Домашнее задание 5

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. конфигурационный файл netplan

```
renderer: networkd
ethernets:
enp0s3:
dhcp4: no
addresses: [192,168,0,8.24]
gateway4: 192.168.1.246
nameservers:
addresses:
- 8.8.8.8
- 1.1.1.1
version: 2
```

   проверяем пингуется ли яндекс `ping 1.1.1.1`

   можем получить адреса яндекса `host -t a yandex.ru`

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.

   добавляем в iptables в таблицу filter доступ к интерфейсу луп `sudo iptables -A INPUT -i lo -j ACCEPT`

   добавляем в iptables в таблицу filter правило, разрешающее подключение по TCP на порт 22, 443, 80 нашего сервера `sudo iptables -A INPUT -p TCP --dport 22 -j ACCEPT`

   `sudo iptables -A INPUT -p TCP --dport 443 -j ACCEPT`

   `sudo iptables -A INPUT -p TCP --dport 80 -j ACCEPT`

   даем возможность нашему серверу находить обновления и если они есть, загружать их. m - match `sudo iptables -A INPUT -m state --state ESTABLISHED, RELATED -j ACCEPT`

   включаем политику по умолчанию `sudo iptables -P INPUT DROP`

3. Запретить любой входящий трафик с IP 3.4.5.6.

   запрещаем любой входящий трафик с указанного айпи. I - insert, s - source `sudo iptables -I INPUT -s 3.4.5.6 -j DROP`

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

Все запросы по tcp на порт 8090 перенаправляем на порт 80 `sudo 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.

   сбрасываем настройки 22 порта по умолчанию для tcp `sudo iptables -I INPUT -p TCP --dport 22 -j DROP`

   `sudo iptables -I INPUT -p TCP --dport 22 -s 192.168.0.0/24 -j ACCEPT`