OpenVPN-клиент – нюансы

1. В текущей версии прошивки используется библиотека **OpenSSL** версии **1.1.1j**.

Необходимо, чтобы на стороне OpenVPN-сервера была поддержка этой версии библиотеки. Если сервер поддерживает только более свежие версии библиотеки, то в веб-конфигураторе контроллера на вкладке **Состояние – Журналы – Системный журнал** отобразится подобное сообщение:

№	Временная метка	Тег	Приоритет	Категория	Сообщение
570	21.11.2024 13:01:34	openvpn(ovpn)[15596]	Error	daemon	TLS Error: tls-crypt unwrapping failed from [AF_INET]10.2.80.80:1194
569	21.11.2024 13:01:34	openvpn(ovpn)[15596]	Error	daemon	tls-crypt unwrap error: packet authentication failed
568	21.11.2024 13:01:18	openvpn(ovpn)[15596]	Error	daemon	TLS Error: tls-crypt unwrapping failed from [AF_INET]10.2.80.80:1194
567	21.11.2024 13:01:18	openvpn(ovpn)[15596]	Error	daemon	tls-crypt unwrap error: packet authentication failed
566	21.11.2024 13:01:10	openvpn(ovpn)[15596]	Error	daemon	TLS Error: tls-crypt unwrapping failed from [AF_INET]10.2.80.80:1194
565	21.11.2024 13:01:10	openvpn(ovpn)[15596]	Error	daemon	tls-crypt unwrap error: packet authentication failed
564	21.11.2024 13:01:06	openvpn(ovpn)[15596]	Error	daemon	TLS Error: tls-crypt unwrapping failed from [AF_INET]10.2.80.80:1194
563	21.11.2024 13:01:06	openvpn(ovpn)[15596]	Error	daemon	tls-crypt unwrap error: packet authentication failed
562	21.11.2024 13:01:04	openvpn(ovpn)[15596]	Notice	daemon	TLS: Initial packet from [AF_INET]10.2.80.80:1194, sid=882f427d 76727ea5

2. В прошивках версии **3.6.xxxx.xxxx** и ниже подключение с использование логина и пароля требовало дополнительных манипуляций в файловой системе контроллера. Они описаны по ссылке.

Начиная с версии прошивки **3.7.xxxx.xxxx** этих действий не требуется – достаточно задать логин и пароль в настройках OpenVPN-клиента (на вкладке **Службы – OpenVPN клиент – Конфигурация** в настройках экземпляра клиента).

Но в любом из вариантов требуется корректная настройка пользователей на стороне сервера.

Пример подобной настройки с использованием docker-контейнера OpenVPN-сервера (создан на базе этой инструкции):

2.1. Создадим на диске рабочий каталог для хранения конфигурации OpenVPN-сервера. Например:

```
/home/igor/my_repos/OpenVpn_Docker
```

2.2. В данном каталоге создадим скрипт для автоматического создания каталога конфигурации и запуска контейнера.

```
#!/bin/bash
#
# Create configuration for openvpn
#
export configdir=/home/igor/my_repos/OpenVpn_Docker/config
mkdir -r $configdir
docker run -v $configdir:/etc/openvpn --rm kylemanna/openvpn ovpn_genconfig -
u udp://IP_Вашего_сервера:11194 -e "duplicate-cn"
```

2.3. Создадим центр выдачи сертификатов.

```
docker run -v /home/igor/my_repos/OpenVpn_Docker/config:/etc/openvpn --rm -it
kylemanna/openvpn ovpn_initpki
```

2.4. Запустим сервер.

```
docker run -v /home/igor/my_repos/OpenVpn_Docker/config:/etc/openvpn -d --
name openvpn --restart=always -p 11194:1194/udp --cap-add=NET_ADMIN
kylemanna/openvpn
```

2.5. Создадим конфигурацию для клиента.

Важно: замените CLIENTNAME на нужное вам имя.

```
docker run -v $configdir:/etc/openvpn --rm -it kylemanna/openvpn easyrsa
build-client-full CLIENTNAME nopass
```

2.6. Выгрузим конфигурацию из контейнера на хостовую машину.

```
docker run -v $configdir:/etc/openvpn --rm kylemanna/openvpn ovpn_getclient
CLIENTNAME > CLIENTNAME.ovpn
```

2.7. Добавляем в каталог конфигурации (в рамках примера это **/home/igor/my_repos/OpenVpn_Docker/config**) скрипт авторизации.

Важно: скрипт авторизации может быть реализован и другими способами; ниже приведен лишь один из вариантов.

В рамках примера созданы два пользователя:

- пользователь **cliwp** с паролем **testtest**
- пользователь **testo** с паролем **testo**

```
#!/bin/sh

USERS="cliwp:testtest testo:testo"

for USER in $USERS
do
   [ "$username:$password" = "$USER" ] && exit 0
done
exit 1
```

2.8. В конфигурацию сервера (в рамках примера это **/home/igor/my_repos/OpenVpn_Docker/config/openvpn.conf**) добавляем следующие строки:

```
script-security 3
auth-user-pass-verify /etc/openvpn/auth.sh via-env
```

2.9. Перезапускаем контейнер. Сервер готов к работе.

```
sudo docker restart openvpn
```

3. Если используемый в конфигурации клиента (**.ovpn**) публичный ключ защищен паролем, то на стороне контроллера следует ввести его с помощью команд Linux (сделать это через веб-конфигуратор нельзя):

```
uci set openvpn.cliwp.cert_password='your_password'
uci commit
```

4. Для настройки **tls-auth** не поддерживается использование параметра **key-direction**. См. подробности по ссылке. В случае использования параметра в логе сервера при попытке подключения со стороны контроллера возникнут подобные ошибки:

```
2025-03-10 11:39:19 Authenticate/Decrypt packet error: packet HMAC
authentication failed
2025-03-10 11:39:19 TLS Error: incoming packet authentication failed from
[AF_INET]<ip>:<port>
```