

Лабораторная работа №8. Настройка безопасного удаленного доступа (VPN) в ОС Debian

Для проведения лабораторных работ будет использована схема сети, представленная на рисунке

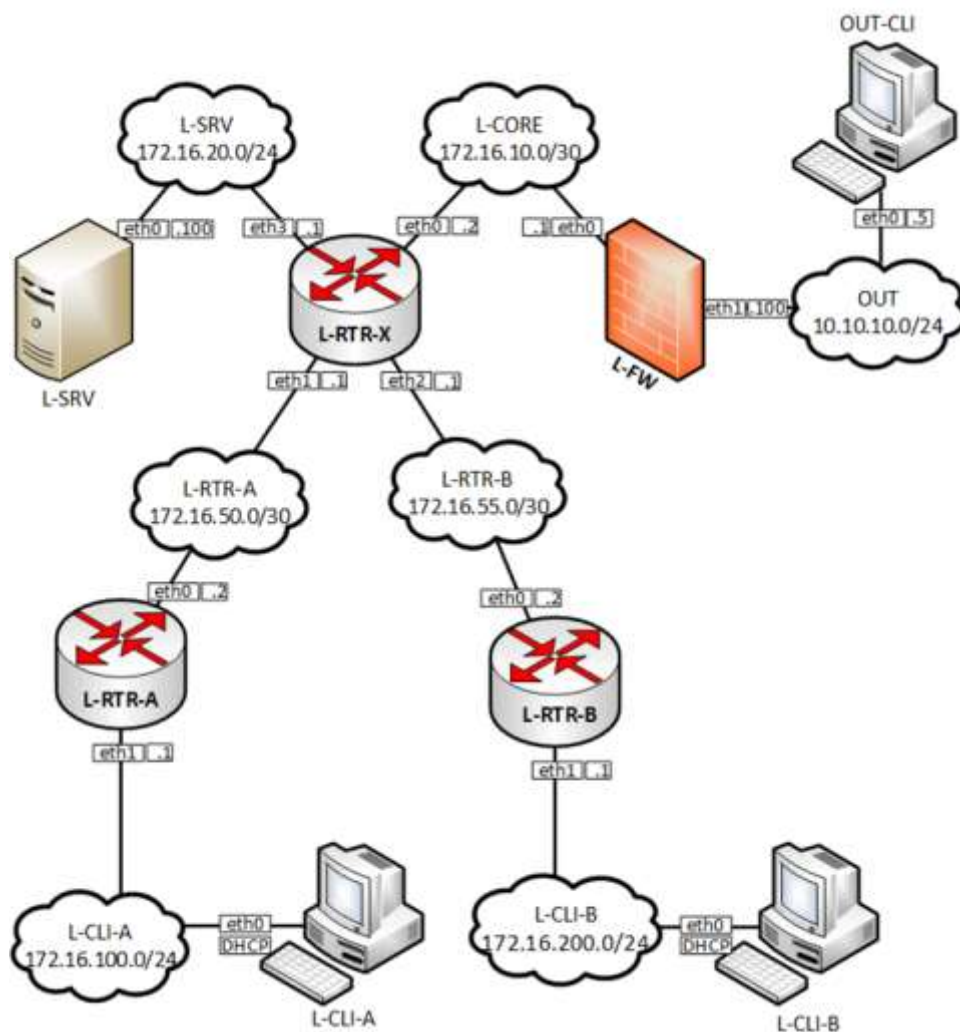


Рисунок 1. Топология сети

Схема сети содержит 8 виртуальных машин, выполняющих различные роли: L-RTR-X, L-RTR-A, L-RTR-B выполняют роли промежуточных сетевых устройств – маршрутизаторов, L-SRV, L-FW выполняют роль конечных устройств – серверов, L-CLI-A, L-CLI-B, OUT-CLI выполняют роль рабочих станций пользователей. Все виртуальные машины работают под управлением ОС Debian.

Настройка сервера доступа

- 1) Скачать скрипт установки
wget https://git.io/vpn -O openvpn-install.sh
- 2) Запустить скрипт
bash openvpn-install.sh
- 3) Ответить на вопросы мастера

```
Welcome to this OpenVPN "road warrior" installer!

I need to ask you a few questions before starting the setup.
You can leave the default options and just press enter if you are ok with them.

First, provide the IPv4 address of the network interface you want OpenVPN
listening to.
IP address: 10.10.10.100 ✓

This server is behind NAT. What is the public IPv4 address or hostname?
Public IP address / hostname: 192.168.1.241

Which protocol do you want for OpenVPN connections?
  1) UDP (recommended)
  2) TCP
Protocol [1-2]: 2 ✓

What port do you want OpenVPN listening to?
Port: 1200 ✓

Which DNS do you want to use with the VPN?
  1) Current system resolvers
  2) 1.1.1.1
  3) Google
  4) OpenDNS
  5) Verisign
DNS [1-5]: 1 ✓

Finally, tell me your name for the client certificate.
Please, use one word only, no special characters.
Client name: outcli ✓
```

ПРИМЕЧАНИЕ пункты 1, 2 и 3 при использовании виртуальных машин внутри ЛВС кафедры (без доступа в интернет)

=====начало=====

Скопировать с флешки два файла: скрипт установки **openvpn-install.sh** и пакет **EasyRSA**. Для этого:

- 1) получить у преподавателя указанные файлы
- 2) примонтировать флешку в файловую систему L-FW
 - а) Подключите флешку и выполните:

```
#fdisk -l
```

```
/dev/sdb6 158541824 1953501183 1794959360 855,96 Microsoft basic data
/dev/sdb7 1953501184 1953523711 22528 11M BIOS boot

Disk /dev/sdc: 14,5 GiB, 15514730496 bytes, 30302288 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x000b94f5

Device Boot Start End Sectors Size Id Type
/dev/sdc1 2048 30302287 30300160 14,5G b W95 FAT32
```

Здесь мы можем посмотреть детальную информацию об устройстве. Имя файла, список разделов, формат таблицы разделов, список разделов. А главное

для нас, **размер раздела** и его **файловую систему**. Теперь не сложно понять какая из них флешка. В этом примере это **/dev/sdc1**

б) Создаем папку для монтирования:

```
# mkdir /mnt/usb
```

в) Теперь монтируем флешку с помощью команды mount:

```
# mount /dev/sdc1 /mnt/usb
```

3) скопировать файлы в домашнюю папку

```
#cp openvpn-install.sh
```

```
#cp EasyRSA-3.0.8.tgz
```

4) создать каталог /etc/openvpn/server/easy-rsa

5) выполнить команду

```
#cat EasyRSA-3.8.0.tgz | tar xz -C /etc/openvpn/server/easy-rsa/  
--strip-components 1
```

6) После завершения работы с флешкой ее необходимо отмонтировать с помощью команды:

```
# umount /dev/sdc1
```

7) Запустить скрипт

```
# bash openvpn-install.sh
```

8) Ответить на вопросы мастера

```
Welcome to this OpenVPN "road warrior" installer!  
  
I need to ask you a few questions before starting the setup.  
You can leave the default options and just press enter if you are ok with them.  
  
First, provide the IPv4 address of the network interface you want OpenVPN  
listening to.  
IP address: 10.10.10.100 ✓  
  
This server is behind NAT. What is the public IPv4 address or hostname?  
Public IP address / hostname: 192.168.1.241  
  
Which protocol do you want for OpenVPN connections?  
  1) UDP (recommended)  
  2) TCP  
Protocol [1-2]: 2 ✓  
  
What port do you want OpenVPN listening to?  
Port: 1200 ✓  
  
Which DNS do you want to use with the VPN?  
  1) Current system resolvers  
  2) 1.1.1.1  
  3) Google  
  4) OpenDNS  
  5) Verisign  
DNS [1-5]: 1 ✓  
  
Finally, tell me your name for the client certificate.  
Please, use one word only, no special characters.  
Client name: outcli ✓
```

=====конец примечания=====

4) Создать директорию **/opt/vpn/keys**

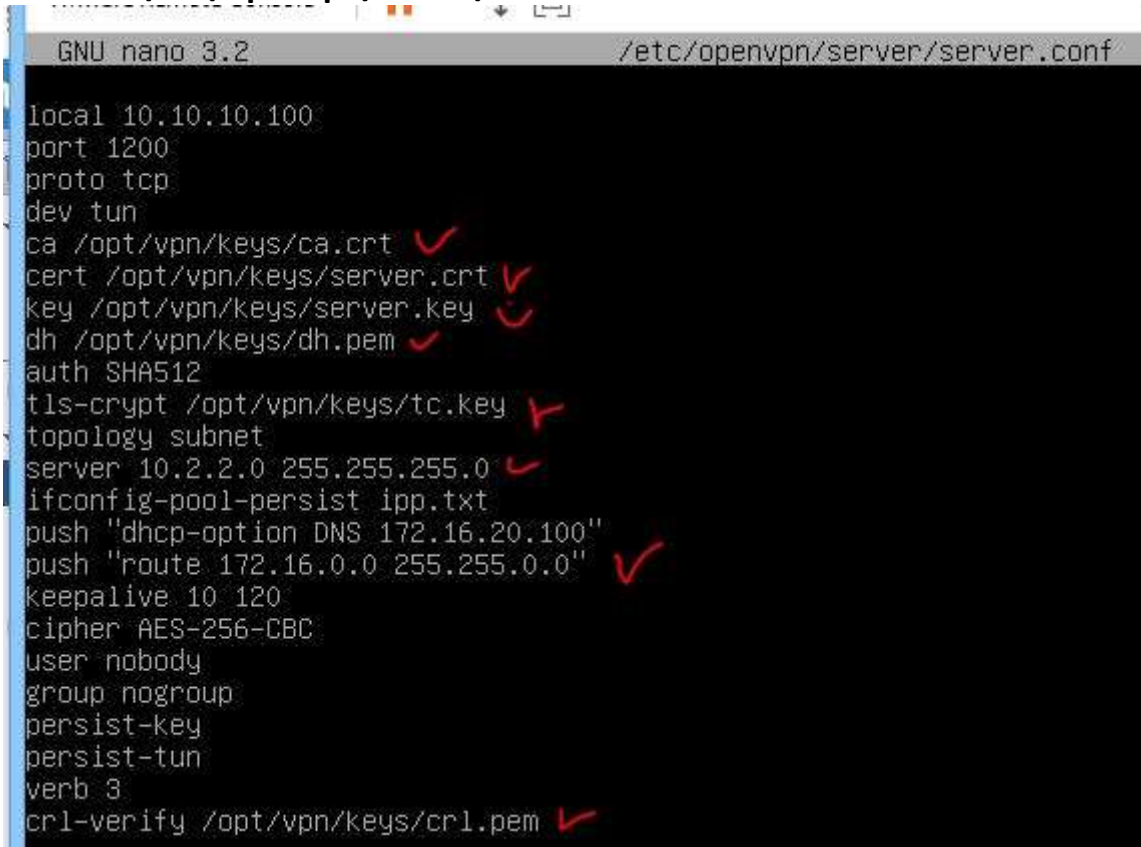
```
root@fw:~# mkdir /opt/vpn  
root@fw:~# mkdir /opt/vpn/keys  
root@fw:~# _
```

5) Переместить в директорию **/opt/vpn/keys** ключи

```
# mv /etc/openvpn/server/ca.crt /opt/vpn/keys
```

```
# mv /etc/openvpn/server/dh.pem /opt/vpn/keys
# mv /etc/openvpn/server/server.crt /opt/vpn/keys
# mv /etc/openvpn/server/crl.pem /opt/vpn/keys
# mv /etc/openvpn/server/server.key /opt/vpn/keys
# mv /etc/openvpn/server/tc.key /opt/vpn/keys
```

- 6) Внести изменения в файл конфигурации
/etc/openvpn/server/server.conf



```
GNU nano 3.2 /etc/openvpn/server/server.conf
local 10.10.10.100
port 1200
proto tcp
dev tun
ca /opt/vpn/keys/ca.crt ✓
cert /opt/vpn/keys/server.crt ✓
key /opt/vpn/keys/server.key ✓
dh /opt/vpn/keys/dh.pem ✓
auth SHA512
tls-crypt /opt/vpn/keys/tc.key ✓
topology subnet
server 10.2.2.0 255.255.255.0 ✓
ifconfig-pool-persist ip.txt
push "dhcp-option DNS 172.16.20.100"
push "route 172.16.0.0 255.255.0.0" ✓
keepalive 10 120
cipher AES-256-CBC
user nobody
group nogroup
persist-key
persist-tun
verb 3
crl-verify /opt/vpn/keys/crl.pem ✓
```

+ добавить пункт: compress lzo на сервере и клиенте (если в задании указан пункт об использовании сжатия).

- 7) Перезагрузить систему

```
# reboot
```

- 8) Скопировать на OUT-CLI файл конфигурации **outcli.ovpn** и ключи:

outcli.ovpn – находится в домашней папке ~/

/opt/vpn/keys/ca.crt

/opt/vpn/keys/tc.key

/etc/openvpn/server/easy-rsa/pki/private/outcli.key

/etc/openvpn/server/easy-rsa/pki/issued/outcli.crt

- a. Создать директорию

```
root@fw:~# mkdir /opt/vpn
root@fw:~# mkdir /opt/vpn/keys
root@fw:~# _
```

- b. Переместить ключи в директорию **/opt/vpn/keys**

Настройка удаленного клиента OUT-CLI.

- 9) Установить на OUT-CLI **openvpn**
#apt-get install openvpn
- 10) Скопировать **outcli.ovpn** в директорию **/etc/openvpn**
cp outcli.ovpn /etc/openvpn/client.conf
- 11) Внести изменения в файл конфигурации **client.conf**. **ВСЕ ЧТО НИЖЕ - УДАЛИТЬ**

```
GNU nano 3.2 /etc/openvpn/client.conf
client
dev tun
proto tcp
remote 10.10.10.100 1200 ✓
ca /opt/vpn/keys/ca.crt ✓
cert /opt/vpn/keys/outcli.crt ✓
key /opt/vpn/keys/outcli.key ✓
tls-crypt /opt/vpn/keys/tc.key ✓
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
auth SHA512
cipher AES-256-CBC
ignore-unknown-option block-outside-dns
block-outside-dns
verb 3
```

- 12) Запустить VPN клиент
systemctl start openvpn@client
- 13) Проверить работу: **ping srv.wsr.left** на **OUT-CLI**

Автоматизация удаленного доступа

Подготовка удаленного клиента (Выполнить на CLI-OUT)

*Для автоматического подключения с использованием конфигурации **client.conf***

- ```
mkdir /opt/vpn
nano /opt/vpn/connect_left
```
- 14) Внести в файл **connect\_left** строки  
**# !/bin/bash**  
**systemctl start openvpn@client**
  - 15) Сделать файл скрипта исполняемым

```
chmod ugo+x /opt/vpn/connect_left
```

- 16) В папке /usr/local/bin создать символическую ссылку

```
ln -s /opt/vpn/connect_left /usr/local/bin/connect_left
```

- 17) Запуск скрипта для авторизованного доступа от имени **root**.

```
connect_left
```

*Для автоматического отключения с использованием конфигурации client.conf*

```
nano /opt/vpn/disconnect_any
```

- 18) Внести в файл **disconnect\_any** строки

```
!/bin/bash
systemctl stop openvpn@client
```

- 19) Сделать файл скрипта исполняемым

```
chmod ugo+x /opt/vpn/disconnect_any
```

- 20) В папке /usr/local/bin создать символическую ссылку

```
ln -s /opt/vpn/disconnect_any /usr/local/bin/disconnect_any
```

- 21) Запуск скрипта для автоматического тключения от имени **root**.

```
disconnect_any
```

## ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ

1. Установить и настроить защищённое подключение удаленного клиента OUT-CLI к ресурсам локальной сети. Проверить работу vpn-соединения с помощью проверки доступности внутренних ip адресов