

Маскарад, SNAT, DNAT

Зачем нам все это? Чтобы держать подсетку за одним адресом.

- SNAT - преобразование **исходящего трафика** 1 к 1. Т.е. локально на хосте 10.0.0.2, а во внешнюю сеть он ходит через 8.8.8.8. Несколько хостов за один адрес нельзя пустить, только 1.
- DNAT - преобразование **входящего трафика** (Много из внешки к Одному локальному). Можно пробросить как все порты, так и какой-то конкретный.
- PAT/NAPT/Masquerade - преобразование много адресов к одному + много портов. С помощью этой технологии работают домашние роутеры. Т.е. клиент за маскарадом может открыть у себя любой порт и установить с него соединение с хостом во внешней сети и его порт будет автоматически проброшен при соединении на такой же порт, только уже во внешней сети. Сокет (связка адрес+порт) должна быть уникальна, только тогда получится установить соединение.

SNAT+DNAT

Например, у нас есть host-vm, внутри которой есть внешний интерфейс eth0 с адресами 192.168.101.4/24 и 192.168.101.5/24 и бридж br0, на котором висит контейнер test2 со внутренним адресом 10.13.37.2/24. Мы хотим, чтобы по адресу 192.168.101.5 мы попадали на 10.13.37.2.

Так сделано, например, у облачных провайдеров, например AWS или Yandex.Cloud.

```
# Хост машина с контейнером внутри
losted@host-vm:~$ ip -4 a show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    altname enp0s18
    inet 192.168.101.4/24 brd 192.168.101.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet 192.168.101.5/24 scope global secondary eth0
        valid_lft forever preferred_lft forever

losted@host-vm:~$ ip -h -4 a show br0
4: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
```

```
inet 10.13.37.1/24 scope global br0
    valid_lft forever preferred_lft forever
```

Контейнер внутри

```
root@test2:/# ip a show eth0
```

```
2: eth0@if7: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
```

```
    link/ether 00:16:3e:83:51:d8 brd ff:ff:ff:ff:ff:ff link-netnsid 0
```

```
    inet 10.13.37.2/24 scope global eth0
```

```
        valid_lft forever preferred_lft forever
```

Пускаем трафик из сети 10.13.37.0/24 во вне через адрес 192.168.101.5

```
losted@host-vm:~$ sudo iptables -t nat -A POSTROUTING -o eth0 -s 10.13.37.0/24 -j SNAT --to-source 192.168.101.5
```

Все что приходит на 192.168.101.5 перенаправляем на 10.13.37.2

```
losted@host-vm:~$ sudo iptables -t nat -A PREROUTING -d 192.168.101.5 -j DNAT --to-destination 10.13.37.2
```

Проверяем

```
losted in ~ λ ping 192.168.101.5
```

```
PING 192.168.101.5 (192.168.101.5) 56(84) bytes of data.
```

```
64 bytes from 192.168.101.5: icmp_seq=1 ttl=63 time=3.32 ms
```

```
64 bytes from 192.168.101.5: icmp_seq=2 ttl=63 time=5.97 ms
```

```
root@test2:/# nc -l 123
```

```
dsf
```

```
losted in ~ λ nc 192.168.101.5 123
```

```
dsf
```

Контейнер видит подключение с правильного адреса

```
root@test2:/# ss -tpn
```

State	Recv-Q	Send-Q	Local Address:Port	Peer
Address:Port	Process			
ESTAB	0	0	10.13.37.2:123	
192.168.101.105:49352	users:(("nc",pid=673,fd=4))			

```
losted in ~ λ ip -h -4 a show wlp2s0
```

```
4: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
```

```
    inet 192.168.101.105/24 brd 192.168.101.255 scope global dynamic noprefixroute wlp2s0
```

```
valid_lft 4294sec preferred_lft 4294sec
```

Теперь при обращении к любому порту по 192.168.101.5 будет перенаправлено на 10.13.37.2.

Masquerade + DNAT/SNAT

```
iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
```

Revision #10

Created 20 May 2023 16:10:16 by Ivan

Updated 28 August 2024 22:07:23 by Ivan