***Базовая настройка интерфейсов (правда, вроде как все уже преднастроено):***

*nano /etc/network/interfaces*

Правила настройки:

auto <name> - автоматическое включение интерфейса

iface <name> inet static - перевод интерфейса в режим статического ip.

address <IP>/<MASK> - установка ip адреса и маски подсети

gateway <gateway> - шлюз по-умолчанию.

<name> - имя сетевого интерфейса

<IP> - ip адрес в соответствии с топологией

<MASK> - маска подсети в соответствии с топологией

<gateway> - ip адрес шлюза по-умолчанию. Для оконечных устройств шлюзом будет являться вышестоящий маршрутизатор или сетевой экран. На маршрутизаторах не нужно указывать шлюз по-умолчанию

После настройки конфигурационного файла необходимо перезапустить службу networking такой командой:

*systemctl restart networking*

**Добавление доверенного репозитория:**

nano /etc/apt/sources.list

Вписать deb [trusted=yes] http://...

apt update (загрузка пакетов из репозитория)

Чтобы посмотреть все загруженные пакеты смотрим через ls /var/lib/apt/lists/. Там будет папка с репозитория

**GRE если есть ip:**

Для создания GRE туннеля необходимо создать сетевой интерфейс tunnel. Выполнить указанную задачу возможно это при помощи утилиты ip. Но после перезагрузки, созданный интерфейс пропадет. Чтобы этого не происходило, есть решение в виде bash скрипта, который создает интерфейс при запуске машины.

**RTR-DATA-1**

Пусть bash скрипт для первого туннеля называется gre1.up, для второго – gre2.up. Находиться они будут в папке /etc

nano /etc/gre1.up

#!/bin/bash

Ip tunnel add tun1 mode gre local 100.10.10.10 remote 200.20.20.10 ttl 225

Ip link set tun1 up

Ip addr add 10.5.5.0/24 dev tun1

Chmod +x /etc/gre.up

Nano /etc/crontab

Вписываем в конец @reboot root /etc/gre1.up

nano /etc/gre2.up

#!/bin/bash

Ip tunnel add tun2 mode gre local 100.10.10.10 remote 9.9.9.10 ttl 225

Ip link set tun2 up

Ip addr add 10.6.6.0/24 dev tun2

Chmod +x /etc/gre.up

Nano /etc/crontab

Вписываем в конец @reboot root /etc/gre2.up

**RTR-EKB-1** (аналогично RTR-DATA-1, но меняем два адреса местами)

nano /etc/gre1.up

#!/bin/bash

Ip tunnel add tun1 mode gre local 200.20.20.10 remote 100.10.10.10 ttl 225

Ip link set tun1 up

Ip addr add 10.5.5.0/24 dev tun1

Chmod +x /etc/gre.up

Nano /etc/crontab

Вписываем в конец @reboot root /etc/gre1.up

**RTR-KRR-02** (аналогично RTR-DATA-1, но меняем два адреса местами)

nano /etc/gre2.up

#!/bin/bash

Ip tunnel add tun1 mode gre local 9.9.9.10 remote 100.10.10.10 ttl 225

Ip link set tun1 up

Ip addr add 10.6.6.0/24 dev tun1

Chmod +x /etc/gre.up

Nano /etc/crontab

Вписываем в конец @reboot root /etc/gre1.up

**Настройка динамической маршрутизации по OSPF с использованием пакета FRR:**

Ищем и ставим пакет frr

Apt search frr

Apt install frr

Nano /ec/frr/daemons > ospfd=yes

vtysh

conf t или configure terminal

router ospf

**RTR-DATA-1 ISP не обозначаем**

Passive-interface ens\* (имя не помню)

Passive-interface ens\* (имя не помню)

Passive-interface ens\* (имя не помню)

Network 10.5.5.0/24 area 0 (тут мы обозначаем наш будущий GRE туннель, а не выход в исп)

Network 10.6.6.0/24 area 0

Network 192.168.100.0/24 area 0

Network 10.200.100.0/24 area 0

Network 172.16.100.0/24 area 0

Default-information originate

Exit

Write

**RTR-EKB-01**

Passive-interface ens\* (имя не помню)

Passive-interface ens\* (имя не помню)

Network 10.5.5.0/24 area 0 (GRE)

Network 10.15.10.0/24 area 0

Network 10.20.10.0/24 area 0

Default-information originate

Exit

Write

**RTR-KRR-02**

Passive-interface ens\* (имя не помню)

Passive-interface ens\* (имя не помню)

Network 10.6.6.0/24 area 0

Network 10.20.100.0/24 area 0

Network 10.10.100.0/24 area 0

Чтобы адреса передавались ОБЯЗАТЕЛЬНО нужно сделать

Systemctl net.ipv4.ip\_forward=1

Cat /proc/sys/net/ipv4/ip\_forward

***Как проверить что все работает?***

Show ip ospf neighbor

Show ip route

Выполнять команды нужно в конфигураторе

**Настройка интернет шлюзов для организации доступа в «интернет»:**

Apt install iptables-persistance –y (Если она есть. Если нет – ну я надеюсь, что есть хотя бы просто iptables и можно сделать через скрипт)

Начинаем настраивать маскарад на ip

**RTR-DATA-1**

Iptables –t nat –A POSTROUTING –s 192.168.100.0/24 –o <внешний интерфейс который смотрит на ISP> -j MASQUERADE

Iptables –t nat –A POSTROUTING –s 10.200.100.0/24 –o <внешний интерфейс который смотрит на ISP> -j MASQUERADE

Iptables –t nat –A POSTROUTING –s 172.16.100.0/24 –o <внешний интерфейс который смотрит на ISP> -j MASQUERADE

**RTR-EKB-01**

Iptables –t nat –A POSTROUTING –s 10.15.10.0/24 –o <внешний интерфейс который смотрит на ISP> -j MASQUERADE

Iptables –t nat –A POSTROUTING –s 10.20.10.0/24 –o <внешний интерфейс который смотрит на ISP> -j MASQUERADE

**RTR-KRR-02**

Iptables –t nat –A POSTROUTING –s 10.10.100.0/24 –o <внешний интерфейс который смотрит на ISP> -j MASQUERADE

Iptables –t nat –A POSTROUTING –s 10.20.100.0/24 –o <внешний интерфейс который смотрит на ISP> -j MASQUERADE

Если вдруг потребуется пробросить конкретный порт:

Iptables –t nat –A PREROUTING –p udp –dport 53 –I <внешний интерфейс который смотрит на ISP> -j DNAT –to-destination 172.16.100.0/24 (например)

После **ОБЯЗАТЕЛЬНО** сохраняем все изменения

Iptables-save > /etc/iptables/rules.v4

iptables-restore < /etc/iptables/rules.v4

**Если вдруг потребуется настраивать ipsec:**

**RTR-DATA-1**

1. Nano /etc/ipsec.d/ipsec1.conf

conn vpn

auto=start

type=tunnel

authby=secret

ike=aes256;dh21

esp=aes256-sha512

left=10.5.5.2 (local ip адрес)

right=10.5.5.3 (remote ip адрес)

leftprotoport=gre (используется гре)

rightprotoport=gre

pfs=no

Далее нужно создать файл с секретным ключом

Nano /etc/ipsec.secrets

В этом файле нужно описать всего одну строчку содержащую:

1) Локальный ip адрес

2) Удаленный ip адрес

3) : PSK

4) Ключ в кавычках

10.5.5.2 10.5.5.3 : PSK "AtomSkills2024"

chmod 600 /etc/ipsec.d/ipsec1.secret

После перезапустить ipsec:

ipsec restart

Проверка:

Ipsec status

1. Nano /etc/ipsec.d/ipsec2.conf

conn vpn

auto=start

type=tunnel

authby=secret

ike=aes256;dh21

esp=aes256-sha512

left=10.6.6.2 (local ip адрес)

right=10.6.6.1 (remote ip адрес)

leftprotoport=gre (используется гре)

rightprotoport=gre

pfs=no

Далее нужно создать файл с секретным ключом

Nano /etc/ipsec.secrets

В этом файле нужно описать всего одну строчку содержащую:

1) Локальный ip адрес

2) Удаленный ip адрес

3) : PSK

4) Ключ в кавычках

10.6.6.2 10.6.6.1 : PSK "AtomSkills2024"

chmod 600 /etc/ipsec.d/ipsec2.secret

После перезапустить ipsec:

ipsec restart

Проверка:

Ipsec status

**RTR-EKB-01**

Nano /etc/ipsec.d/ipsec.conf

conn vpn

auto=start

type=tunnel

authby=secret

ike=aes256;dh21

esp=aes256-sha512

left=10.5.5.3 (local ip адрес)

right=10.5.5.2 (remote ip адрес)

leftprotoport=gre (используется гре)

rightprotoport=gre

pfs=no

Далее нужно создать файл с секретным ключом

Nano /etc/ipsec.secrets

В этом файле нужно описать всего одну строчку содержащую:

1) Локальный ip адрес

2) Удаленный ip адрес

3) : PSK

4) Ключ в кавычках

10.5.5.3 10.5.5.2 : PSK "AtomSkills2024"

chmod 600 /etc/ipsec.d/ipsec.secret

После перезапустить ipsec:

ipsec restart

Проверка:

Ipsec status

**RTR-KRR-02**

Nano /etc/ipsec.d/ipsec.conf

conn vpn

auto=start

type=tunnel

authby=secret

ike=aes256;dh21

esp=aes256-sha512

left=10.6.6.1 (local ip адрес)

right=10.6.6.2 (remote ip адрес)

leftprotoport=gre (используется гре)

rightprotoport=gre

pfs=no

Далее нужно создать файл с секретным ключом

Nano /etc/ipsec.secrets

В этом файле нужно описать всего одну строчку содержащую:

1) Локальный ip адрес

2) Удаленный ip адрес

3) : PSK

4) Ключ в кавычках

10.6.6.1 10.6.6.2 : PSK "AtomSkills2024"

chmod 600 /etc/ipsec.d/ipsec.secret

После перезапустить ipsec:

ipsec restart

Проверка:

Ipsec status