

- [Урок 5](#)
 - [Настройка сети и IPtables](#)
 - [Задание](#)

Урок 5

Настройка сети и 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.

```
cat /etc/netplan/01-netcfg.yaml
network:
  version: 2
  renderer: networkd
  ethernets:
    ens7:
      dhcp4: no
      addresses:
        - 192.168.1.195/24
      routes:
        - to: default
          via: 192.168.1.1
      mtu: 1500
      nameservers:
        addresses:
          - 8.8.8.8
          - 77.88.8.8
```

pin 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

```
cat /etc/iptables.rules
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -i lo -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A INPUT -p tcp --dport 22 -j ACCEPT
-A INPUT -p tcp --dport 80 -j ACCEPT
-A INPUT -p tcp --dport 443 -j ACCEPT
-A INPUT -p tcp --dport 8080 -j ACCEPT # Для сервера обновлений
-A INPUT -j DROP
COMMIT
```

- Запретить любой входящий трафик с IP 3.4.5.6.

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

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

```
# Разрешить входящий трафик на порт 8090
sudo iptables -A INPUT -p tcp --dport 8090 -j ACCEPT
sudo iptables -t nat -A OUTPUT -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 -p tcp --dport 22 -s 192.168.0.0/24 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 22 -j DROP
```