Задание:

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.

Смотрим текущую конфигурацию настройки сети:

```
abubakirov@abubakirov-VirtualBox:/etc/netplan$ ip a
```

Смотрим текущую маршрутизацию:

```
abubakirov@abubakirov-VirtualBox:/etc/netplan$ ip r
```

Переходим в папку с настройками сети:

```
abubakirov@abubakirov-VirtualBox:/etc/netplan$ cd /etc/netplan
```

Копируем файл конфигурации для бэкапа в домашнюю папку:

```
cp /etc/netplan/01-network-manager-all.yaml /home/abubakirov
```

Редактируем файл настроек:

```
abubakirov@abubakirov-VirtualBox:~$ sudo nano 01-network-manager-all.yaml
```

Настройки:

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [10.0.1.12/24, 192.168.0.1/24] //IP-адреса
      routes:
        - to: default  // маршрут по умолчанию
          via: 10.0.1.5  //шлюз
      nameservers:
        addresses:
          - 1.1.1.1
          - 8.8.8.8
```

Применим новые настройки:

```
abubakirov@abubakirov-VirtualBox:/etc/netplan$ sudo netplan try
```

Проверим новые настройки:

```
abubakirov@abubakirov-VirtualBox:/etc/netplan$ ip a
abubakirov@abubakirov-VirtualBox:/etc/netplan$ ip r
```

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.

Просматриваем текущие разрешения и политики:

```
sudo iptables -L -nv
```

Разрешаем входящий трафик TCP по SSH на 22 порт:

```
sudo iptables -A INPUT -p tcp --dport=22 -j ACCEPT
```

Разрешаем входящий трафик TCP на 80, 443 порты:

```
sudo iptables -A INPUT -p tcp --dport=80 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport=443 -j ACCEPT
```

(можно одной командой –

iptables -A INPUT -p tcp -m multiport --dport 80,443 -j ACCEPT)

Разрешаем любой траффик по loopback:

```
sudo iptables -A INPUT -i lo -j ACCEPT
```

Разрешаем входящие подключения от других серверов, к котоым был сделан исходящий запрос (в том числе к серверу обновления):

```
sudo iptables -I INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Разрешаем ICMP:

```
sudo iptables -A INPUT -p icmp -j ACCEPT
```

Включаем политику запрещения всех неразрешенных пакетов:

```
sudo iptables -P INPUT DROP
```

3. Запретить любой входящий трафик с IP 3.4.5.6.

```
sudo iptables -A INPUT -s 3.4.5.6 -j DROP
```

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

```
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.

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

Старое правило удаляем:

```
sudo iptables -D INPUT 2
```