УДК 004.7

Поротиков А.А.,
студент магистратуры
2 курс, факультет «Магистратуры»
Поволжский Государственный Университет Телекоммуникаций и Информатики
Россия, г. Самара
Научный руководитель: Стефанова Ирина Алексеевна

ПРИМЕНЕНИЕ VPN СЕТЕЙ В УСЛОВИЯХ ПАНДЕМИИ

Аннотация: *в статье рассматриваются понятие VPN сетей. Рассмотрены их разновидности и способы применения. Кратко описаны особенности каждой из видов и их сценарии использования в наши дни.*

Ключевые слова: *Корпоративная сеть, сеть, VPN, Интернет, безопасность, построение, соединение.*

Annotation: *The article discusses the concept of VPN networks. Their varieties and methods of application are considered. The features of each of the types and their usage scenarios are briefly described today.*

Key words: *corporate network, network, VPN, Internet, security, building, connection.*

Совсем недавно никто не мог подумать, как может изменится образ жизни и работы. За последний год все больше и больше организаций переходят на труд удаленных сотрудников, которые работают на домашних компьютерах, а также работают в каких-либо других условиях. Так же если организация имеет множество филиалов или партнеров, с которыми тесно сотрудничает, то нужно как-то соединять их с головным офисом.

Сейчас для сотрудников как никогда является очень важным

возможность подключиться к корпоративной сети. При этом им требуется широкополосное соединение независимо от того, используется ли фиксированная сеть или же Wi–Fi, так как нередко сотрудники вынуждены работать в пути. Сейчас более популярными становятся виртуальные технологии, которые занимают в современной компании приоритетное положение.

VPN (Virtual Private Network) или виртуальная частная сеть – это технология, при реализации которой выполняется обмен информации по виртуальному каналу с удаленной локальной сетью через сеть общего пользования с воспроизведением частного подключения. Для работы таких технологий не требуется навсегда однозначное размещение сотрудников в офисе, нет необходимости вообще там находиться – достаточно использовать удаленное подключение. Кроме того, многие компании предусматривают возможность доступа только к определенным корпоративным ресурсам и приложениям для партнеров, консультантов и клиентов.

VPN соединение всегда состоит из канала типа точка–точка, которое также называют туннель. Туннель строится в незащищённой сети, которой в основном выступает Интернет. Соединение точка–точка значит, что такое соединение устанавливается между двумя или более компьютерами, которые называются узлами. Задача узла состоит в шифровании данных перед их попаданием в туннель, а также за расшифровку этих данных после того, как они покинут туннель.

Корпоративные VPN сети реализуются по следующим схемам: Intranet VPN, Remote Access VPN, Extranet VPN, client/server VPN.

- **Intranet VPN или внутрикорпоративные VPN.**

Позволяет объединить в единую защищенную сеть несколько распределенных филиалов одной организации, взаимодействующих по открытым каналам связи. Именно этот вариант получил широкое распространение во всем мире, и именно его в первую очередь реализуют

компании-разработчики. Intranet VPN позволяет заказчику устанавливать связь между своими офисами, используя IP-сеть.

Эта технология использует методы туннелирования GRE, L2TP или IPSec. Туннели устанавливаются между офисными маршрутизаторами для создания между офисами виртуальных соединений. Для повышения безопасности данные в виртуальном канале могут шифроваться. Шифрование выполняется только на выходе из офисов во внешние сети. Такая топология образует "защищенный периметр" вокруг ЛВС корпорации.

- **Remote Access VPN или VPN с удаленным доступом.**

Между частью корпоративной сети (например, центральным офисом или ее филиалом) и отдельным пользователем, который работает из другой точки, не находясь в офисе (к примеру, из дома), создается защищенный канал. Сотрудник подключается к ресурсам компании с любого устройства, будь то домашний компьютер, корпоративный ноутбук, смартфон.

Построение такой виртуальной частной сети подразумевает наличие VPN сервера в главном офисе, к которому подключаются удаленные пользователи.

- **Extranet VPN или межкорпоративные VPN.**

Когда происходит подключение сторонних пользователей к сети, уровень доверия к ней будет ниже, потому что речь идет не о сотрудниках компании, а, например, о партнерах, как в нашем случае. Поэтому нужно обеспечивать специальный уровень защиты, чтобы предотвратить или ограничить доступ сторонних лиц к особо ценной информации.

Одной из наиболее важных причин, делающих виртуальные сети extranet настолько популярными, является возможность совершать с их помощью безопасные сделки через Internet. Эта технология обычно включает использование цифровых сертификатов, которые предоставляют более высокий уровень пользовательской аутентификации, а также ту или иную систему регулирования ключей шифрования.

В случае такой реализации значительно урезается возможность использования сети компании для сторонних пользователей, они будут ограничены доступом к ресурсам организации, которые нужны им для работы с клиентами, например, сайт с коммерческими предложениями, а VPN будет использоваться для безопасной пересылки конфиденциальных данных.

- **client/server VPN.**

Служит для обеспечения защиты передаваемой информации между двумя узлами единой сети используется данный тип. В основном такие узлы расположены в одной части. Удобен для разделения трафика между разными отделами одной компании. Например, когда надо разделить трафик между финансовым департаментом и отделом кадров, которые обращаются к серверам, находящимся в одном физическом сегменте. Решается задача защиты трафика ряда приложений внутри офиса, при этом образуются отдельные, непересекающиеся VPN для выделенных групп пользователей или приложений.

Также нужно отметить сети, с которыми придется работать, бывают: защищенные и доверительные.

Защищённые. Являются самым распространённым типом виртуальных частных сетей. Сеть, спроектированная в данной работе, так же является ее представителем. Благодаря им появляется возможность создать защищённую, а главное, надежную сеть используя имеющуюся ненадёжную сеть, которой, как правило, выступает Интернет. К защищённым VPN можно отнести: PPTP; IPSec; OpenVPN; L2TP.

Доверительные. Используется тогда, когда среда передачи является надежной и нужно создать виртуальную подсеть в рамках большой сети. Проблемы с безопасностью в данном случае становятся неактуальными. Примерами подобных VPN решений являются: MPLS и L2TP.

Список литературы:

1. Ибе, О. Сети и удаленный доступ. Протоколы, проблемы, решения: справочник / О. Ибе; пер. с англ. - М.: ДМК Пресс, 2002.

2. Михеева, Е.В. Информационные технологии в профессиональной деятельности [Текст]: учебное пособие для вузов / Е.В. Михеева – М.: Академия, 2011. - 384 с.

3. Russel, J. Анализатор трафика [Текст]: справочник / J. Russel. – М.: Bookvika, 2012. – 108 с.