**L3**

sudo nano /etc/network/interfaces

auto eth0

iface eth0 inet static

address 192.168.1.10

netmask 255.255.255.0

gateway 192.168.1.254

Better option – **nmtui**

**SSH**

sudo –l (enter the root)

adduser username

#AllowUser username (в файле /etc/ssh/sshd\_config)

**Fail2Ban**

sudo systemctl enable fail2ban (чтобы запускалась при перезагрузке сервера)

Создадим новый конфигурационный файл

sudo nano /etc/fail2ban/jail.local

Текст прилагаю ниже

[sshd]

enabled = true

maxretry = 6

findtime = 1h

bantime = 1d

ignoreip = 127.0.0.1/8 23.34.45.56 (тут впишем адреса, с которых МОЖНО подключаться)

IP-адрес, с которого было произведено 6 неудачных попыток SSH-подключения за последний час (3600 секунд), будет заблокирован на одни сутки (86400 секунд).

https://jino.ru/spravka/articles/f2b.html#структура-конфигурационного-файла

**OSPF**

https://doc.s-terra.ru/rh\_output/4.3/Scenarios/output/mergedProjects/ver\_4\_3\_scn\_1\_18\_L3\_external\_balancing/настройка\_динамической\_маршрутизации.htm

sudo apt install frr

vtysh

2. Переходим в режим конфигурации:

Hub-Router# configure terminal

Hub-Router(config)#

3. Включаем процесс OSPF:

Hub-Router(config)# router ospf

Hub-Router(config-router)#

4. Задаем router-id:

Hub-Router(config-router)# ospf router-id 192.168.100.1 (ну или что у нас там)

5. Отрубаем отправку Hello пакетов на всех интерфейсах по умолчанию:

Hub-Router(config-router)# passive-interface default

6. Включаем отправку Hello пакетов на интерфейсах tunnel1 и tunnel2:

Hub-Router(config-router)# no passive-interface tunnel1

Hub-Router(config-router)# no passive-interface tunnel2

7. Включаем OSPF для подсети центрального офиса (адрес/маска) и для подсетей GRE туннелей (адрес/маска и адрес/маска):

Hub-Router(config-router)# network 192.168.100.0/24 area 0 (заменить адрес)

Hub-Router(config-router)# network 100.100.101.0/30 area 0 (заменить адрес)

Hub-Router(config-router)# network 100.100.102.0/30 area 0 (заменить адрес)

8. Выходим из режима конфигурации OSPF:

Hub-Router(config-router)# exit

Hub-Router(config)#

9. Завершаем процедуру конфигурации:

Hub-Router(config)# end

10. Сохраняем (!!!!!) текущую конфигурацию (она будет записана в файл /etc/frr/frr.conf):

Hub-Router# write memory

Note: this version of vtysh never writes vtysh.conf

Building Configuration...

Integrated configuration saved to /etc/frr/frr.conf

[OK]

11. Выходим из консоли FRR обратно в linux-консоль:

Hub-Router# exit

root@Hub-Router:~#

В конфигурационном файле /etc/frr/daemons нужно поставить значение yes для демона ospfd:

ospfd=yes

Перезапускаем сервис FRR:

root@Hub-Router:~# service frr restart

Проверяем, что демон ospfd запущен:

root@Hub-Router:~# ps -ef | grep "ospfd"

root 484 1 0 12:34 ? 00:00:00 /usr/lib/frr/watchfrr -d -F traditional zebra ospfd staticd

frr 543 1 0 12:34 ? 00:00:00 /usr/lib/frr/ospfd -d -F traditional -A 127.0.0.1

**PAT**

PAT, или Port Address Translation, является разновидностью Network Address Translation (NAT), которая позволяет нескольким устройствам в локальной сети делиться одним публичным IP-адресом для доступа к интернету.

sudo apt-get update

sudo apt-get install iptables

На RTR-DATA-1:

sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

sudo iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j DNAT --to-destination 192.168.1.100:80 (весь трафик перенаправляется на сервер с этим адресом)

На RTR-BR-2:

sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

sudo iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j DNAT --to-destination 192.168.2.100:80 (весь трафик перенаправляется на сервер с этим адресом)

**ICMP-Unreachable** для внешних запросов:

sudo iptables -A INPUT -p icmp --icmp-type echo-request -j DROP

sudo iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT

-A INPUT -p icmp --icmp-type echo-request -j DROP:

Это правило блокирует все входящие ICMP запросы типа echo-request (ping). Это делает роутер “невидимым” для пинга извне.

-A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT:

Это правило разрешает исходящие ICMP ответы типа echo-reply (pong), которые роутер генерирует в ответ на успешные пинги.

**Запрет доступа к 77.88.8.1:80**:

sudo iptables -A INPUT -p tcp --dport 80 -s 77.88.8.1 -j DROP

-A INPUT -p tcp --dport 80 -s 77.88.8.1 -j DROP:

Это правило блокирует все входящие TCP соединения на порт 80 (HTTP) от источника 77.88.8.1. Это запрещает доступ к HTTP-сервисам на этом IP-адресе.

**Доступ к подсети офиса с подсети клиентов**:

sudo iptables -A FORWARD -i eth0 -o eth1 -p tcp --dport 389 -j ACCEPT # LDAP

sudo iptables -A FORWARD -i eth0 -o eth1 -p tcp --dport 443 -j ACCEPT # HTTPS

sudo iptables -A FORWARD -i eth0 -o eth1 -p tcp --dport <номер\_порта\_системы\_администрирования> -j ACCEPT # Система администрирования

sudo iptables -A FORWARD -i eth0 -o eth1 -j DROP # Запрет прочего трафика