Настройка VPN сервера

Докладчик: Фокин Арсений

Ссылки

1. Официальная документация
2. Установка и настройка (Краткое руководство)
3. Установка и настройка (Кратко-полное руководство)
4. Установка и настройка (Полное руководство)

Общая информация и назначение VPN

Простыми словами, VPN (англ. Virtual Private Network “виртуальная частная сеть”) - это онлайн-сервис, который может скрыть ваш IP-адрес и местоположение, а также зашифровать ваши интернет-данные и трафик. Это позволит защитить данные при передаче через интернет и получить доступ к санкционным ресурсам :)

Почему сеть VPN называется виртуальной и частной?

Виртуальная она потому, что узлы сети объединяются не физическими линиями, а виртуальными соединениями, которые создаются программным обеспечением (ПО) VPN.

Сеть VPN частная, так как к ней могут подключаться только узлы компании, создавшей эту сеть, а не все желающие. На каждом узле сети VPN должно работать ПО VPN. Еще там должны находиться ключи и сертификаты, обеспечивающие узлам доступ к сети VPN и криптографическую защиту передаваемых данных.

Таким образом, сеть VPN может объединять ресурсы (серверы и рабочие станции) компании в единую безопасную виртуальную сеть, созданную на базе Интернета. И теперь сотрудники, работающие удаленно (из дома или из другой страны) будут находиться как бы в общей сети своей компании. Сеть VPN подходит и для консолидации территориально разделенных офисов компании.

Общая информация OpenVPN

OpenVPN — это VPN-протокол и ПО, которое использует методы VPN для защиты соединений типа “точка-точка” и “сайт-сайт”. В настоящее время это один из самых популярных VPN-протоколов среди пользователей VPN.

Он был разработан Джеймсом Йонаном и выпущен в 2001 году. OpenVPN — один из VPN-протоколов с нативным приложением и с открытым исходным кодом

Обзор возможностей по сетевой настройке

Компоненты сети OpenVPN

Удостоверяющий центр (англ. Certification authority, CA)
Выдает сертификаты по запросу узлов сети VPN, подписанные сертификатом удостоверяющего центра. 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, Интернета. Этот туннель обеспечивает безопасный зашифрованный трафик между узлами — участниками обмена данными в сети OpenVPN.

Клиент 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 клиентами и сервером OpenVPN.

Сертификаты (публичные ключи) X.509
Сертификаты X.509 представляют собой публичные ключи, заверенные удостоверяющим центром CA. Они используются для шифрования данных. Факт заверения сертификата удостоверяющим центром CA позволяет идентифицировать сторону, передающую зашифрованные данные.

Приватные ключи
Приватные ключи секретные. Они должны создаваться и храниться на каждом узле сети OpenVPN, предназначены для расшифрования данных и никогда не должны передаваться по сети.

Список отзыва сертификатов CRL
Содержит список сертификатов, утративших доверие. Он создается и редактируется на узле удостоверяющего центра CA.
Чтобы отключить узел от сети, достаточно занести его сертификат в список CRL.

Файл Диффи-Хеллмана
Используется, чтобы в случае похищения ключей исключить расшифровку трафика, записанного еще до этого похищения. Создается на сервере OpenVPN.

Статический ключ HMAC
Служит для проверки подлинности передаваемой информации. Обеспечивает защиту от DoS-атак и флуда. Создается на сервере OpenVPN.

Установка и настройка сервера

Скрипты для быстрой настройки сервера:

1. https://github.com/Nyr/openvpn-install (15k stars)

2. https://github.com/angristan/openvpn-install (8.1k stars)

P.s. Далее рассматриваем первый скрипт

1. Заходим на удалённую машину
   ssh имя_пользователя@айпи_адресс

2. Обновляем данные о пакетах и устанавливаем утилиту для скачивания файлов

   apt-get update

   apt-get install wget

3. Скачиваем скрипт

   wget https://git.io/vpn -O openvpn-install.sh

4. Запускаем скрипт

chmod +x openvpn-install.sh

sudo ./openvpn-install.sh

5. Настройка

5.1. Выбор протокола

UDP - OpenVPN лучше всего работает по UDP (согласно данным OpenVPN.net), поэтому сервер доступа OpenVPN сначала пытается установить UDP-соединения. Если это не удаётся, только тогда сервер пробует создать соединение по протоколу TCP.

5.2. Порт (1194)

5.3. DNS сервер (Текущий)

5.4. Имя клиента (client1) (Должны быть уникальны)

6. Скрипт создал нам полную иерархию настроек OpenVPN сервера в /etc/openvpn (Настройки сервера - /etc/openvpn/server/server.conf) и файл для клиента client1.ovpn

Установка и настройка клиента из консоли

1. Копируем файл с настройками клиента с сервера

   scp имя_пользователя@айпи_адресс:путь_до_файла_на_сервера путь_до_файла_на_клиенте

   Пример: scp имя_пользователя@айпи_адресс:/root/client1.ovpn /etc/openvpn/

2. Узнаем свой текущий внешний ip адрес

   curl ifconfig.me/ip

3. Устанавливаем openvpn

   sudo apt-get update

   sudo apt-get install openvpn

4. Запускаем клиент

   sudo openvpn –config /etc/openvpn/client1.ovpn

6. Ждем (1-2 минуты)

7. Проверяем

    curl ifconfig.me/ip - Должен быть новый IP

    P.s. Если вы выполняете это на машине из за границы, то должен появиться доступ к Instagram

8. VPN подключен :)

Отзыв сертификата

1. Удаляем клиент из папки easy-rsa

   ./easy-rsa revoke имя_клиента
2. Перезапускаем сервис

   service openvpn restart
3. Проверяем, что доступ пропал

Задания

1. Создать сервер. Установить клиент. Подключить к серверу по VPN, проверить внешний IP адрес. Попробовать установить клиент на телефон.
2. Создать несколько клиентов, отозвать сертификаты
3. Настроить сервер по полному руководству из источников