OpenVPN

Свободная реализация технологии (VPN) с открытым исходным кодом для создания зашифрованных каналов типа точка-точка или сервер-клиенты между компьютерами.

http://openvpn.net/

Установка

```
apt install openvpn
```

Для Debian 11 (Bullseye):

```
apt install -t bullseye-backports openvpn
```

Настройка

Варианты управление ключами и сертификатами:

1. Стандартный вариант с использованием easy-rsa
2. Работа в XCA

Настоятельно рекомендуется все операции с ключами производить на отдельном компьютере. Файл **`ca.key`** позволяет создавать ключи и сертификаты поэтому должен быть только у Администратора!

TAP — эмулирует Ethernet устройство и работает на канальном уровне модели OSI, оперируя кадрами Ethernet. Используется для создания сетевого моста. Если же у вас стоит задача объединить удаленные сети в единое адресное пространство, например сделать и в офисе и в филиале единую сеть 192.168.10.0/24, то тогда бы мы использовали tap интерфейс и указывали бы на компьютерах в обоих сетях не пересекающиеся адреса из одной подсети.

TUN — сетевой туннель, работает на сетевом уровне модели OSI, оперируя IP пакетами. Используется для маршрутизации.

Установка и настройка openvpn на CentOS 7 Выбор устройства openvpn — TAP или TUN

https://ru.wikipedia.org/wiki/TUN/TAP

Изменение пароля к клиентскому ключу

Change passphrase for private key

Пример:

```
openssl rsa -des3 -in client.key -out client_new.key
```

Пример для MS Windows:

change_passphrase.cmd

```
set OPENSSL="C:\Program Files\OpenVPN\bin\openssl"
%OPENSSL% rsa -des3 -in "C:\Program Files\OpenVPN\config\old.key" -out "C:\Program
Files\OpenVPN\config\new.key"
```

Файлы

ca.crt

Корневой сертификат

ta.key

Ключ шифрования начала сессии

dh{n}.pem

Алгоритм обмена Диффи-Хеллмана (DH)

Параметры Диффи — Хеллмана для шифрования со стороны сервера

server.crt

Сертификат сервера

server.key

Ключ сервера

crl.pem

Список отозванных сертификатов

client.crt

Сертификат клиента

client.key

Ключ клиента

ta.key

Ключ шифрования начала сессии

Сервер

- ca.crt
- ta.key
- dh{n}.pem
- server.crt
- server.key
- crl.pem
- server.conf

Запуск

```
systemctl start openvpn@server
```

Статус

```
systemctl status openvpn@server
```

Перезапуск

```
systemctl start openvpn@server
```

Останов

```
systemctl stop openvpn@server
```

server.conf

Fix Me!

Fix Me! Директива `client-to-client`

Путь к настройкам: `/etc/openvpn/server`

Пример: `/usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz`

/etc/openvpn/server.conf

```
local IP_АДРЕС_СЕРВЕРА
port 1194
dev tun
proto udp
tun-mtu 1280
ca /etc/openvpn/server/ca.crt
cert /etc/openvpn/server/server.crt
key /etc/openvpn/server/server.key  # This file should be kept secret
dh /etc/openvpn/server/dh2048.pem
crl-verify /etc/openvpn/server/crl.pem
server 192.168.168.0 255.255.255.0

ifconfig-pool-persist /etc/openvpn/ipp.txt
connect-retry-max 5

#auth-user-pass-verify /etc/openvpn/checkpsw.sh via-env
#script-security 3 system

;client-config-dir ccd
;route 192.168.40.128 255.255.255.248
```

```
push "route 192.168.168.0 255.255.255.0"
push "route 10.1.0.0 255.255.255.0"

push "dhcp-option DNS 192.168.168.1"
push "dhcp-option DOMAIN domain.ru"

keepalive 10 120

tls-auth /etc/openvpn/keys/ta.key 0 # This file is secret
comp-lzo
max-clients 5
user nobody
group nogroup

persist-key
persist-tun

status openvpn-status.log

log-append /var/log/openvpn.log
verb 3
mute 20

#client-connect /etc/openvpn/client-connect.sh
```

ipp.txt

Fix Me!

/etc/openvpn/ipp.txt

```
client01,192.168.168.22
client02,192.168.168.26
client03,192.168.168.30
client04,192.168.168.34
```

Особенности ipp.txt в OpenVPN версии 2.4.0

Для выдачи нужных адресов используем такую конструкцию:

/etc/openvpn/server/ipp.txt

```
N002,10.1.0.2
N003,10.1.0.3
Client-01,10.1.0.4
Client-02,10.1.0.5
Client-03,10.1.0.6
N007,10.1.0.7
N008,10.1.0.8
N009,10.1.0.9
N010,10.1.0.10
Client-04,10.1.0.11
Client-05,10.1.0.12
Client-06,10.1.0.13
```

где `N002`, `N003`, `N007`, `N008`, `N009` и `N010` это несуществующие клиенты для резервирования неиспользуемых адресов.

ipp-restart.sh

Скрипт для обновления `/etc/openvpn/server/ipp.txt`, новый файл: `/etc/openvpn/server/ipp.txt-new`

/usr/local/bin/openvpn-ipp-restartp.sh

```
#!/bin/bash

systemctl stop openvpn@server
sleep 3
cp /etc/openvpn/server/ipp.txt-new /etc/openvpn/server/ipp.txt
sleep 3
systemctl start openvpn@server
systemctl status openvpn@server
```

Особенности работы с MS Windows клиентами

Fix Me!

OpenVPN выделяет для каждого клиента подсеть с маской `/30` для обеспечения совместимости с клиентами MS Windows из-за ограничения режима эмуляции `TUN` драйвера `TAP-Win32`.

Если к серверу OpenVPN не будут подключаться клиенты MS Windows, то можно отключить такой порядок выделения адресов указав в настройках сервера директиву `ifconfig-pool-linear`

192.168.1.4/30	
192.168.1.**4**	Сетевой адрес (network address)
192.168.1.**5**	Адрес виртуального маршрутизатора, шлюза, в качестве которого выступает сервер OpenVPN (virtual IP address in the OpenVPN Server)
192.168.1.**6**	Адрес выдаваемый клиенту (assigned to the client)
192.168.1.**7**	Широковещательный адрес (broadcast address)

Драйвер `TAP-Win32` включает DHCP-сервер, который назначает клиенту адрес `192.168.1.`**`6`**, а адрес `192.168.1.`**`5`** определяется как адрес DHCP-сервера.

Такой подход приводит к потере части IP-адресов, но это лучший способ обеспечения совместимости с всеми клиентами OpenVPN.

---

http://openvpn.net/index.php/open-source/faq/community-software-server/273-qifconfig-poolq-option-use-a-30-subnet-4-private-ip-addresses-per-client-when-used-in-tun-mode.html

Настройка OpenVPN клиента на Windows

Настройка OpenVPN клиента на Windows 10

Выполнение команд при подключении клиента

Нужно задать имя скрипта:

/etc/openvpn/openvpn.conf

```
client-connect /etc/openvpn/client-connect.sh
```

Пример кода скрипта:

/etc/openvpn/client-connect.sh

```
case ${common_name} in
Client01)
        sudo /usr/sbin/etherwake 00:11:22:33:44:55
        ;;
Client02)
        sudo /usr/sbin/etherwake 55:44:33:22:11:00
        ;;
esac

exit 0
```

Пример настройки sudo:

```
nobody ALL = (ALL) NOPASSWD:/usr/sbin/etherwake
```

logrotate

Настройка ротации протокола с помощью logrotate:

/etc/logrotate.d/openvpn

```
/var/log/openvpn.log {
        daily
        rotate 8
        compress
        delaycompress
        missingok
        copytruncate
        notifempty
        create 640 root
}
```

Клиент

Все настройки клиента в одном файле

Папка с ключами должна быть внутри папки `config`

Список ключей и сертификатов клиента:

- `ca.crt`
- `client.crt`
- `client.key`
- `ta.key`
- `client.ovpn`

client.ovpn

Файл настроек клиента

Пример файла:

client1.ovpn

```
client
dev tun
proto udp
remote vpn.domain.ru
resolv-retry infinite
nobind
persist-key
persist-tun
ns-cert-type server
comp-lzo
verb 3
ca ca.crt
cert client1.crt
key client1.key
tls-auth ta.key 1
```

Запуск через sudo

Пример настройки sudo:

```
user ALL = (ALL) NOPASSWD:/usr/sbin/openvpn
```

Пример скрипта запуска:

```
sudo /usr/sbin/openvpn client.ovpn
```

update-resolv-conf

Для того, чтобы использовать DNS сервер полученный от сервера OpenVPN нужно:

1. Установить пакет `resolvconf`

   ```
   apt-get install resolvconf
   ```

2. Добавить в конец файла настроек клиента `client.ovpn` следующие строки:

   ```
   script-security 2
   up /etc/openvpn/update-resolv-conf
   down /etc/openvpn/update-resolv-conf
   ```

Проблемы с версией TLS

Вариант 1

Новый клиент не подключается с старому серверу из-за версии TLS, для решения проблемы нужно добавить в файл настройки клиента:

```
tls-cipher "DEFAULT:@SECLEVEL=0"
tls-version-min 1.0
```

Вариант 2

Старый клиент не подключается с новому серверу из-за версии TLS, в протоколе сервера ошибка:

```
TLS_ERROR: BIO read tls_read_plaintext error
```

Решение: изменить в настройках OpenSSL версию TLS в параметре `MinProtocol`

/etc/ssl/openssl.cnf

```
[system_default_sect]
MinProtocol = TLSv1.2
```

на

```
MinProtocol = TLSv1
```

Debian openvpn client TLS handshake failed - VPN - XG Firewall - Sophos Community

Подавление предупреждений

1. `WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this`

   Нужно указать в `client.ovpn`

   ```
   auth-nocache
   ```

   [РЕШЕНО] Auth-nocache - Warning в OpenVPN | Obu4alka

Клиенты для MS Windows

Клиент для MS Windows 7/8 (2.4.4-i601)

Для версии OpenVPN 2.4.4 файлы настройки клиента размещаются в `OpenVPN/config/`

В версии OpenVPN 2.4.6 файлы размещаются аналогично в `OpenVPN/config/`

Клиент для MS Windows XP (2.3.18-i001)

Portable клиент для MS Windows XP (2.3.18-i001)

---

https://openvpn.net/index.php/open-source/downloads.html

https://portapps.io/app/openvpn-portable/

Автозапуск

Файл с настройками:
`/etc/openvpn/client.conf`

Подготовка:

```
systemctl enable openvpn@client.service
systemctl daemon-reload
```

Запуск `openvpn`

```
service openvpn start
```

Состояние:

```
systemctl status openvpn@client.service
```

Останов клиента:

```
systemctl stop openvpn@client.service
```

запуск клиента:

```
systemctl start openvpn@client.service
```

Guide: Configure OpenVPN to autostart on systemd Linux | SHB

Zabbix

Zabbix

Мониторинг openvpn подключений пользователей в zabbix

Ссылки

- Логотип
- Логотип (иконка)
- Установка и настройка OpenVPN-сервера в Debian
- Описание команд и параметров OpenVPN
- http://openvpn.net/index.php/open-source/documentation/howto.html#pki
- OpenVPN — не просто, а ОЧЕНЬ просто
- Клиент openVPN на Android
- Мобильное системное администрирование на Android
- **Использование скриптов**
- Установка OpenVPN
- OpenVPN Connect Android FAQ
- A bit of everything: OpenVPN and systemd
- openvpn и авторизация по логину/паролю
- Configure openvpn on a Debian server and client
- Настройка OpenVPN с использованием сертификатов X.509 (На примере FreeBSD и роутера на DD-WRT)
- Debian. Поднимаем свой OpenVPN сервер, настраиваем форвардинг и клиента / Мастерская интернет-разработчика
- Openvpn24ManPage – OpenVPN Community

http://sysadminmosaic.ru/openvpn/openvpn

2023-11-13 13:27