

# OpenVPN-сеть

## Основные настройки

Добавление OpenVPN-сети

Основные настройки

Шифрование и сертификаты

Название \*

Ир-адрес/Префикс \*

Новая OpenVPN-сеть

10.8.0.0/24

Протокол

Порт сервера \*

UDP

1194

☐ Использовать NAT

☒ Разрешить трафик между клиентами

☐ Передать клиенту маршрут по умолчанию

Передать клиентам маршруты до сетей

Передать клиентам маршруты до сетей

Передать клиентам DNS сервера

Передать клиентам DNS сервера

☐ Разрешить управление ИКС через веб

☐ Разрешить управление ИКС через SSH

## Шифрование и сертификаты

## Добавление OpenVPN-сети

Основные настройки

Шифрование и сертификаты

Алгоритм шифрования

AES-256-CBC

Алгоритм хеширования

SHA256

☐ Включить сжатие LZO☒ Включить TLS Auth

link-MTU \*

1500

Корневой сертификат \*

VPN\_CA ✕

Сертификат сервера \*

VPN\_serv ✕

Добавить

Отмена

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, инициируя 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=1591865886](https://doc-old.a-real.ru/doku.php?id=ics70:openvpn_net&rev=1591865886)

Last update: 2020/06/11 11:58

