OpenVPN

Перед использованием клиента OpenVPN на АТОЛ HUB-19 на вашем предприятии должны быть настроены удостоверяющий центр и сервер OpenVPN. Подробности их настройки и взаимодействия не входят в данное руководство, обратитесь к документации на программное обеспечение генерации сертификатов для удостоверяющего центра и к вашему дистрибутиву сервера OpenVPN.

Компоненты сети OpenVPN

Удостоверяющий центр

Выдает сертификаты по запросу узлов сети VPN, подписанные его собственным сертификатом CA. Предоставляет узлам сети VPN свой собственный сертификат для проверки удостоверяющей стороны. Управляет списком отзыва сертификатов – CRL.

Сервер OpenVPN

ПО сервера OpenVPN создает туннель внутри незащищенной сети, например, Интернет. Этот туннель обеспечивает безопасный зашифрованный трафик между узлами — участниками обмена данными в сети OpenVPN. Для идентификации клиентов сервер OpenVPN проверяет полученные от них сертификаты, при помощи сертификата CA и списка CRL.
Адрес сервера OpenVPN должен быть известен и доступен всем подключаемым к нему клиентам. Сервер может иметь несколько подключений к сети Интернет для обеспечения стабильности доступа к нему и, соответственно, несколько адресов.

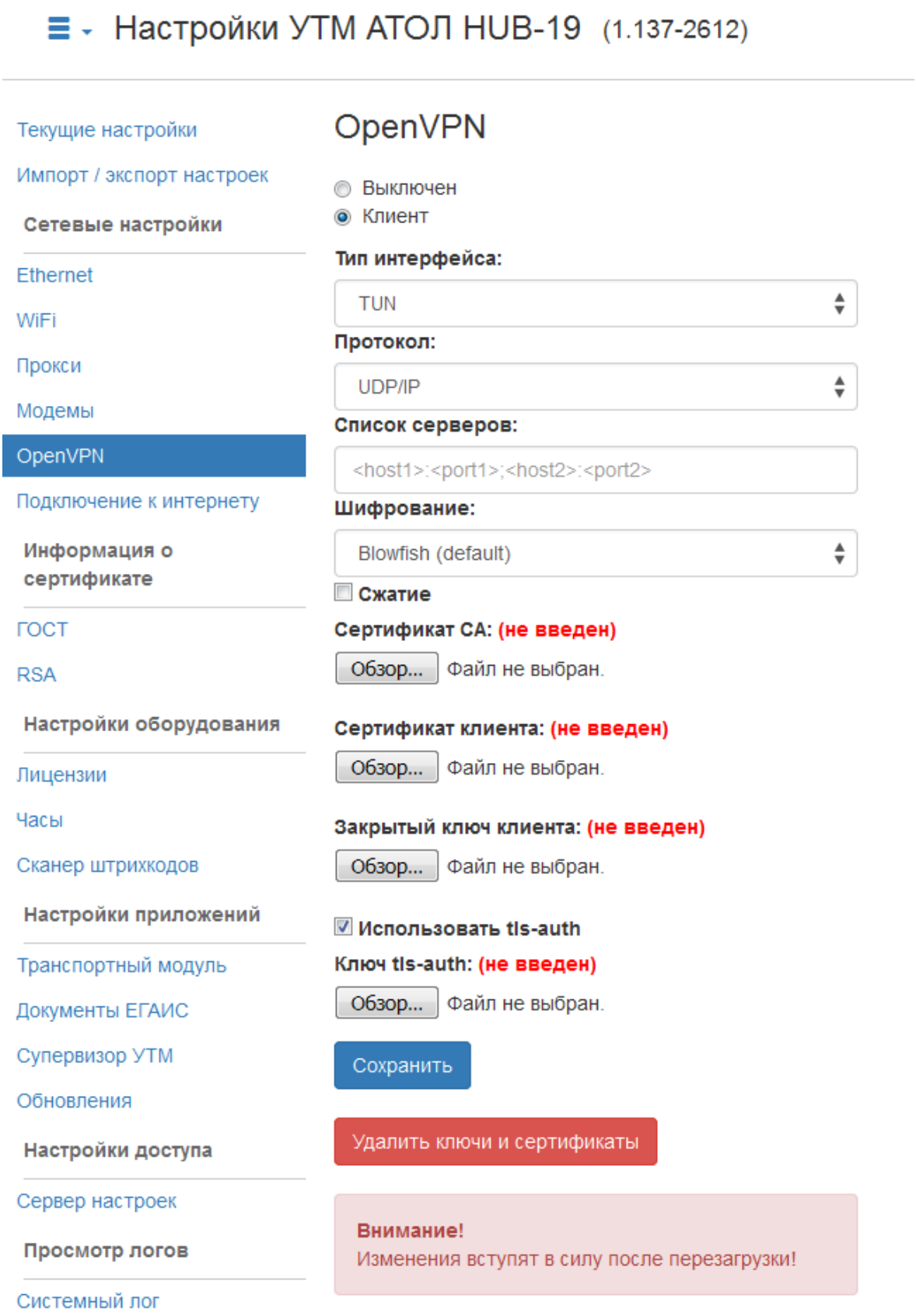
Клиенты OpenVPN

ПО клиента OpenVPN устанавливается на все узлы, которым необходим защищенный канал передачи данных с сервером OpenVPN. При соответствующей настройке сервера OpenVPN возможна защищенная передача данных между клиентами OpenVPN, а не только между клиентом и сервером OpenVPN.

На АТОЛ HUB-19 установлено ПО клиента OpenVPN, в виде пакета обновлений ***hub19-openvpn.***

Настройка подключения АТОЛ HUB-19 к сети OpenVPN

Для подключения АТОЛ HUB-19 к вашей сети OpenVPN необходимо включить флаг ***Клиент*** в разделе «OpenVPN» и заполнить параметры подключения в соответствии с информацией, полученной от системного администратора данной сети.



Тип интерфейса – тип выбранного при настройке сервера OpenVPN сетевого интерфейса:

- TUN (когда в конфигурации сервера OpenVPN указано ***dev tun***);
- TAP (***dev tap***).

Протокол – используемый для создания защищенного туннеля протокол интернет-соединения, выбранный при настройке сервера OpenVPN:

- TCP/IP (когда в конфигурации сервера OpenVPN указано ***proto tcp***);
- UDP/IP (***proto udp***).

Список серверов - список адресов, по которым ваш сервер OpenVPN может быть доступен АТОЛ HUB-19. Адрес состоит из имени или IP-адреса, двоеточия и номера порта, если адресов несколько они разделяются точкой с запятой.

Шифрование - тип используемого шифрования на вашем сервере OpenVPN:

- Blowfish (когда в конфигурации сервера OpenVPN указано ***cipher BF-CBC***);
- AES (***cipher AES-128-CBC***);
- Triple DES (***cipher DES-EDE3-CBC***).

Сжатие – установите данный флаг, если ваш сервер OpenVPN использует алгоритм сжатия LZO (когда в конфигурации сервера указано ***comp-lzo***).

Сертификат CA – загрузите в данное поле сертификат (в формате ***X509***) удостоверяющего центра вашей сети OpenVPN, предоставленный системным администратором.

Сертификат клиента – загрузите в данное поле сертификат клиента (в формате ***X509***), идентифицирующий данный АТОЛ HUB-19 в Вашей сети OpenVPN.

Закрытый ключ клиента – загрузите в данное поле ключ клиента (в формате ***PEM***), идентифицирующий данный АТОЛ HUB-19 в вашей сети OpenVPN.

Сертификат клиента и **Закрытый ключ клиента** для АТОЛ HUB-19 создаются системным администратором сети OpenVPN в ПО удостоверяющего центра.

Использовать tls-auth – включите данный флаг, если ваш сервер OpenVPN настроен с использованием дополнительной защиты соединения по протоколу SSL/TLS (когда в конфигурации сервера указаны параметры ***tls-auth***), при этом потребуется загрузить файл ключа.

Ключ tls-auth – загрузите в данное поле ключ (в формате ***OpenVPN Static key***) для установки соединения по протоколу SSL/TLS, предоставленный системным администратором.

После всех изменений необходимо нажать на кнопку *Сохранить* и перезагрузить HUB-19.

Если использование OpenVPN на данном УТМ АТОЛ HUB-19 более не требуется, рекомендуется удалить ключи и сертификаты во избежание компрометирования вашей сети OpenVPN.