Настройка VPN подключения на базе IKEv2

29.03.2024 18:50:37

Печать статьи FAQ

Категория:	Решения::Решение "VPN"	**Голоса:**	0
Состояние:	общедоступное (всем)	**Результат:**	0.00 %
Язык:	ru	**Последнее обновление:**	17:27:40, Чтв 12 Янв, 2023 г.

Ключевые слова

IKEv2 Windows, IKEv2 Android, IKEv2 Ubuntu, IKEv2 iOS, IKEv2 MAC OS

Симптомы (общедоступное)

Преимущества IKEv2 — очень быстрое подключение, работает быстрее остальных VPN, клиенту передаются маршруты в сеть подключения, из одного офиса можно выполнить несколько подключений, простое подключение.

Недостатки: один логин — одно подключение.

Проблема (общедоступное)

Необходимо настроить подключение к IKEv2 VPN на устройствах:
Windows
Linux
Android
MAC OS
iOS

Решение (общедоступное)

Для подключения нами будут использованы:

адрес сервера для подключения

логин с доменом от доменной учетной записи (домен\пользователь или пользователь@домен)

пароль от доменной учетной записи

Подключение в Windows

Сетевые настройки — VPN — новое подключение

Вводим имя подключения (любое)

Выбираем «Windows встроенное»

Выбираем IKEv2

Вводим логин и пароль.

Сохранить

В Windows по умолчанию ставит для всех VPN «шлюз по умолчанию». Это приводит к тому, что весь трафик отправляется в туннель VPN, что нам не нужно. Идем в сетевые настройки — сетевые адаптеры, находим наше созданное подключение, заходим в Свойства — сеть — IPv4 — Дополнительно. Снять галку «шлюз по умолчанию».

Для того, что бы открывались сервера по DNS именам нужно снять галочку "автоматическое назначение метрики" и установить значение 10.

Подключение в Linux Ubuntu\Kubuntu\Mint

apt updateapt install strongswan libcharon-extra-pluginsUbuntu:sudo apt-get install -y strongswan libcharon-extra-pluginssudo apt-get install -y network-manager-strongswan

Настроить сетевые подключения (Configure network connections). Добавить новое подключение — выбираем IPSec based VPN (strongswan) (подпись IKEv2 based VPN). Вводим в поля имя (любое), адрес сервера для подключения, логин и пароль.

Для того, что бы открывались сервера по DNS именам нужно указать в настройках (вкладка IPv4) указать поисковый домен (Search Domains): blitzteam.local

Подключение в Linux Centos 8\Centos 9

dnf install epel-release

dnf update

dnf install strongswan strongswan-charon-nm

Настроить сетевые подключения (Configure network connections). Добавить новое

подключение — выбираем IPSec based VPN (strongswan) (подпись IKEv2 based VPN).
Вводим в поля имя (любое), адрес сервера для подключения, логин и пароль.

Подключение Android

Необходимо через Google Play установить приложение Strongswan VPN Client.

Открываем приложение. Новое подключение и заполняем адрес сервера, логин и пароль. Тип подключения не меняем (он должен быть IKEv2 EAP (логин и пароль).

Подключение MacOS

Переходим в Сеть — нажимаем + (новое подключение). Интерфейс VPN, тип IKEv2, имя службы — любое. Далее заполняем.

Адрес сервера — наш адрес подключения

Удаленный ID — повторяем наш адрес подключения

Настройки аутентификации — логин и пароль.

Особенность: не возможность работать с доменными именами серверов. Маршруты и search домен передаются клиенту, но их метрика (if_index при вводе scutil --dns можно увидеть) для VPN подключения выше, чем для текущего интернета и запрос просто не проходит. Обходным решением будет только прописать нужные сервера в файл /etc/hosts.

Подключение iOS

Настройки — Сеть — новое подключение — IKEv2. Там вводим адрес подключения, Удаленный ID — тоже самое (адрес подключения), логин и пароль. Имя любое.