Выполнил Мешечкин Д. Инфобез-2345

Задание 1: Произвести настройку сети (статический IP) в Ubuntu через команду ip и систему netplan.

Для настройки статического IP в файле /etc/netplan/00-installer-config.yaml необходимо произвести изменения с соблюдением отступов:

```
network:
 version:2
 renderer: networkd
 ethernets:
  enp0s3:
   dhcp4: no
   addresses: [192.168.1.20/24,192.168.1.120/24] #где второй адрес был добавлен ради интереса]
   routes:
    - to: default
      via: 192.168.1.1
   nameservers:
    addresses:
     - 8.8.8.8
     - 8.8.4.4
#после чего выход с сохранением, проверка через #netplan try.
```

Далее произвел перезагрузку виртуального сервера. В настройках роутера убедился в получении виртуальным сервером статического IP x.x.x.20, после чего в консоли сервера произвел проверки ping, ip r, resolve ctl.
Подключение по ssh к виртуальному серверу работает через оба IP (настроено через мост).

Для добавления IP адреса командами через терминал:

```
ip addr add 192.168.1.121/255.255.255.0 broadcast 192.168.1.255 dev enp0s3 #в данной ситуации добавленный IP не будет сохранён после перезагрузки сервера, добавленный IP будет отображаться как "вторичный" через "ip a".
ip route add default via 192.168.1.1 #добавляет дефолтный шлюз .
```

Задание 2: Переключить настройку сети на автоматическую через DHCP, проверить получение адреса.

Для автоматического получения IP необходимо снова редактировать файл /etc/netplan/00-*.yaml

```
network:
 version: 2
 renderer: networkd
 ethernets:
  enp0s3:
   dhcp4: yes
   nameservers:
    addresses:
     - 8.8.8.8
     - 8.8.4.4

#Далее выход с сохранением, netplan try, при видимости приглашения нажатия Enter настройки сохраняются. В противном случае откатываются назад через 2 минуты (в моём случае роутер автоматически выдал IP 192.168.1.37 и ssh соединение было разорвано. Через 2 минуты конфиг виртуального сервера вернулся к результатам первой части задания 1, где прописаны 2 адреса x.x.x.20 и .120.
```

Задание 3: Изменить адрес DNS на 1.1.1.1 и проверить доступность интернета, например, открыв любой браузер на адрес https://geekbrains.ru.

В данном случае смена DNS сервера с 8.8.8.8 на 1.1.1.1 ничего не поменяет, т.к. 1.1.1.1 - является бесплатным DNS сервером Cloudflare. В то время как 8.8.8.8 - Google public DNS.

Задание 4*: Настроить правила iptables, чтобы из внешней сети можно было обратиться только к портам 80 и 443. Запросы на порт 8080 перенаправлять на порт 80.

Для обеспечения дальнейшей работы по SSH на удаленном сервере:
#iptables -A INPUT -p tcp --dport=22 -j ACCEPT, где будет разрешено подключение по 22порту.

```
iptables -A INPUT -p tcp --dport=80 -j ACCEPT #для подключения через порт 80 протоколами tcp
```

iptables -A INPUT -p tcp --dport=443 -j ACCEPT #для подключения через порт 443 протоколами tcp
iptables -A INPUT -p udp --dport=80 -j ACCEPT #для подключения через порт 80 протоколами udp
iptables -A INPUT -p udp --dport=443 -j ACCEPT #для подключения через порт 443 протоколами udp
iptables -P INPUT DROP #для запрета входящих соединений
iptables -t nat -I PREROUTING -p tcp --dport 8080 -j REDIRECT --to-port 80 #переадрессация пакетов tcp порта с 8080 на порт 80
iptables -t nat -I PREROUTING -p udp --dport 8080 -j REDIRECT --to-port 80 #переадрессация пакетов tcp порта с 8080 на порт 80

В данном задании не уверен на 100%. Вроде указание портов с какого на какой правильно указал. Не до конца разобрался с построутингом и маскарадом.

Задание 5*: Дополнительно к предыдущему заданию настроить доступ по ssh только из указанной сети.

Для данного задания необходимо будет сначала добавить правило в iptables, после чего убрать правило из задания 4*.

iptables -I INPUT -i enp0s3 -p tcp -s 192.168.1.0/24 --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT #данной командой были разрешены все новые и установленные соединения по SSH порт 22 из локальной сети.
iptables -I OUTPUT -o enp0s3 -p tcp -sport 22 -m state -- ESTABLISHED -j ACCEPT #данной командой были разрешены все установленные SSH соединения. Так же можно создать дополнительные правила для других исходящих соединений и указать правило для цепочки OUTPUT.
iptables -D INPUT -p tcp --dport=22 #в данной ситуации удаление требует дополнительных параметров, которые невозможно задать (вроде как). Поэтому была предпринята попытка полного удаления цепочки INPUT, а дальше "ножками" до сервера и устанавливать разрешения по новой для доступа по SSH и остальные стёртые. Соответственно это разрешение (доступ к серверу по SSH из локальной сети) должно быть указано одним из первых и все остальные далее после него.