

Установка и настройка OpenVPN (клиента и сервера) и Easy-RSA 3 в CentOS 7

OpenVPN — свободная реализация технологии виртуальной частной сети с открытым исходным кодом для создания зашифрованных каналов типа точка-точка или сервер-клиенты между компьютерами.

Easy-RSA — программа для создания и ведения инфраструктуры открытых ключей (PKI) в openVPN

Установка необходимого софта

Добавляем репозиторий EPEL и обновляемся

```
[root@localhost ~]# yum install epel-release -y  
[root@localhost ~]# yum update -y
```

Устанавливает OpenVPN 2.4 и Easy-RSA 3

```
[root@localhost ~]# yum install openvpn easy-rsa -y
```

Проверим их версии

```
[root@localhost ~]# openvpn --version  
[root@localhost ~]# ls -lah /usr/share/easy-rsa/
```

```
[root@localhost ~]# openvpn --version  
OpenVPN 2.4.7 x86_64-redhat-linux-gnu [Fedora EPEL patched] [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb 20  
2019  
library versions: OpenSSL 1.0.2k-fips 26 Jan 2017, LZO 2.06  
Originally developed by James Yonan  
Copyright (C) 2002-2018 OpenVPN Inc <sales@openvpn.net>  
Compile time defines: enable_async_push=no enable_comp_stub=no enable_crypto=yes enable_crypto_ofb_cfb=yes enable_debug=yes enable_def_auth=y  
es enable_dependency_tracking=no enable_dlopen=unknown enable_dlopen_self=unknown enable_dlopen_self_static=unknown enable_fast_install=yes e  
nable_fragment=yes enable_iproute2=yes enable_lbttool_lock=yes enable_lz4=yes enable_lzo=yes enable_management=yes enable_multihome=yes enabl  
e_pam_dlopen=no enable_pedantic=no enable_pf=yes enable_pkcs11=yes enable_plugin_auth_pam=yes enable_plugin_down_root=yes enable_plugins=yes  
enable_port_share=yes enable_selinux=yes enable_server=yes enable_shared=yes enable_shared_with_static_runtimes=no enable_small=no enable_sta  
tic=yes enable_strict=no enable_strict_options=no enable_systemd=yes enable_werror=no enable_win32_dll=yes enable_x509_alt_username=yes with_  
aix_soname=aix with_crypto_library=openssl with_gnu_ld=yes with_mem_check=no with_sysroot=no  
[root@localhost ~]# ls -lah /usr/share/easy-rsa/  
итого 4,0K  
drwxr-xr-x. 3 root root 39 апр 18 09:46 .  
drwxr-xr-x. 83 root root 4,0K апр 18 09:46 ..  
lrwxrwxrwx. 1 root root 5 апр 18 09:46 3 -> 3.0.3  
lrwxrwxrwx. 1 root root 5 апр 18 09:46 3.0 -> 3.0.3  
drwxr-xr-x. 3 root root 62 апр 18 09:46 3.0.3
```

Проверка версий OpenVPN и Easy-RSA

Настройка Easy-RSA 3

Скопируем скрипты easy-rsa в каталог /etc/openvpn/

```
[root@localhost ~]# cp -r /usr/share/easy-rsa /etc/openvpn/
```

Переходим в каталог `/etc/openvpn/easy-rsa/3/` и создаем там файл `vars`

```
[root@localhost ~]# cd /etc/openvpn/easy-rsa/3/  
[root@localhost ~]# nano vars
```

Содержимое файла:

```
set_var EASYRSA "$PWD"  
set_var EASYRSA_PKI "$EASYRSA/pki"  
set_var EASYRSA_DN "cn_only"  
set_var EASYRSA_REQ_COUNTRY "RU"  
set_var EASYRSA_REQ_PROVINCE "Moscow"  
set_var EASYRSA_REQ_CITY "Moscow"  
set_var EASYRSA_REQ_ORG "My Organisation"  
set_var EASYRSA_REQ_EMAIL "admin@itdraft.ru"  
set_var EASYRSA_REQ_OU "IT department"  
set_var EASYRSA_KEY_SIZE 4096  
set_var EASYRSA_ALGO rsa  
set_var EASYRSA_CA_EXPIRE 7500  
set_var EASYRSA_CERT_EXPIRE 3650  
set_var EASYRSA_NS_SUPPORT "no"  
set_var EASYRSA_NS_COMMENT "CERTIFICATE AUTHORITY"  
set_var EASYRSA_EXT_DIR "$EASYRSA/x509-types"  
set_var EASYRSA_SSL_CONF "$EASYRSA/openssl-1.0.cnf"  
set_var EASYRSA_DIGEST "sha512"
```

Делаем файл исполняемым

```
[root@localhost ~]# chmod +x vars
```

Создание ключа и сертификата для OpenVPN Сервера

Прежде чем создавать ключ, нам нужно инициализировать каталог PKI и создать ключ CA.

```
[root@localhost ~]# cd /etc/openvpn/easy-rsa/3/  
root@localhost ~]# ./easyrsa init-pki  
Note: using Easy-RSA configuration from: ./vars
```

```
init-pki complete; you may now create a CA or requests.  
Your newly created PKI dir is: /etc/openvpn/easy-rsa/3/pki
```

```
[root@localhost ~]# ./easysrsa build-ca
```

На этом необходимо придумать пароль для своего CA-ключа, чтобы сгенерировались файлы 'ca.crt' и 'ca.key' в каталоге 'pki'.
Этот пароль нам потребуется дальше

```
[root@localhost 3]# ./easysrsa build-ca  
Note: using Easy-RSA configuration from: ./vars  
Generating a 4096 bit RSA private key  
.....++  
.....++  
writing new private key to '/etc/openvpn/easy-rsa/3/pki/private/ca.key.IQ9aPur6JR'  
Enter PEM pass phrase: _____  
Verifying - Enter PEM pass phrase: _____  
-----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:  
  
CA creation complete and you may now import and sign cert requests.  
Your new CA certificate file for publishing is at:  
/etc/openvpn/easy-rsa/3/pki/ca.crt
```

Создаем корневой сертификат

Создадим ключ сервера (название сервера **srv-openvpn**)

```
[root@localhost ~]# ./easysrsa gen-req srv-openvpn nopass
```

опция **nopass** — отключение пароля для srv-openvpn

```
[root@localhost 3]# ./easysrsa gen-req srv-openvpn nopass

Note: using Easy-RSA configuration from: ./vars
Generating a 4096 bit RSA private key
.....++
.....++
writing new private key to '/etc/openvpn/easy-rsa/3/pki/private/srv-openvpn.key.39uKHKh0I1'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [srv-openvpn]:

Keypair and certificate request completed. Your files are:
req: /etc/openvpn/easy-rsa/3/pki/reqs/srv-openvpn.req
key: /etc/openvpn/easy-rsa/3/pki/private/srv-openvpn.key
```

Создаем ключ сервера

Подпишем ключ srv-openvpn используя наш CA-сертификат

```
[root@localhost ~]# ./easysrsa sign-req server srv-openvpn
```

В процессе у нас спросят пароль, который мы задавали ранее

```
[root@localhost 3]# ./easyrsa sign-req server srv-openvpn
47 Делаем файл исполняемым
Note: using Easy-RSA configuration from: ./vars
49
50 Создание ключей для OpenVPN
You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.
55 [root@localhost ~]# ./easyrsa init-pki
Request subject, to be signed as a server certificate for 3650 days:
57
subject=
commonName = srv-openvpn
59 You have created PKI dir = /etc/openvpn/easy-rsa/3/pki
60
61 [root@localhost ~]# ./easyrsa build-ca
Type the word 'yes' to continue, or any other input to abort.
6: Confirm request details: yes для своего CA-ключа, чтобы сгенерировались файлы
Using configuration from /etc/openvpn/easy-rsa/3/openssl-1.0.cnf
Enter pass phrase for /etc/openvpn/easy-rsa/3/pki/private/ca.key:
Check that the request matches the signature
Signature ok
[root@localhost ~]# ./easyrsa gen-req srv-openvpn nopass
The Subject's Distinguished Name is as follows
commonName      :ASN.1 12:'srv-openvpn'
Certificate is to be certified until Apr 15 07:44:24 2029 GMT (3650 days)
71
Write out database with 1 new entries
Data Base Updated: [root@localhost ~]# ./easyrsa sign-req server srv-openvpn
74 В процессе у нас спросят пароль, который мы задавали ранее
Certificate created at: /etc/openvpn/easy-rsa/3/pki/issued/srv-openvpn.crt
```

Подписываем ключ, используя CA-сертификат

Проверим файлы сертификата, чтобы убедиться, что сертификаты сгенерировались без ошибок

```
[root@localhost ~]# openssl verify -CAfile pki/ca.crt pki/issued/srv-  
openvpn.crt  
pki/issued/srv-openvpn.crt: OK
```

Все сертификата OpenVPN сервера созданы.

- Корневой сертификат расположен: 'pki/ca.crt'
- Закрытый ключ сервера расположен: 'pki/private/srv-openvpn.key'
- Сертификат сервера расположен: 'pki/issued/srv-openvpn.crt'

Создание ключа клиента

Сгенерируем ключ клиента client-01

```
[root@localhost ~]# ./easysrsa gen-req client-01 nopass
```

```
[root@localhost 3]# ./easysrsa gen-req client-01 nopass
Note: using Easy-RSA configuration from: ./vars
Generating a 4096 bit RSA private key
.....++
.....++
writing new private key to '/etc/openvpn/easy-rsa/3/pki/private/client-01.key.dmEW0bpnNr'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [client-01]:

Keypair and certificate request completed. Your files are:
req: /etc/openvpn/easy-rsa/3/pki/reqs/client-01.req
key: /etc/openvpn/easy-rsa/3/pki/private/client-01.key
```

Генерируем ключ клиента

Теперь подпишем ключ client-01, используя наш CA сертификат

```
[root@localhost ~]# ./easysrsa sign-req client client-01
```

В процессе у нас спросят пароль, который мы задавали ранее

```
[root@localhost ~]# ./easyrsa sign-req client client-01
Note: using Easy-RSA configuration from: ./vars

You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a client certificate for 3650 days:

subject=
  commonName                = client-01

Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes
Using configuration from /etc/openvpn/easy-rsa/3/openssl-1.0.cnf
Enter pass phrase for /etc/openvpn/easy-rsa/3/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'client-01'
Certificate is to be certified until Apr 15 08:00:46 2029 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /etc/openvpn/easy-rsa/3/pki/issued/client-01.crt
```

Подписываем ключ клиента, используя корневой сертификат

Проверим файлы сертификата

```
[root@localhost ~]# openssl verify -CAfile pki/ca.crt
pki/issued/client-01.crt
pki/issued/client-01.crt: OK
```

Дополнительная настройка OpenVPN сервера

Сгенерируем ключ Диффи-Хеллмана

```
[root@localhost ~]# ./easyrsa gen-dh
```



```
[root@localhost 3]# ./easyrsa gen-crl

Note: using Easy-RSA configuration from: ./vars
Using configuration from /etc/openvpn/easy-rsa/3/openssl-1.0.cnf
Enter pass phrase for /etc/openvpn/easy-rsa/3/pki/private/ca.key:

An updated CRL has been created.
CRL file: /etc/openvpn/easy-rsa/3/pki/crl.pem
```

Генерируем CRL-ключ

Для того, что бы отозвать сертификат надо выполнить команду:

```
[root@localhost ~]# ./easyrsa revoke client-02
```

где **client-02** имя сертификата, который мы отзываем

Все необходимые сертификаты созданы, теперь их надо скопировать в директории

Копируем сертификаты сервера

```
[root@localhost ~]# cp pki/ca.crt /etc/openvpn/server/
[root@localhost ~]# cp pki/issued/srv-openvpn.crt /etc/openvpn/server/
[root@localhost ~]# cp pki/private/srv-openvpn.key
/etc/openvpn/server/
```

Копируем сертификаты клиента

```
[root@localhost ~]# cp pki/ca.crt /etc/openvpn/client/
[root@localhost ~]# cp pki/issued/client-01.crt /etc/openvpn/client/
[root@localhost ~]# cp pki/private/client-01.key /etc/openvpn/client/
```

Копируем ключи DH и CRL

```
[root@localhost ~]# cp pki/dh.pem /etc/openvpn/server/
[root@localhost ~]# cp pki/crl.pem /etc/openvpn/server/
```

!!! Проверить, надо ли регенерировать CRL и заново копировать его в каталог /etc/openvpn/server/ после отзыва сертификата !!!

Настройка OpenVPN сервера

Создадим файл конфигурации server.conf

```
[root@localhost ~]# cd /etc/openvpn/  
[root@localhost ~]# nano server.conf
```

Содержимое файла:

```
# OpenVPN Port, Protocol and the Tun  
port 1194  
proto udp  
dev tun  
  
# OpenVPN Server Certificate - CA, server key and certificate  
ca /etc/openvpn/server/ca.crt  
cert /etc/openvpn/server/srv-openvpn.crt  
key /etc/openvpn/server/srv-openvpn.key  
  
# DH and CRL key  
dh /etc/openvpn/server/dh.pem  
crl-verify /etc/openvpn/server/crl.pem  
  
# Network Configuration - Internal network  
# Redirect all Connection through OpenVPN Server  
server 10.10.1.0 255.255.255.0  
push "redirect-gateway def1"  
  
# Using the DNS from https://dns.watch  
push "dhcp-option DNS 84.200.69.80"  
push "dhcp-option DNS 84.200.70.40"  
  
# Enable multiple client to connect with same Certificate key  
duplicate-cn  
  
# TLS Security  
cipher AES-256-CBC  
tls-version-min 1.2  
tls-cipher TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-  
AES-256-CBC-SHA256:TLS-DHE-RSA-WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-  
WITH-AES-128-CBC-SHA256  
auth SHA512  
auth-nocache
```

```
# Other Configuration
keepalive 20 60
persist-key
persist-tun
comp-lzo yes
daemon
user nobody
group nobody

# OpenVPN Log
log-append /var/log/openvpn.log
verb 3
```

Настройка Firewalld

Активируем модуль ядра port-forwarding

```
[root@localhost ~]# echo 'net.ipv4.ip_forward = 1' >> /etc/sysctl.conf
[root@localhost ~]# sysctl -p
net.ipv4.ip_forward = 1
```

Добавим службу openvpn в firewalld, и интерфейс tun0 в доверенную зону

```
[root@localhost ~]# firewall-cmd --permanent --add-service=openvpn
[root@localhost ~]# firewall-cmd --permanent --zone=trusted --add-
interface=tun0
```

Активируем 'MASQUERADE' для доверенной зоны firewalld

```
[root@localhost ~]# firewall-cmd --permanent --zone=trusted --add-
masquerade
```

Активируем NAT

```
[root@localhost ~]# SERVERIP=$(ip route get 84.200.69.80 | awk 'NR==1
{print $(NF-2)}')
[root@localhost ~]# firewall-cmd --permanent --direct --passthrough
ipv4 -t nat -A POSTROUTING -s 10.10.1.0/24 -o $SERVERIP -j MASQUERADE
```

Перезапустим firewalld

```
[root@localhost ~]# firewall-cmd --reload
```

Запустим OpenVPN и добавим его в автозагрузку

```
[root@localhost ~]# systemctl start openvpn@server
[root@localhost ~]# systemctl enable openvpn@server
```

Проверим

```
[root@localhost ~]# netstat -plntu
[root@localhost ~]# systemctl status openvpn@server
```

```
[root@localhost openvpn]# netstat -plntu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN      17000/sshd
tcp        0      0 127.0.0.1:5432         0.0.0.0:*               LISTEN      17030/postgres
tcp        0      0 127.0.0.1:25          0.0.0.0:*               LISTEN      17193/master
tcp6       0      0 :::22                  :::*                     LISTEN      17000/sshd
tcp6       0      0 :::1:25                :::*                     LISTEN      17193/master
udp        0      0 0.0.0.0:1194          0.0.0.0:*               *          18639/openvpn
udp        0      0 127.0.0.1:323         0.0.0.0:*               *          26995/chronyd
udp6       0      0 :::1:323                :::*                     *          26995/chronyd
[root@localhost openvpn]# systemctl status openvpn@server
● openvpn@server.service - OpenVPN Robust And Highly Flexible Tunneling Application On server
   Loaded: loaded (/usr/lib/systemd/system/openvpn@server.service; enabled; vendor preset: disabled)
   Active: active (running) since Чт 2019-04-18 11:33:48 MSK; 25s ago
     Main PID: 18639 (openvpn)
    Status: "Initialization Sequence Completed"
   CGroup: /system.slice/system-openvpn.slice/openvpn@server.service
           └─18639 /usr/sbin/openvpn --cd /etc/openvpn/ --config server.conf

anp 18 11:33:48 localhost.localdomain systemd[1]: Starting OpenVPN Robust And Highly Flexible Tunneling Application On server...
anp 18 11:33:48 localhost.localdomain systemd[1]: Started OpenVPN Robust And Highly Flexible Tunneling Application On server.
```

Проверяем, запущен ли OpenVPN

Настройка OpenVPN клиента

Создадим файл конфигурации **client-01.ovpn**

```
[root@localhost ~]# cd /etc/openvpn/client
[root@localhost ~]# nano client-01.ovpn
```

Содержимое файла:

```
client
dev tun
proto udp
```

```
remote xx.xx.xx.xx 1194
```

```
ca ca.crt
```

```
cert client-01.crt  
key client-01.key
```

```
cipher AES-256-CBC  
auth SHA512  
auth-nocache  
tls-version-min 1.2  
tls-cipher TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-  
AES-256-CBC-SHA256:TLS-DHE-RSA-WITH-AES-128-GCM-SHA256:TLS-DHE-RSA-  
WITH-AES-128-CBC-SHA256
```

```
resolv-retry infinite  
compress lzo  
nobind  
persist-key  
persist-tun  
mute-replay-warnings  
verb 3
```

В строке **'remote xx.xx.xx.xx 1194'** надо прописать IP-адрес вместо **'xx.xx.xx.xx'**

Теперь для надо заархивировать сертификаты (**ca.crt**, **client-01.crt**), ключ клиента (**client-01.key**), файл конфигурации (**client-01.ovpn**), и передать их на ПК, который будет подключаться к OpenVPN серверу

Установим архиватор zip и создадим архив с файлами

```
[root@localhost ~]# yum install zip unzip -y  
[root@localhost ~]# cd /etc/openvpn/  
[root@localhost ~]# zip client/client-01.zip client/*
```

Пробуем подключиться с другого ПК к OpenVPN серверу и смотрим лог:

```
[root@localhost ~]# tail -f /var/log/openvpn.log
```

```
Thu Apr 18 12:00:06 2019 192.168.1.45:54538 Control Channel: TLSv1.2, cipher TLSv1/SSLv3 DHE-RSA-AES256-GCM-SHA384, 4096 bit RSA  
Thu Apr 18 12:00:06 2019 192.168.1.45:54538 [client-01] Peer Connection Initiated with [AF_INET]192.168.1.45:54538  
Thu Apr 18 12:00:06 2019 client-01/192.168.1.45:54538 MULTI_sva: pool returned IPv4=10.10.1.6, IPv6=(Not enabled)  
Thu Apr 18 12:00:06 2019 client-01/192.168.1.45:54538 MULTI: Learn: 10.10.1.6 -> client-01/192.168.1.45:54538  
Thu Apr 18 12:00:06 2019 client-01/192.168.1.45:54538 MULTI: primary virtual IP for client-01/192.168.1.45:54538: 10.10.1.6  
Thu Apr 18 12:00:07 2019 client-01/192.168.1.45:54538 PUSH: Received control message: 'PUSH_REQUEST'  
Thu Apr 18 12:00:07 2019 client-01/192.168.1.45:54538 SENT CONTROL [client-01]: 'PUSH_REPLY,redirect-gateway def1,dhcp-option DNS 84.200.69.8  
0,dhcp-option DNS 84.200.70.40,route 10.10.1.1,topology net30,ping 20,ping-restart 60,ifconfig 10.10.1.6 10.10.1.5,peer-id 0,cipher AES-256-G  
CM' (status=1)  
Thu Apr 18 12:00:07 2019 client-01/192.168.1.45:54538 Data Channel: using negotiated cipher 'AES-256-GCM'  
Thu Apr 18 12:00:07 2019 client-01/192.168.1.45:54538 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key  
Thu Apr 18 12:00:07 2019 client-01/192.168.1.45:54538 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
```

Смотрим log-файл OpenVPN сервера

Установка и настройка OpenVPN (клиента и сервера) и Easy-RSA 3 в CentOS 7

5/5

1