

Enp0s3 – делать внутренним интерфейсом

Enp0s8 – Делать внешним интерфейсом, чтобы было удобнее

Включаем на всех

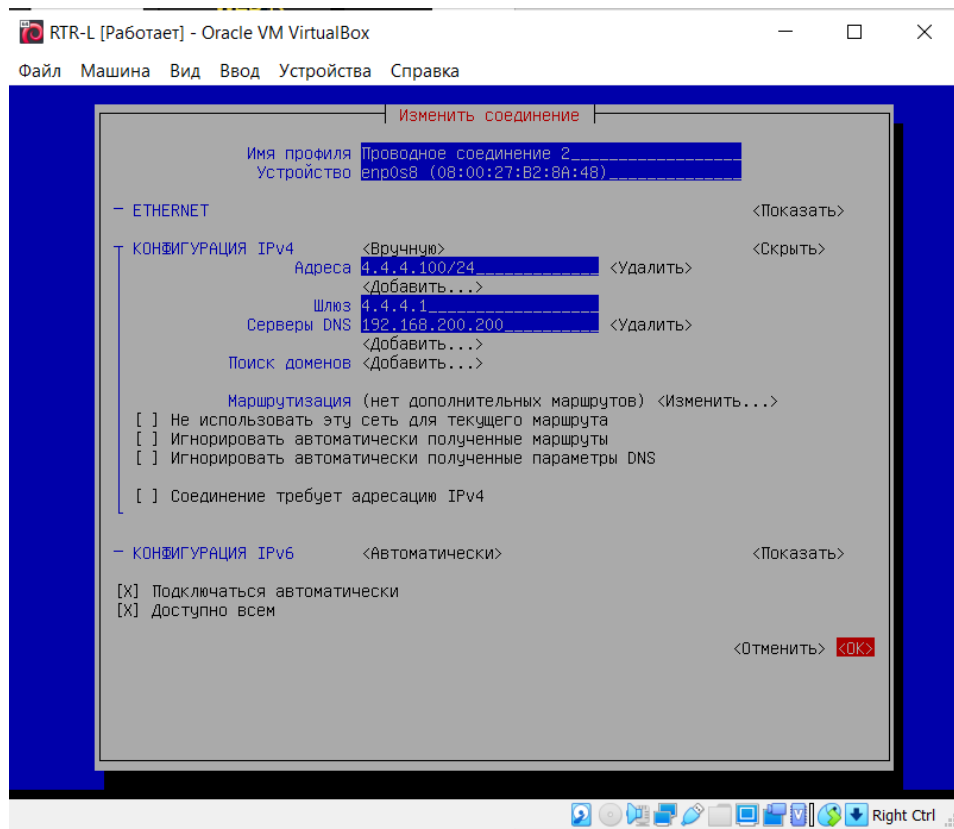
RTR-L

#apt install -y network-manager firewalld wireguard wireguard-tools (сделать пока включен nat)

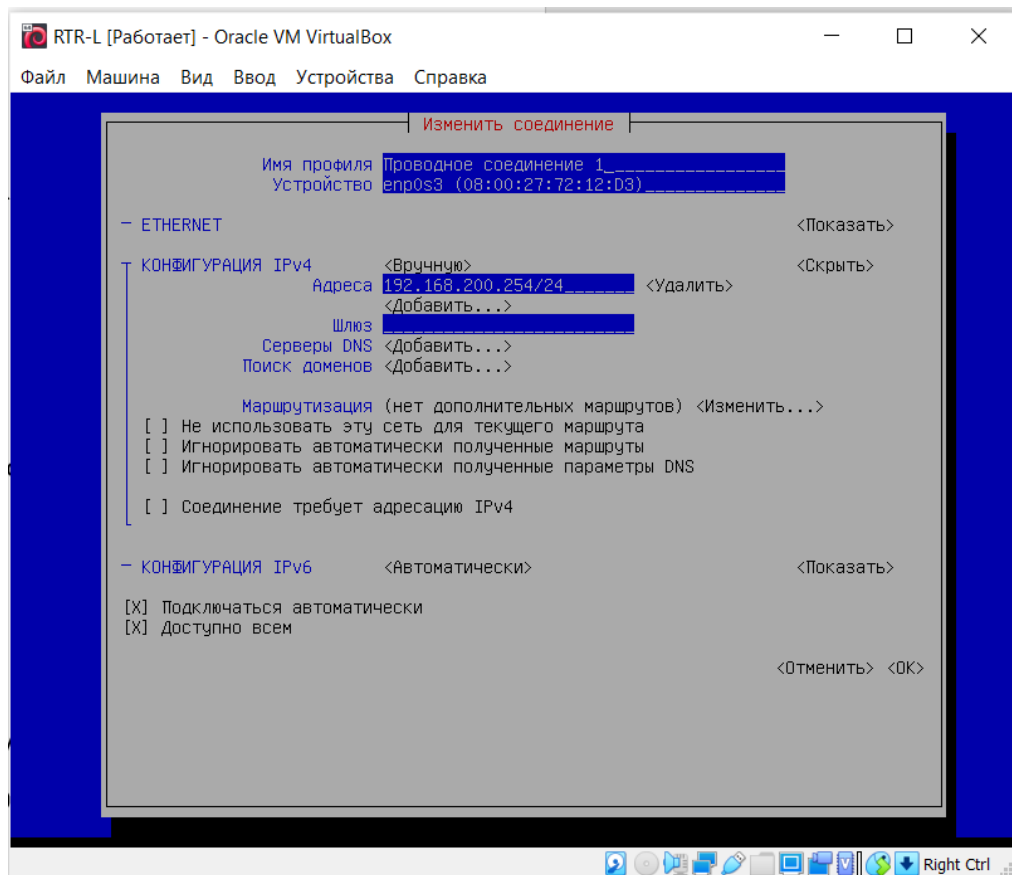
#nmtui

Переставить на всех с Автоматически на Ручную на всех VM

int WiredConnection 2 (Enp0s8) ip 4.4.4.100/24, gateway 4.4.4.1 DNS 192.168.100.200



int WiredConnection 1 (Enp0s3) ip 192.168.100.254/24



hostname RTR-L

#reboot

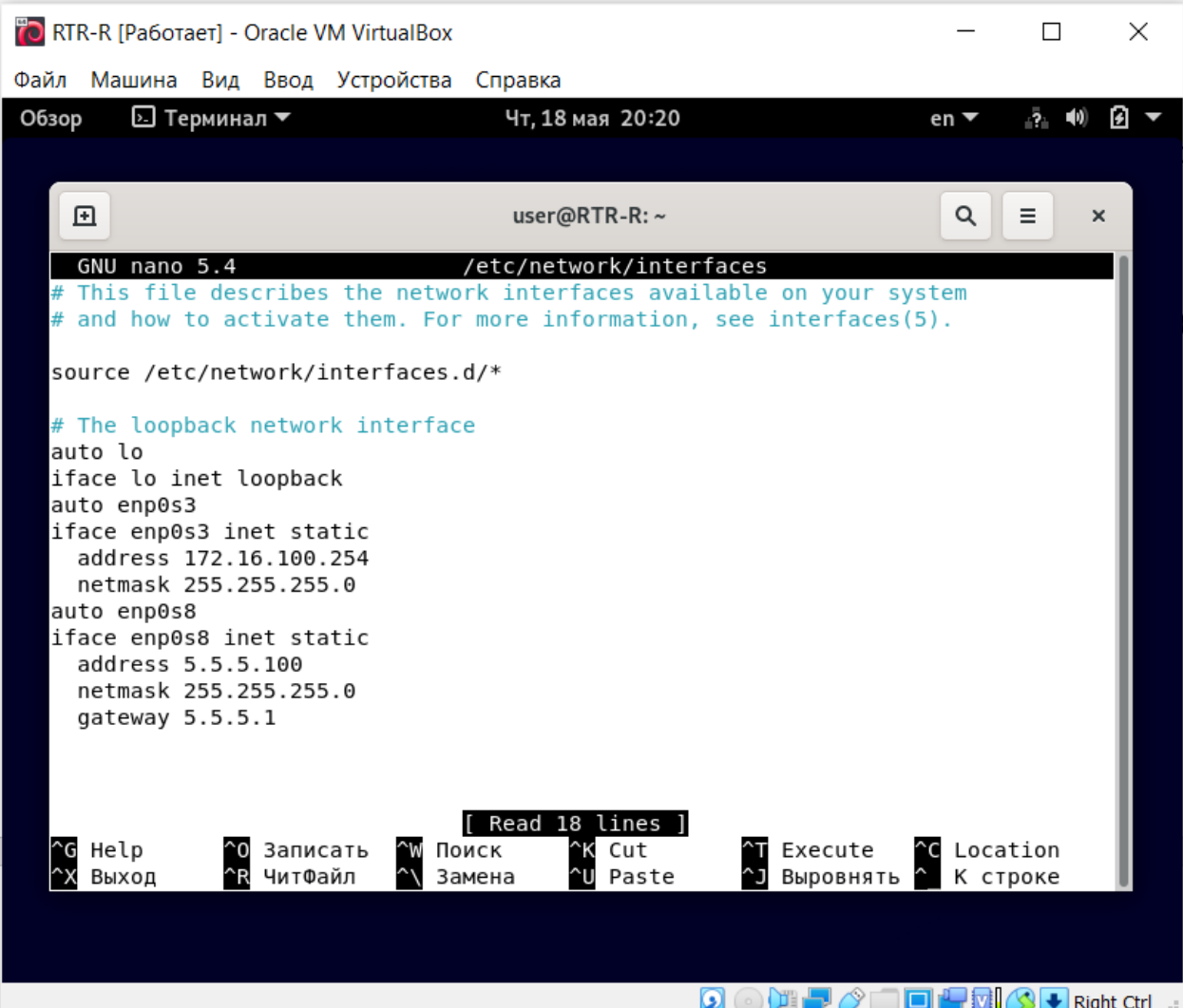
RTR-R С графическим интерфейсом

#apt install -y network-manager openssh-server firewalld wireguard wireguard-tools

# nano /etc/network/interfaces

int WiredConnection 1 (Enp0s8) ip 5.5.5.100/24, gateway 5.5.5.1 DNS 4.4.4.100

int WiredConnection 2 (Enp0s3) ip 172.16.100.254/24



The screenshot shows a terminal window titled "RTR-R [Работает] - Oracle VM VirtualBox". The terminal is running the nano text editor on the file /etc/network/interfaces. The file content is as follows:

```
GNU nano 5.4 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
auto enp0s3
iface enp0s3 inet static
    address 172.16.100.254
    netmask 255.255.255.0
auto enp0s8
iface enp0s8 inet static
    address 5.5.5.100
    netmask 255.255.255.0
    gateway 5.5.5.1
```

At the bottom of the terminal window, there is a status bar with the text "[ Read 18 lines ]" and a set of keyboard shortcuts for nano:

^G Help	^O Записать	^W Поиск	^K Cut	^T Execute	^C Location
^X Выход	^R ЧитФайл	^_ Замена	^U Paste	^J Выводить	^_ К строке

hostname RTR-R

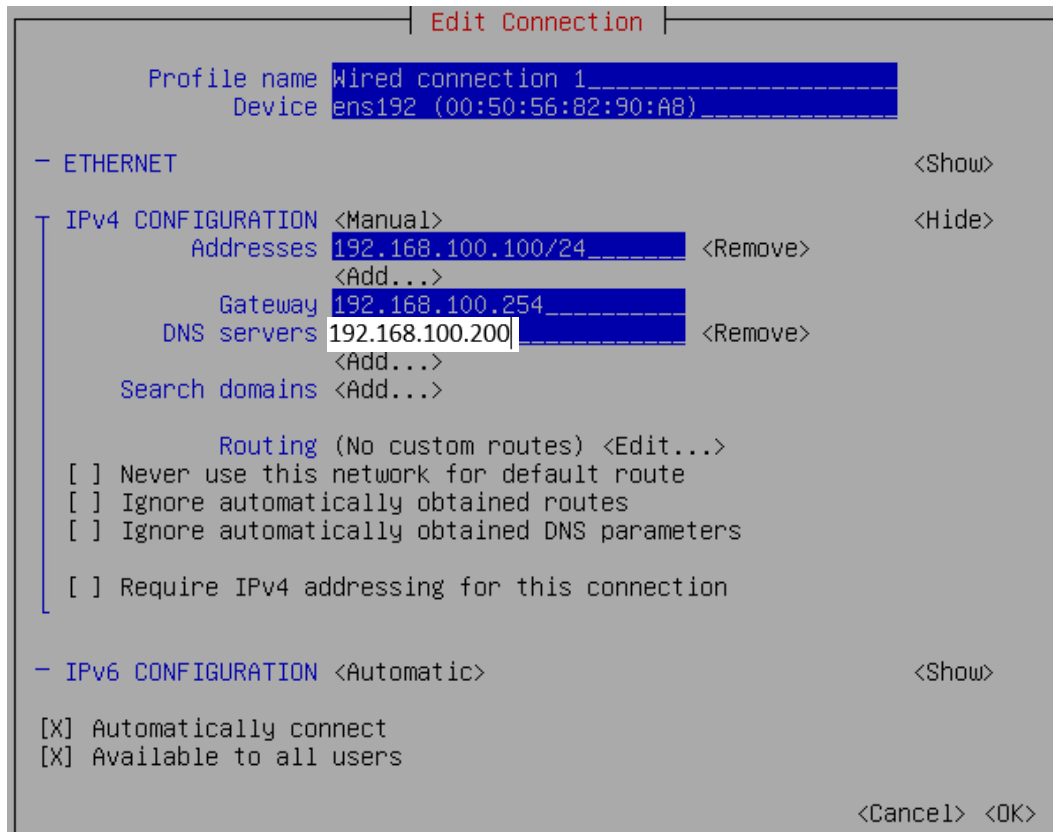
#reboot

WEB-L

#apt install -y network-manager chrony openssh-server nginx lynx cifs-utils

```
#nmtui
```

```
int WiredConnection 1 (Enp0s3) ip 192.168.100.100/24, gateway  
192.168.100.254, DNS 192.168.100.200
```



```
hostname WEB-L
```

```
#reboot
```

```
WEB-R
```

```
#apt install -y network-manager chrony openssh-server nginx lynx cifs-utils
```

```
#nmtui
```

```
int WiredConnection 1 (Enp0s3) ip 172.16.100.100/24, gateway 172.16.100.254,  
DNS 4.4.4.100
```

Edit Connection

Profile name

Wired connection 1

Device

ens192 (00:50:56:82:FF:A2)

ETHERNET

Show

IPv4 CONFIGURATION

Manual

Hide

Addresses

172.16.100.100/24

Remove

Add...

Gateway

172.16.100.254

DNS servers

4.4.4.100

Remove

Add...

Search domains

Add...

Routing (No custom routes)

Edit...

Never use this network for default route

Ignore automatically obtained routes

Ignore automatically obtained DNS parameters

Require IPv4 addressing for this connection

IPv6 CONFIGURATION

Automatic

Show

Automatically connect

Available to all users

Cancel

OK

hostname WEB-R

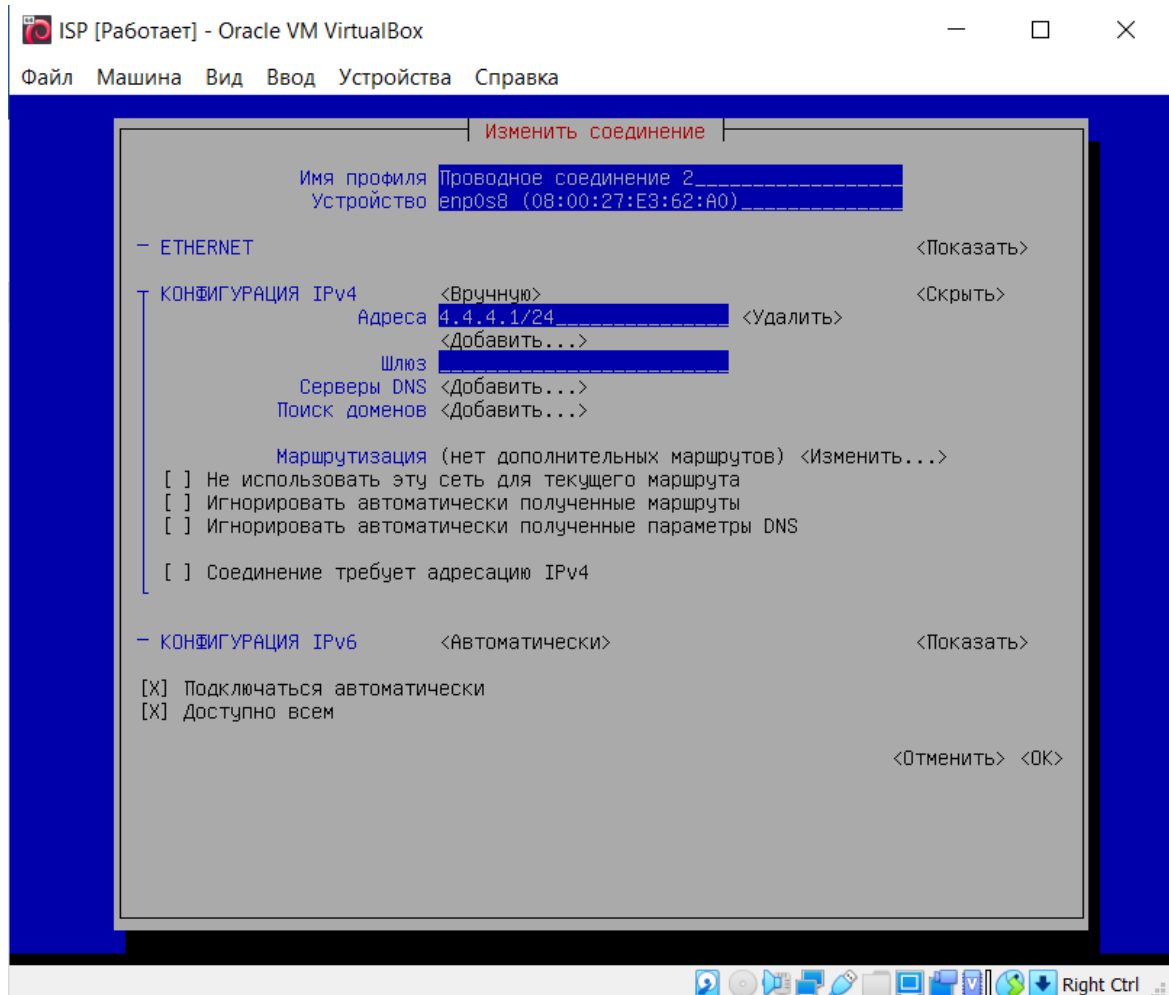
#reboot

ISP Enp0s3 – Центральный Enp0s8 – Левый Enp0s9 - Правый

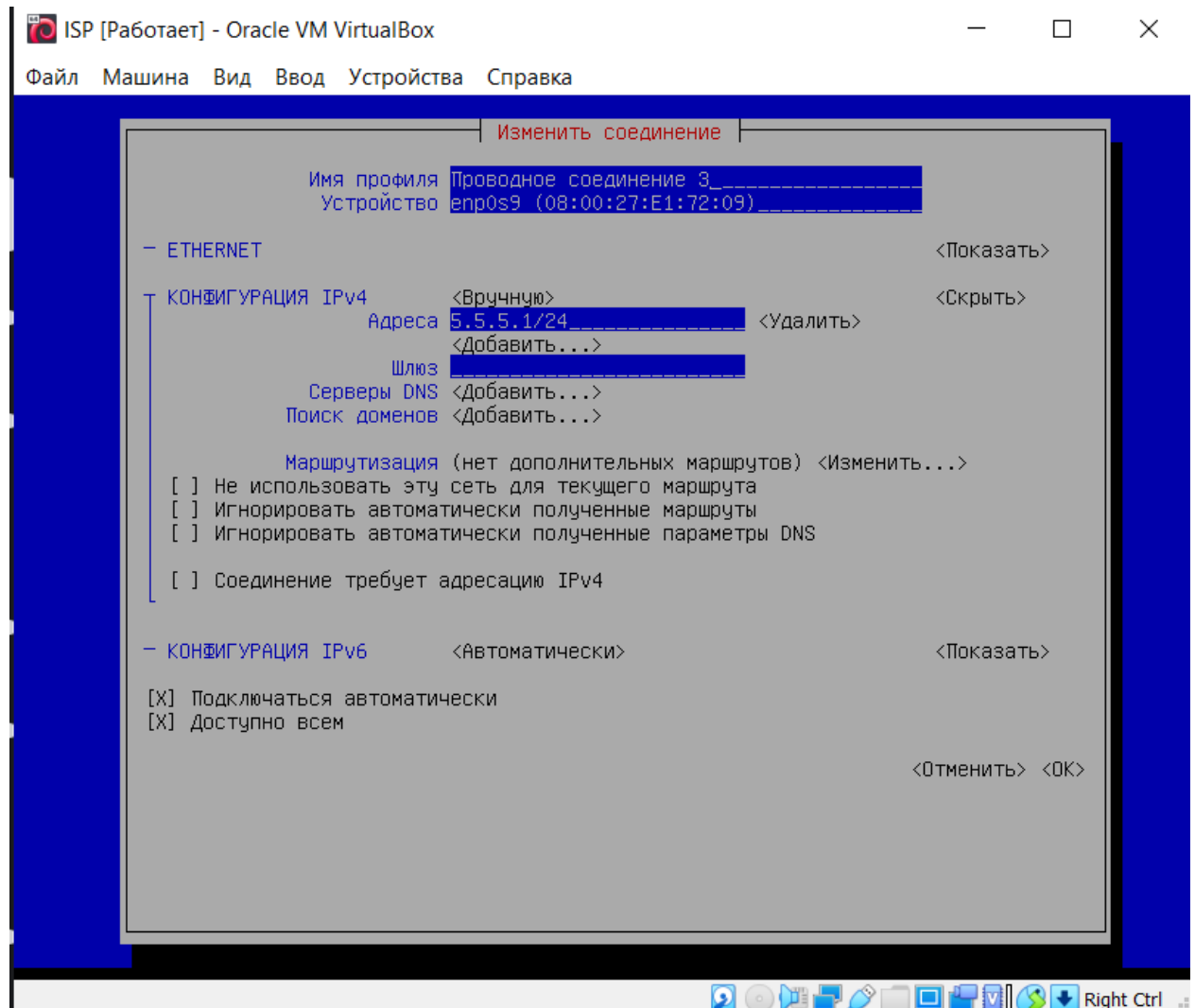
```
#apt install -y network-manager bind9 chrony dnstools openssh-server bind9utils
```

```
#nmtui
```

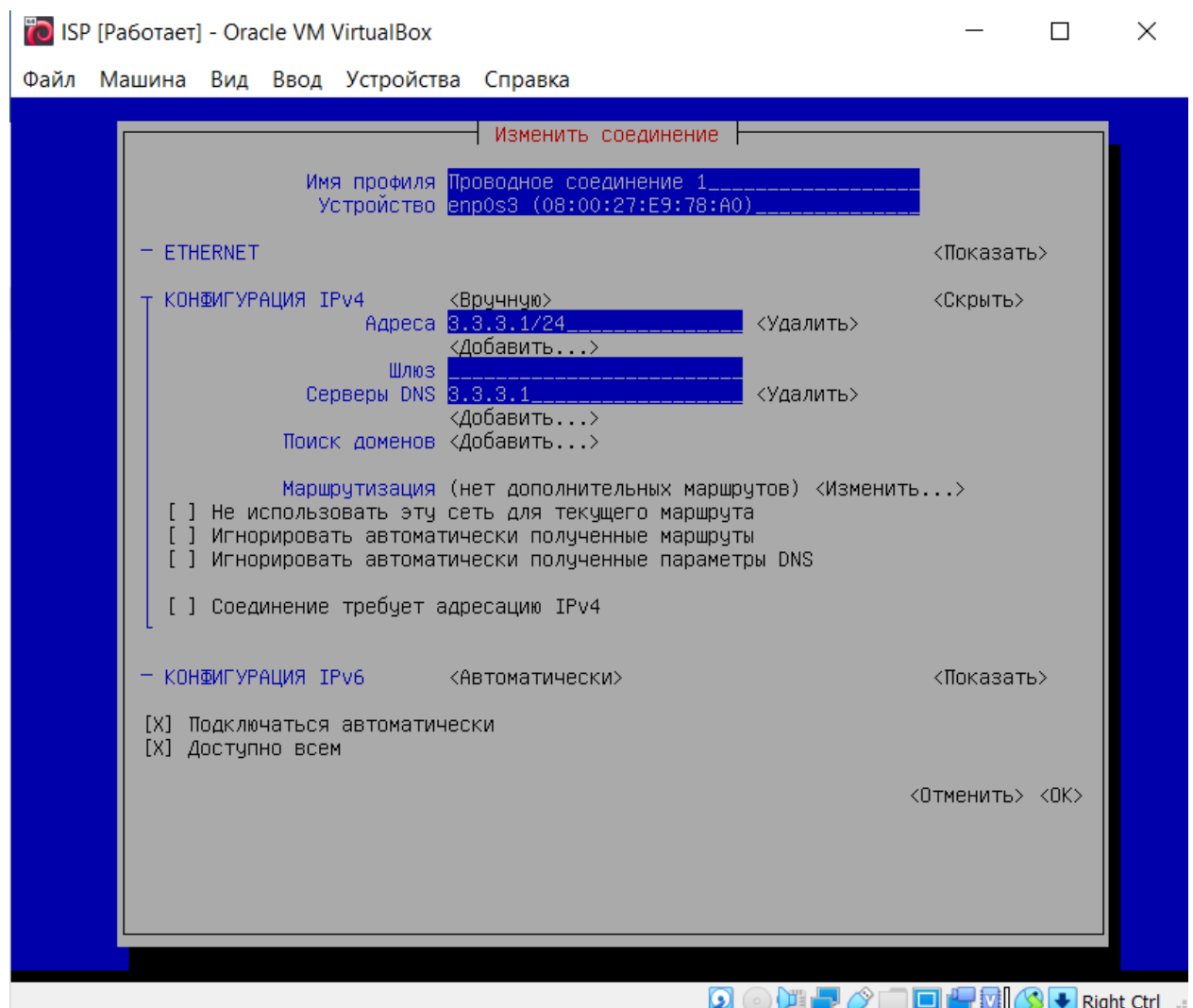
```
int WiredConnection 1 (enp0s8) ip 4.4.4.1/24
```



int WiredConnection 2 (enp0s9) ip 5.5.5.1/24



int WiredConnection 3 (enp0s3) ip 3.3.3.1/24, DNS 3.3.3.1



ISP, RTR-R, RTR-L

nano /etc/sysctl.conf

net.ipv4.ip\_forward=1



WEB-L, WEB-R, RTR-R

Настройка SSH

nano /etc/ssh/sshd\_config

```
GNU nano 5.4 /etc/ssh/sshd_config
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

Help Записать Поиск Cut Execute Location M-U Отмена
Выход Читайл Замена ^U Paste Выворнять К строке M-E Повтор
```

Меняем в PermitRootLogin на yes и убираем #

RTR-R, RTR-L Установка Firewallld

apt install -y firewallld

Настройка

Удалить из public все идентификаторы

firewall-cmd --zone=public --remove-interface=Название интерфейса

firewall-cmd --zone=trusted --add-interface=Внутренний интерфейс

firewall-cmd --zone=external --add-interface=Внешний интерфейс

firewall-cmd --zone=external --add-service= http

firewall-cmd --zone=external --add-service= https

firewall-cmd --zone=external --add-service= dns

firewall-cmd --zone=external --add-service= ssh

firewall-cmd --zone=external --add-port= 12345/udp

RTR-L

```
firewall-cmd --zone=external --add-forward-  
port=port=2222:proto=tcp:toport=22:toaddr=192.168.100.100
```

```
firewall-cmd --zone=external --add-forward-  
port=port=80:proto=tcp:toport=80:toaddr=192.168.100.100
```

```
firewall-cmd --zone=external --add-forward-  
port=port=53:proto=udp:toport=53:toaddr=192.168.100.100-IP WEB-L
```

RTR-R

```
firewall-cmd --zone=external --add-forward-  
port=port=2244:proto=tcp:toport=22:toaddr=172.16.100.100-IP WEB-R
```

```
firewall-cmd --zone=external --add-forward-  
port=port=80:proto=tcp:toport=80:toaddr=172.16.100.100
```

На обоих пишется для сохранения изменений

```
firewall-cmd --runtime-to-permanent
```

Перезапускаем фаерволл

```
firewall-cmd --reload
```

Проверяем работу ssh

RTR--R

```
ssh root@4.4.4.100 -p 2222
```

RTR--L

```
ssh root@5.5.5.100 -p 2244
```

Создание защищенного туннеля между RTR-R и RTR-L

```
apt install -y wireguard wireguard-tools
```

Создаём директиву

```
mkdir /etc/wireguard/keys
```

```
cd /etc/wireguard/keys
```

Генерируем закрытый и открытый ключ

Делаем это на RTR-L

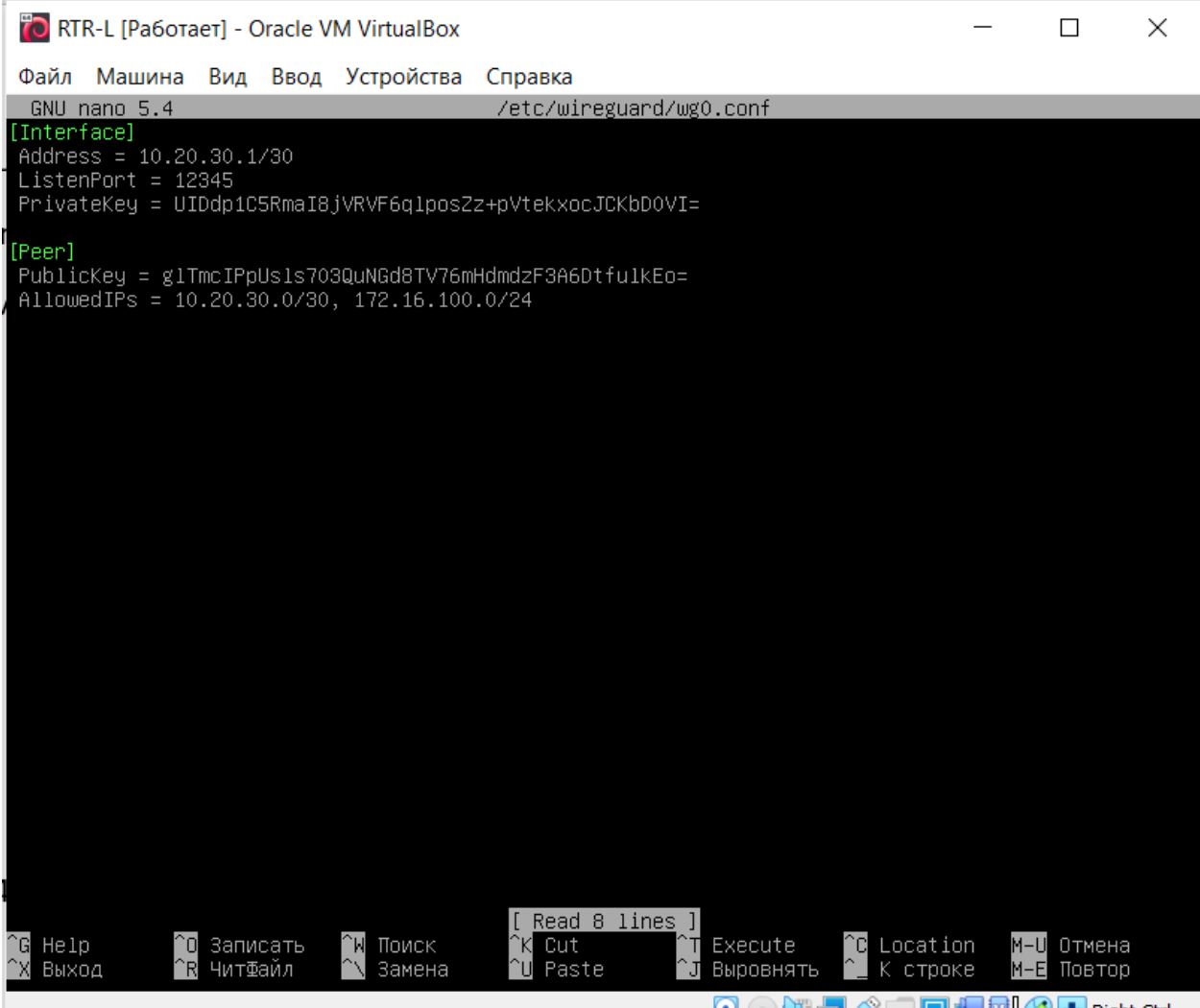
```
wg genkey | tee srv-sec.key | wg pubkey > srv-pub.key
```

```
wg genkey | tee cli-sec.key | wg pubkey > cli-pub.key
```

Переносим сгенерированный ключ в wg0.conf

```
cat srv-sec.key cli-pub.key >> /etc/wireguard/wg0.conf
```

Открываем и редактируем wg0.conf



```
RTR-L [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
GNU nano 5.4 /etc/wireguard/wg0.conf
[Interface]
Address = 10.20.30.1/30
ListenPort = 12345
PrivateKey = UIDdp1C5RmaI8jVRVF6qlposZz+pVtekxocJCKbD0VI=
[Peer]
PublicKey = glTmcIPpUsIs703QuNGd8TV76mHdmdzF3A6Dtfu1kEo=
AllowedIPs = 10.20.30.0/30, 172.16.100.0/24

[ Read 8 lines ]
^G Help      ^O Записать  ^W Поиск    ^K Cut       ^T Execute   ^C Location  M-U Отмена
^X Выход     ^R Чит.файл ^M Замена   ^U Paste     ^J Выводить  ^_ К строке  M-E Повтор
```

Сохраняем

```
systemctl enable --now wg-quick@wg0
```

Делаем это на RTR-R

```
mkdir /etc/wireguard/keys
```

```
cd /etc/wireguard/keys
```

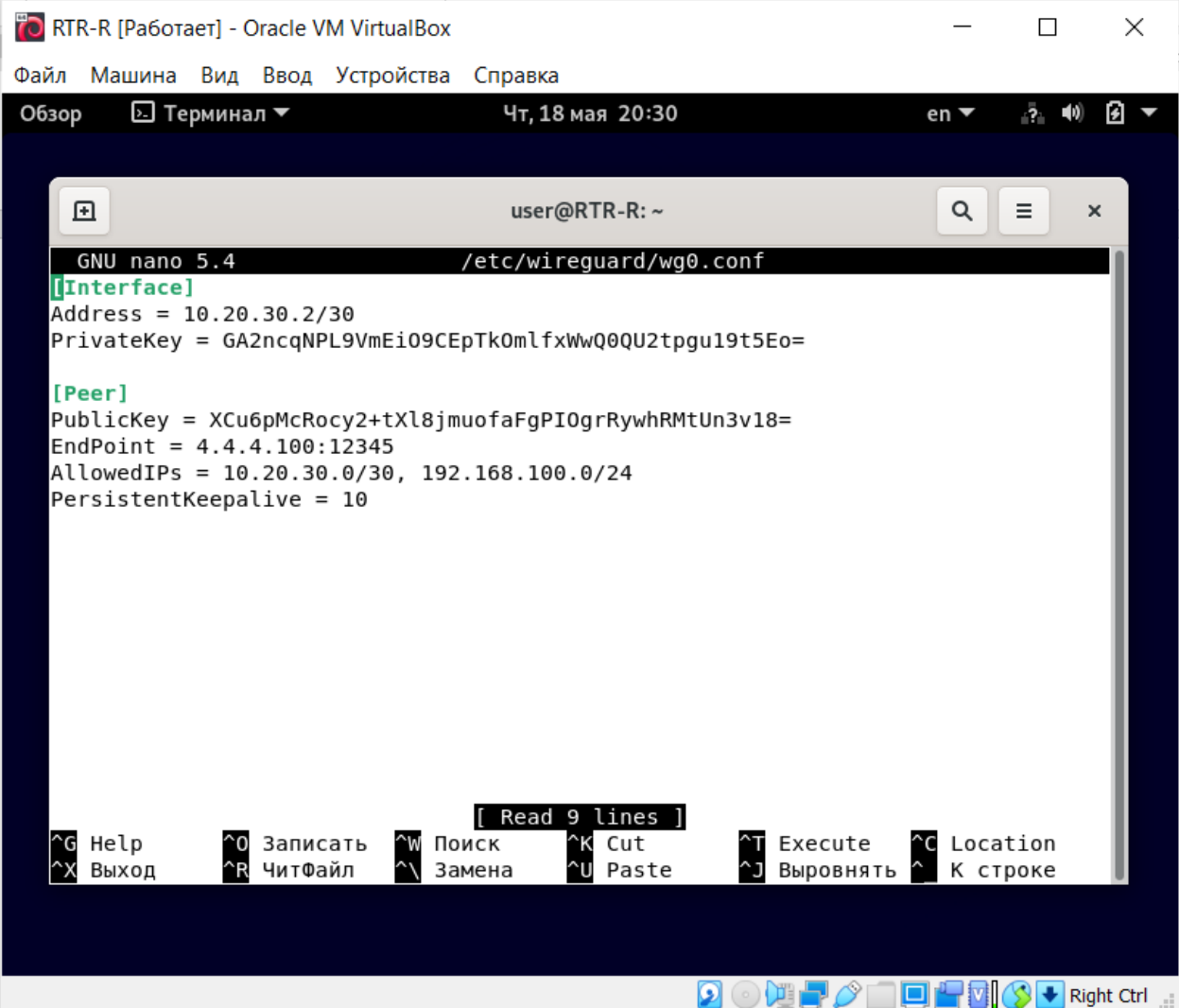
Переносим с RTR-L на RTR-R ключи

```
scp cli-sec.key srv-pub.key 5.5.5.100:/etc/wireguard/keys
```

Переносим ключи в wg0.conf

```
cat cli-sec.key srv-pub.key >> /etc/wireguard/wg0.conf
```

Открываем и редактируем wg0.conf



```
RTR-R [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал  Чт, 18 мая 20:30  en  [?] [Speaker] [Disk]
user@RTR-R: ~
GNU nano 5.4 /etc/wireguard/wg0.conf
[Interface]
Address = 10.20.30.2/30
PrivateKey = GA2ncqNPL9VmEi09CEpTk0mlfxWwQ0QU2tpgu19t5Eo=

[Peer]
PublicKey = XCu6pMcRocy2+tXl8jmuofaFgPI0grRywhRMtUn3v18=
EndPoint = 4.4.4.100:12345
AllowedIPs = 10.20.30.0/30, 192.168.100.0/24
PersistentKeepalive = 10

[ Read 9 lines ]
^G Help      ^O Записать  ^W Поиск    ^K Cut       ^T Execute   ^C Location
^X Выход     ^R ЧитФайл  ^_ Замена   ^U Paste     ^J Выводить  ^_ К строке
```

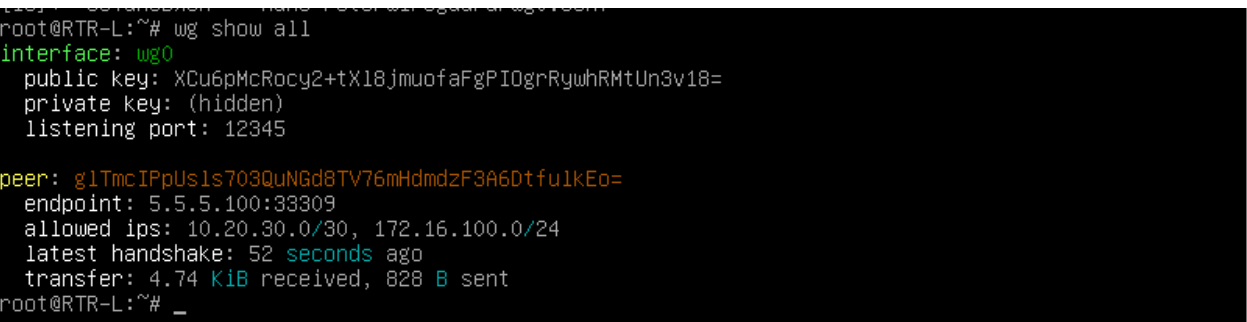
Сохраняем

```
systemctl enable --now wg-quick@wg0
```

Проверяем

```
wg show all
```

Смотрим на transer



```
root@RTR-L:~# wg show all
interface: wg0
  public key: XCu6pMcRocy2+tXl8jmuofaFgPI0grRywhRMtUn3v18=
  private key: (hidden)
  listening port: 12345

peer: glTmcIPpUs1s703QuNGd8TV76mHdmdzF3A6Dtfu1kEo=
  endpoint: 5.5.5.100:33309
  allowed ips: 10.20.30.0/30, 172.16.100.0/24
  latest handshake: 52 seconds ago
  transfer: 4.74 KiB received, 828 B sent
root@RTR-L:~#
```

```
root@RTR-R:~# wg show all
interface: wg0
  public key: glTmcIPpUsls703QuNGd8TV76mHdmdzF3A6DtfulkEo=
  private key: (hidden)
  listening port: 33309

peer: XCu6pMcRocy2+tXl8jmuofaFgPI0grRywhRMtUn3v18=
  endpoint: 4.4.4.100:12345
  allowed ips: 10.20.30.0/30, 192.168.100.0/24
  latest handshake: 1 minute, 25 seconds ago
  transfer: 828 B received, 4.83 KiB sent
  persistent keepalive: every 10 seconds
```