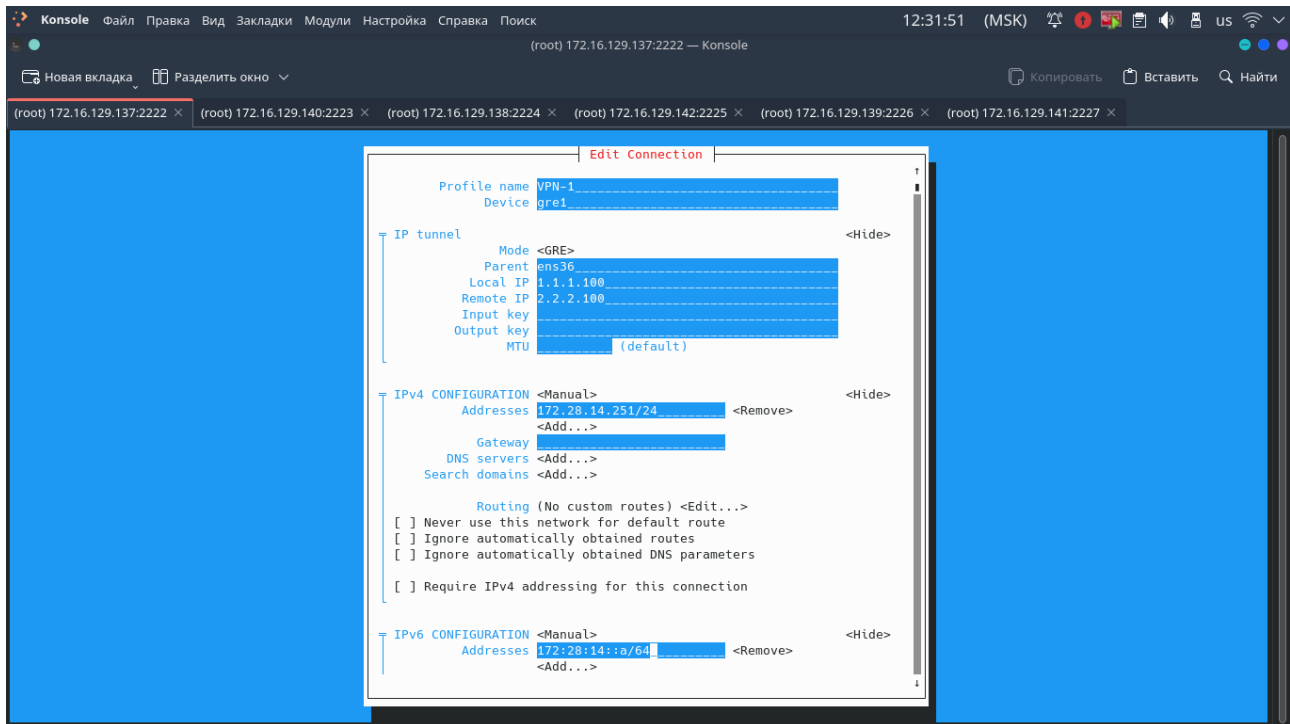


Создание VPN tunnel

R1:

nmtui-edit → <Add> → IP tunnel

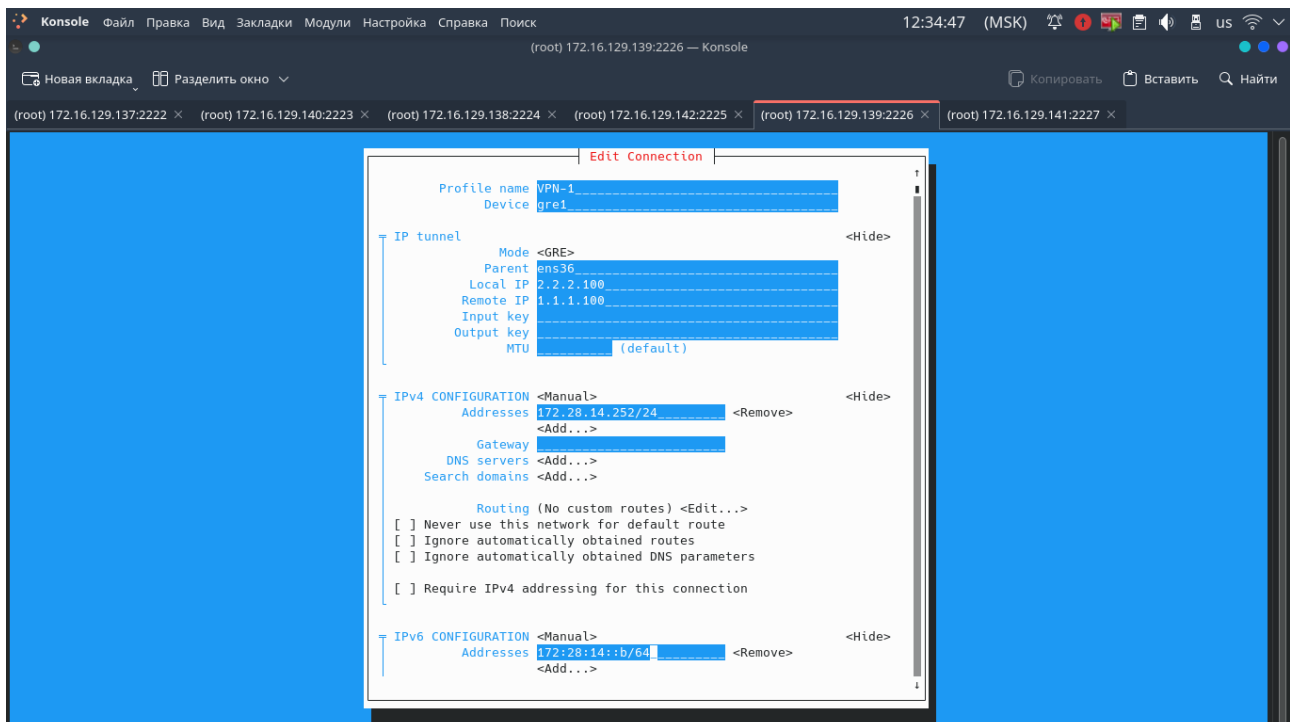


Command: nmcli connection modify VPN-1 ip-tunnel.ttl 64

Данная команда настраивает ограничение на количество промежуточных маршрутизаторов, которые могут пройти пакеты через VPN-соединение, устанавливая значение TTL на 64.

R2:

nmtui-edit → <Add> → IP tunnel



Проверка доступности сети

R1:

- ping -c 2 172.28.14.252
- traceroute 172.28.14.252
- ping -c 2 172:28:14::b
- traceroute 172:28:14::b

R2:

- ping -c 2 172.28.14.251
- ping -c 2 172:28:14::a
- traceroute 172.28.14.251
- traceroute 172:28:14::a

Данные проверки позволяют узнать доступность ранее созданного VPN соединения.

Далее нам нужно включить переадресацию сетевых интерфейсов на сервере R1 и R2.

R1:

```
# nano /etc/sysctl.conf  
  
    net.ipv4.ip_forward=1  
    net.ipv6.conf.all.forwarding=1  
    net.ipv6.conf.ens37.accept_ra=2
```

Затем применить команду **sysctl -p**, чтобы «sysctl.conf» применил настройки маршрутизации.

На сервере R2 нужно провести аналогичную настройку, но без добавлением строки связанную с **accept_ra=2**, которая предназначена для автоматической конфигурации адресов IPv6 и других параметров сети.

Примечание:

Для настройки OSPF сети скачайте программное обеспечение frr (apt install frr).

Настройка OSPF

На серверах R1 и R2 настроить конфигурационный файл daemons, изменив следующее:

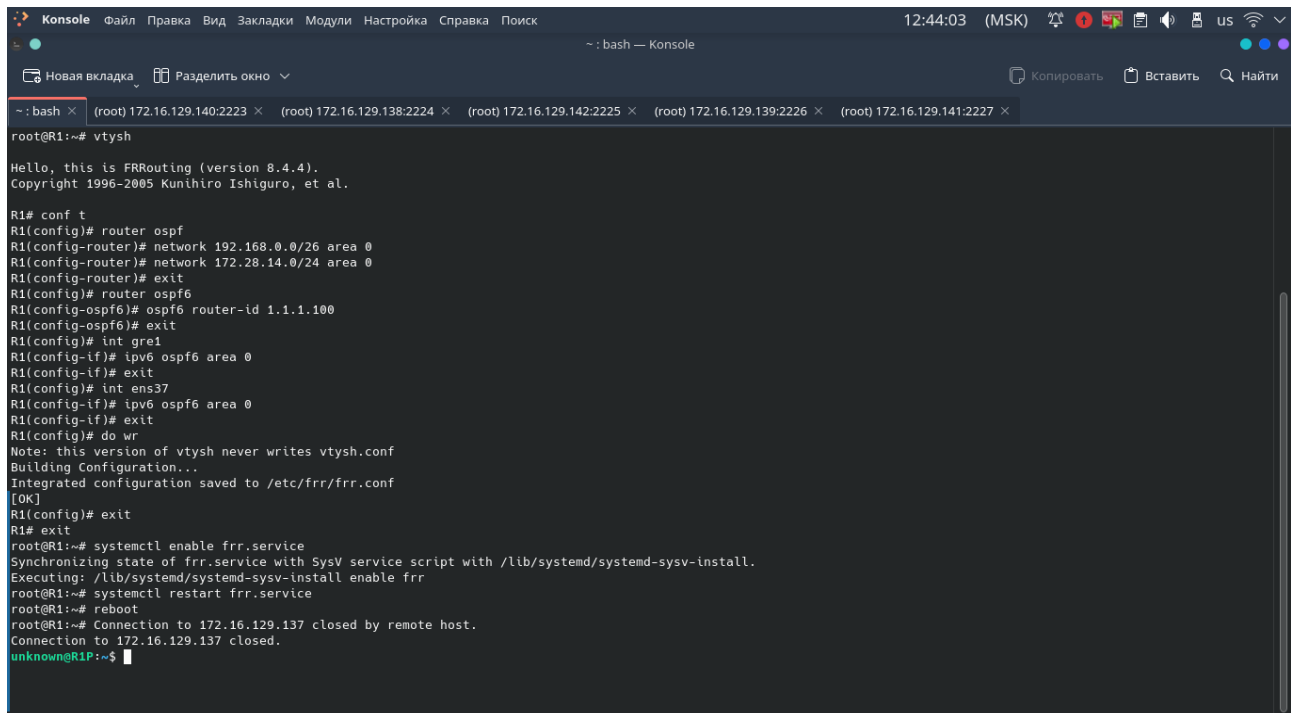
```
# nano /etc/frr/daemons
```

```
ospfd=yes
```

```
ospf6d=yes
```

```
# systemctl restart frr.service
```

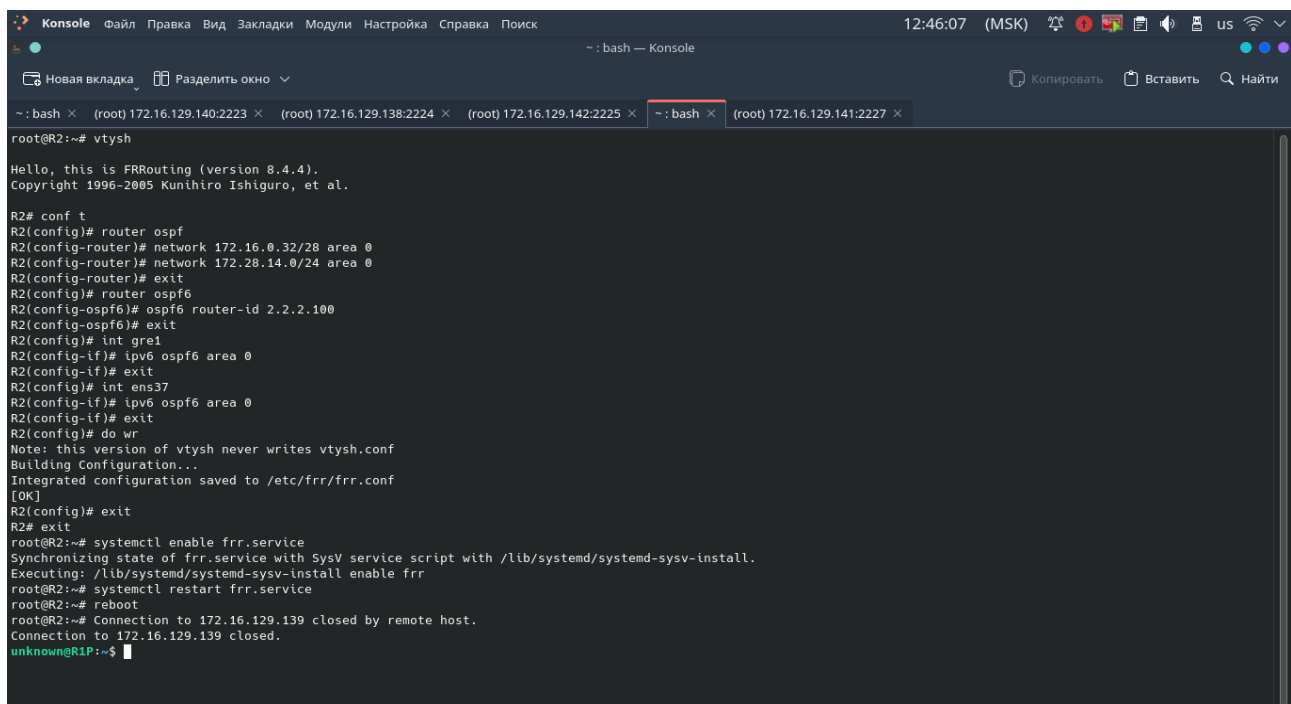
R1:



```
~: bash x (root) 172.16.129.140:2223 x (root) 172.16.129.138:2224 x (root) 172.16.129.142:2225 x (root) 172.16.129.139:2226 x (root) 172.16.129.141:2227 x
root@R1:~# vtysh
Hello, this is FRRouting (version 8.4.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

R1# conf t
R1(config)# router ospf
R1(config-router)# network 192.168.0.0/26 area 0
R1(config-router)# network 172.28.14.0/24 area 0
R1(config-router)# exit
R1(config)# router ospf6
R1(config-ospf6)# ospf6 router-id 1.1.1.100
R1(config-ospf6)# exit
R1(config)# int gre1
R1(config-if)# ipv6 ospf6 area 0
R1(config-if)# exit
R1(config)# int ens37
R1(config-if)# ipv6 ospf6 area 0
R1(config-if)# exit
R1(config)# do wr
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
R1(config)# exit
R1# exit
root@R1:~# systemctl enable frr.service
Synchronizing state of frr.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable frr
root@R1:~# systemctl restart frr.service
root@R1:~# reboot
root@R1:~# Connection to 172.16.129.137 closed by remote host.
Connection to 172.16.129.137 closed.
unknown@R1P:~$
```

R2:



```
~: bash x (root) 172.16.129.140:2223 x (root) 172.16.129.138:2224 x (root) 172.16.129.142:2225 x ~: bash x (root) 172.16.129.141:2227 x
root@R2:~# vtysh
Hello, this is FRRouting (version 8.4.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

R2# conf t
R2(config)# router ospf
R2(config-router)# network 172.16.0.32/28 area 0
R2(config-router)# network 172.28.14.0/24 area 0
R2(config-router)# exit
R2(config)# router ospf6
R2(config-ospf6)# ospf6 router-id 2.2.2.100
R2(config-ospf6)# exit
R2(config)# int gre1
R2(config-if)# ipv6 ospf6 area 0
R2(config-if)# exit
R2(config)# int ens37
R2(config-if)# ipv6 ospf6 area 0
R2(config-if)# exit
R2(config)# do wr
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
R2(config)# exit
R2# exit
root@R2:~# systemctl enable frr.service
Synchronizing state of frr.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable frr
root@R2:~# systemctl restart frr.service
root@R2:~# reboot
root@R2:~# Connection to 172.16.129.139 closed by remote host.
Connection to 172.16.129.139 closed.
unknown@R1P:~$
```

Проверка доступности настроенной сети

R1:

```
Konsole  Файл  Правка  Вид  Закладки  Модули  Настройка  Справка  Поиск  12:49:22 (MSK)
(root) 172.16.129.140:2223 — Konsole

Новая вкладка  Разделить окно  Копировать  Вставить  Найти

(root) 172.16.129.137:2222 x (root) 172.16.129.140:2223 x (root) 172.16.129.138:2224 x (root) 172.16.129.142:2225 x (root) 172.16.129.139:2226 x (root) 172.16.129.141:2227 x

root@R1-PC:~# ping -c 2 172.16.0.42
PING 172.16.0.42 (172.16.0.42) 56(84) bytes of data.
64 bytes from 172.16.0.42: icmp_seq=1 ttl=62 time=2.59 ms
64 bytes from 172.16.0.42: icmp_seq=2 ttl=62 time=3.80 ms

--- 172.16.0.42 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 2.588/3.192/3.797/0.604 ms
root@R1-PC:~# traceroute 172.16.0.42
traceroute to 172.16.0.42 (172.16.0.42), 30 hops max, 60 byte packets
 1 192.168.0.1 (192.168.0.1) 0.609 ms 0.384 ms 0.425 ms
 2 172.28.14.252 (172.28.14.252) 4.270 ms 4.033 ms 3.840 ms
 3 172.16.0.42 (172.16.0.42) 6.413 ms 6.222 ms 6.391 ms
root@R1-PC:~#
```

R2:

```
Konsole  Файл  Правка  Вид  Закладки  Модули  Настройка  Справка  Поиск  12:49:14 (MSK)
(root) 172.16.129.141:2227 — Konsole

Новая вкладка  Разделить окно  Копировать  Вставить  Найти

(root) 172.16.129.137:2222 x (root) 172.16.129.140:2223 x (root) 172.16.129.138:2224 x (root) 172.16.129.142:2225 x (root) 172.16.129.139:2226 x (root) 172.16.129.141:2227 x

root@PC-R2:~# ping -c 2 192.168.0.60
PING 192.168.0.60 (192.168.0.60) 56(84) bytes of data.
64 bytes from 192.168.0.60: icmp_seq=1 ttl=62 time=2.36 ms
64 bytes from 192.168.0.60: icmp_seq=2 ttl=62 time=2.47 ms

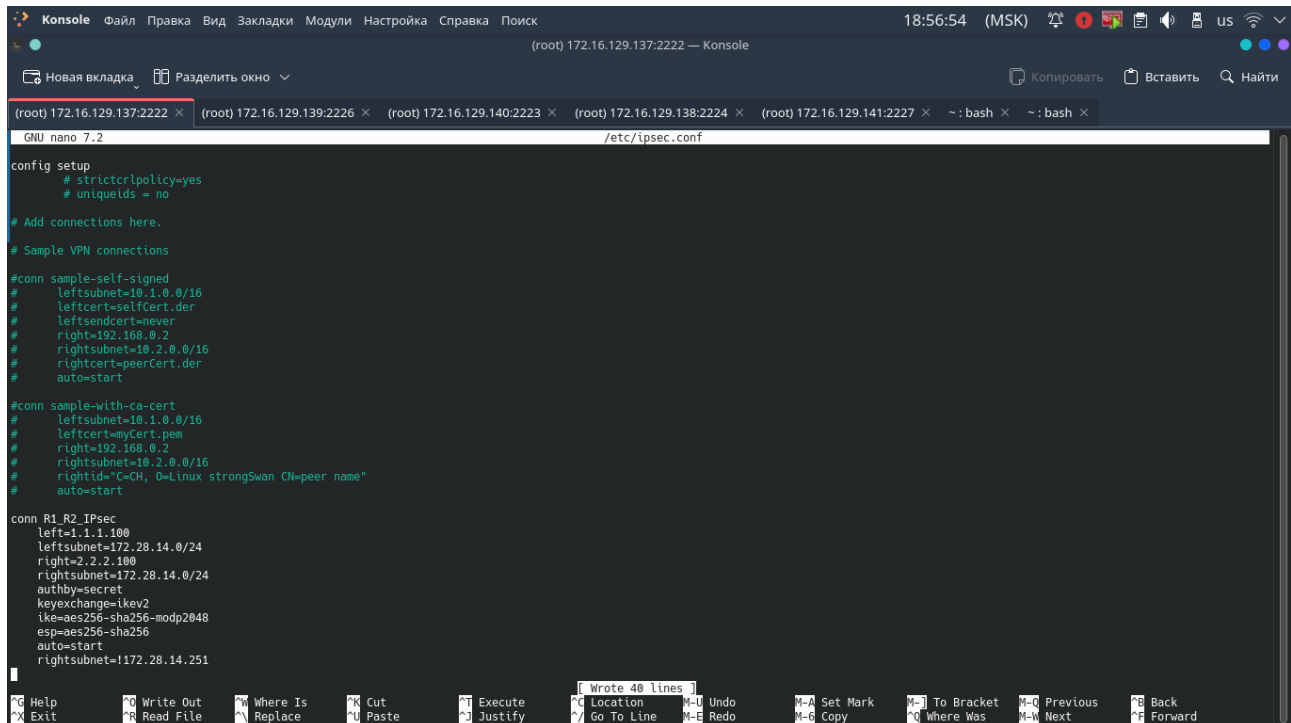
--- 192.168.0.60 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 2.362/2.415/2.468/0.053 ms
root@PC-R2:~# traceroute 192.168.0.60
traceroute to 192.168.0.60 (192.168.0.60), 30 hops max, 60 byte packets
 1 172.16.0.33 (172.16.0.33) 0.918 ms 0.557 ms 0.370 ms
 2 172.28.14.251 (172.28.14.251) 4.759 ms 4.976 ms 11.605 ms
 3 192.168.0.60 (192.168.0.60) 11.415 ms 11.203 ms 11.004 ms
root@PC-R2:~#
```

Обеспечение безопасности VPN (IPsec)

1) Установка арт: *apt-get install strongswan*

2) Настраиваем конфигурационный файл "/etc/ipsec.conf":

R1:



```
GNU nano 7.2 /etc/ipsec.conf

config setup
    # strictcrpolicy=yes
    # uniqueids = no

# Add connections here.

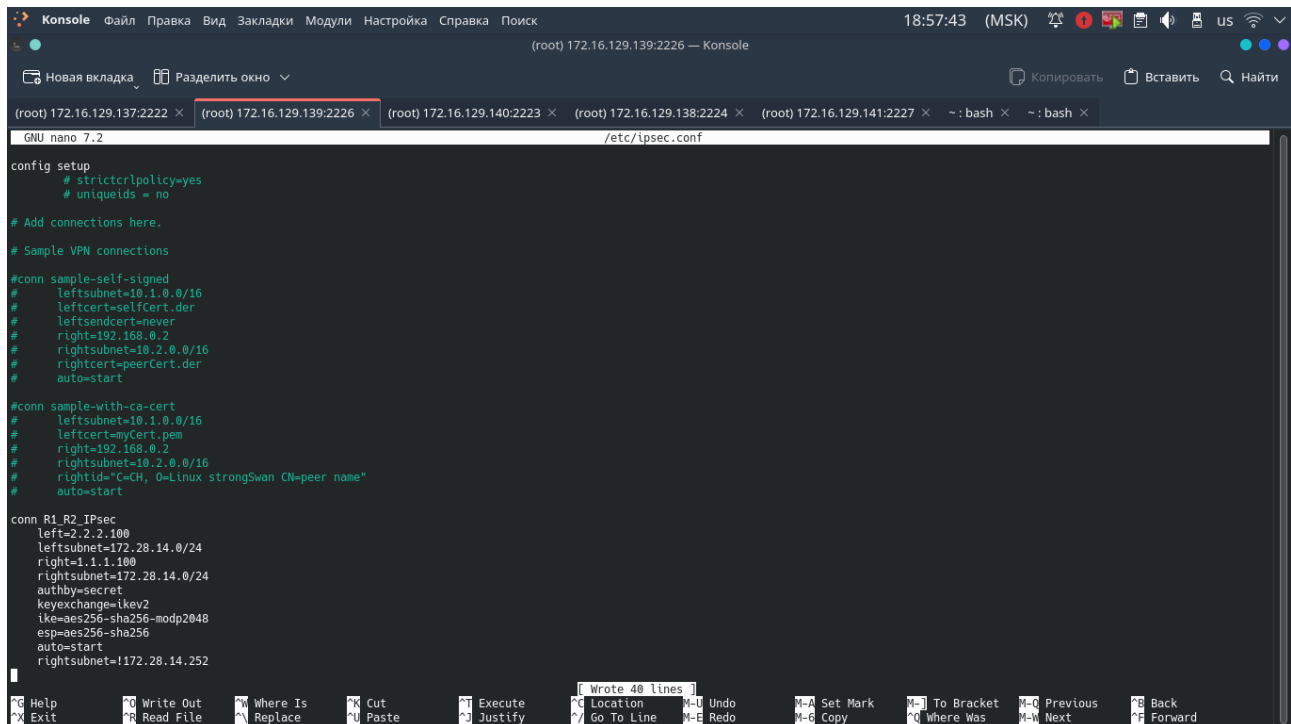
# Sample VPN connections

#conn sample-self-signed
#    leftsubnet=10.1.0.0/16
#    leftcert=selfCert.der
#    leftsendcert=never
#    right=192.168.0.2
#    rightsubnet=10.2.0.0/16
#    rightcert=peerCert.der
#    auto=start

#conn sample-with-ca-cert
#    leftsubnet=10.1.0.0/16
#    leftcert=myCert.pem
#    right=192.168.0.2
#    rightsubnet=10.2.0.0/16
#    rightid="C=CH, O=Linux strongSwan CN=peer name"
#    auto=start

conn R1_R2_IPsec
    left=1.1.1.100
    leftsubnet=172.28.14.0/24
    right=2.2.2.100
    rightsubnet=172.28.14.0/24
    authby=secret
    keyexchange=ikev2
    ike=aes256-sha256-modp2048
    esp=aes256-sha256
    auto=start
    rightsubnet=!172.28.14.251
```

R2:



```
GNU nano 7.2 /etc/ipsec.conf

config setup
    # strictcrpolicy=yes
    # uniqueids = no

# Add connections here.

# Sample VPN connections

#conn sample-self-signed
#    leftsubnet=10.1.0.0/16
#    leftcert=selfCert.der
#    leftsendcert=never
#    right=192.168.0.2
#    rightsubnet=10.2.0.0/16
#    rightcert=peerCert.der
#    auto=start

#conn sample-with-ca-cert
#    leftsubnet=10.1.0.0/16
#    leftcert=myCert.pem
#    right=192.168.0.2
#    rightsubnet=10.2.0.0/16
#    rightid="C=CH, O=Linux strongSwan CN=peer name"
#    auto=start

conn R1_R2_IPsec
    left=2.2.2.100
    leftsubnet=172.28.14.0/24
    right=1.1.1.100
    rightsubnet=172.28.14.0/24
    authby=secret
    keyexchange=ikev2
    ike=aes256-sha256-modp2048
    esp=aes256-sha256
    auto=start
    rightsubnet=!172.28.14.252
```

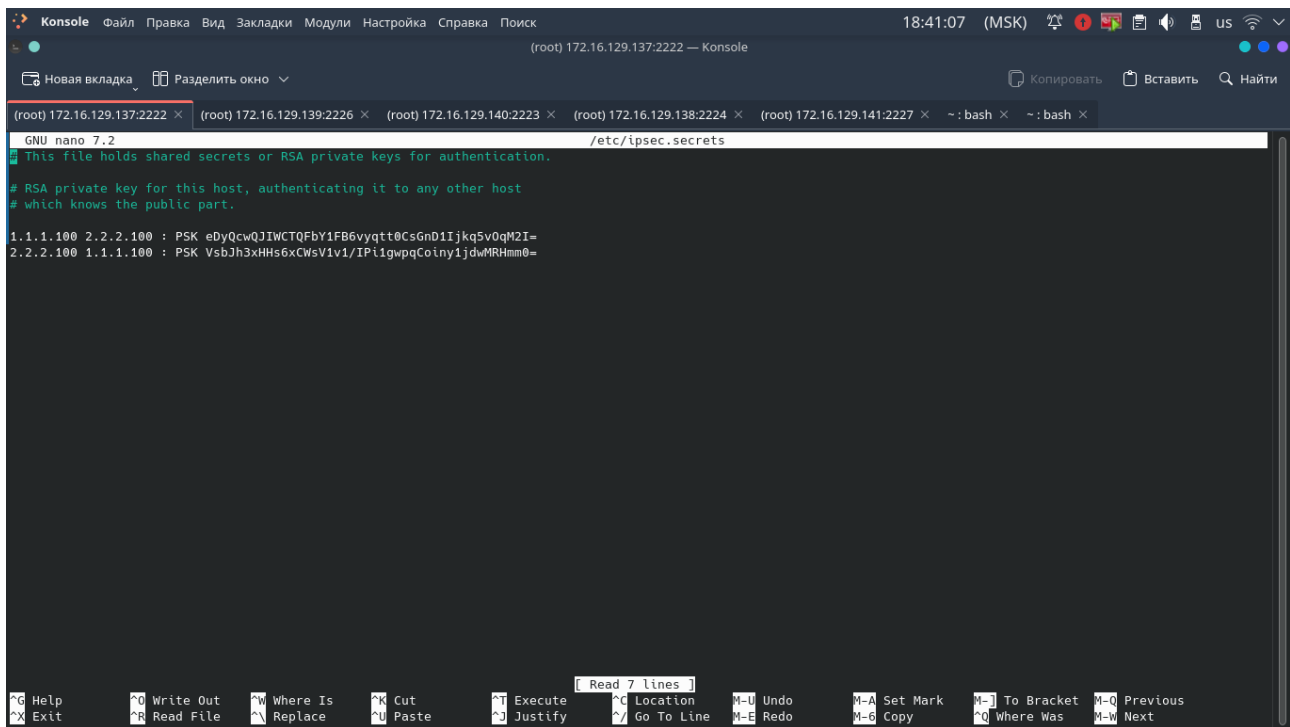
3) Генерируем PSK на сервере R1 и R2: ***openssl rand -base64 32***

4) Настраиваем конфигурационный файл `"/etc/ipsec.secrets"` на серверах R1 и R2:

Примечание:

R1 → `openssl rand -base64 32 (copy_r1)` → 1.1.1.100 ... PSK ... (paste_r1)

R2 → `openssl rand -base64 32 (copy_r2)` → 2.2.2.100 ... PSK ... (paste_r2)



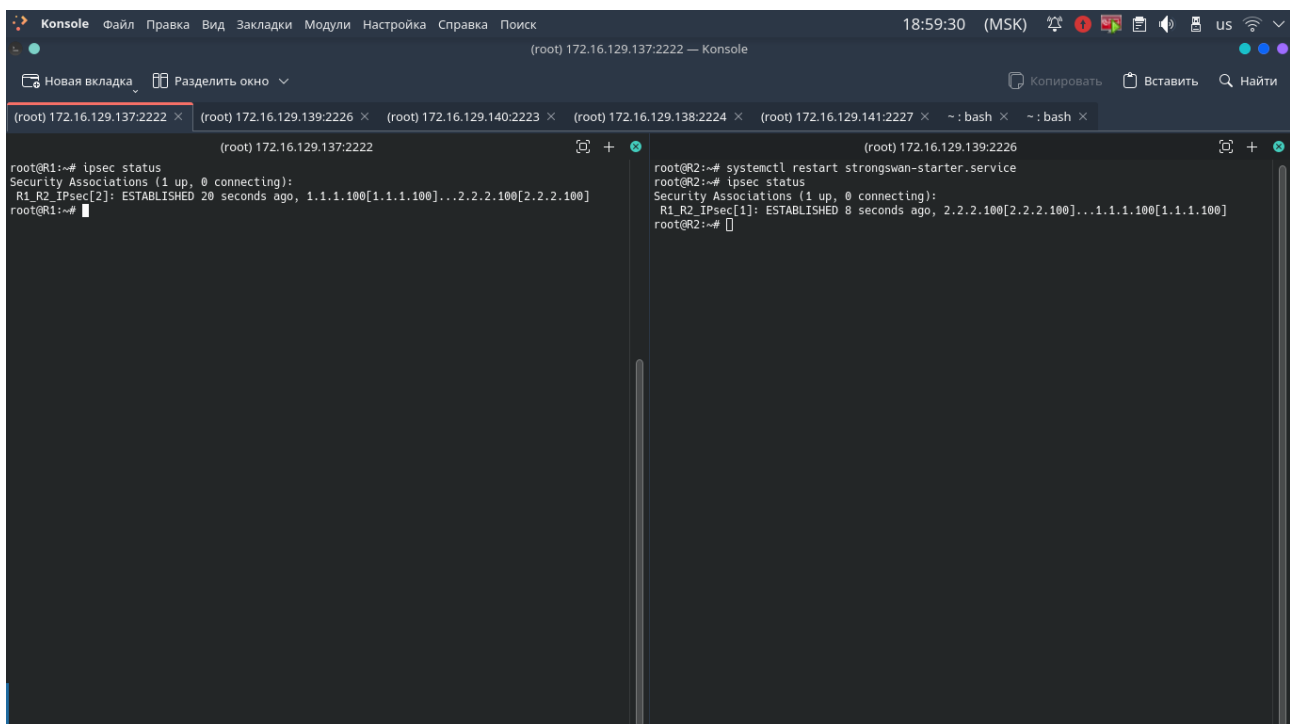
The screenshot shows a terminal window titled 'Konsole' with a dark theme. The active tab is '(root) 172.16.129.137:2222'. The terminal displays the contents of the file `/etc/ipsec.secrets` using the `nano` editor. The file contains the following text:

```
GNU nano 7.2 /etc/ipsec.secrets
# This file holds shared secrets or RSA private keys for authentication.
#
# RSA private key for this host, authenticating it to any other host
# which knows the public part.
1.1.1.100 2.2.2.100 : PSK eDyQcwQJIWCTQFbY1FB6vyqtt0CsGnD1Ijkq5v0qM2I=
2.2.2.100 1.1.1.100 : PSK VsbJh3xHhS6xCWsV1v1/IPi1gwpqCoiny1jdWNRHm0=
```

The terminal window includes a menu bar at the top with options like 'Файл', 'Правка', 'Вид', 'Закладки', 'Модули', 'Настройка', 'Справка', and 'Поиск'. At the bottom, there is a status bar with various keyboard shortcuts for editing and navigation.

5) Перезагружаем «strongswan»: ***systemctl restart strongswan-starter.service***

6) Проверяем настроенное IPsec соединение между серверами:



The screenshot shows two terminal windows side-by-side. The left window is titled '(root) 172.16.129.137:2222' and shows the output of the `ipsec status` command on server R1. The right window is titled '(root) 172.16.129.139:2226' and shows the output of the `systemctl restart strongswan-starter.service` command followed by `ipsec status` on server R2.

Left terminal (R1):

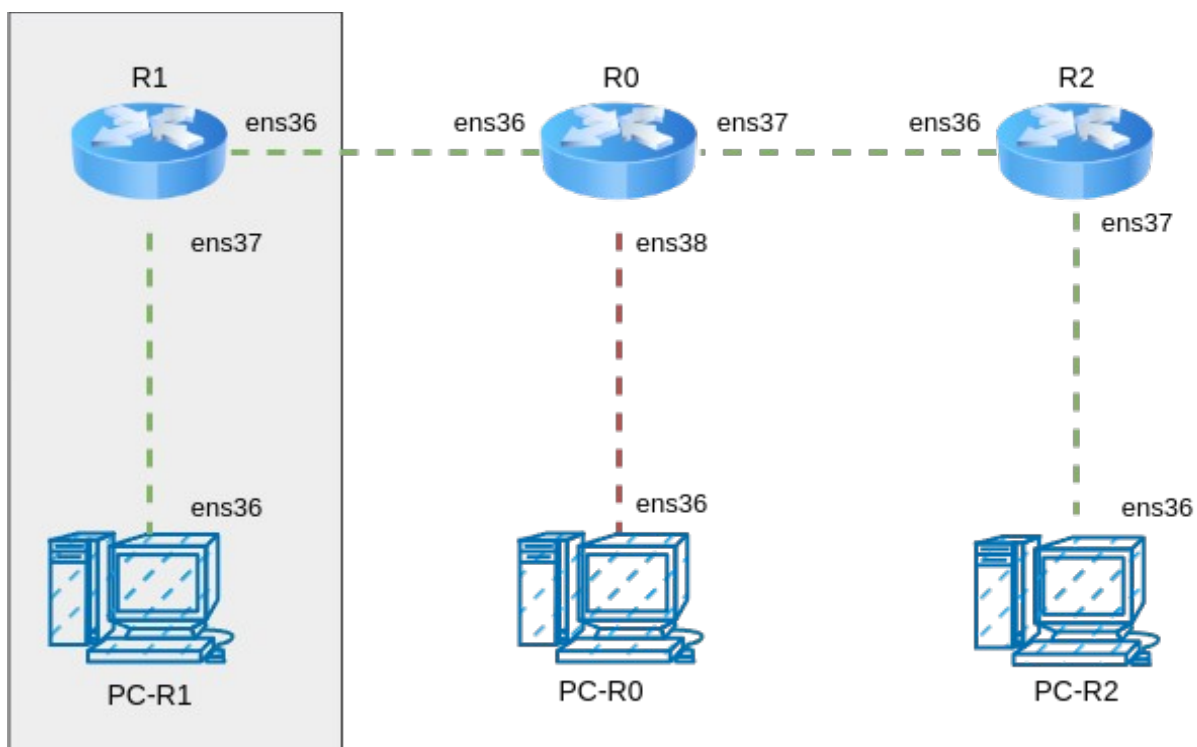
```
root@R1:~# ipsec status
Security Associations (1 up, 0 connecting):
R1_R2_IPsec[2]: ESTABLISHED 20 seconds ago, 1.1.1.100[1.1.1.100]...2.2.2.100[2.2.2.100]
root@R1:~#
```

Right terminal (R2):

```
root@R2:~# systemctl restart strongswan-starter.service
root@R2:~# ipsec status
Security Associations (1 up, 0 connecting):
R1_R2_IPsec[1]: ESTABLISHED 8 seconds ago, 2.2.2.100[2.2.2.100]...1.1.1.100[1.1.1.100]
root@R2:~#
```

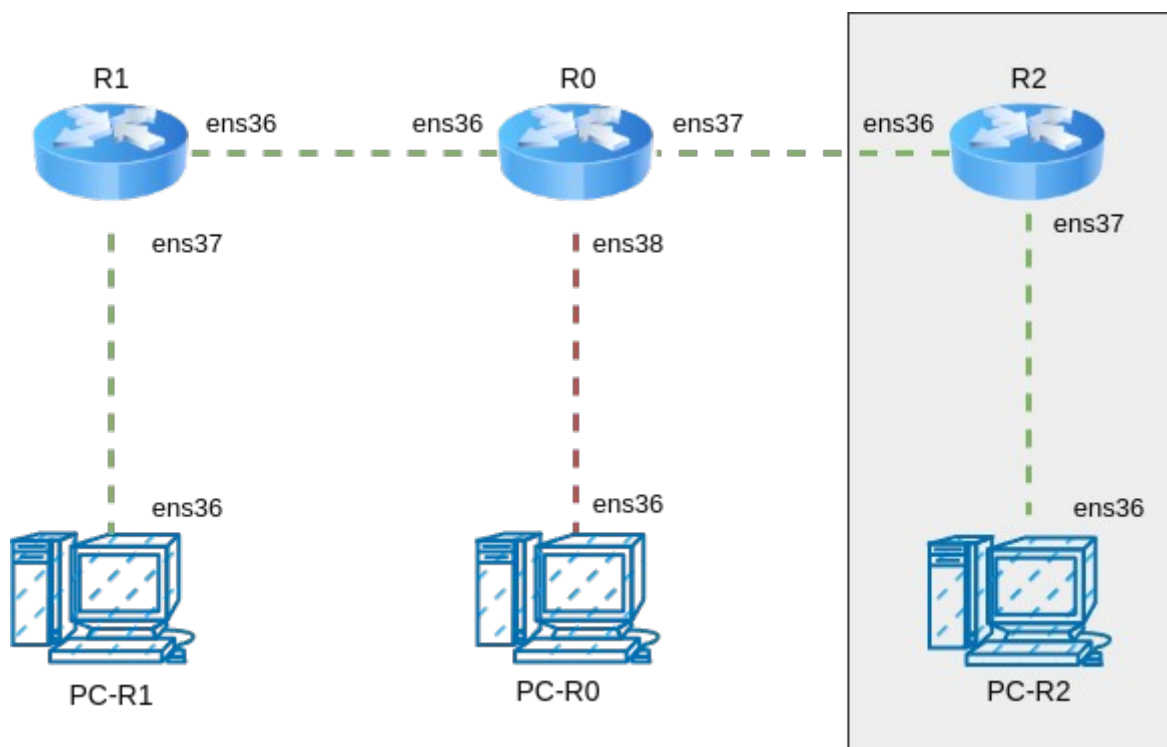
Визуальный пример полученной конфигурации

R1 и PC-R1:



R1 и PC-R1 получили доступ к сети PC-R2.

R2 и PC-R2:



R2 и PC-R2 получили доступ к сети PC-R1.