ВИРТУАЛЬНАЯ СИСТЕМА VPN В СОТОВОЙ СЕТИ LTE

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ловенецкий Д.А.

Саломатин С.Б.. – к.т.н.,доцент

Несмотря на «сетевую» интерпретацию, технологии VPN на самом деле имеют и более широкую трактовку, поскольку по своим принципам в некотором смысле напоминают функционирование прокси-серверов с установкой защищенного соединения и шифрованием передаваемой и принимаемой информации. Для осуществления подключения через VPN применяется принцип так называемого туннелирования.

Собственно, особой разницы между тем, что собой представляет доступ в Интернет посредством использования VPN на стационарных компьютерах, ноутбуках, смартфонах или планшетах, нет.

Это самое обычное туннелирование, которое по принципам работы несколько похоже на функционирование анонимных прокси-серверов, иначе называемых анонимайзерами. VPN в телефонах это инструмент, позволяющий изменить внешний IP девайса для доступа на заблокированные ресурсы. При смене IP соответственно меняется и местоположение пользователя, который пытается войти на определенную страницу, к которой доступ в его регионе не разрешен. Кроме того, при таком положении дел пользователь остается как бы неузнанным в Сети, а его данные полностью шифруются на основе защиты WPA. Правда, только буквально на днях стало известно, что протокол WPA2, в большинстве случаев используемый для подключений через Wi-Fi, имеет достаточно серьезные уязвимости, которые позволяют злоумышленникам отслеживать исходящий и входящий трафик целиком и полностью.

Защищенные виртуальные сети способны обеспечить надежную шифрованную передачу данных через Интернет. В качестве примера можно привести PPTP, OpenVPN и IPSec. В случае, если передающая среда считается достаточно надежной и вопросы безопасности решены в рамках базовой локальной инфраструктуры, можно настроить и использовать доверительные ВПН-соединения L2TP (обычно используется в тандеме с IPSec) или MPLS.

В качестве алгоритма кодирования наиболее часто применяется Triple DES. Он обеспечивает 168-разрядное шифрование тремя различными ключами. Это дает стопроцентную гарантию того, что прочитать данные сможет лишь пользователь, обладающий соответствующими правами. Эффективных алгоритмов криптографических атак на этот симметричный шифр не существует, а значит вероятность его расшифровки даже профессиональным хакером стремится к нулю.

Основные преимущества VPN:

- пользователю предоставляется выделенная полоса (нет распределения на конкурентной основе);
- при увеличении количества абонентов затухание в WDM-мультиплексоре растёт в меньшей степени чем в оптическом сплиттере;
- сигналы абонентов физически изолированы;
- анонимной работы в сети интернет;
- загрузки приложений, в случае, когда ip адрес расположен в другой региональной зоне страны;
- безопасной работы в корпоративной среде с использованием коммуникаций;
- простоты и удобства настройки подключения;
- обеспечения высокой скорости соединения без обрывов;
- создания защищённого канала без хакерских атак.

Преимуществ в использовании таких технологий хватает. Но есть и свои проблемы. Самая главная из них состоит в том, что используемый туннель не может одновременно следить за разными типами сетей, по которым осуществляется подключение к Интернету. Например, связь может пропадать при смене Wi-Fi на 3G/4G. Проблему начали устранять только недавно. На выделенных VPN-серверах появилась специальная авторизация, которая позволила осуществлять двустороннюю передачу данных, вне зависимости от того, какая именно сеть используется в данный момент. Тут основное преимущество состоит в том, что в криптографическом плане и виртуальный интерфейс пользовательского гаджета, и сеть оператора, и сам протокол доступа стали одинаковыми.

Список использованных источников:

1 Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. / В.Г. Олифер, Н.А. Олифер –СПб. Питер, 2010. – 944 с

2 Олвейн, В.. Структура и реализация современной технологии MPLS.: Пер. с англ. – М. Вильямс, 2004. – 480 с.

3 Virtual Local Area Network [Электронный ресурс]. – Режим доступа : http://www.admindoc.ru/.