Урок 5. Настройка сети в Linux. Работа с IPtables
Задание

• 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.

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

```
 # Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.0.0/16]
      routes:
        - to: default
        via: 192.168.0.254
      nameservers:
        addresses:
          - 1.1.1.1
          - 8.8.8.8
```

```
sudo ip addr add 192.168.0.9/255.255.255.0 broadcast 192.168.0.255 dev
enp0s3
ping ya.ru
```

• 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.

```
sudo iptables -L
sudo iptables -A INPUT -p TCP --dport 22 -j ACCEPT
sudo iptables -A INPUT -p TCP --dport 80 -j ACCEPT
sudo iptables -A INPUT -p TCP --dport 443 -j ACCEPT
sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
sudo iptables -P INPUT DROP
```

• Запретить любой входящий трафик с IP 3.4.5.6.

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

•* 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
sudo iptables -t nat -L
```

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

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