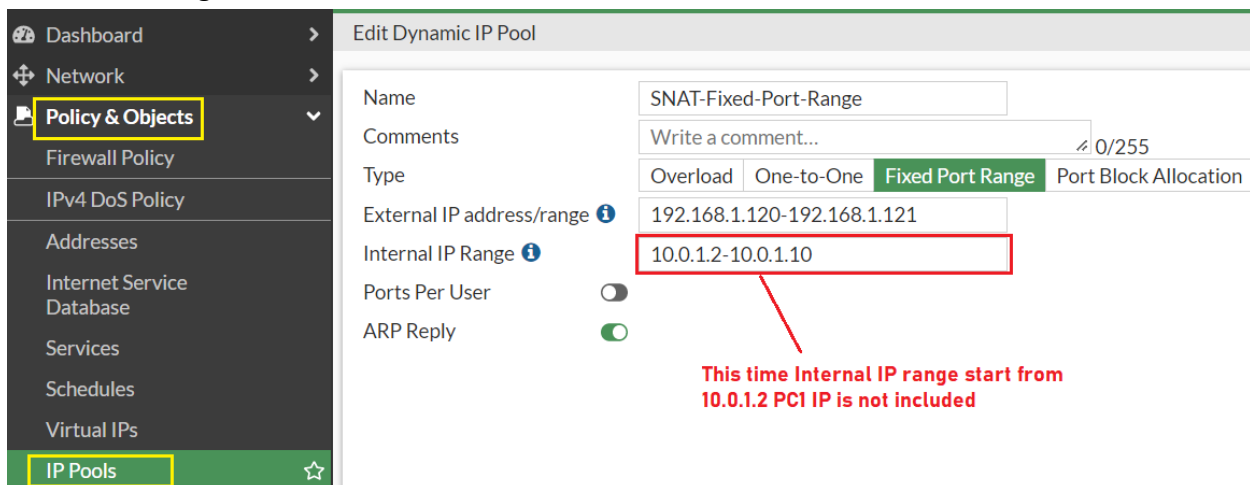
Source	Destination	Destination Interface	Application	Source NAT Address
10.0.1.1	8.8.8.8	WAN-1 (port1)	ICMP/8	192.168.1.120
10.0.1.10	8.8.8.8	WAN-1 (port1)	ICMP/8	192.168.1.121

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
icmp   59      10.0.1.1:1     192.168.1.120:12084  8.8.8.8:8      -
udp    76      192.168.1.102:2213 -                8.8.8.8:53     -
tcp    9       192.168.1.102:1737 -                192.168.3.1:179 -
icmp   59      10.0.1.10:5474 192.168.1.121:53806 8.8.8.8:8      -
udp    37      127.0.0.1:18329 -                127.0.0.1:9980 -
udp    168     192.168.1.102:2213 -                1.1.1.1:53     -
udp    170     127.0.0.1:11049 -                127.0.0.1:12121 -
tcp    3578   10.0.1.2:14167 -                10.0.1.254:179 -
```

Let's go back to **Policy & Objects > IP Pools** and edit **Fixed Port Range** entries and change the Internal IP Range to 192.168.1.1-192.168.1.3 this time 192.168.1.4 is not included.



Edit Dynamic IP Pool

Name: SNAT-Fixed-Port-Range

Comments: Write a comment... 0/255

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

External IP address/range: 192.168.1.120-192.168.1.121

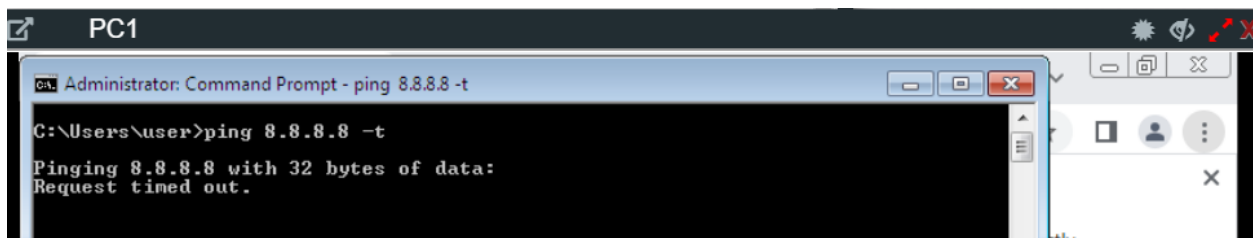
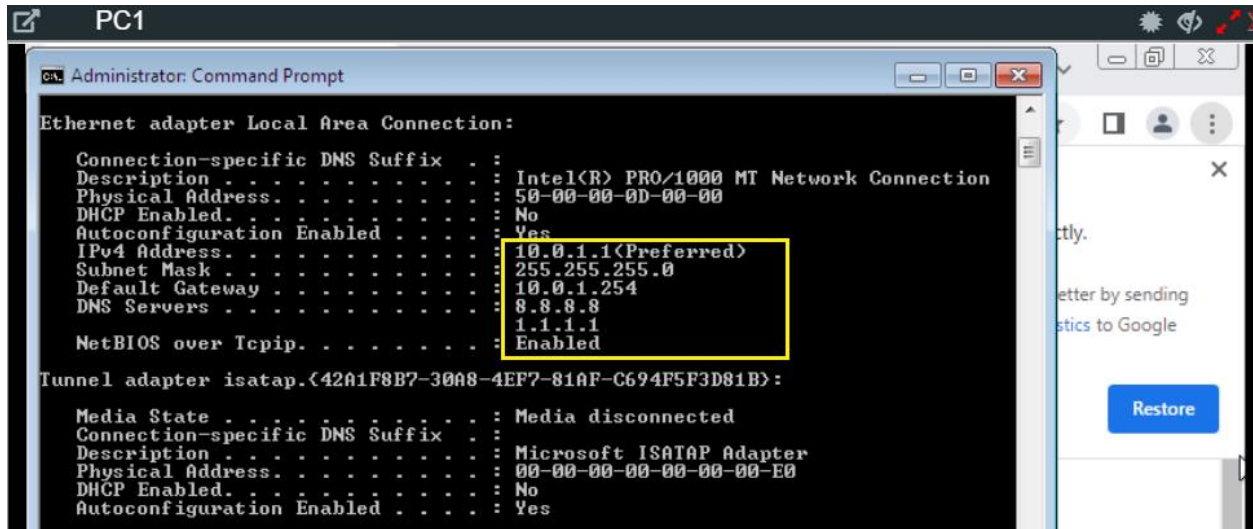
Internal IP Range: **10.0.1.2-10.0.1.10**

Ports Per User:

ARP Reply:

This time Internal IP range start from 10.0.1.2 PCI IP is not included

Communication is not working anymore from PC1 IP 10.0.1.1 because it's not included in Internal IP Range of Fixed Port Range.



Dynamic SNAT Types: Fixed port range

Internal Source IP	Source Port	Translated Source IP	Translated Port
10.1.100.1	200.1.100.1	5117-11157
10.1.100.2	200.1.100.1	11158-17198
10.1.100.3	200.1.100.1
.....	200.1.100.1
10.1.100.10	200.1.100.1	59486-65526