Доклад по теме Виртуальные частные сети

Ильин Никита Евгеньевич, НФИбд-01-19

Содержание

List of Figures

List of Tables

1 Что такое виртуальные частные сети

Виртуальные частные сети (VPN) - это технология, которая позволяет создавать сетевые соединения типа “точка-точка”, поверх другой сети. Подключиться к такой сети может только тот, кому предоставили к ней доступ, а весь трафик в ней шифруется.

2 Для чего применяются виртуальные частные сети

С помощью VPN можно объединить офисы одной компании, которые могут находиться в разных частях города, или даже в разных точках мира. Также с помощью VPN можно изолировать или объединить отделы внутри компании. Во времена пандемии сотрудники часто работали из дома, именно с помощью VPN они могли получить доступ к сети своей организации, а соответственно к сервисам и всей документации. Такое соединение безопасно, данные сложно перехватить, и даже если данные будут перехвачены, то их будет тяжело расшифровать.

С помощью VPN также можно получить доступ к сайтам, которые заблокированы в стране. Сейчас в нашей стране есть некоторые социальные сети, к которым у нас нет доступа, но с помощью VPN можно получить доступ к ним. Также в путешествиях можно получать доступ к сайтам, которые заблокированы в тех странах.

Еще с VPN можно создать безопасное подключение для использования в публичных сетях, то есть Ваши данные социальных сетей, банковских приложений, и другая конфиденциальная информация не будет преехвачена злоумышленниками.

3 Как использовать VPN

Чтобы подключиться к VPN сети нужно устанавить на свое устройство специальную программу - VPN-клиент. Это самый простой способ, но в большинстве сервисов выдается случайный IP-адрес, принадлежащий случайной стране, без возможности выбора. А чтобы подключиться к своему рабочему месту, необходимо зайти в настройки сети ОС, найти функцию подключения к удаленной сети, и ввести данные сети.

4 Недостатки VPN

Прежде всего - низкая скорость подключения, потому что сеть чаще всего находится на большом растоянии, а также весь трафик проходит шифрование.

Периодически сети разрывают подключение, из-за чего трафик выходит в публичную сеть. Сами сети не умеют восстанавливать подлкючения, но многие современные ОС имеют функцию переплдключения в случае разрыва.

На законодательном уровне тоже могут возникнуть проблемы. Не во всех странах разрешен VPN, а трафик часто проходит через другие страны.

Многие сервисы имеют бесплатные возможности, но по-настоящему безопасные VPN сервисы требуют платы за свои услуги. Также бесплатные провайдеры могут отслеживать вашу активность в сети, так как они имеют доступ к своей сети.

5 Как работает VPN

Виртуальная частная сеть состоит из следующих компонентов: * VPN-сервер * шифрующие алгоритмы * система аутентификации пользователей * протокол сети VPN

Виртуальная частная сеть является посредником между устройством пользователя и сетью(подключение типа “клиент-сервер”), или же она является локальной сетью с двумя маршрутизаторами(подключение типа “сервер-сервер”). Клиент подключается к сети с помощью сервера доступа, который подключается к внешней, и к внутренней сети. В момент, когда вы подключаетесь к сети VPN, система проверяет вашу сеть, и авторизует вас в своей сети, между компьютером пользователя и сервером создается зашифрованный канал, который можно назвать своеобразным тоннелем. В этот момент IP пользователя меняется на IP сервера, откуда все данные передаются ресурсам, с которыми вы работаете. VPN-пакеты смешиваются с трафиком основной сети, а затем шифруются, чтобы сохранить конфиденциальность данных, которые передаются в данной сети. Чтобы виртуальная сеть работала, создаются специальные протоколы типа TCP/IP, которые называются туннельными. Все точки сети поддерживают несколько соединений с другими точками, но при этом они все являются изолированными.

Виртуальные частные сети могут создавать соединения трех видов: узел-узел, узел-сеть и сеть-сеть. Тип соединения зависит от применяемых протоколов, и назначения сети.

Подключение типа “сеть-сеть” соединяет между собой два сегмнта частных

сетей, что позволяет устанавливать маршрутизируемые подключения между различными структурами одной компании, обеспечив безопасную связь между ними. Сервер удаленного доступа отвечает на запрос от вызывающей стороны, проверяет подлинность пакетов, а затем передает данные между клиентом и сетью.

Подключение типа “узел-сеть” соединяет любое внешнее устройство с VPN-сервером. Для установки соединения устройство должно пройти авторизацию, что дает пользователям возможность работать удаленно, из любой точки, используя любую публичную точку доступа. Для пользователя создается выделенный частный канал, следовательно реальная инфраструктура сети не имеет никакого значения.

6 Классификация VPN

Основные параметры классификации: * Способ реализации сети * Степень защищенности * Назначение сети * Тип протокола

Сети могут быть реализованы следующими способами:

- В виде программно-аппаратного обеспечения(такая реализация обеспечивает высокую степень защиты, и скорость работы)
- В виде программного решения(установленное ПО на устройство пользователя)
- Интегрированное решение(функциональность обеспечивается с помощью комплекса, который решает задачи фильтрации, организации сетевого экрана, и обеспечения производительности)

Самый распространенный вариант использования VPN - создание защищенной сети, на основе ненадежной сети. Самыми известными примерами защищенной сети являются IPSec, OpenVPN и PPTP. Также бывают и незащищенные VPN соединения, но используются они только если среду можно считать надежной. Например, если необходимо создать виртуальную подсеть в рамках большой сети, где проблемы безопасности неактуальны. Примером такого решения можно считать протоколы MPLS и L2TP.

MPLS - масштабируемый и независимый протокол передачи данных, который маркирует пакеты по степени важности, что увеличивает производительность работы важных программ.

L2TP - протокол, который не обеспечивает должного уровня конфиденциальности информации, поэтому его используют только в описанном выше случае, либо с дополнительными протоколами шифрования.

Существует несколько назначений VPN:

- Internet VPN - единая защищеннач сеть между несколькими филиалами однйо компании, располоденных в разных точках. Также часто провайдеры создают VPN-сервер, если к одному физическому каналу подключены несколько устройств.
- Intranet VPN - защищенная сеть, передающая данынй по открытым каналам связи, и объединяющая несколько филиалов одной организации в единую сеть. Для организации такой сети необходим VPN-сервер в каждом филиале.
- Remote Access VPN - создание защищенного канал связи между корпоративной сетью и пользователем, который подключается к сети удаленно.
- Extranet VPN - сеть, имеющая возможность подключения внешних пользователей. В настоящее время сильно распространена, в связи с развитием электронной коммерции.
- Client-Server VPN - сеть, которая строится между узлами в одном сегменте сети, например между рабочей станцией и сервером. Такая возможность очень часто необходима в крупных компаниях ,чтобы разделить трафик между различными отделами компании

Далее рассмотрим протоколы VPN:

Поскольку данные в виртуальных частных сетях передаются через общедоступную сеть, следовательно, они должны быть надежно защищены. Для реализации защиты передаваемой информации существует множество протоколов, которые защищают VPN, но все они подразделяются на два вида и работают в паре:

- протоколы, инкапсулирующие данные и формирующие VPN соединение;
- протоколы, шифрующие данные внутри созданного туннеля.

Первый тип протоколов устанавливает туннелированное соединение, а второй тип отвечает непосредственно за шифрование данных.

Рассмотрим некоторые стандартные, предлагаемые всемирно признанным мировым лидером в области разработки операционных систем, решения. В качестве стандартного набора предлагается сделать выбор из двух протоколов (точнее будет сказать наборов), являющихся встроенными в клиент удаленного доступа операционных систем Microsoft:

1. PPTP (Point-to-Point Tunneling Protocol) – туннельный протокол являющийся расширением протокола PPP (Point-to-Point Protocol), следовательно, использует его механизмы подлинности, сжатия и шифрования. При стандартном выборе данного протокола предлагается использовать метод шифрования MPPE (Microsoft Point-to-Point Encryption). Можно передавать данные без шифрования в открытом виде. Инкапсуляция данных по протоколу PPTP происходит путем добавления заголовка GRE (Generic Routing Encapsulation) и заголовка IP к данным обработанных протоколом PPP. Не требователен к ресурсам сети и аппаратных средств.

2. L2TP (Layer Two Tunneling Protocol) – более совершенный протокол, родившийся в результате объединения протоколов PPTP (от Microsoft) и L2F (от Cisco), вобравший в себя все лучшее из этих двух протоколов. Предоставляет более защищенное соединение, нежели первый вариант, шифрование происходит средствами протокола IPSec (IP-security). L2TP также является более предпочтительным в плане безопасности. Инкапсуляция данных происходит путем добавления заголовков L2TP и IPSec к данным обработанным протоколом PPP. Шифрование данных достигается путем применения алгоритма DES (Data Encryption Standard) или 3DES. Именно в последнем случае достигается наибольшая безопасность передаваемых дан-

ных, однако в этом случае придется расплачиваться скоростью соединения, а также ресурсами центрального процессора.

Рассмотренные примеры протоколов не являются единственными, существует множество альтернативных решений, например, PopTop – Unix реализация PPTP, или FreeSWAN – протокол для установления IPSec соединения под Linux, а также: OpenVPN (стабильный и сверхбезопасный), Vtun, Racoon, ISAKMPD и др.

7 Шифрование Данных

Для обеспечения конфиденциальности данные шифруются отправителем и расшифровываются получателем. Успешность процессов шифрования и расшифровки гарантируется в том случае, когда отправитель и получатель используют общий ключ шифрования. Содержание перехваченных пакетов, отправленных по VPN-подключению в транзитной сети, понятно только владельцам общего ключа. Длина ключа шифрования - это важный параметр безопасности: 1024-битный Ключ Шифрования гарантированно защищает личную информацию - чтобы взломать данный ключ суперкомпьютеру понадобится более миллиона лет.

Выбор алгоритма не имеет принципиального значения, если он будет стандартным и в достаточной степени мощным. Гораздо больше влияет на общий уровень безопасности реализация системы. Чтобы получить доступ к информации, передаваемой через VPN, злоумышленник должен: • захватить весь сеанс соединения, т.е. разместить устройство прослушивания между противоположными концами соединения в том месте, через которое должен передаваться весь трафик VPN; • использовать большие вычислительные мощности и большое количество времени для перехвата ключа и дешифрования трафика.

8 Аутентификация и проверка подлинности

Система аутентификации VPN должна быть двухфакторной, т.е. с использованием того, что они знают, того, что у них есть или с помощью данных о том, кем они являются. Хорошей комбинацией средств аутентификации являются смарт-карты в паре с персональным идентификационным номером или паролем.

Существует три различные формы проверки подлинности для VPN-подключений:

1. Взаимная проверка подлинности выполняется на уровне пользователя по протоколу PPP. Проверяется требуемая авторизация VPN-клиента и проверка подлинности VPN-сервера, что гарантирует защиту от компьютеров, выдающих себя за VPN-серверы.

2. Взаимная проверка подлинности выполняется по протоколу IKE, при котором происходит обмен сертификатами компьютеров или предварительным ключом. Эта проверка подлинности на уровне компьютера выполняется только для подключений L2TP/IPsec.

3. Целостность данных (а также взаимная проверка подлинности) обеспечивается контрольной суммой шифрования, основанной на ключе шифрования, который известен только отправителю и получателю. Доступно только для подключений L2TP/IPsec.

9 Источники

- Олифер В.Г., Олифер Н.А. “Компьютерные сети. Принципы, технологии, протоколы. Учебник для ВУЗов” - СПБ:Питер, 2001
- Интернет-ресурс: https://www.smartydns.com/ - Что такое VPN-сервер?
- Статья: Виртуальная частная сеть (VPN), технология, принципы работы и использования