## Урок 6. 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.**

*** 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.**

**Решение:**

1. **Настройка статической конфигурации через ip и netplan в Ubuntu**

Откройте терминал на сервере Ubuntu и выполните команду:

**Sudo nano/etc/netplan/00-installer-config.yaml**

Для открытия этой конфигурации.

Внесите следующую информацию в файл конфигурации:

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      addresses: [192.168.0.10/24]
      gateway4: 192.168.0.1
      nameservers:
        addresses: [1.1.1.1, 8.8.8.8]
```

Мы настраиваем сетевой интерфейс enp0s3 на адрес 192.168.0.10 с маской подсети /24, устанавливаем шлюз по умолчанию 192.168.0.1 и настраиваем DNS-сервера на 1.1.1.1 и 8.8.8.8.

После внесения изменений сохраните файл и выполните команду:

**Sudo netplan apply**

Для применения новой конфигурации.

Для проверки работоспособности сети можно выполнить команду:

**Ping google.com**

Для проверки доступности интернета или:

**Ping 192.168.0.1**

Для проверки связи с шлюзом по умолчанию.

2. **Настройка правил iptables для доступности сервисов TCP-портах 22, 80 и 443.**

Выполните команду:

**Sudo iptables –F**

Для очистки всех правил iptables.

Создайте правила iptables для доступности сервисов на TCP-портах 22, 80 и 443:

**Sudo iptables –A INPUT –p tcp –dport 22 –s 192.168.0.0/24 -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 –p tcp –dport 80 –d 127.0.0.1 --dport 8090 j ACCEPT**

**Sudo iptables –A OUTPUT –p tcp –dport 80 –s 127.0.0.1 --dport 8090 j ACCEPT**

**Sudo iptables -P INPUT DROP**

**Sudo iptables -P FORWARD DROP**

**Sudo iptables -P OUTPUT ACCEPT**

В этом примере мы разрешаем подключение к SSH только из сети 192.168.0.0/24, а также открываем доступ к портам 80 и 443 для всех. Так же мы перенаправляем запросы на порт 8090 на 80 и разрешаем подключение серверу обновлений.

3. **Сохраните правила iptables, выполнив команду:**

**Sudo servise iptables- persistem save**

Запрет входящего трафика с IP 3.4.5.6

1) Выполните команду:

**Sudo iptables -A INPUT –s 3.4.5.6 -j DROP**

Для запрета входящего трафика с IP-адреса 3.4.5.6

2) Сохраните правила iptables, выполнив команду

**Sudo servece iptables- persistent save**

Перенаправление запросов на порт 8090 на порт 80

1) Выполните команду:

**Sudo iptables –A PREROUTING –t tcp –dport 22 –s 192.168.0.0/24 j ACCEPT**

Для разрешения подключения к SSH только из сети 192.168.0.0/24.

2) Сохраните правила iptables, выполнив команду

**Sudo servece iptables- persistent save**