Настройка клиента OpenVPN в macOS для аутентификации по Рутокен

1 Введение
2 Стенд
3 Общий порядок действий

Введение

В данной инструкции описывается, как настроить авторизацию в OpenVPN с помощью Рутокен ЭЦП в macOS.

Стенд

Нам понадобится Рутокен ЭЦП, отформатированный через Панель управления Рутокен и содержащий сгенерированные ключи.

Общий порядок действий

1. Скачиваем и устанавливаем OpenVPN-клиент Tunnelblick для macOS.

2. Создаем конфигурационный файл под названием `newconnect.ovpn` с подобным содержимым:

```
client
dev tap
proto tcp
remote xxx.xxx.xxx.xxx 1194
resolv-retry infinite
nobind
persist-key
persist-tun

ca CA.crt
pkcs11-providers '/Library/Aktiv Co/Rutoken ECP/lib/librtpkcs11ecp.dylib'
pkcs11-id Aktiv\\x20Co\\x2E/Rutoken\\x20ECP/2d105684/Rutoken\\x20ECP\\x20\\x3Cno\\x20label\\x3E/C67F8A314C24E080

pkcs11-pin-cache 300

comp-lzo
verb 3
```

В параметре `ca` указываем полный путь к корневому сертификату.

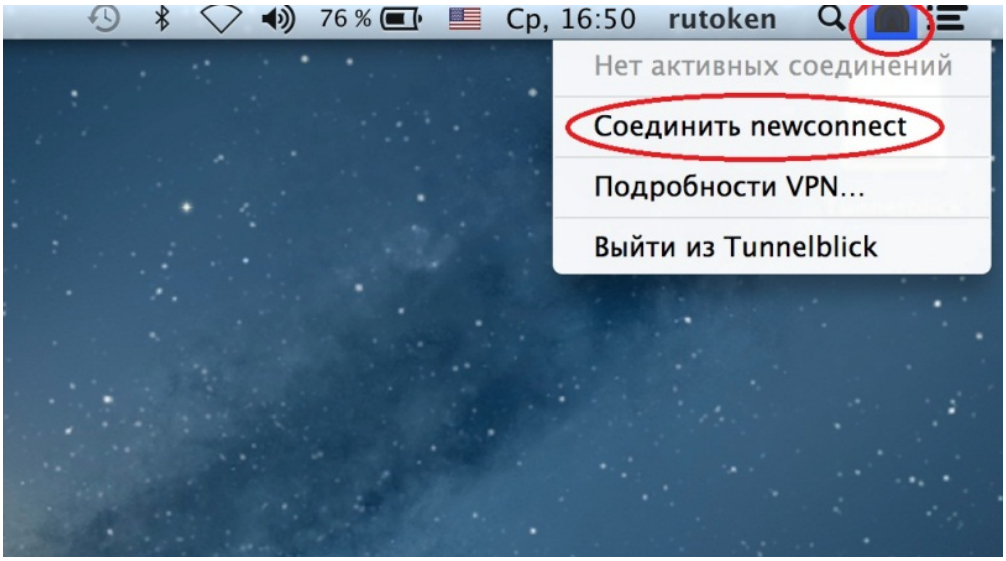
В параметре `pkcs11-providers` указываем путь к библиотеке PKCS#11.

В параметре `pkcs11-id` указываем ID контейнера, в котором на Рутокен ЭЦП хранятся ключ и сертификат. Узнать этот ID можно с помощью команды:

```
# /Applications/Tunnelblick.app/Contents/Resources/openvpn/openvpn-2.2.1/openvpn --show-pkcs11-ids '/Library
/Aktiv Co/Rutoken ECP/lib/librtpkcs11ecp.dylib'
```

3. При запуске Tunnelblick спросит, есть ли конфигурационный файл, на что отвечаем положительно и в следующем диалоге выбираем «Конфигурация OpenVPN» и далее «Открыть папку личных конфигураций». Помещаем в нее наш конфигурационный файл и жмем «Готово».

4. Подключаемся к VPN-серверу: нажимаем на значок Tunnelblick и выбираем наше соединение. По запросу вводим PIN-код Рутокен.


76 %
Ср, 16:50
rutoken
Нет активных соединений
Соединить newconnect
Подробности VPN...
Выйти из Tunnelblick