

# OpenVPN-сеть

### Добавление OpenVPN-сети

Основные настройки    Шифрование и сертификаты

Название \*     Ip-адрес/Префикс \*

Протокол     Порт сервера \*

Использовать NAT

Разрешить трафик между клиентами

Передать клиенту маршрут по умолчанию

Передать клиентам маршруты до сетей

Передать клиентам DNS сервера

Разрешить управление ИКК через веб

Разрешить управление ИКК через SSH

### Добавление OpenVPN-сети

Основные настройки    Шифрование и сертификаты

Алгоритм шифрования     Алгоритм хеширования

Включить сжатие LZO

Включить TLS Auth

link-MTU \*

Корневой сертификат \*     Сертификат сервера \*

  

Флаг «Включить TLS Auth». Если флаг не установлен, то клиент не должен использовать tls auth key. Параметр TLS Auth добавляет использование еще одной подписи HMAC к handshake-пакетам SSL/TLS, иницируя дополнительную проверку целостности. Теперь пакет, не имеющий такой подписи, будет отбрасываться, не обрабатываясь. Это обеспечит дополнительный уровень безопасности протокола SSL/TLS, защищая систему от таких атак, как:

- Сканирование прослушиваемых VPN-сервером портов - Инициация SSL/TLS-соединения несанкционированной машиной (хотя подобные рукопожатия не проходят и при стандартной конфигурации OpenVPN, но TLS Auth отсекает их на значительно более раннем этапе) - DoS-атаки и флуд на порты OpenVPN - Переполнение буфера SSL/TLS

From:

<https://doc-old.a-real.ru/> - **Документация**

Permanent link:

[https://doc-old.a-real.ru/doku.php?id=ics70:openvpn\\_net&rev=1591865757](https://doc-old.a-real.ru/doku.php?id=ics70:openvpn_net&rev=1591865757)

Last update: **2020/06/11 11:55**

