



NFTABLES

- Разрешаем только нужные порты (SSH, HTTP, VPN)
- Блокируем всё остальное
- Ограничиваем количество пакетов (защита от DDoS)

1. PAT/NAT (для выхода в интернет)

ЧТО ЭТО:

- Серверы в локальной сети (192.168.x.x) не видны из интернета
- NAT переводит их адреса в публичный IP роутера

КОМАНДА:

```
apt install -y nftables

nft add table ip nat
nft add chain ip nat postrouting { type nat hook postrouting
priority 100 \; }
nft add rule ip nat postrouting oifname "eth0" masquerade
```

ЧТО ЭТО ДЕЛАЕТ:

- Все пакеты, выходящие через `eth0` (внешний интерфейс), меняют IP на IP роутера

2. RATE LIMIT (не больше 100 пакетов/сек)

ЗАЧЕМ: Защита от DDoS (когда хакер отправляет миллионы пакетов).

```
nft add table inet filter
nft add chain inet filter input { type filter hook input priority 0 \; policy drop \; }
nft add rule inet filter input ct state established,related accept
nft add rule inet filter input iif lo accept
nft add rule inet filter input tcp dport 22 accept
nft add rule inet filter input limit rate 100/second accept
nft add rule inet filter input drop
```

ЧТО ЭТО ЗНАЧИТ:

- `policy drop` → по умолчанию всё запрещено
- `ct state established,related accept` → разрешить существующие соединения
- `tcp dport 22 accept` → разрешить SSH
- `limit rate 100/second` → не больше 100 пакетов в секунду

Сохранить правила:

```
nft list ruleset > /etc/nftables.conf
systemctl enable nftables
```