

Установка и настройка openvpn.

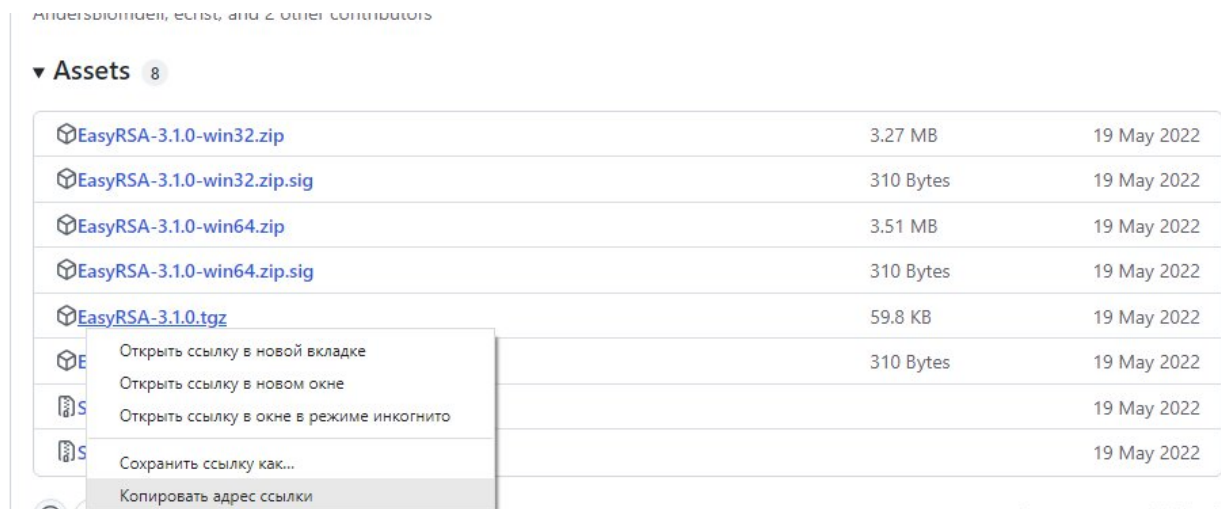
Обновите локальный индекс пакетов и установите OpenVPN:

```
sudo apt update
```

```
sudo apt install openvpn
```

Зайти на github по ссылке <https://github.com/OpenVPN/easy-rsa/releases>

Найти последнюю версию easyrsa в моем случае 3.1.0



Копирую адрес ссылки, устанавливаю с помощью wget

```
wget https://github.com/OpenVPN/easy-rsa/releases/download/v3.1.0/EasyRSA-3.1.0.tgz
```

Разархивирую:

```
tar xvf EasyRSA-3.1.0.tgz
```

Удаляю архив, перехожу в папку.

```
rm EasyRSA-3.1.0.tgz
```

```
cd EasyRSA-3.1.0/
```

В каталоге найдите файл vars.example. Скопируйте его и назовите копию vars без расширения.

```
cp vars.example vars
```

Откройте новый файл в текстовом редакторе:

```
nano vars
```

Найти, раскомментировать строки:

```
set_var EASYRSA_REQ_COUNTRY "RU"  
set_var EASYRSA_REQ_PROVINCE "SPBLO"  
set_var EASYRSA_REQ_CITY "SPb"  
set_var EASYRSA_REQ_ORG "TKUiK"  
set_var EASYRSA_REQ_EMAIL "me@example.net"  
set_var EASYRSA_REQ_OU "Laba"
```

Не в 1 из строк нельзя писать &, будут ошибки.

```
./easysrsa init-pki
```

```
rm pki/vars
```

Создаем центр сертификации.

```
./easysrsa build-ca
```

Если вы не хотите указывать пароль при каждом взаимодействии с ЦС, вы можете ввести команду build-ca с параметром nopass:

```
./easysrsa build-ca nopass
```

Common Name – это имя для ссылки на этот компьютер в контексте центра сертификации. В качестве Common Name для СА можно ввести любую строку символов.

Создайте в нем надежный ключ Диффи-Хеллмана, который будет использоваться при обмене ключами:

```
./easysrsa gen-dh
```

Это может занять несколько минут.

Нужно создать подпись HMAC, чтобы усилить функции проверки целостности TLS:

```
openvpn --genkey --secret ta.key
```

Создание сертификатов.

```
./easysrsa gen-req server nopass
```

```
./easysrsa sign-req server server
```

Перемещаем ключ и сертификат в папку /etc/openvpn

```
mv /root/EasyRSA-3.1.0/pki/issued/server.crt /etc/openvpn
```

```
mv /root/EasyRSA-3.1.0/pki/private/server.key /etc/openvpn
```

```
cp ta.key /etc/openvpn/
```

```
cp pki/dh.pem /etc/openvpn/
```

```
cp pki/ca.crt /etc/openvpn/
```

Создание конфига сервера.

```
cd /etc/openvpn/
```

```
nano server.conf
```

Вставить строчки.

```
port 1194
```

```
proto udp
```

```
dev tun
ca /etc/openvpn/ca.crt
cert /etc/openvpn/server.crt
key /etc/openvpn/server.key
dh /etc/openvpn/dh.pem
server 192.168.10.0 255.255.255.0
ifconfig-pool-persist /etc/openvpn/ipp.txt
keepalive 10 120
comp-lzo
cipher AES-256-GCM
persist-key
persist-tun
verb 3
push "redirect-gateway def1"
push "dhcp-option DNS 77.88.8.8"
client-to-client
```

Сохранить и выйти

Заполняю файл ipp.txt

```
nano ipp.txt
```

```
client1,192.168.10.100
```

```
client2,192.168.10.200
```

Сохраняю и выхожу.

Запускаю VPN сервер: `systemctl start openvpn@server`

Создание конфигов и ключей для клиентов.

Создаем структуру каталогов для хранения конфигов и ключей.

```
mkdir -p ~/client-configs/keys
```

```
chmod -R 700 ~/client-configs
```

Создаем ключи и сертификаты.

```
./easyrsa gen-req client1 nopass
```

```
./easyrsa gen-req client2 nopass
```

```
./easyrsa gen-req client3 nopass
```

```
./easyrsa gen-req client4 nopass
```

```
./easyrsa gen-req client5 nopass
```

Подписываем сертификаты.

```
./easyrsa sign-req client client1
```

```
./easyrsa sign-req client client2
```

```
./easyrsa sign-req client client3
```

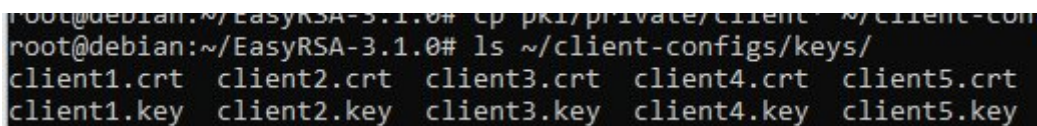
```
./easyrsa sign-req client client4
```

```
./easyrsa sign-req client client5
```

Переносим ключи и сертификаты в папку с ключами клиентов.

```
cp pki/issued/client* ~/client-configs/keys/
```

```
cp pki/private/client* ~/client-configs/keys/
```



```
root@debian:~/EasyRSA-3.1.0# cp pki/private/client* ~/client-configs/keys/
root@debian:~/EasyRSA-3.1.0# ls ~/client-configs/keys/
client1.crt  client2.crt  client3.crt  client4.crt  client5.crt
client1.key  client2.key  client3.key  client4.key  client5.key
```

Создаю шаблон для файлов клиента.

```
Cd /etc/openvpn
```

```
nano client.conf
```

```
client
```

```
cipher AES-256-GCM
```

```
tls-client
```

```
dev tun
```

```
proto udp
```

```
remote 10.13.100.199 1194
```

```
remote-cert-tls server
```

```
nobind
```

```
persist-key
```

```
persist-tun
```

```
float
```

```
keepalive 10 120
```

verb 3

auth-nocache

reneg-sec 43200

comp-lzo no

<ca>

</ca>

<cert>

</cert>

<key>

</key>

Между тегами необходимо вставить содержимое сертификатов.

nano ca.crt

Копирую ВСЕ содержимое и вставляю между тегов <ca></ca>

```
comp-lzo no
<ca>
-----BEGIN CERTIFICATE-----
MIIDMDCCAhiGAwIBAgIUXG1G1/JB05Hkv045K17hvk1HX1ewDOYJKoZIhvcNAOE
E
w
A
g
x
2
L
s
C
1
x
e
x
h
1
CQxUERL0Z1W1K1EJAMV0T1ZEEK10Z10G1Z1Z1G1W1V1Q117Q1L01Z1Z1V1C1D1Y1D1K1D
2qcoWA==
-----END CERTIFICATE-----
</ca>
```

Копирую шаблон в папку с конфигурацией клиентов.

cp client.conf ~/client-configs/client1.conf

cp client.conf ~/client-configs/client2.conf

cp client.conf ~/client-configs/client3.conf

cp client.conf ~/client-configs/client4.conf

cp client.conf ~/client-configs/client5.conf

Перехожу в папку с кофнигами, открываю файл на редактирование.

cd ~/client-configs/

nano client1.conf

Заходим через 2 терминал в файлы с ключами и сертификатам и копируем их содержимое в файл клиента.

Файлы клиентов заполнены, теперь необходимо передать их на ПК клиентов.

Используем ssh.

Scp root@10.13.100.199:/root/client-configs/client1.conf /etc/openvpn/

И запускаем конфиг: `systemctl start openvpn@client1`

Клиент и сервер настроен, весь трафик пойдет через сервер.

С помощью `ip -s` а проверяем созданся ли туннель,

Если туннеля нет смотрим `systemctl status openvpn@client1` (Гуглим ошибки, решаем).