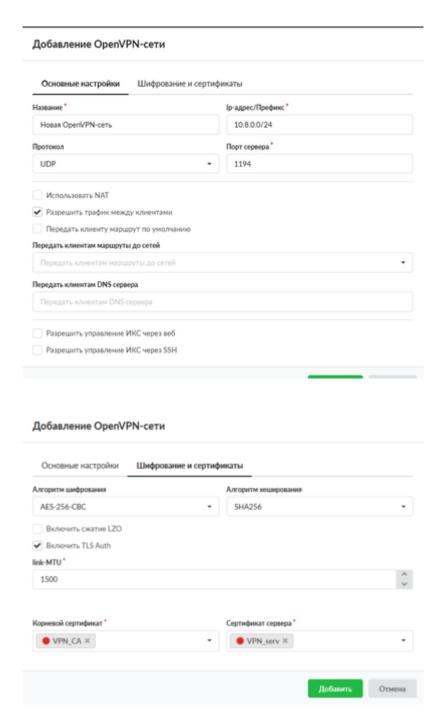
2025/11/04 05:41 1/2 ОрепVPN-сеть

OpenVPN-сеть



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 - Переполенение буфера SSL/TLS

Last update: 2020/06/11 11:55

From:

https://doc-old.a-real.ru/ - Документация

Permanent link:

https://doc-old.a-real.ru/doku.php?id=ics70:openvpn_net&rev=1591865757

Last update: 2020/06/11 11:55



https://doc-old.a-real.ru/ Printed on 2025/11/04 05:41