VPN: Основные понятия и технологии.
MPLS на службе VPN.

Студент группы 111
Бикбов Евгений

Оглавление.

VPN

Введение.

VPN (Virtual Private Network) – это частная сеть, которая использует общественную сеть (чаще всего интернет) для соединения сетей или пользователей.

Исторически частные глобальные сети с использованием выделенных линий. Такое решение является весьма дорогостоящим. Кроме этого в таких системах не возможно разделить недоиспользованную полосу пропускания с другими заказчиками, и наоборот, трудно динамически изменять имеющуюся пропускную способность канала между двумя сайтами (удаленные локальные сети), чтобы удовлетворять кратковременные запросы на пиковую скорость передачи данных.

Большинство подобных проблем решается при помощи VPN. Конфиденциальность в VPN достигается с помощью шифрования. Данные передаются по публичной сети при помощи организации туннеля. Технологии VPN постоянно совершенствуются, становятся надежнее и безопасней, привлекая все большее внимание корпораций.

Типы VPN

VPN можно подразделить на три типа:

* **trusted**
* **secured**
* **hybrid**

В VPN типа trusted производится разделение потоков данных разных клиентов. Надо отметить, что в этом типе VPN не производится шифрование данных. Даже если каналы разных клиентов могут проходить через одно и тоже сетевое оборудование, но провайдер гарантировал, что клиенты не будут иметь доступ к сетям друг друга. Так же клиенты могли применять свою политику безопасности и сами настраивать IP адреса.

В VPN сетях класса secured применялось кодирование данных. Злоумышленник мог удалить пакет, но не мог прочитать или изменить. Так как изменение пакета можно легко проверить.

В VPN сетях типа hybrid используется как разделение потоков данных разных клиентов, так и шифрование данных.

В этой статье я рассмотрю некоторые технологии, применяемые для создания VPN.

MPLS VPN

Введение.

MPLS VPN привлекают сегодня всеобщее внимание. Все больше провайдеров по всему миру применят технологию MPLS для организации VPN. От других способов построения VPN, MPLS VPN выгодно отличает высокая масштабируемость, возможность автоматического конфигурирования и естественная интеграция с другими сервисами IP.

Теперь по подробней рассмотрим протокол MPLS в его применение при построении сетей VPN.

Протокол MPLS

MPLS (Multiprotocol Label Switching) – это технология быстрой коммутации пакетов в много протокольных сетях, основанная на использовании меток.

Метка передается в месте с пакетом данных. Конкретное положение этой метки в пакете зависит от протокола канального уровня, который используется в данной сети. Поэтому область применения этой технологии не ограничивается IP сетями.

Каждому классу сетевого уровня ставится в соответствие некоторая метка. И в основе технологии MPLS лежит принцип обмена метками, причем метки уникальны только между соседними узлами сети.

Эти узлы так же называются маршрутизаторами, коммутирующими по меткам. Информацию о топологии сети маршрутизаторы получают при помощи различных протоколов маршрутизации.

Архитектура MPLS позволяет передавать в месте с пакетом не одну метку, а стек меток. Маршрутизация производится только по верхней метке. Используя этот механизм легко создавать иерархию потоков в MPLS сети, и производить туннельную передачи пакетов.

Стек может хранить произвольное число элементов размера 32 бит. Под метку отводится 20 бит, 8 бит занимает время жизни пакета, 1 бит используется на обозначение «дна» стека и 3 бита не используются.

Каждый маршрутизатор составляет таблицу, по которой он производит маршрутизацию пакетов. Паре входной интерфейс и метка он ставит в соответствие префикс адреса получателя, выходной интерфейс и выходная метка.

Из преимуществ MPLS можно перечислить:

*Более быстрая коммутация.
*Поддержка VPN и QoS .
*В одну сеть можно объединить сети с различными протоколами канального уровня, что для провайдеров не мало важно.

Типичное устройство сети провайдера с использованием технологии MPLS.

Сеть MPLS VPN делится на две части. Первая – это сети IP клиентов, вторая – внутренняя сеть провайдера, где непосредственно и реализуется MPLS сеть.

Клиентская сеть может иметь произвольную структуру. Она может состоять из нескольких подсетей. Это может быть корпоративная сеть или муниципальная сеть или просто физическое лицо, которое подключается по модему. Чаще всего клиент соединяются физическим каналом, на котором работает какой-нибудь протокол канального уровня: PPP, FR, ATM **и** Ethernet.

Рассмотрим для примера клиентскую корпоративную сеть, которая состоит из нескольких изолированных IP сетей. Такие изолированные сети принято называть сайтами. Эти сайты соединяются между собой при помощи магистральной сети провайдера.

Роутер клиента, который подключается к магистральной сети провайдера, называют CE(Customer Edge router). CE может иметь сразу несколько каналов подключения к провайдеру. Маршрутизатор CE не подозревает о существовании VPN.

Магистральная MPLS сеть провайдера состоит из маршрутизаторов с коммутацией меток (LSR, Label Switch Router). LSR делятся на внутренние маршрутизаторы (P, Provider router), которые составляют ядро сети, и

внешние (PE, Provider Edge router), которые непосредственно соединяются с CE клиента. Из всех роутеров провайдера о существовании VPN знаю только PE. С точки зрения VPN P роутеры не с ним не взаимодействуют.

Основная нагрузка по поддержанию VPN возлагается на PE маршрутизаторы.
В частности они занимаются разграничением маршрутов и данных, поступающих от разных клиентов. Оконечными точками пути LSP(Label Switch Path) между сайтами клиентов служат PE маршрутизаторы.

Пути LSP могут быть проложены либо с применение 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 P и PE, образующих данный LSP.

Для корректной работы VPN требуется, чтобы информация о маршрутах через магистральную сеть не распространялась за её пределы, а сведения о маршрутах в клиентских сайтах не становились известными за границами определенных VPN.

В MPLS VPN маршрутизаторы играют роль барьеров для распространения информации о маршрутах. Через PE проходит невидимая граница между зоной клиентских сайтов и зоной ядра сети провайдера. С одной стороны на PE поступает информация о маршрутах магистральной сети, с другой стороны - информация о маршрутах в сетях клиентских сайтов.

Адресные пространства MPLS VPN.

Так как MPLS обеспечивает распространение маршрутной информации в пределах отдельных VPN, то это позволяет назначать адреса в этой сети произвольным образом.

Часто сам клиент не хочет полной изолированности сети: они могут нуждаться в выходе интернет. Это желание клиента накладывает определённые ограничения на выбор адресного пространства в VPN клиента. Произвольный выбор адресов может привести к совпадению внутренних адресов сайтов с уже выделенными публичными адресами. В этом случае доступ в интернет будет не возможен. Использование частных адресов совместно с техникой трансляции адресов (NAT, Network Address Translation) обычно решается проблема доступа в интернет.

Т.к. существует возможность возникновения одинакового сетевого адреса у различных клиентов различных сетей, то для корректной маршрутизации используется дополнительный адрес RD (Route Distinguisher), для однозначного соответствия какого-либо клиента к данной сети. Поле RD представляет собой фактически идентификатор сети клиента. Пакеты, имеющие одинаковый сетевой адрес, в сети VPN будут представлены комбинацией одинакового сетевого и различного RD-адресов, и таким образом будут отличаться. Для избегания стандартизации и обеспечения уникальности RD-адресов используют различные параметры VPN-сети, про уникальность которых заранее известно. Например, это могут быть глобальные адреса интерфейсов или номера автономных систем.

Различитель маршрутов RD имеет длину 8 байт и состоит из трех полей. Первое поле Type длиной 2 байта определяет тип и разрядность второго поля. Второе поле носит название Administrator и однозначно определяет провайдера. Значение нуль поля Type говорит о том, что второе поле указывает IP – адрес интерфейса маршрутизатора PE, и длина этого поля составляет 4 байта. Если же значение поля Type равно единице, в качестве идентификатора провайдера выбран номер его автономной системы, в этом случае длина поля составит 2 байта. Третье поле носит название Assigned Number, которая обеспечивает уникальность адресов VPN. Значение поля Type равное нулю более удобно, так как ограничивает требование уникальности значения Assigned Number пределами отдельного PE.

Применение технологии MPLS в построение сетей VPN можно было бы описать по подробней, но ввиду существующих ограничений на размер статьи, это не возможно.

Список литераторы.

1) VPN Consortium (VPNC), “VPN Technologies: Definitions and Requirements”, VPN Consortium, January 2003.
http://www.vpnc.org/

2) “MPLS – VPN Services and Security” Ravi Sinha July 14, 2003.
http://www.sans.org/rr/whitepapers/vpns/1124.php

3) “Описание MPLS/VPN” Юшков Тарас 27.01.2005
<http://www.mpls-exp.ru/docs/mplsvpn.pdf>