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.
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.

- Запретить любой входящий трафик с IP 3.4.5.6.
- * Запросы на порт 8090 перенаправлять на порт 80 (на этом же сервере).
- * Разрешить подключение по SSH только из сети 192.168.0.0/24.

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.

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

network:
version: 2
renderer: NetworkManager
ethernets:
enp0s3:
dhcp4: no
addresses: [192.168.31.88/24]
routes:
 - to: default
 via: 192.168.31.1
 nameservers:
 addresses:
 - 8.8.8.8
 - 1.1.1.1
sudo netplan try
ping gb.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.

```
iptables -A INPUT -i eth0 -p TCP --dport 22 -j ACCEPT
iptables -A OUTPUT -o eth0 -p TCP --sport 22 -j ACCEPT

iptables -A INPUT -i eth0 -p TCP --dport 80 -j ACCEPT
iptables -A OUTPUT -o eth0 -p TCP --sport 80 -j ACCEPT

iptables -A INPUT -i eth0 -p TCP --dport 80 -j ACCEPT
iptables -A OUTPUT -o eth0 -p TCP --sport 80 -j ACCEPT

sudo  iptables -A INPUT -p TCP -m state --state ESTABLISHED,RELATED -j ACCEP
sudo iptables -A INPUT -p UDP -m state --state ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A INPUT -p icmp-m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -P INPUT DROP
iptables -P OUTPUT DROP
```

* Запретить любой входящий трафик с IP 3.4.5.6.

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

sudo apt install iptables-persistent netfilter-persistent
sudo netfilter-persistent save
sudo netfilter-persistent start
```

* * 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
```

* * 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
sudo iptables -A INPUT -p tcp --dport 22 -j DROP
```