1. Настроить статическую конфигурацию (без DHCP) в Ubuntu через ip и netplan. Настроить IP, маршрут по умолчанию и DNS-сервера (1.1.1.1 и 8.8.8.8). Проверить работоспособность сети.

Откроем файл

nano /etc/netplan/01-network-manager-all.yaml

Отредактируем:

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [10.0.2.77/24]
      routes:
        - to: default
          via: 10.0.2.2
      nameservers:
        addresses:
          - 8.8.8.8
          - 1.1.1.1
```

Применим изменения

netplan try

Посмотрим сведения:

ip -c a

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
      valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
      valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:92:3c:05 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.77/24 brd 10.0.2.255 scope global noprefixroute enp0s3
      valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe92:3c05/64 scope link
      valid_lft forever preferred_lft forever
```

---

2. Настроить правила iptables для доступности сервисов на TCP-портах 22, 80 и 443. Также сервер должен иметь возможность устанавливать подключения к серверу обновлений. Остальные подключения запретить.

Разрешим входящий доступ к портам 22, 80 и 443:

iptables -I INPUT -p tcp --dport=22 -j ACCEPT

iptables -I INPUT -p tcp --dport=80 -j ACCEPT

iptables -I INPUT -p tcp --dport=443 -j ACCEPT

Остальные запретим:

iptables -P INPUT DROP

Разрешим исходящий доступ для сервера обновлений:

Получим ip сервера обновлений

host ru.archive.ubuntu.com

mirror.yandex.ru has address 213.180.204.183

iptables -A OUTPUT -d 213.180.204.183 -j ACCEPT

Остальные запретим:

iptables -P OUTPUT DROP

---

3. Запретить любой входящий трафик с IP 3.4.5.6.

iptables -A INPUT -s 3.4.5.6 -j DROP

4.* Запросы на порт 8090 перенаправлять на порт 80 (на этом же сервере).

iptables -t nat -I PREROUTING -p tcp --dport 8090 -j REDIRECT --to-port 80

5.* Разрешить подключение по SSH только из сети 192.168.0.0/24.

iptables -A INPUT -s 192.168.0.0/24 -p tcp --dport 22 -j ACCEPT