Предварительный список софта: ssh, frr, sudo, iperf, isc-dhcp server, chrony, bind9, strongswan, mdadm, cronetab

Рассчитать IP адресацию сети. Для IPV4 рассчитываем по следующей таблице:

Маска подсети	Маска в двоичной системе	Префикс	Количество адресов	Обратная маска
255.255.255.255	11111111.11111111.11111111.11111111	/32	1	0.0.0.0
255.255.255.254	11111111.11111111.11111111.11111110	/31	2	0.0.0.1
255.255.255.252	11111111.11111111.11111111.11111100	/30	4	0.0.0.3
255.255.255.248	11111111.11111111.11111111.11111000	/29	8	0.0.0.7
255.255.255.240	11111111.11111111.11111111.11110000	/28	16	0.0.0.15
255.255.255.224	11111111.11111111.11111111.11100000	/27	32	0.0.0.31
255.255.255.192	11111111.11111111.11111111.11000000	/26	64	0.0.0.63
255.255.255.128	11111111.11111111.11111111.10000000	/25	128	0.0.0.127
255.255.255.0	11111111.11111111.11111111.00000000	/24	256	0.0.0.255
255.255.254.0	11111111.11111111.11111110.00000000	/23	512	0.0.1.255
255.255.252.0	11111111.11111111.11111100.00000000	/22	1024	0.0.3.255
255.255.248.0	11111111.11111111.11111000.00000000	/21	2048	0.0.7.255
255.255.240.0	11111111.11111111.11110000.00000000	/20	4096	0.0.15.255
255.255.224.0	11111111.11111111.11100000.00000000	/19	8192	0.0.31.255
255.255.192.0	11111111.11111111.11000000.00000000	/18	16384	0.0.63.255
255.255.128.0	11111111.11111111.10000000.00000000	/17	32768	0.0.127.255
255.255.0.0	11111111.11111111.00000000.00000000	/16	65536	0.0.255.255
255.254.0.0	11111111.11111110.00000000.00000000	/15	131072	0.1.255.255
255.252.0.0	11111111.11111100.00000000.00000000	/14	262144	0.3.255.255
255.248.0.0	11111111.11111000.00000000.00000000	/13	524288	0.7.255.255
255.240.0.0	11111111.11110000.00000000.00000000	/12	1048576	0.15.255.255
255.224.0.0	11111111.11100000.00000000.00000000	/11	2097152	0.31.255.255
255.192.0.0	11111111.11000000.00000000.00000000	/10	4194304	0.63.255.255
255.128.0.0	11111111.10000000.00000000.00000000	/9	8388608	0.127.255.255
255.0.0.0	11111111.00000000.00000000.00000000	/8	16777216	0.255.255.255
254.0.0.0	11111110.00000000.00000000.00000000	/7	33554432	1.255.255.255
252.0.0.0	11111100.00000000.00000000.00000000	/6	67108864	3.255.255.255
248.0.0.0	11111000.00000000.00000000.00000000	/5	134217728	7.255.255.255
240.0.0.0	11110000.00000000.00000000.00000000	/4	268435456	15.255.255.255
224.0.0.0	11100000.00000000.00000000.00000000	/3	536870912	31.255.255.255
192.0.0.0	11000000.00000000.00000000.00000000	/2	1073741824	63.255.255.255
128.0.0.0	10000000.00000000.00000000.00000000	/1	2147483648	127.255.255.255
0.0.0.0	00000000.00000000.00000000.00000000	/0	4294967296	255.255.255.255

В случае 3 варианта нужно выдать сети HQ до 30, а BR до 10.

Составим IP план сети

ISP	
cli – ens33	3.3.3.1/30
hq core – ens34	4.4.4.1/30
br core – ens35	5.5.5.1/30
CLI	
cli – ens34	3.3.3.2/30
HQ-R	
hq core – ens33	4.4.4.2/30
hq net – ens34	192.168.1.1/28
BR-R	

br core – ens33	5.5.5.2/30
br net – ens34	172.168.1.1/29
HQ-SRV	
hq net – ens34	192.168.1.2-15/28
BR-SRV	
br net – ens34	172.168.1.2-7/29
HQ-CLI	
hq net – ens34	192.168.1.2-15/28
HQ-AD	
hq net – ens34	192.168.1.2-15/28

1.named устройств можно сделать при помощи команды:

hostnamectl set-hostname “name”

Перезапустить терминал можно при помощи команды:

exec bash

Для выдачи IP адресов нужно перейти в директорию /etc/network и через редактор текста открыть interface.

Для настройки порта нужно написать следующее:

Auto ens(number on interface, check ip –be a)

iface ens(n) inet static (dhcp if it is)

address «ip»

gateway «gate» (if it is gate – DELITE IT!)

Включить ip forwarding

Через редактор текстовых документов (vi, vim, nano)

В /etc/sysctl.conf убрать комментарии с net.ipv4.ip_forward=1 на маршрутизаторах и isp

Проверить sysctl -p

2.Настройка маршрутизации через frr и протокол ospf

В директории /etc/frr находятся конфиги. В daemon меняем no на yes в нужном протоколе маршрутизации. Я делаю через OSPF.

Рестартим через systemctl restart frr.service. Можно посмотртреть через status.

vtysh – оболочка для конфигурации. Пишем, заходим, конфигурируем.

conf t

router ospf

ospf router-id 3.3.3.1 # только на isp

passive-interface ens33 # только на isp

network 3.3.3.0/30 area 0

network 4.4.4.0/30 area 0

network 5.5.5.0/30 area 0

Для сохранения пишем do wr.

Для ip forwarding пишем ашгщытпшфтшптф в режиме конфигурации.(**СЛЕТАЕТ ПО РОФЛУ, ДЕЛАТЬ ЧЕРЕЗ ФАЙЛ**)

Для проверки

show interface [имя интерфейса] - без указания конкретного интерфейса, показывает информацию о все доступных интерфейсах (IP-адрес, MAC, Тип и др.)

show ip route - список сетевых маршрутов

OSPF

show ip ospf - сумма параметров OSPF (router-id, ...).

show ip ospf interface - отображает интерфейсы анонсированных сетей.

show ip ospf neighbor- указывает устройства с которыми установлено соседство.

show ip ospf route - список маршрутов и источников, откуда они были получены

3.DHCP HQ-R

/etc/default/isc-dhcp-server - файл для указания интерфейсов, на которых DHCP-сервер будет ожидать запросы;

/etc/dhcp/dhcpd.conf - основной файл конфигурации DHCP-сервера для IPv4-адресов (подсети, группы подсетей, одиночные хосты);

/usr/share/doc/isc-dhcp-server/ - хранилище доков по DHCP-серверу (есть бэкап файла конфигурации);

/var/lib/dhcp/dhcp.leases - файл учета выданных адресов.

В /etc/dhcp/dhcpd.conf

```
option domain-name "example.org";
option domain-name-servers ns1.example.org, ns2.example.org;

default-lease-time 600;
max-lease-time 7200;
```

```
ddns-update-style none;
```

```
subnet 192.168.1.0 netmask 255.255.255.224 {
  range 192.168.1.2 192.168.1.14;
  option domain-name-servers ns.wsr.mv;
  option domain-name "wsr.mv";
  option routers 192.168.1.1;
  option broadcast-address 192.168.1.15;
  default-lease-time 600;
  max-lease-time 7200;
}
```

В /etc/default/isc-dhcp-server писать интерфейс

```
INTERFACESv4="ens35"
INTERFACESv6=""
```

4. Создание человеческой души. Руководство для чайников

sudo adduser username

Либо

useradd -c "Admin" admin -U -s bim/bash

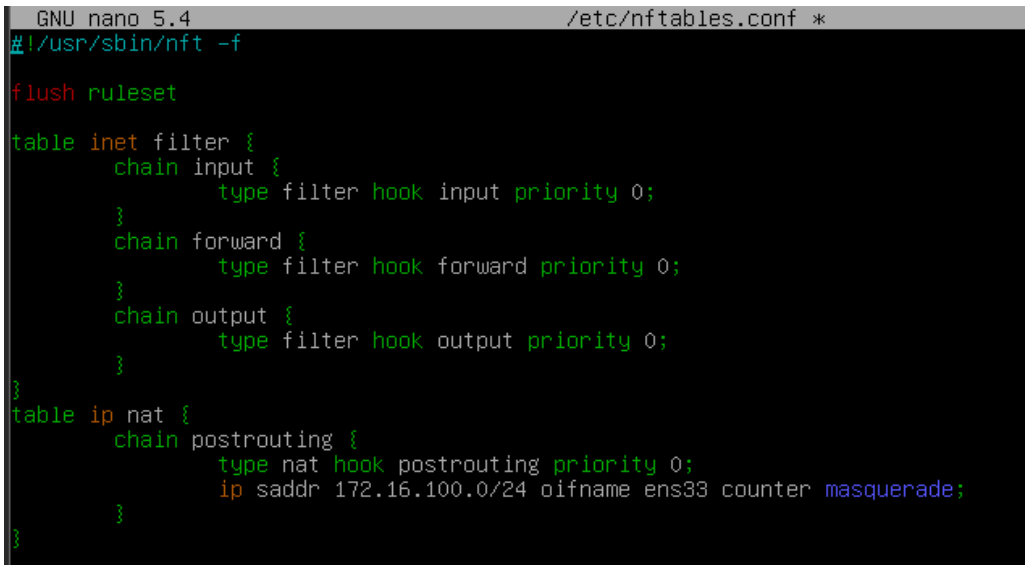
passwd admin

5.Замер пропускной способности при помощи iperf3

Скачать – на роутере левой сети пишем iperf3 –s, с ISP iperf3 –c 4.4.4.2 адрес куда посылаем.

6. Nftables и стулья

Если ориентироваться на догму февральскую, то делаем так (только на боках):



Новый взгляд предлагает

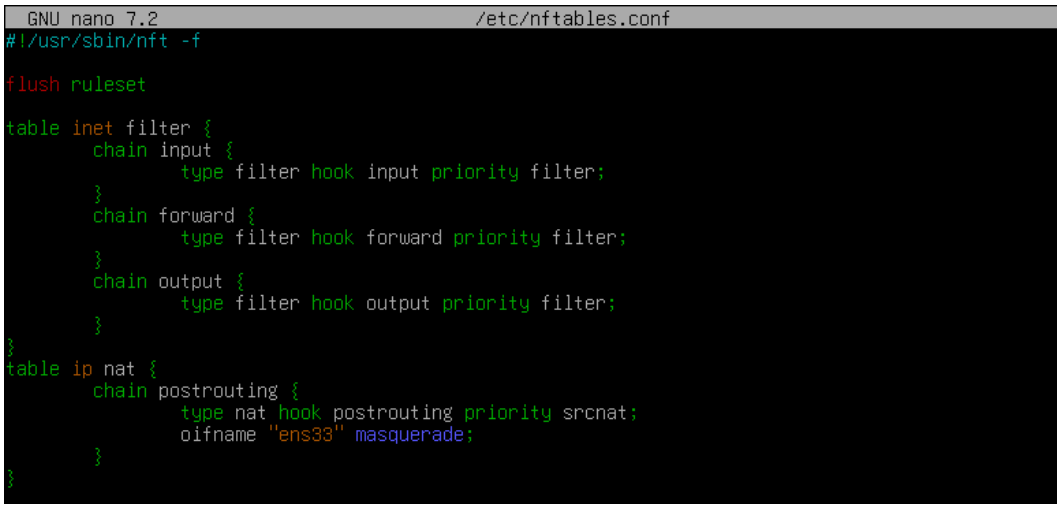


table inet nat {

chain POSTROUTING {

type nat hook postrouting priority srcnat;

oifname "ВНЕШНИЙ ПОРТ СМОТРЯЩИЙ НА ИНТЕРНЕТ" masquerade;

}

}

Для проверки используется команда nft -f /etc/nftables.conf

Для активации NAT надо добавить скрипт в автозапуск systemctl enable nftables

7. **SSH**

Конфиг в nano /etc/ssh/sshd_config. Тут ставим порт, указанный в задании.

Я хз по поводу перенаправления без дениса, там не статика и всё взорвётся

Переходим к настройке перенаправления трафика на HQ-R.

nano /etc/nftables.conf

ПЕРЕД НАСТРОЙКОЙ NAT ПИШЕМ СЛЕДУЮЩИЕ СТРОЧКИ

chain PREROUTING {

type nat hook prerouting priority filter;

ip daddr 1.1.1.2 tcp dport 3035(в зависимости от варианта) dnat ip to 192.168.1.2:3035 (в зависимости от ip и варианта)

}

```
#!/usr/sbin/nft -f

flush ruleset

table inet filter {
        chain input {
                type filter hook input priority filter;
        }
        chain forward {
                type filter hook forward priority filter;
        }
        chain output {
                type filter hook output priority filter;
        }
}
table inet nat {
        chain postrouting {
                type nat hook postrouting priority srcnat;
                oifname "ens33" masquerade;
        }
        chain prerouting {
                type nat hook prerouting priority filter;
                ip daddr 4.4.4.2 tcp dport 3035 dnat ip to 192.168.1.2:3035
        }
}
```

8. **ЗАПРЕТ CLI**

На устройстве, к которому подключаются, нужно через nftable поставить следующие правила:

table inet filter {

chain input {

type filter hook input priority filter;

ip saddr 10.10.10.2/30 tcp dport 3035 counter drop }

}

```
  GNU nano 7.2                                  /etc/nftables.conf
#!/usr/sbin/nft -f

flush ruleset

table inet filter {
        chain input {
                type filter hook input priority filter;
        }
        chain forward {
                type filter hook forward priority filter;
        }
        chain output {
                type filter hook output priority filter;
        }
}
table inet filter {
        chain input {
        type filter hook input priority filter;
        ip saddr 3.3.3.2/30 tcp dport 3035 counter drop;
        }
}
```

9. **ГИРЯ**

На боковых пишем такое nano /etc/gre.up

На левом

#!/bin/bash

ip tunnel add tun0 mode gre local 4.4.4.2 remote 5.5.5.2

ip addr add 10.5.5.1/30 dev tun0

ip link set up tun0

ip route add 172.168.1.0/29 via 10.5.5.2

После даём права chmod +x /etc/gre.up. Для активации просто нужно ввести путь к файлу

```
lo               UNKNOWN        127.0.0.1/8 ::1/128
ens33            UP             4.4.4.2/30 fe80::20c:29ff:feb5:82c3/64
ens34            UP             192.168.1.1/28 fe80::20c:29ff:feb5:82cd/64
ens35            DOWN           fe80::20c:29ff:feb5:82d7/64
gre0@NONE        DOWN
gretap0@NONE     DOWN
erspan0@NONE     DOWN
tun0@NONE        UNKNOWN        10.5.5.1/30 fe80::404:402/64
```

На правом

#!/bin/bash

ip tunnel add tun0 mode gre local 5.5.5.2 remote 4.4.4.2

ip addr add 10.5.5.2/30 dev tun0

ip link set up tun0

ip route add 192.168.1.0/28 via 10.5.5.1

```
root@BR-R:~# ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
ens33            UP             5.5.5.2/30 fe80::20c:29ff:feaf:c96a/64
ens34            UP             172.168.1.1/29 fe80::20c:29ff:feaf:c974/64
ens35            DOWN
gre0@NONE        DOWN
gretap0@NONE     DOWN
erspan0@NONE     DOWN
tun0@NONE        UNKNOWN        10.5.5.2/30 fe80::505:502/64
```

Через crontab пихаем в автозапуск /etc/crontab пишем внизу @reboot root /etc/gre.up.

11. **Секс по телефону**

Качаем strongswan открываем /etc/ipsec

На левом пишем:

conn vpn

auto=start

type=tunnel

authby=secret

left=5.5.5.1

right=4.4.4.1

leftsubnet=0.0.0.0/0

rightsubnet=0.0.0.0/0

leftprotoport=gre

rightprotoport=gre

ike=aes128-sha256-modp3072

esp=aes128-sha256

left - локальный

На параллельном так:

conn vpn

auto=start

type=tunnel

authby=secret

left=4.4.4.1

right=5.5.5.1

leftsubnet=0.0.0.0/0

rightsubnet=0.0.0.0/0

leftprotoport=gre

rightprotoport=gre

ike=aes128-sha256-modp3072

esp=aes128-sha256

На обоих роутерах в /etc/ipsec.secret пишем

4.4.4.1 5.5.5.1 : PSK “P@ssw0rd”