Содержание

Введение 2

1. Глава 1. VPN – Виртуальные частные сети 3

1.1 Как все начиналось 3

1.2 Что такое VPN 4

1.3 Принцип работы технологии VPN 4

1.4 Общее описание технологии VPN 5

1.5 Основы туннелирования 8

1.6 Протоколы 8

1.7 Достоинства VPN 11

1.8 Недостатки VPN 13

1.9 Перспективы VPN 14

2. Глава 2. Обзор технологии VPN 16

2.1 Оверлейная модель 16

2.2 Недостатки оверлейной модели 17

2.3 Одноранговая модель (Peer Model) 18

2.4 Преимущества одноранговой модели 20

2.5 Трудности реализации одноранговой модели 20

2.6 Варианты построения 21

3. Глава 3. Техноогия MPLS-VPN 24

3.1 Компоненты MPLS VPN 24

3.2 Путешествие пакета по сети MPLS VPN 27

3.3 Стандарты MPLS VPN 30

3.4 Терминология 31

3.5 Преимущества организации VPN на базе MPLS 32

3.6 Безопасность в сетях MPLS-VPN 33

Заключение 36

Список литературы 37

**ВВЕДЕНИЕ**

Cовременное развитие информационных технологий и, в частности, сети Internet, приводит к необходимости защиты информации, передаваемой в рамках распределенной корпоративной сети, использующей сети открытого доступа. При использовании своих собственных физических каналов доступа эта проблема так остро не стоит, так как в эту сеть не имеет доступа никто из посторонних. Однако стоимость таких каналов высока, поэтому не каждая компания позволит себе использовать их. В связи с этим Internet является наиболее доступным. Internet является незащищенной сетью, поэтому приходиться изобретать способы защиты конфиденциальных данных, передаваемых по незащищенной сети.

VPN - это технология, которая объединяет доверенные сети, узлы и пользователей через открытые сети, которым нет доверия". На мой взгляд, это наиболее яркий образ технологии, которая получает все большее распространение среди не только технических специалистов, но и среди рядовых пользователей, которым также требуется защищать свою информацию (например, пользователи Internet-банков или Internet-порталов).

Специалисты в области технологии VPN используют сугубо технические понятия, такие как "используемый алгоритм криптографического преобразования", "туннелирование", "сервер сертификатов" и т.д. Но для конечных пользователей эта терминология ничего не скажет. Скорее их интересует несколько иная интерпретация вопросов - сколько лет можно не беспокоиться за сохранность своей информации и насколько медленнее будет работать сеть, защищенная с помощью VPN-устройства.

ГЛАВА 1. VPN – Виртуальные частные сети

Любая организация, будь она производственной, торговой, финансовой компании или государственным учреждением, обязательно сталкивается с вопросом передачи информации между своими филиалами, а также с вопросом защиты этой информации. Не каждая фирма может себе позволить иметь собственные физические каналы доступа, и здесь помогает технология VPN, на основе которой и соединяются все подразделения и филиалы, что обеспечивает достаточную гибкость и одновременно высокую безопасность сети, а также существенную экономию затрат.

Виртуальная частная сеть (VPN - Virtual Private Network) создается на базе общедоступной сети Интернет. И если связь через Интернет имеет свои недостатки, главным из которых является то, что она подвержена потенциальным нарушениям защиты и конфиденциальности, то VPN могут гарантировать, что направляемый через Интернет трафик так же защищен, как и передача внутри локальной сети. В тоже время виртуальные сети обеспечивают существенную экономию затрат по сравнению с содержанием собственной сети глобального масштаба.

1.1 Как все начиналось

История появления VPN тесно связана с услугой Centrex в телефонных сетях. Понятие Centrex появилось на рубеже шестидесятых годов в США как общее название способа предоставления услуг деловой связи абонентам нескольких компаний на основе совместно используемого оборудования одной учрежденческой станции PBX (Private Branch Exchange). С началом внедрения в США и Канаде станций с программным управлением термин приобрел иной смысл и стал означать способ предоставления деловым абонентам дополнительных услуг телефонной связи, эквивалентных услугам PBX, на базе модифицированных станций сети общего пользования. Основное преимущество Centrex заключалось в том, что фирмы и компании при создании выделенных корпоративных сетей экономили значительные средства, необходимые на покупку, монтаж и эксплуатацию собственных станций. Хотя для связи между собой абоненты Centrex используют ресурсы и оборудование сети общего пользования, сами они образуют так называемые замкнутые группы пользователей CUG (Closed Users Group) с ограниченным доступом извне, для которых в станциях сети реализуются виртуальные PBX.

В стремлении преодолеть свойственные Centrex ограничения была выдвинута идея виртуальной частной сети VPN - как объединение CUG, составляющих одну корпоративную сеть и находящихся на удалении друг от друга

1.2 Что такое VPN

Что же такое VPN? Существует множество определений, однако главной отличительной чертой данной технологии является использование сети Internet в качестве магистрали для передачи корпоративного IP-трафика. Сети VPN предназначены для решения задач подключения конечного пользователя к удаленной сети и соединения нескольких локальных сетей. Структура VPN включает в себя каналы глобальной сети, защищенные протоколы и маршрутизаторы.

1.3 Принцип работы технологии VPN

VPN-устройство располагается между внутренней сетью и Интернет на каждом конце соединения. Когда данные передаются через VPN, они исчезают «с поверхности» в точке отправки и вновь появляются только в точке назначения. Этот процесс принято называть «туннелированием». Это означает создание логического туннеля в сети Интернет, который соединяет две крайние точки. Благодаря туннелированию частная информация становится невидимой для других пользователей Интернета. Прежде чем попасть в интернет-туннель, данные шифруются, что обеспечивает их дополнительную защиту. Протоколы шифрования бывают разные. Все зависит от того, какой протокол туннелирования поддерживается тем или иным VPN-решением. Еще одной важной характеристикой VPN-решений является диапазон поддерживаемых протоколов аутентификации. Большинство популярных продуктов работают со стандартами, основанными на использовании открытого ключа, такими как X.509. Это означает, что, усилив свою виртуальную частную сеть соответствующим протоколом аутентификации, вы сможете гарантировать, что доступ к вашим защищенным туннелям получат только известные вам люди.

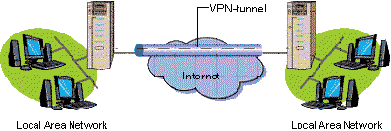


Рисунок 1. Принцип работы технологии VPN

1.4 Общее описание технологии VPN

Сегодня технология VPN (Virtual Private Network - виртуальная частная сеть) завоевала всеобщее признание и любой администратор считает своим долгом организовать VPN-каналы для сотрудников, работающих вне офиса (рисунок 2).

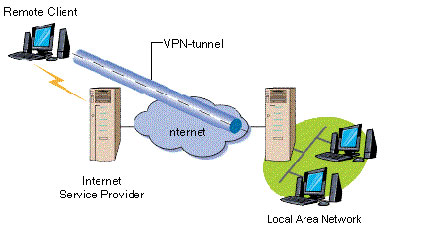


Рисунок 2. VPN для удаленных пользователей

VPN (рисунок 3) представляет собой объединение отдельных машин или локальных сетей в виртуальной сети, которая обеспечивает целостность и безопасность передаваемых данных. Она обладает свойствами выделенной частной сети и позволяет передавать данные между двумя компьютерами через промежуточную сеть (internetwork), например Internet.

VPN отличается рядом экономических преимуществ по сравнению с другими методами удаленного доступа. Во-первых, пользователи могут обращаться к корпоративной сети, не устанавливая c ней коммутируемое соединение, таким образом, отпадает надобность в использовании модемов. Во-вторых, можно обойтись без выделенных линий.

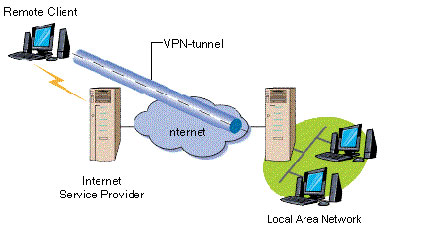


Рисунок 3. VPN для двух офисных сетей

Имея доступ в Интернет, любой пользователь может без проблем подключиться к сети офиса своей фирмы. Следует заметить, что общедоступность данных совсем не означает их незащищенность. Система безопасности VPN - это броня, которая защищает всю корпоративную информацию от несанкционированного доступа. Прежде всего, информация передается в зашифрованном виде. Прочитать полученные данные может лишь обладатель ключа к шифру. Наиболее часто используемым алгоритмом кодирования является Triple DES, который обеспечивает тройное шифрование (168 разрядов) с использованием трех разных ключей.

Подтверждение подлинности включает в себя проверку целостности данных и идентификацию пользователей, задействованных в VPN. Первая гарантирует, что данные дошли до адресата именно в том виде, в каком были посланы. Самые популярные алгоритмы проверки целостности данных - MD5 и SHA1. Далее система проверяет, не были ли изменены данные во время движения по сетям, по ошибке или злонамеренно. Таким образом, построение VPN предполагает создание защищенных от постороннего доступа туннелей между несколькими локальными сетями или удаленными пользователями.

Для построения VPN необходимо иметь на обоих концах линии связи программы шифрования исходящего и дешифрования входящего трафиков. Они могут работать как на специализированных аппаратных устройствах, так и на ПК с такими операционными системами как Windows, Linux или NetWare.

Управление доступом, аутентификация и шифрование - важнейшие элементы защищенного соединения.

1.5 Основы туннелирования

Туннелирование (tunneling), или инкапсуляция (encapsulation), - это способ передачи полезной информации через промежуточную сеть. Такой информацией могут быть кадры (или пакеты) другого протокола. При инкапсуляции кадр не передается в сгенерированном узлом-отправителем виде, а снабжается дополнительным заголовком, содержащим информацию о маршруте, позволяющую инкапсулированным пакетам проходить через промежуточную сеть (Internet). На конце туннеля кадры деинкапсулируются и передаются получателю.

Этот процесс (включающий инкапсуляцию и передачу пакетов) и есть туннелирование. Логический путь передвижения инкапсулированных пакетов в транзитной сети называется туннелем.

1.6 Протоколы

Протокол VPN определяет, каким образом система VPN взаимодействует с другими системами в интернете, а также уровень защищенности трафика. Если рассматриваемая организация использует VPN только для внутреннего информационного обмена, вопрос о взаимодействии можно оставить без внимания. Однако если организация использует VPN для соединения с другими организациями, собственные протоколы использовать, скорее всего, не удастся. В разговоре об алгоритме шифрования было упомянуто, что внешние окружающие факторы могут оказывать большее влияние на безопасность системы, чем алгоритм шифрования. Протокол VPN оказывает влияние на общий уровень безопасности системы. Причиной этому является тот факт, что протокол VPN используется для обмена ключами шифрования между двумя конечными узлами. Если этот обмен не защищен, злоумышленник может перехватить ключи и затем расшифровать трафик, сведя на нет все преимущества VPN.

Для того чтобы была возможность создания VPN на базе оборудования и программного обеспечения от различных производителей необходим некоторый стандартный механизм. Таким механизмом построения VPN является протокол Internet Protocol Security (IPSec). IPSec описывает все стандартные методы VPN. Этот протокол определяет методы идентификации при инициализации туннеля, методы шифрования, используемые конечными точками туннеля и механизмы обмена и управления ключами шифрования между этими точками. Из недостатков этого протокола можно отметить то, что он ориентирован на IP.

Другими протоколами построения VPN являются протоколы PPTP (Point-to-Point Tunneling Protocol), разработанный компаниями Ascend Communications и 3Com, L2F (Layer-2 Forwarding) - компании Cisco Systems и L2TP (Layer-2 Tunneling Protocol), объединивший оба вышеназванных протокола. Однако эти протоколы, в отличие от IPSec, не являются полнофункциональными (например, PPTP не определяет метод шифрования)

Говоря об IPSec, нельзя забывать о протоколе IKE (Internet Key Exchange), позволяющем обеспечить передачу информации по туннелю, исключая вмешательство извне. Этот протокол решает задачи безопасного управления и обмена криптографическими ключами между удаленными устройствами, в то время, как IPSec кодирует и подписывает пакеты. IKE автоматизирует процесс передачи ключей, используя механизм шифрования открытым ключом, для установления безопасного соединения. Помимо этого, IKE позволяет производить изменение ключа для уже установленного соединения, что значительно повышает конфиденциальность передаваемой информации.

Инкапсуляция - обеспечивает мультиплексирование нескольких транспортных протоколов по одному каналу;

Протокол LCP - PPP задает гибкий LCP для установки, настройки и проверки канала связи. LCP обеспечивает согласование формата инкапсуляции, размера пакета, параметры установки и разрыва соединения, а также параметры аутентификации. В качестве протоколов аутентификации могут использоваться PAP, CHAP и др.;

Протоколы управления сетью - предоставляют специфические конфигурационные параметры для соответствующих транспортных протоколов. Например, IPCP протокол управления IP.

Для формирования туннелей VPN используются протоколы PPTP, L2TP, IPsec, IP-IP.

Протокол PPTP - позволяет инкапсулировать IP-, IPX- и NetBEUI-трафик в заголовки IP для передачи по IP-сети, например Internet.

Протокол L2TP - позволяет шифровать и передавать IP-трафик с использованием любых протоколов, поддерживающих режим “точка-точка” доставки дейтаграмм. Например, к ним относятся протокол IP, ретрансляция кадров и асинхронный режим передачи (АТМ).

Протокол IPsec - позволяет шифровать и инкапсулировать полезную информацию протокола IP в заголовки IP для передачи по IP-сетям.

Протокол IP-IP - IP-дейтаграмма инкапсулируется с помощью дополнительного заголовка IP. Главное назначение IP-IP - туннелирование многоадресного трафика в частях сети, не поддерживающих многоадресную маршрутизацию.

Для технической реализации VPN, кроме стандартного сетевого оборудования, понадобится шлюз VPN, выполняющий все функции по формированию туннелей, защите информации, контролю трафика, а нередко и функции централизованного управления.

На сегодняшний день VPN - это экономичное, надежное и общедоступное решение организации удаленного доступа. Каким бы ни было расстояние, VPN обеспечит соединение с любой точкой мира и сохранность передачи самых важных данных.

1.7 Достоинства VPN

Виртуальные частные сети имеют несколько преимуществ над традиционными частными сетями. Главные из них - экономичность, гибкость и удобство использования.

Экономичность. С помощью VPN-сетей предприятиям удается хотя бы частично ограничить рост числа модемов, серверов доступа, коммутируемых линий и других технических средств, которые организации вынуждены внедрять, чтобы обеспечить удаленным пользователям доступ к своим корпоративным сетям. Кроме того, виртуальные частные сети дают возможность удаленным пользователям обращаться к сетевым ресурсам компании не по дорогим арендованным линиям, а через местную телефонную связь.

Особенно выгодны виртуальные частные сети в тех случаях, когда пользователи удалены на большие расстояния и поэтому арендованные линии обходятся очень дорого, а также когда таких пользователей много, в связи с чем и им требуется большое количество арендованных линий. Однако эти преимущества могут сойти на нет, если объем трафика в VPN-сети настолько велик, что система не успевает зашифровывать и расшифровывать пакеты данных. Чтобы избежать возникновения таких узких мест, предприятие вынуждено покупать дополнительное оборудование.

Кроме того, из-за относительной новизны технологии VPN и сложности используемых средств безопасности системный администратор для виртуальной сети обходится дороже, чем для традиционной.

Исследовательская компания Forrester Research опубликовала следующие данные, характеризующие преимущество применения VPN поверх Internet (из расчета 1000 пользователей) по сравнению с созданием центра удаленного доступа (Remote Access Service).

*Таблица 1*

Преимущество применения VPN поверх Internet

|  |  |  |
| --- | --- | --- |
| Статья затрат | Удаленный доступ (в млн. долл.) | VPN(в млн. долл.) |
| Оплата услуг провайдера связи | 1,08 | 0,54 |
| Расходы на эксплуатацию | 0,3 | 0,3 |
| Капиталовложения | 0,1 | 0,02 |
| Прочие расходы | 0,02 | 0,03 |
| Всего | 1,5 | 0,89 |

Из таблицы можно видеть, что использование VPN позволяет снизить многие статьи затрат, включая закупку коммуникационного оборудования, оплату услуг Internet-провайдера и т.д. Эти, а также другие исследования, позволили Международной Ассоциации Компьютерной Безопасности (International Computer Security Association, ICSA) причислить технологию VPN к десятке самых известных технологий, которые будут в первую очередь применяться многими компаниями. Это подтверждает и компания Gartner Group, которая в одном из своих отчетов предсказала, что средства построения VPN будут применяться в 2002 г. в 90% компаний. Именно с этим связан прогноз рынка средств VPN, который исчисляется 11,94 миллиардами долларов в 2002 году и 18,77 миллиардами в 2004 году (по данным Frost & Sullivan).

Гибкость и удобство. Эти достоинства виртуальных частных сетей объясняются тем, что в отличие от традиционных такие сети могут обеспечить удаленный доступ к ресурсам компании любому уполномоченному пользователю, имеющему связь с Internet. Благодаря этому VPN-сети позволяют партнерам легко получить доступ к сетевым ресурсам предприятия через Internet, что способствует укреплению альянсов и повышению конкурентоспособности. Этого трудно достичь с помощью традиционных частных сетей, так как предприятия, желающие совместно использовать сетевые ресурсы, часто имеют несовместимые системы. Особенно остро эта проблема возникает, когда большое число организаций, таких как крупное предприятие розничной торговли и его поставщики, хотят работать вместе через сеть.

1.8 Недостатки VPN

Проблемы защиты данных, недостаток надежности и производительности, а также отсутствие открытых стандартов затрудняют широкое распространение виртуальных частных сетей.

Защита. Для большинства технологий Internet вопросы обеспечения безопасности при передаче данных являются ключевыми. И виртуальные частные сети не исключение. Для них главные проблемы заключаются в аутентификации пользователей с помощью паролей и защите зашифрованного VPN-канала (тоннеля). Кроме того, сетевые администраторы должны тщательно выбирать методы, которые помогают пользователям получать доступ к виртуальным частным сетям.

Эти проблемы заставили некоторых потенциальных пользователей усомниться в том, что степень защиты данных будет удовлетворительной, если виртуальной частной сетью управляет провайдер услуг Internet. Чтобы успокоить недоверчивых пользователей, провайдеры поддерживают широкий набор различных схем шифрования и аутентификации. Например, фирма Aventail, выпускающая ПО для виртуальных частных сетей, предлагает пакет программ для аутентификации клиентов и шифрования на уровне сеанса. Компания VPNet Technologies поставляет оборудование, устанавливаемое между маршрутизатором и глобальной сетью, которое выполняет шифрование, аутентификацию и сжатие данных.

Большинство поставщиков используют методы шифрования с 56-разрядным ключом, соответствующие стандарту DES. По их мнению, такая длина ключа обеспечивает достаточно высокий уровень безопасности. Однако многие эксперты и аналитики полагают, что 56-разрядный ключ недостаточно надежен. Некоторые поставщики продуктов для виртуальных частных сетей предлагают шифрование со 112-разрядным ключом. Тем не менее следует помнить, что увеличение длины ключа снижает производительность, так как чем сложнее алгоритм шифрования, тем более интенсивной вычислительной обработки он требует.

1.9 Перспективы VPN

По мере своего развития VPN превратятся в системы взаимосвязанных сетей, которые будут соединять мобильных пользователей, торговых партнеров и поставщиков с критически важными корпоративными приложениями, работающими в протоколе IP. VPN станут фундаментом для новых коммерческих операций и услуг, которые будут стимулировать рынок и помогать модернизировать производство.

Вероятно, первым из основных компонентов завтрашних VPN станет сервер каталогов, содержащий профили конечных пользователей и данные о конфигурации сети. Это отдельная компьети, управляемая провайдером VPN. При наличии сетевых каталогов и обеспечении безопасности информации и качества обслуживания конечные пользователи смогут практически мгновенно устанавливать соединения по VPN.

Вполне возможно, что будет использоваться протокол IpV6, работы над которым активно продолжаются. Данный протокол обладает всеми возможностями взаимодействия с VPN, какие только могут пожелать сетевые разработчики, в частности, управление полосой пропускания, определение принадлежности IpV6-пакетов к конкретному потоку (например, высший приоритет будут получать пакеты мультимедийных данных для передачи в реальном времени).

Главные игроки сетевого рынка уже активно готовятся к грядущему буму VPN. Нынешние вендоры программного обеспечения и оборудования предлагают наборы устройств для создания и эксплуатации VPN.

Выгоду от развертывания VPN следующего поколения получат не только сетевые разработчики. Не менее заинтересованы в них и операторы. Фирмы AT&T Level 3 Communications, MCI Worldcom и Sprint создают высокоскоростные IP-каналы в АТМ-сетях для передачи видео, голоса и данных. VPN в настоящее время оказывают едва ли не решающее влияние на разработку стратегии глобальных операторов, в частности, Unisource (AT&T, Telia, PTT Suisse и PTT Netherlands), Concert (BT/MCI) и Global One (Deutsche Telekom, France Telekom). Чем больше компаний будут предлагать VPN-услуги, тем заметнее будет расти их качество и падать цены, что, в свою очередь, повлияет на число клиентов.

Каждая революция в бизнесе начиналась с изобретения, которое способствовало активизации частной инициативы. Например, разделение перевозчиков и компаний, эксплуатирующих государственную железную дорогу, привело к резкому росту коммерческих перевозок. То же самое происходит при создании VPN поверх национальных и международных телекоммуникационных инфраструктур. Ближайшее время покажет, к каким изменениям это приведет.

ГЛАВА 2. Обзор технологии VPN

Чтобы составить правильное представление о преимуществах сетей MPLS-VPN в плане масштабирования, нужно для начала рассмотреть различные модели VPN, доступные на современном рынке. Вначале мы рассмотрим ограничения, присущие оверлейной или наложенной модели, а затем посмотрим, какие преимущества по сравнению с ней дает одноранговая модель.

2.1 Оверлейная модель

Сервис-провайдер предоставляет корпоративному заказчику технологию соединений между его офисами и отделениями по частной WAN IP-сети. Для этого в каждой точке подключения нужно установить маршрутизатор и связать его по какому-либо IGP-протоко-лу маршрутизации по крайней мере с центральным маршрутизатором. В этом случае мы говорим, что сервис-провайдер предоставляет корпоративному заказчику частную сетевую магистраль (private network backbone).

Если транспортная сеть и магистральные коммутаторы действительно принадлежат корпорации, это значит, что она имеет настоящую частную сеть. Однако чаще всего транспортная сеть и по крайней мере часть магистральных коммутаторов принадлежат сервис-провайдеру и совместно используются несколькими корпоративными сетями. В этом случае мы говорим, что каждая из этих корпоративных сетей является не настоящей, а виртуальной частной сетью (VPN). В сети VPN с коммутацией каналов маршрутизаторы, которые находятся в разных отделениях компании, связываются между собой либо по выделенным, либо по коммутируемым линиям. В любом случае роль магистрали будет чаще всего выполнять телефонная сеть общего доступа. Сети Frame Relay и ATM основаны на технологии коммутации каналов. В этом случае маршрутизаторы, находящиеся в отделениях компании-заказчика, связываются между собой с помощью виртуальных каналов. Эти виртуальные каналы, подобно реальным, поддерживают соединения типа «точка—точка».

Корпоративные маршрутизаторы могут поддерживать соединения «точка—точка» и с помощью средств 1Р-тун-нелирования, например, IPSec или GRE. В таких частных или виртуальных частных сетях задачи дизайна и функционирования магистральной топологии решает сама корпорация или сервис-провайдер (если в сети предоставляются услуги по управлению). Маршрутизаторы, установленные в отделениях корпорации, связываются с соседними маршрутизаторами по каналам «точка—точка». Обмен данными о маршрутизации происходит напрямую по этим каналам.

С точки зрения магистральной сети сервис-провайдера, передаваемая маршрутная информация представляет собой обычные данные, которые обрабатываются «прозрачно», то есть так же, как и все остальные. Со своей стороны, корпоративные маршрутизаторы не имеют ни знаний, ни средств контроля над маршрутизирующими функциями магистрали. Этот домен относится к сфере, за которую отвечает сервис-провайдер.

Мы говорим, что в этом случае корпоративная IP-сеть является оверлейной, то есть «накладывается» поверх провайдерской магистрали. При этом корпоративную сеть можно рассматривать как сеть более высокого уровня, а магистраль — как сеть более низкого уровня. Обе сети существуют независимо друг от друга. Такой способ построения сети более высокого уровня поверх сети более низкого уровня называется оверлейной моделью.

2.2 Недостатки оверлейной модели

Чтобы добиться оптимальной маршрутизации в корпоративной сети, надстроенной поверх магистрали, корпоративная сеть должна иметь узловую структуру (meshed network). Это означает, что в каждом отделении корпорации должен устанавливаться маршрутизатор, соединенный с соседними маршрутизаторами, находящимися в других отделениях.

Если корпоративная сеть будет хотя бы частично отклоняться от узловой топологии (meshed), то возникнут случаи, когда трафик будет передаваться от одного корпоративного маршрутизатора в магистраль провайдера, затем поступать на корпоративный магистральный (центральный) маршрутизатор, затем передаваться обратно в провайдерскую магистраль и лишь затем поступать на оконечный (удаленный) маршрутизатор в пункте назначения. Поскольку удаленные маршрутизаторы подключаются к общей магистрали (магистрали сервис-провайдера), вариант, при котором трафик покидает магистраль, проходит через второй маршрутизатор и снова попадает в магистраль, нельзя признать эффективным.

Если сеть имеет полносвязную структуру (fully meshed), вышеуказанная ситуация не встречается, однако возникают другие проблемы. Корпорация должна платить за виртуальные каналы (а провайдер должен подкреплять их соответствующими сетевыми ресурсами), но при увеличении количества корпоративных отделений количество каналов возрастает в геометрической прогрессии. Помимо высокой стоимости проблема усугубляется тем, что алгоритмы IP-маршрутизации плохо масштабируются в случае наращивания количества прямых связей между маршрутизаторами.

2.3 Одноранговая модель (Peer Model)

Для того, чтобы пользоваться услугами VPN, предприятию совсем не нужно проектировать и эксплуатировать собственную магистральную сеть. Сервис-провайдер, который уже имеет магистральную сетевую инфраструктуру, вполне может взять эту задачу на себя. Одноранговая модель VPN требует только подключения маршрутизатора заказчика к одному из маршрутизаторов сервис-провайдера.

В одноранговой VPN два маршрутизатора С считаются одноранговыми только в том случае, когда они находятся на одном сайте. Поэтому принадлежащий заказчику маршрутизатор С1 не имеет одноранговых (соседских) отношений с маршрутизатором С2, который принадлежит тому же заказчику, но установлен на другом сайте (в другом месте). Получается, что на каждом сайте заказчика имеется по крайней мере один корпоративный маршрутизатор (СЕ), связанный одноранговыми отношениями по крайней мере с одним маршрутизатором сервис-провайдера (РЕ).

СЕ-маршрутизаторы не обмениваются друг с другом данными о маршрутах. Нет вообще никакой необходимости в обмене какими-либо данными между СЕ-маршрути-заторами. Данные передаются от входящего СЕ-маршру-тизатора через входящий РЕ-маршрутизатор сервис-провайдера и проходят через один или несколько магистральных Р-маршрутизаторов. В итоге они достигают исходящего РЕ-маршрутизатора сервис-провайдера и попадают на исходящий корпоративный СЕ-маршрутизатор.Таким образом маршрутизация становится оптимальной.

Поскольку СЕ-маршрутизаторы не обмениваются друг с другом данными о маршрутах, корпорации не нужно иметь свою магистраль или управлять ею. Разумеется, корпоративный заказчик может пользоваться IP-магистралью так, как будто у него имеется сеть Frame Relay, и создавать своего рода «виртуальные каналы» между СЕ-маршрутизаторами. Обычно для этого используется одна из форм IP-туннелирования. Однако это приводит нас обратно к оверлейной модели со всеми ее проблемами. Одноранговая модель таких проблем не имеет.

2.4 Преимущества одноранговой модели

Одноранговая модель имеет целый ряд преимуществ:

1) В одноранговой модели количество работы, которую должен выполнить сервис-провайдер для технического обеспечения и управления VPN, прямо пропорционально количеству сайтов заказчика, подключенных к VPN. В оверлейной модели количество этой работы пропорционально квадрату сайтов заказчика, подключенных к VPN.

2) Одноранговая модель поддерживает оптимальную маршрутизацию пользовательского трафика по магистрали сервис-провайдера, так как в этой модели нет необходимости в транзитных СЕ-устройствах. Корпоративному заказчику не нужно управлять собственной магистралью. Ему нужно только подключить СЕ-маршрутизатор на каждом сайте.

Таким образом, одноранговая модель выгодна и сервис-провайдеру, и заказчику. Для провайдера она означает сокращение объема работ, а для корпоративного заказчика — более ценные услуги.

2.5 Трудности реализации одноранговой модели

Хотя одноранговая модель имеет множество преимуществ по сравнению с оверлейной, на пути ее реализации также стоит ряд проблем, которые перечислены ниже:

1) Перегрузка Р-маршрутизаторов информацией о маршрутах. Одной из основных проблем крупных IP-магистралей является большое количество ресурсов (памяти, процессорных мощностей, полосы пропускания), необходимых для хранения данных о маршрутизации. Если взять IP-магистраль и пустить по ней данные о маршрутах всех корпоративных сетей, Р-маршрутизаторы никогда с ней не справятся.

2) Несогласованные (несмежные) адресные пространства. Обычно Интернет-сервис-провайдеры (ISP) стараются присваивать адреса осмысленно. Это значит, что адрес системы должен указывать на место, в котором эта система подключается к сети ISP. Однако многие корпоративные сети имеют адресные схемы, которые трудно совместить с магистральной топологией любого сервис-провайдера. В этих схемах адреса сайтов распределяются без какого-либо учета точки, в которой осуществляется подключение к провайдерской сети. Это сокращает возможности агрегации маршрутов и увеличивает объем данных о маршрутах, которые передаются по Р-сети.

3) Частная адресация в С-сетях. Адреса во многих корпоративных сетях не являются уникальными. Это значит, что тот или иной адрес является уникальным только в пределах одного предприятия, но теряет уникальность при связи между предприятиями. Если IP-магистраль сервис-провайдера используется как общая магистраль для двух разных корпоративных сетей и если адреса в этих сетях не являются уникальными, Р-маршрутизаторы не смогут гарантировать доставку пакетов по месту назначения.

4) Подслушивание. Для защиты данных нужно устанавливать шифрованные туннели «точка—точка» между каждой парой СЕ-маршрутизаторов (модель IPSec). Это решение хорошо подходит для оверлейной модели, полькольку она и без того использует туннель «точка—точка» между парами «соседних» СЕ-маршрутизаторов. Для одноранговой модели это решение подходит не столь хорошо, потому что здесь СЕ-маршрутизатор никогда не может определить, куда он будет передавать следующий пакет.

2.6 Варианты построения

Можно выделить четыре основных варианта построения сети VPN, которые используются во всем мире. Данная классификация предлагается компанией Check Point Software Technologies, которая не без основания считается законодателем моды в области VPN. Так, например, по данным независимых консалтинговых и аналитических агентств компания Check Point захватила 52% мирового рынка VPN-решений (по данным Dataquest).

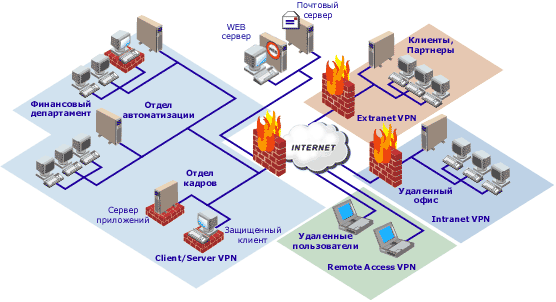
Вариант "Intranet VPN", который позволяет объединить в единую защищенную сеть несколько распределенных филиалов одной организации, взаимодействующих по открытым каналам связи. Именно этот вариант получил широкое распространение во всем мире, и именно его в первую очередь реализуют компании-разработчики.

Вариант "Remote Access VPN", который позволяет реализовать защищенное взаимодействие между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который подключается к корпоративным ресурсам из дома (домашний пользователь) или через notebook (мобильный пользователь). Данный вариант отличается от первого тем, что удаленный пользователь, как правило, не имеет статического адреса, и он подключается к защищаемому ресурсу не через выделенное устройство VPN, а прямиком со своего собственного компьютера, на котором и устанавливается программное обеспечение, реализующее функции VPN. Компонент VPN для удаленного пользователя может быть выполнен как в программном, так и в программно-аппаратном виде. В первом случае программное обеспечение может быть как встроенным в операционную систему (например, в Windows 2000), так и разработанным специально (например, АП "Континент-К"). Во втором случае для реализации VPN используются небольшие устройства класса SOHO (Small Office\Home Office), которые не требуют серьезной настройки и могут быть использованы даже неквалифицированным персоналом. Такие устройства получают сейчас широкое распространение за рубежом.

Вариант "Client/Server VPN", который обеспечивает защиту передаваемых данных между двумя узлами (не сетями) корпоративной сети. Особенность данного варианта в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например, между рабочей станцией и сервером. Такая необходимость очень часто возникает в тех случаях, когда в одной физической сети необходимо создать несколько логических сетей. Например, когда надо разделить трафик между финансовым департаментом и отделом кадров, обращающихся к серверам, находящимся в одном физическом сегменте.

Последний вариант "Extranet VPN" (Рисунок 4) предназначен для тех сетей, к которым подключаются пользователи "со стороны" (партнеры, заказчики, клиенты и т.д.), уровень доверия к которым намного ниже, чем к своим сотрудникам. Хотя по статистике чаще всего именно сотрудники являются причиной компьютерных преступлений и злоупотреблений.

Рисунок 4. Последний вариант "Extranet VPN"



ГЛАВА 3. ТЕХНОЛОГИЯ MPLS-VPN

Виртуальные частные сети на основе MPLS (MPLS VPN) привлекают сегодня всеобщее внимание. Количество ведущих провайдеров услуг, предлагающих своим клиентам воспользоваться новым видом сервиса для экономичного построения сетей Intranet и Extranet, постоянно растет, делая MPLS VPN доступными для пользователей все большего числа стран и регионов. От других способов построения виртуальных частных сетей, подобно VPN на базе ATM/FR или IPSec, MPLS VPN выгодно отличает высокая масштабируемость, возможность автоматического конфигурирования и естественная интеграция с другими сервисами IP, которые сегодня входят в обязательное меню любого успешного провайдера: доступом к Internet, Web и почтовыми службами, хостингом.

3.1 Компоненты MPLS VPN

Прежде всего, сеть MPLS VPN делится на две области: сети IP клиентов и внутренняя (магистральная) сеть MPLS провайдера, которая необходима для объединения сетей клиентов (см. Рисунок 5).

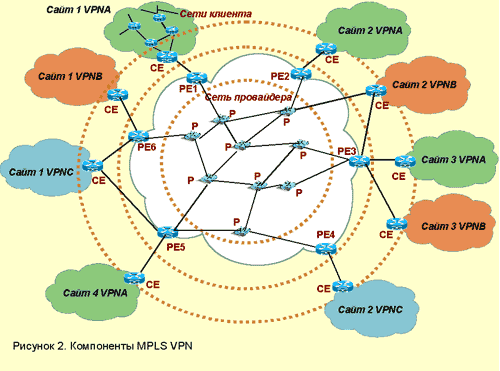


Рисунок 5. Компоненты MPLS VPN

В общем случае у каждого клиента может быть несколько территориально обособленных сетей IP, каждая из которых в свою очередь может включать несколько подсетей, связанных маршрутизаторами. Такие территориально изолированные сетевые «островки» корпоративной сети принято называть сайтами. Принадлежащие одному клиенту сайты обмениваются пакетами IP через сеть провайдера и образуют виртуальную частную сеть этого клиента. Например, о корпоративной сети, в которой сеть центрального отделения связывается с тремя удаленными филиалами, можно сказать, что она состоит из четырех сайтов. Для обмена маршрутной информацией в пределах сайта узлы пользуются одним из внутренних протоколов маршрутизации (Interior Gateway Protocol, IGP), область действия которого ограничена автономной системой: RIP, OSPF или IS-IS.

Маршрутизатор, с помощью которого сайт клиента подключается к магистрали провайдера, называется пограничным маршрутизатором клиента (Customer Edge router, CE). Будучи компонентом сети клиента, CE ничего не знает о существовании VPN. Он может быть соединен с магистральной сетью провайдера несколькими каналами.

Магистральная сеть провайдера является сетью MPLS, где пакеты IP продвигаются на основе не IP-адресов, а локальных меток (более подробно о технологиях этого типа можно прочитать в статье Н. Олифер «Пути-дороги через сеть» в данном номере). Сеть MPLS состоит из маршрутизаторов с коммутацией меток (Label Switch Router, LSR), которые направляют трафик по предварительно проложенным путям с коммутацией меток (Label Switching Path, LSP) в соответствии со значениями меток. Устройство LSR — это своеобразный гибрид маршрутизатора IP и коммутатора, при этом от маршрутизатора IP берется способность определять топологию сети с помощью протоколов маршрутизации и выбирать рациональные пути следования трафика, а от коммутатора — техника продвижения пакетов с использованием меток и локальных таблиц коммутации. Устройства LSR для краткости часто называют просто маршрутизаторами, и в этом есть свой резон — они с таким же успехом способны продвигать пакеты на основе IP-адреса, если поддержка MPLS отключена.

В сети провайдера среди устройств LSR выделяют пограничные маршрутизаторы (Provider Edge router, PE), к которым через маршрутизаторы CE подключаются сайты клиентов и внутренние маршрутизаторы магистральной сети провайдера (Provider router, P). Маршрутизаторы CE и PE обычно связаны непосредственно физическим каналом, на котором работает какой-либо протокол канального уровня — например, PPP, FR, ATM или Ethernet. Общение между CE и PE идет на основе стандартных протоколов стека TCP/ IP, поддержка MPLS нужна только для внутренних интерфейсов PE (и всех интерфейсов P). Иногда полезно различать относительно направления продвижения трафика входной PE и выходной (удаленный) PE.

В магистральной сети провайдера только пограничные маршрутизаторы PE должны быть сконфигурированы для поддержки виртуальных частных сетей, поэтому только они «знают» о существующих VPN. Если рассматривать сеть с позиций VPN, то маршрутизаторы провайдера P непосредственно не взаимодействуют с маршрутизаторами заказчика CE, а просто располагаются вдоль туннеля между входным и выходным маршрутизаторами PE.

Маршрутизаторы PE являются функционально более сложными, чем P. На них возлагаются главные задачи по поддержке VPN, а именно разграничение маршрутов и данных, поступающих от разных клиентов. Маршрутизаторы PE служат также оконечными точками путей LSP между сайтами заказчиков, и именно PE назначает метку пакету IP для его транзита через внутреннюю сеть маршрутизаторов P.

Пути LSP могут быть проложены двумя способами: либо с применением технологии ускоренной маршрутизации (IGP) с помощью протоколов LDP, либо на основе технологии Traffic Engineering с помощью протоколов RSVP или CR-LDP. Прокладка LSP означает создание таблиц коммутации меток на всех маршрутизаторах PE и P, образующих данный LSP

В совокупности эти таблицы задают множество путей для разных видов трафика клиентов. В VPN применяется различная топология связей: полносвязная, «звезда» (часто называемая в англоязычной литературе hub-and-spoke) или ячеистая.

3.2 Путешествие пакета по сети MPLS VPN

Теперь, когда мы обсудили схему распространения маршрутной информации по сети MPLS VPN, давайте посмотрим, как перемещаются данные между узлами одной VPN.

Пусть, например, из сайта 1 в VPN A узел с адресом 10.2.1.1/16 отправляет пакет узлу сайта 2 этой же VPN, имеющему адрес 10.1.0.3/16 (см. Рисунок 6).

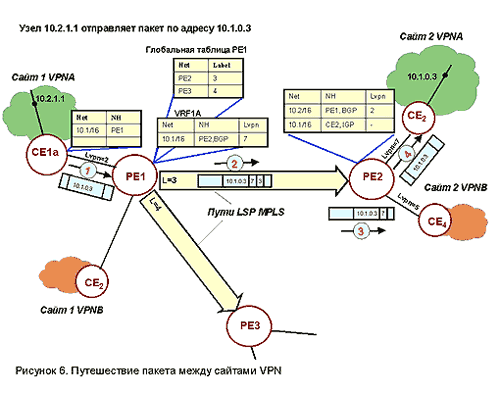


Рисунок 6. Путешествие пакета между сайтами VPN

Стандартными транспортными средствами IP пакет доставляется на пограничный маршрутизатор сайта CE1A, в таблице которого для номера сети 10.1.0.0 в качестве следующего маршрутизатора указан PE1. На маршрутизатор PE1 пакет поступает с интерфейса int2, поэтому для выбора дальнейшего продвижения пакета он обращается к таблице VRF1а, связанной с данным интерфейсом.

В таблице VRF1A адресу 10.1.0.0 соответствует запись протокола BGP, которая указывает, что очередным маршрутизатором для пакета определен PE2. Следующее поле записи содержит значение метки Lvpn=7, определяющей интерфейс выходного маршрутизатора PE, которое должно быть присвоено пакету для того, чтобы он попал в нужную VPN. Здесь также указывается, что запись была сделана протоколом BGP, а не IGP. На этом основании маршрутизатор PE «понимает», что очередной маршрутизатор не является непосредственным соседом, и путь к нему надо искать в глобальной таблице маршрутизации.

В глобальной таблице для адреса PE2 указывается начальное значение метки L пути LSP, равное 3. Способ его прокладки между маршрутизаторами PE1 и PE2 не имеет в данном случае принципиального значения — главное, чтобы такой путь существовал.

Технология MPLS VPN использует иерархические свойства путей MPLS, за счет чего пакет может быть снабжен несколькими метками, помещаемыми в стек. На входе во внутреннюю сеть провайдера, образуемую маршрутизаторами P, пакет будет снабжен двумя метками — внутренней Lvpn=7 и внешней L=3. Метка Lvpn интерпретируется как метка нижнего уровня — оставаясь на дне стека, она не используется, пока пакет путешествует по туннелю PE1-PE2. Продвижение пакета происходит на основании метки верхнего уровня, роль которой отводится метке L. Каждый раз, когда пакет проходит очередной маршрутизатор P вдоль туннеля, метка L анализируется и заменяется новым значением. И только после достижения конечной точки туннеля маршрутизатора PE2 из стека извлекается метка Lvpn. В зависимости от ее значения пакет направляется на тот или иной выходной интерфейс маршрутизатора PE2.

Из таблицы VRF2А, связанной с данным интерфейсом и содержащей маршруты VPNA, извлекается запись о маршруте к узлу назначения, указывающая на CE2 в качестве следующего маршрутизатора. Заметим, что она была помещена в таблицу VRF2a протоколом IGP. Последний отрезок путешествия пакета от CE2 до узла 10.1.0.3 осуществляется традиционными средствами IP.

Несмотря на достаточно громоздкое описание механизмов MPLS VPN, процесс конфигурирования новой VPN или модификации существующей достаточно прост, поэтому он хорошо формализуется и автоматизируется. Для исключения возможных ошибок конфигурирования — например, приписывания сайту ошибочной политики импорта/экспорта маршрутных объявлений, что может привести к присоединению сайта к чужой VPN, — некоторые производители разработали автоматизированные программные системы конфигурирования MPLS. Примером может служить Cisco VPN Solution Center, который снабжает администратора средствами графического интерфейса для формирования состава каждой VPN, а затем переносит полученные конфигурационные данные в маршрутизаторы PE.

Повысить степень защищенности MPLS VPN можно с помощью традиционных средств: например, применяя средства аутентификации и шифрования IPSec, устанавливаемые в сетях клиентов или в сети провайдера. Услуга MPLS VPN может легко интегрироваться с другими услугами IP, например, c предоставлением доступа к Internet для пользователей VPN с защитой их сети средствами межсетевого экрана, установленного в сети провайдера. Провайдер также может предоставлять пользователям MPLS VPN услуги, базирующиеся на других возможностях MPLS: в частности, услуги c предоставлением гарантированного качества обслуживания на основе методов MPLS Traffic Engineering. Что же касается сложностей ведения в маршрутизаторах провайдера таблиц маршрутизации пользователей, на которые указывают некоторые аналитики, то они, на наш взгляд, несколько преувеличены, так как таблицы создаются автоматически, с помощью стандартных протоколов маршрутизации, и только на пограничных маршрутизаторах PE. Механизм виртуального маршрутизатора полностью изолирует эти таблицы от глобальных таблиц маршрутизации провайдера, что обеспечивает необходимые уровни надежности и масштабируемости решений MPLS VPN. Впрочем, реальное качество данной технологии покажет время и, скорее всего, достаточно скоро.

3.3 Стандарты MPLS VPN

Что больше всего сбивает с толку в ситуации с MPLS VPN, так это отсутствие четко определенных и полностью готовых для реализации стандартов. И это притом, что всего существует более 50 стандартов и проектов стандартов MPLS.

Хотя технология MPLS VPN описана в рамках общих стандартов на MPLS, в организации IETF существуют специальные рабочие группы, занимающиеся проработкой отдельных вопросов MPLS VPN. Например, рабочая группа PPVPN (Provider Provisioned Virtual Private Network) занята созданием “каркаса” VPN с улучшенными механизмами безопасности, масштабируемости и управляемости.

Три основных типа VPN, над которыми работает группа PPVPN, — это MPLS BGP VPN, MPLS Virtual Routers и MPLS Layer 2 VPN. Группа координирует свою деятельность с другой рабочей группой — PWE3 (Pseudo Wire Emulation Edge to Edge), создающей стандарты для туннельных сквозных соединений через сети ATM и MPLS на первом и втором уровнях.

Виртуальные частные сети второго уровня (Layer 2 VPN) также определены в проекте, получивший название Martini, этот проект находится на рассмотрении рабочей группы IETF PWE3. Идея заключается в организации туннелей для трафика Ethernet, Frame Relay, ATM и PPP через сеть MPLS. Группа PWE3 работает и над другими похожими предложениями, но со стороны сервис-провайдеров наибольший интерес вызвал проект Martini.

3.4 Терминология

Каналы MPLS можно назвать VPN”. Это так. Но термин VPN здесь используется несколько в ином значении. Классическая технология VPN обеспечивает передачу информации по зашифрованным туннелям поверх протокола третьего (сетевого) уровня. Шифрование делает невозможным чтение посторонними адреса и содержимого передаваемого пакета. Зашифрованная информация передается по сети и расшифровывается узлом-получателем.

MPLS VPN — это тоже частные виртуальные каналы, подобно IPsec или PPTP (Point-to-Point Tunneling Protocol) VPN, но на этом вся их схожесть и заканчивается. В MPLS VPN нет никакого шифрования. Пакеты “прячутся” от посторонних глаз, поскольку передаются по маршруту меток MPLS. Трафик с определенными метками читают только маршрутизаторы LSR (Label Switch Routers), находящиеся на маркированном маршруте. Обычные способы IP-маршрутизации в сети MPLS не применяются — трафик передается только вдоль траекторий меток. Подобный уровень безопасности обеспечивается и в сетях АТМ и Frame Relay, где информация “путешествует” по виртуальным каналам тоже в незашифрованном виде. Но, собственно говоря, никто не запрещает вам дополнительно шифровать пакеты MPLS

3.5 Преимущества организации VPN на базе MPLS

Основными преимуществами организации VPN на базе MPLS можно назвать:

* масштабируемость;
* возможность пересечения адресных пространств, узлов подключенных в различные VPN;
* изолирование трафика VPN друг от друга на втором уровне модели OSI.

Масштабируемость достигается за счет того, что подключение нового узла в существующий VPN производиться только перенастройкой одного PE, к которому подключается данный узел.

В различных VPN адресные пространства могут пересекаться, что может быть чрезвычайно полезным, в случае если оператору необходимо предоставить VPN нескольким клиентам, использующим одинаковое приватное адресное пространство, например адреса 10.0.0.0/8.

Устройства P (LSR) при коммутации анализируют только внешнюю метку, определяющую LSP между PE, и не анализируют заголовок IP пакета, то справедливо говорить о том, что P устройства выполняют функции коммутации на втором уровне модели OSI. Устройства PE так же разделяют маршрутную информацию, таблицы маршрутизации, интерфейсы, направленные в сторону устройств CE, между VRF. Тем самым процессы маршрутизации разных VPN полностью разделяются, и обеспечивается разделение трафика от разных VPN на втором уровне модели OSI. На этот предмет компания Miercom провела исследование, и показала, что технология MPLS/VPN в реализации компании Cisco Systems обеспечивает такой же уровень безопасности как сети Frame Relay и ATM.

3.6 Безопасность в сетях MPLS-VPN

Функциональность MPLS-VPN поддерживает уровень безопасности, эквивалентный безопасности оверлейных виртуальных каналов в сетях Frame Relay и ATM. Безопасность в сетях MPLS-VPN поддерживается с помощью сочетания протокола BGP и системы разрешения IP-адресов.

BGP-протокол отвечает за распространение информации о маршрутах. Он определяет, кто и с кем может связываться с помощью многопротокольных расширений и атрибутов community. Членство в VPN зависит от логических портов, которые объединяются в сеть VPN и которым BGP присваивает уникальный параметр Route Distinguisher (RD). Параметры RD неизвестны конечным пользователям, и поэтому они не могут получить доступ к этой сети через другой порт и перехватить чужой поток данных. В состав VPN входят только определенные назначенные порты. В сети VPN с функциями MPLS протокол BGP распространяет таблицы FIB (Forwarding Information Base) с информацией о VPN только участникам данной VPN, обеспечивая таким образом безопасность передачи данных с помощью логического разделения трафика.

Именно провайдер, а не заказчик присваивает порты определенной VPN во время ее формирования. В сети провайдера каждый пакет ассоциирован с RD, и поэтому попытки перехвата пакета или потока трафика не могут привести к прорыву хакера в VPN. Пользователи могут работать в сети интранет или экстранет, только если они связаны с нужным физическим или логическим портом и имеют нужный параметр RD. Эта схема придает сетям Cisco MPLS-VPN очень высокий уровень защищенности.

В опорной сети информация о маршрутах передается с помощью стандартного протокола Interior Gateway Protocol (IGP), такого как OSPP или IS-IS. Пограничные устройства РЕ в сети провайдера устанавливают между собой связи-пути, используя LDP для назначения меток. Назначения меток для внешних (пользовательских) маршрутов распространяется между РЕ-маршрутизаторами не через LDP, а через многопротокольные расширения BGP. Атрибут Community BGP ограничивает рамки информации о доступности сетей и позволяет поддерживать очень крупные сети, не перегружая их информацией об изменениях маршрутной информации. BGP не обновляет информацию на всех периферийных устройствах РЕ, находящихся в провайдерской сети, а приводит в соответствие таблицы PIB только тех РЕ, которые принадлежат к конкретной VPN.

Если виртуальные каналы создаются при оверлейной модели, исходящий интерфейс любого индивидуального пакета данных является функцией только входящего интерфейса. Это означает, что IP-адрес пакета не определяет маршрута его передачи по магистральной сети. Это позволяет предотвратить попадание несанкционированного трафика в сеть VPN и передачу несанкционированного трафика из нее.

В сетях MPLS-VPN пакет, поступающий в магистраль, в первую очередь ассоциируется с конкретной сетью VPN на основании того, по какому интерфейсу (подин-терфейсу) пакет поступил на РЕ-маршрутизатор. Затем IP-адрес пакета сверяется с таблицей передачи (forwarding table) данной VPN. Указанные в таблице маршруты относятся только к VPN принятого пакета. Таким образом, входящий интерфейс определяет набор возможных исходящих интерфейсов. Эта процедура также предотвращает как попадание несанкционированного трафика в сеть VPN, так и передачу несанкционированного трафика из нее.

Заключение

Идея построения собственных виртуальных сетей актуальна в том случае, когда объединять несколько локальных сетей в различных зданиях или организациях для создания собственной сети дорого или слишком долго, однако необходимо обеспечить защиту передаваемых между сегментами сети данных. Ведь далеко не всегда позволительно передавать данные по общедоступным сетям в открытом виде. Впрочем, можно защищать только связи между отдельными компьютерами из различных сегментов, но если корпоративная политика требует обеспечить безопасность большей части информации, то защищать каждый отдельный канал и компьютер становится достаточно сложно. Проблема в том, что у пользователя, как правило, нет достаточной квалификации для поддержания средств защиты информации, а администратор не может эффективно контролировать все компьютеры во всех сегментах организации.

Кроме того, при защите отдельных каналов инфраструктура корпоративной сети остается прозрачной для внешнего наблюдателя. Для решения этих и некоторых других проблем применяется архитектура VPN, при использовании которой весь поток информации, передаваемый по общедоступным сетям, шифруется с помощью так называемых "канальных шифраторов".

Построение VPN позволяет защитить виртуальную корпоративную сеть так же надежно, как и собственную сеть (а иногда даже и лучше). Данная технология сейчас бурно развивается, и в этой области уже предлагаются достаточно надежные решения. Как правило, технология VPN объединяется с межсетевыми экранами (firewall). Собственно, все основные межсетевые экраны дают возможность создания на их базе виртуальной корпоративной сети.

список литературы

Построение виртуальных частных сетей на базе технологии MPLS Автор: Михаил Захватов Издательство: Cisco Systems

Компьютерные сети принципы, технологии, протоколы 3-е издание Авторы: Наталья Олифер (обозреватель «Журнала сетевых решений/LAN».); Виктор Олифер (главный специалист Корпорации ЮНИ.)

http://athena.vvsu.ru/docs/tcpip/mpls/ - Введение в архитектуру MPLS

http://system-administrators.info/?p=1179 - MPLS на службе VPN

http://www.connect.ru/article.asp?id=5343 - Журнал Connect: технология VPN