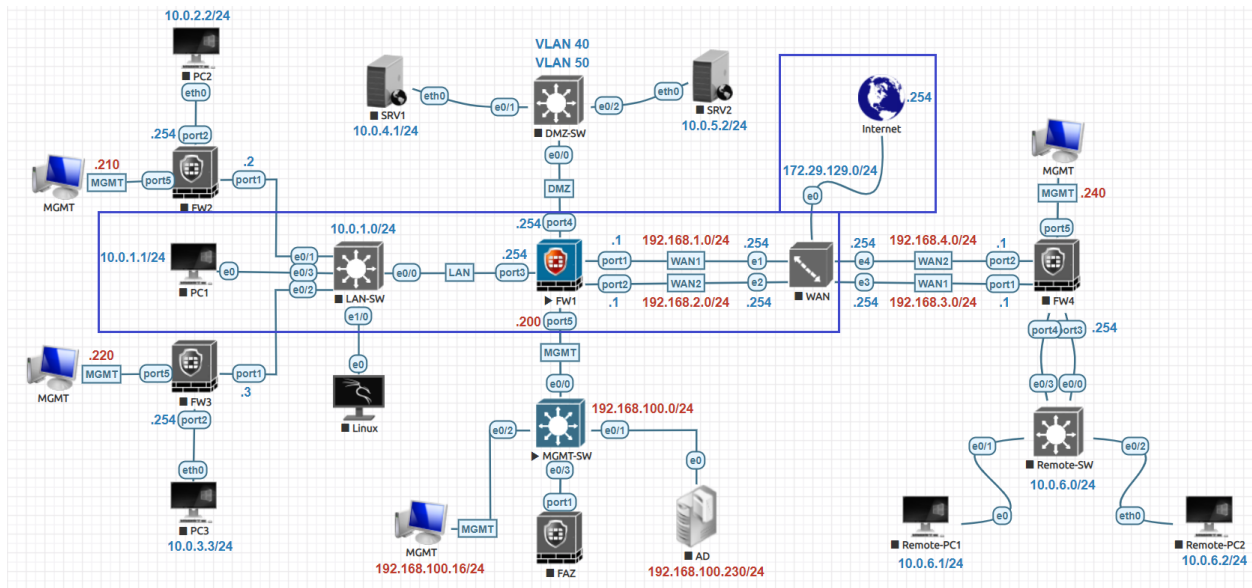
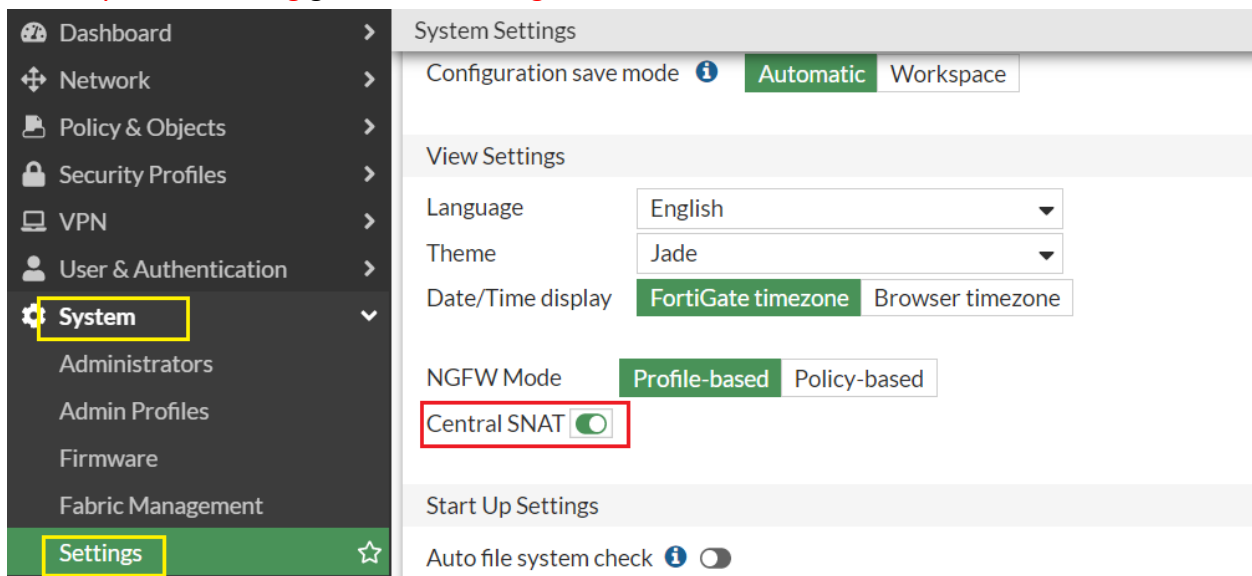


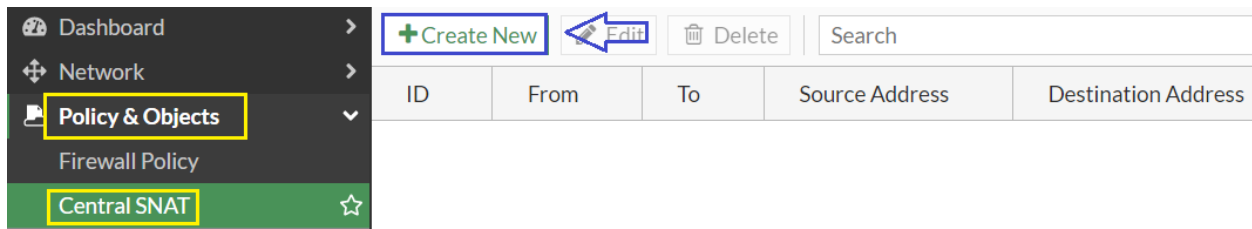
Central SNAT Lab:



Go to **System > Setting** go to **View Settings** click to enable **Central SNAT** click **OK**.



To Create Central SNAT policy go to **Policy & Objects > Central SNAT** and click **Create New**.



Go to **Policy & Objects > Central SNAT** Click Create New as shown below.

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 >

New Policy

Incoming Interface LAN (port3) ×

Outgoing Interface WAN-1 (port1) ×

Source Address all ×

Destination Address all ×

NAT

NAT NAT

IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool

Protocol any TCP UDP SCTP Specify 0

Explicit port mapping

Comments Write a comment... 0/1023

Enable this policy

When go to **Policy & Objects > Firewall Policy** there is no more NAT option it will show below.

Dashboard > Network > **Policy & Objects** > Firewall Policy > **Firewall Policy** ☆

Central SNAT

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

DNAT & Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles >

Edit Policy

Outgoing Interface WAN-1 (port1) ×

Source all ×

Destination all ×

Schedule always

Service ALL ×

Action ACCEPT DENY

Inspection Mode Flow-based Proxy-based

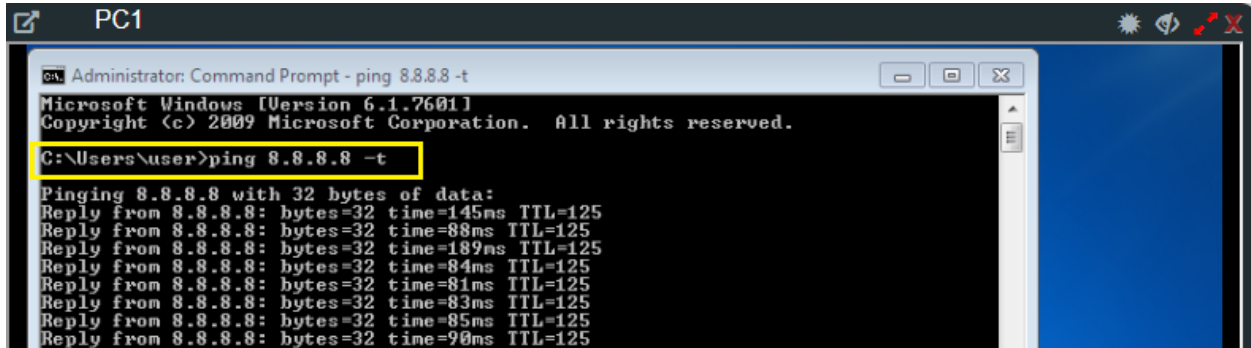
Firewall / Network Options

Central NAT is enabled so NAT settings from matching Central SNAT policies will be applied.

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 an IP address **192.168.1.102**. For packets that match this policy, its source IP address is translated to the IP address of the outgoing interface.

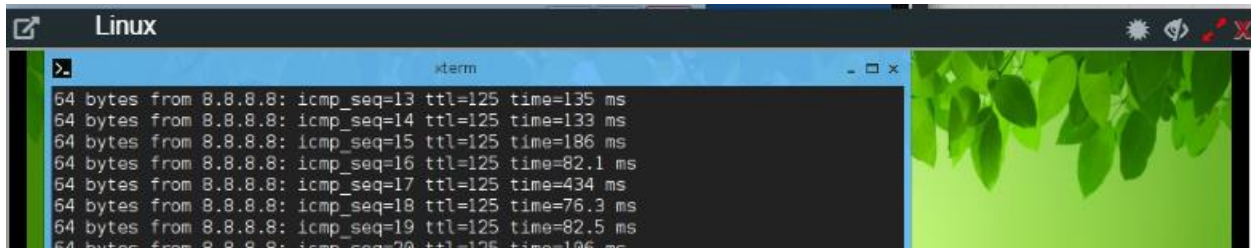
Let's visit and Ping from internal PC1 to outside network.



```
Administrator: Command Prompt - ping 8.8.8.8 -t
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

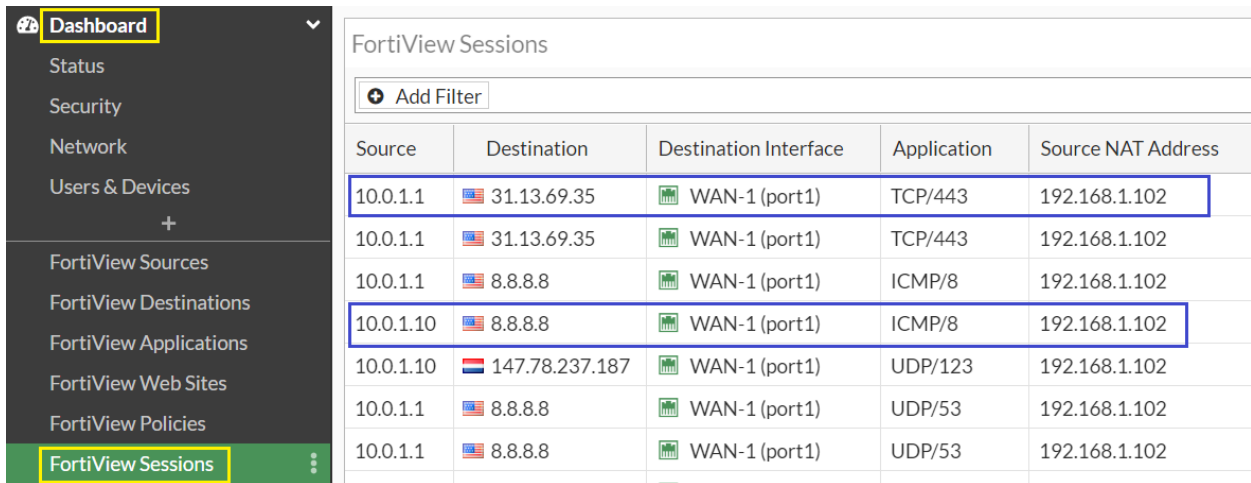
C:\Users\user>ping 8.8.8.8 -t

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=145ms TTL=125
Reply from 8.8.8.8: bytes=32 time=88ms TTL=125
Reply from 8.8.8.8: bytes=32 time=189ms TTL=125
Reply from 8.8.8.8: bytes=32 time=84ms TTL=125
Reply from 8.8.8.8: bytes=32 time=81ms TTL=125
Reply from 8.8.8.8: bytes=32 time=83ms TTL=125
Reply from 8.8.8.8: bytes=32 time=85ms TTL=125
Reply from 8.8.8.8: bytes=32 time=90ms TTL=125
```



```
>
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=106 ms
```

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 | 31.13.69.35 | WAN-1 (port1) | TCP/443 | 192.168.1.102 |
| 10.0.1.1 | 31.13.69.35 | WAN-1 (port1) | TCP/443 | 192.168.1.102 |
| 10.0.1.1 | 8.8.8.8 | WAN-1 (port1) | ICMP/8 | 192.168.1.102 |
| 10.0.1.10 | 8.8.8.8 | WAN-1 (port1) | ICMP/8 | 192.168.1.102 |
| 10.0.1.10 | 147.78.237.187 | WAN-1 (port1) | UDP/123 | 192.168.1.102 |
| 10.0.1.1 | 8.8.8.8 | WAN-1 (port1) | UDP/53 | 192.168.1.102 |
| 10.0.1.1 | 8.8.8.8 | WAN-1 (port1) | UDP/53 | 192.168.1.102 |

Also, can verify by CLI command **get system session list**

```
FW1 # get system session list
PROTO  EXPIRE  SOURCE          SOURCE-NAT      DESTINATION     DESTINATION-NAT
tcp    81      10.0.1.1:49432  192.168.1.102:49432  31.13.69.35:443 -
udp    83      10.0.1.1:57388  192.168.1.102:57388  142.251.37.36:443 -
icmp   59      10.0.1.1:1      192.168.1.102:60417  8.8.8.8:8       -
udp    91      10.0.1.1:52391  192.168.1.102:52391  31.13.69.35:443 -
udp    140     10.0.1.1:62468  192.168.1.102:62468  142.251.37.36:443 -
udp    56      192.168.1.102:2943 -                8.8.8.8:53      -
icmp   59      10.0.1.10:6035  192.168.1.102:6035  8.8.8.8:8       -
tcp    3584   192.168.114.1:62936 -                192.168.114.200:80 -

udp    107     10.0.1.1:60313  192.168.1.102:60313  8.8.4.4:443    -
udp    157     10.0.1.1:64228  192.168.1.102:64228  8.8.8.8:53     -
udp    72      10.0.1.1:53038  192.168.1.102:53038  8.8.8.8:53     -
--More-- █
```