

Задания:

1. Настроить статическую конфигурацию (без DHCP) в Ubuntu через ip и netplan. Настроить IP, маршрут по умолчанию и DNS-серверы (1.1.1.1 и 8.8.8.8). Проверить работоспособность сети.

- sudo ip addr add 192.168.2.1/255.255.255.0 broadcast 192.168.2.255 dev enp0s3

- ip a

- sudo ip route add default via 192.168.2.8 dev enp0s3

- cd /etc/netplan

- sudo nano 00-installer-config.yaml

Содержание файла 00-installer-config.yaml

network:

version: 2

renderer: networkd

ethernets:

enp0s3:

dhcp4: no

address: [192.168.1.107/24]

routes:

- to: default

via: 192.168.1.1

nameservers:

addresses:

- 8.8.8.8

- 1.1.1.1

- sudo netplan try

- ping ya.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. Остальные подключения запретить.

- - sudo su
- iptables-save > ip.rules
- nano ip.rules

Содержание файла:

```
# Generated by iptables-save v1.8.7 on Sun Mar 24 19:50:02 2024

*filter

:INPUT DROP [386:55537]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [20536:1994719]

-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p tcp -m tcp --dport 8080 -j ACCEPT

COMMIT

# Completed on Sun Mar 24 19:50:02 2024

# Generated by iptables-save v1.8.7 on Sun Mar 24 19:50:02 2024

*nat

:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]

COMMIT
```

```
# Completed on Sun Mar 24 19:50:02 2024
```

```
-iptables-restore < ip.rules
```

3. Запретить любой трафик с IP 3.4.5.6.

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

Дополнительные (необязательные) задания:

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

```
- 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.

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