KDE connect в OpenVPN

📖 Оглавление

- г. Перезапусти сервер:

Проблема

```
KDE connect не видит
устройства внутри OpenVPN.
```

Цель

- заставить работать в впн чтобы видел все устройства внутри сети.
- подключенный ПК/Телефон/Приставку.

Краткое решение

проверенный способ (самый простой и надёжный): использование client-config-dir (CCD) + topology subnet + включённый client-to-client.

чтобы конкретным клиентам (ПК и телефон) OpenVPN всегда выдавал один и тот же внутренний VPN-IP, и тогда KDE Connect сможет общаться по этому адресу.

1 Короткая идея

На сервере OpenVPN включаем **topology subnet** и **server 10.8.0.0 255.255.255.0** (или вашу подсеть).

Указываем :

```
client-config-dir
/etc/openvpn/ccd.
```

Для каждого клиента создаём файл в **/etc/openvpn/ccd/** с именем, совпадающим с **Common Name (CN)** его сертификата, и в нём строку **ifconfig-push <IP> <netmask>**.

Включаем **client-to-client** в **server.conf**(может быть другой как у меня более 2 впн на одном сервере), чтобы клиенты видели друг друга напрямую (действует для определенного конфига).

2 Перезапускаем OpenVPN

Пример фрагмента server.conf (на сервере)

В server.conf (или /etc/openvpn/server/server.conf)

```
port 1194
proto udp
dev tun
```

порт 1194 практически всегда заблокирован использовать не советую переделать на другой разблокированный в идеале использовать имитацию http/https tcl соединение

используем "subnet" — проще для статических адресов

```
```

```
topology subnet
server 10.8.0.0
255.255.255.0
```

файлы пулы и persist

```
ifconfig-pool-persist
/etc/openvpn/ipp.txt
```

разрешаем клиентам общаться друг с другом (ВАЖНО для KDE Connect)

```
client-to-client
```

каталог с индивидуальными конфигурациями клиентов

```
client-config-dir
/etc/openvpn/ccd
```

**директория указывается свободно*

уровень логов (по желанию)

```
verb 3
```

3 Создаём каталог CCD

```
sudo mkdir -p
/etc/openvpn/ccd
sudo chown root:root
/etc/openvpn/ccd
```

```
sudo chmod 700
/etc/openvpn/ccd
```

**делаем один раз*

4 Как назвать файл в ccd и что туда писать

Имя файла в **/etc/openvpn/ccd/** должно точно совпадать с **Common Name (CN)** в сертификате клиента, который сервер видит при подключении. Если вы создавали сертификаты через **Easy-RSA, CN** обычно задан при создании (например pc-home или phone-android).

файлы без расширения редактируем через **nano*

Пример:

- дать ПК IP 10.8.0.10, телефону 10.8.0.11.

Файл **/etc/openvpn/ccd/pc-home**:

```
ifconfig-push 10.8.0.10
255.255.255.0
```

Файл **/etc/openvpn/ccd/phone-android**:

```
ifconfig-push 10.8.0.11
255.255.255.0
```

- Если ваш сервер использует старую топологию net30, формат ifconfig-push другой (нужно 2 IP). Поэтому я рекомендую topology subnet — это проще для классических /24 сетей.

5 Важно: клиент должен иметь уникальный сертификат (CN)

Этот метод надёжен, когда у каждого клиента есть свой сертификат с уникальным CN. Если вы используете один и тот же сертификат на нескольких устройствах или включена опция duplicate-cn, то CCD по CN работать не будет (несколько устройств — один CN). В таком случае:

- лучше сгенерировать отдельный сертификат для ПК и для телефона (рекомендую),

- либо использовать client-connect скрипт и логику по username (сложнее).

6 Дополнительно: маршрутизация и firewall

Убедитесь, что на сервере включён форвардинг (для Linux):

чтобы сохранить в **/etc/sysctl.conf: net.ipv4.ip_forward=1**:

```
sudo sysctl -w
net.ipv4.ip_forward=1
```

- Если у вас **firewall (iptables/nftables)**, разрешите трафик внутри **tun** и между **tun** и локалой по необходимости. Но при **client-to-client** трафик между клиентами идёт внутри сервера и обычно проходит без **NAT**.

- Проверьте, что **firewall** не блокирует **multicast/broadcast**, если **KDE Connect** использует обнаружение по локальной сети. Если обнаружение не срабатывает, можно подключаться по IP вручную (в KDE Connect есть возможность подключения по адресу/коду).

7 Перезапуск OpenVPN

После правок перезапустите сервис:

- systemd: имя файла может быть *openvpn-server@server.service* или просто *openvpn.service*

если ваш конфиг называется **server.conf**:

```
sudo systemctl restart
openvpn@server
```

или

```
sudo systemctl restart
openvpn-server
```

8 Проверьте логи:

```
sudo journalctl -u
openvpn@server -f
```

- или **/var/log/syslog** **/var/log/openvpn.log** в зависимости от системы

9 Как узнать CN клиента (если не помните)

Если у вас есть клиентский сертификат (client.crt), можно посмотреть CN так:

```
openssl x509 -in client.crt
-noout -subject
```

пример вывода:

```
subject= /CN=pc-home
```

Именно это имя нужно использовать как имя файла в ccd.

10 Что делать, если KDE Connect не видит устройство

Убедитесь, что оба устройства подключены в VPN и получили те IP, которые вы задали (10.8.0.10 и 10.8.0.11).

Проверьте, что между ними пингуется IP: с ПК

```
ping 10.8.0.11.
```

Если пинг есть, но KDE Connect не видит автоматом — в приложении KDE Connect на одном устройстве используйте ручное добавление по IP (ввод IP и подтверждение/код).

Если пинга нет — проверьте client-to-client, ip_forward и правила фаервола.

11 Пример полной мини-конфигурации

server.conf (самое важное):

```
dev tun
proto udp
```

```
port 1194
topology subnet
server 10.8.0.0
255.255.255.0
ifconfig-pool-persist
/etc/openvpn/ipp.txt
client-to-client
client-config-dir
/etc/openvpn/ccd
verb 3

...
```

ccd/pc-home:

```
ifconfig-push 10.8.0.10
255.255.255.0
```

ccd/phone-android:

```
```

```
ifconfig-push 10.8.0.11
255.255.255.0
```

12 Пул ограничить кол-во выдаваемых ip (необязательно)

Что решает:

- кто первый подключился тот и получит 10.8.0.1
- если kde connect подключен по ip постоянно теряет

Простое решение :

- выдайте фиксированным адреса с конца (если у вас менее 255

устройств одновременно все ок)

пример:

ccd/phone-android:

```
ifconfig-push 10.8.0.199
255.255.255.0
```

Непростое решение :

Команда

```
server 10.8.0.0
255.255.255.0
```

уже автоматически создаёт пул адресов.

Чтобы задать свой диапазон, нужно использовать длинную форму, например:

```
mode server
tls-server
ifconfig 10.8.0.1
255.255.255.0
ifconfig-pool 10.8.0.10
10.8.0.150
```

но это заменяет server.

Так что проще всего — оставить server и убрать ifconfig-pool.

После этого:

```
sudo systemctl restart
openvpn@server
sudo systemctl status
openvpn@server
```

**Если статус active (running) — всё ок*

P.S. Примеры полные условно :

а. Скопируй этот вариант и замени им существующий **/etc/openvpn/server/server.conf** (или /etc/openvpn/server.conf — если у тебя именно он используется):

```
############################
############################
######
# OpenVPN Server
Configuration (TCP/3000)
```

```
############################
############################
######

port 3000
proto tcp
dev tun

# Пользователь и группа для
безопасности
user nobody
group nogroup
persist-key
persist-tun

############################
############################
######
# Сеть VPN
############################
############################
######
topology subnet
server 10.8.0.0
```

```
255.255.255.0

# Сохраняем пул IP-адресов
(необязательно, но полезно)
ifconfig-pool-persist
/etc/openvpn/ipp.txt

# Разрешаем клиентам видеть
друг друга (для KDE Connect
и т.п.)
client-to-client

# Каталог с индивидуальными
конфигами клиентов
(статические IP)
client-config-dir
/etc/openvpn/ccd

############################
############################
######
# Маршрутизация и DNS
############################
############################
```

```
######
# Принудительно направляем
весь трафик клиентов через
VPN
push "redirect-gateway def1
bypass-dhcp"

# DNS Cloudflare
push "dhcp-option DNS
1.1.1.1"
push "dhcp-option DNS
1.0.0.1"

# (при желании можно
добавить свои маршруты)
# push "route 0.0.0.0
128.0.0.0 10.8.0.1"
# push "route 128.0.0.0
128.0.0.0 10.8.0.1"

############################
############################
######
# Оптимизация TCP
```

```
############################
############################
######
# Ограничение MSS для
стабильной работы TCP-over-
TCP
mssfix 1200

############################
############################
######
# Шифрование и безопасность
############################
############################
######
tls-crypt
...openvpn/server/tc.key
tls-version-min 1.2
ecdh-curve prime256v1
data-ciphers AES-256-
GCM:AES-128-GCM
data-ciphers-fallback AES-
256-GCM
auth SHA256
```

```
############################
############################
######
# Сертификаты
############################
############################
######
ca
...openvpn/server/ca.crt
cert
...openvpn/server/server.cr
t
key
...openvpn/server/server.ke
y
dh
...openvpn/server/dh.pem

############################
############################
######
# Тайминги и логирование
############################
```

```
############################
######
keepalive 10 120
verb 3
status
...openvpn/server/openvpn-
status.log

############################
############################
######
# Конец конфигурации
############################
############################
######
```

6. Что теперь:

Убедись, что каталог CCD существует:

```
sudo mkdir -p
/etc/openvpn/ccd
```

```
sudo chmod 700
/etc/openvpn/ccd
```

в. Создай файлы клиентов:

```
/etc/openvpn/ccd/pc-user
/etc/openvpn/ccd/phone-user
```

Содержимое:

```
ifconfig-push 10.8.0.199
255.255.255.0
```

и

```
ifconfig-push 10.8.0.198
255.255.255.0
```

г. Перезапусти сервер:

```
sudo systemctl restart
openvpn@server-tcp587
sudo systemctl status
openvpn@server-tcp587
```

- Если статус active (running) — всё работает.
- Проверь openvpn-status.log, чтобы убедиться, что клиенты получили свои статические IP.