УДК 004.9

Исследования безопасности технологии MPLS VPN

К.В.Зольников, Ли Чтинзюинь

[1]ФГБОУ ВО «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова»

Аннотация: MPLS использует метки, направляющие новую технологию высокоскоростной и эффективной передачи данных в открытой коммуникационной сети. Технология QoS, основанная на MPLS VPN, может сделать голос, видео и другие ключевые виды обеспечения качества обслуживания в режиме реального времени, вполне может решить «Triple Play». В этом документе представлена теория MPLS VPN, затем обсуждаются безопасность и характеристики MPLS VPN. Схема с MPLS VPN состоит из ограничений безопасности, использует шифрование группы доступа VPN и аутентификацию на основе PKI для обеспечения безопасности VPN-подключения и маршрутизации. Наконец, используя программное обеспечение OPNET, проведите имитационные эксперименты для доступа к сайту членов группы VPN, иначе вы не будете захватывать или заливать потоки данных передачи VPN на сайт, который может быть вызван только действительными членами группы VPN.
Ключевые слова: MPLS; VPN; PKI

VPN (виртуальная частная сеть) — это сетевая технология, которая предоставляет нам безопасный способ удаленного доступа к частной сети внутри предприятия через общедоступную сеть. Эта технология использует такие меры, как аутентификация, контроль доступа и целостность данных, для обеспечения конфиденциальности, целостности и доступности информации во время передачи [1][2].

Зрелость технологии MPLS (многопротокольная коммутация по меткам), ее безопасность для передачи IP-данных и широкие возможности управления трафиком, а также гибкие и целевые возможности гарантии QoS для услуг делают эту технологию популярной среди операторов и широко используемой на предприятиях. IP-сети. В этом контексте VPN на основе MPLS обладает такими характеристиками, как предоставление услуг без установления соединения, построение на третьем уровне, высокая масштабируемость, отсутствие интерференции данных между VPN, простота построения, гибкое адресное пространство и т. д. Уникальные преимущества завоевали расположение все больше и больше предприятий [3].

MPLS VPN может использовать преимущества обширных и мощных возможностей передачи в общедоступной магистральной сети, снизить

стоимость строительства внутренней сети предприятия, значительно повысить гибкость работы и управления пользовательской сетью и в то же время удовлетворить требования пользователя к информации. безопасность передачи, в режиме реального времени, высокая потребность в пропускной способности и удобстве.

1 Основные принципы MPLS VPN

MPLS VPN принимает туннельный протокол в качестве технологии MPLS, использует коммутацию по меткам, соединяет различные ветви частной сети через LSP (путь коммутации по меткам) и сочетает традиционную технологию маршрутизации для создания VPN типа «сеть-сеть» (LAN-to-LAN). технологии. Он может относительно хорошо реализовывать соответствующие услуги QoS, поэтому он может удовлетворить потребности различных межсетевых соединений и приложений предприятия, что делает VPN заменой выделенным линиям.

MPLS VPN использует технологию двухуровневых меток для реализации туннеля. Внутренняя метка указывает целевой пользовательский сайт, на который направляется пакет, а внешняя метка указывает путь домена MPLS, по которому пакет направляется к выходному LER (пограничному маршрутизатору с метками), напрямую подключенному к целевому пользовательскому сайту. Когда IP-пакет достигает входного LER, входной LER просматривает LFIB (база данных информации о пересылке меток) и помещает на пакет двухуровневую метку. Инкапсулированный пакет метки пересылается по пути LSP (Label Switching Path) в домене MPLS, а базовый LSR (Label Switching Router) не нуждается и не знает о существовании метки внутреннего уровня, а знает только внешний уровень метка пакета меток обмена. Когда пакет метки достигает LSR предпоследнего перехода, всплывает метка верхнего уровня, и пакет, содержащий только метку внутреннего уровня, отправляется на выходной LER, а выходной LER выталкивает внутреннюю метку и находит связанный IP-маршрут. с внутренней меткой, а затем достигает пункта назначения в соответствии с методом маршрутизации IP-пакета.

Сеть MPLS VPN обычно состоит из трех типов оборудования CE, PE и P, среди которых CE — это пограничный маршрутизатор пользователя, который обеспечивает пользователям подключение к маршрутизаторам PE и, как правило, не требует поддержки протокола MPLS; PE — это пограничный маршрутизатор провайдера, который хранит маршрутную информацию на основе обработки и пересылает данные VPN от CE-маршрутизатора или LSP, а также обменивается маршрутной информацией с другими PE-маршрутизаторами; P является основным маршрутизатором провайдера, который прозрачно пересылает данные VPN в соответствии с внешней меткой пакета, а маршрутизатор P поддерживает только информацию о маршрутизации маршрутизатора PE, которая не поддерживает информацию о маршрутизации, связанную с VPN. И PE, и P должны поддерживать протокол MPLS. Структура сети показана на рисунке

1.

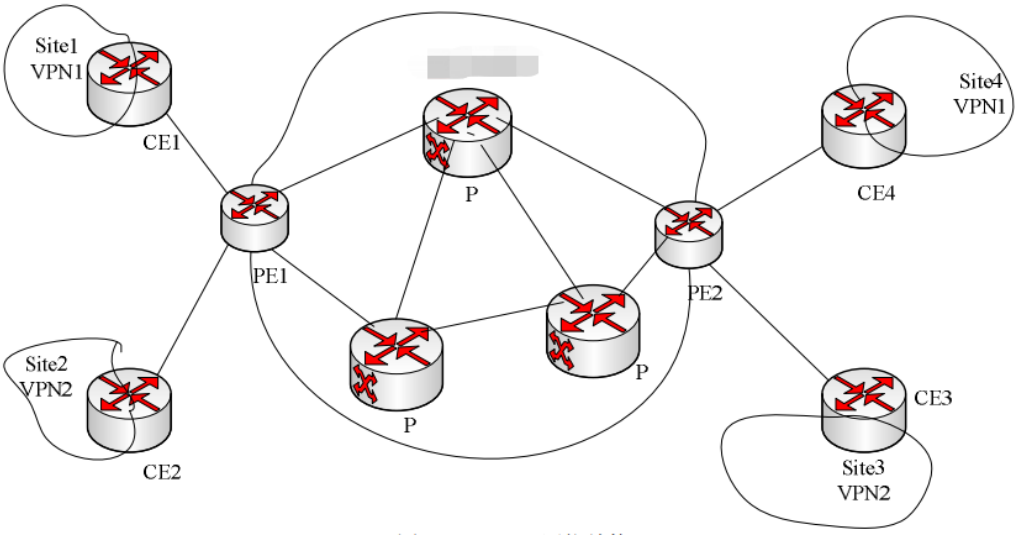

Рис. 1 Структура сети MPLS VPN

2 Безопасность MPLS VPN

Безопасность MPLS VPN достигается с помощью таких методов, как независимость от адреса, изоляция маршрута, защита от атак и подмена флага отказа [5].

Независимость от адреса: ядро сети оператора использует дискриминатор маршрутизации RD для расширения семейства адресов IPv4 пользователей VPN до семейства адресов VPNv4, гарантируя, что адресное пространство пользователей VPN сохраняет глобальную уникальность в ядре сети оператора, то есть , разные пользователи VPN, основные сети Все могут использовать одно и то же адресное пространство, между ними не будет конфликтов, адреса друг друга невидимы, а сеть недоступна.

Изоляция маршрута: каждый PE-маршрутизатор поддерживает отдельный экземпляр Virtual Route Forwarding Instance (VFI) для каждой подключенной VPN, и каждый VFI-хост размещает маршруты из одной и той же VPN (либо статически настроенной, либо использующей протокол маршрутизации между PE и CE). Поскольку каждая VPN создает независимый VFI, на него не будут влиять другие VPN на PE-маршрутизаторе.

Защита от атак: операторы скрывают информацию о своей основной сети и информацию о реализации VPN, которая прозрачна для любых пользователей VPN. Это позволяет пользователям VPN максимально атаковать других членов своей сети VPN, но не может обнаруживать информацию базовой сети и других сетей VPN, теоретически предотвращая атаки проникновения из

пользовательской сети VPN на ядро и другие сети VPN.

Запретить подмену тегов: в сетях MPLS пересылка пакетов выполняется на основе тегов, прикрепленных PE-маршрутизаторами, а не IP-адресов назначения. Подобно атакам с подменой IP-адресов, злоумышленники также могут выполнять подмену тегов в пакетах MPLS. Однако PE-маршрутизаторы не могут принимать помеченные пакеты данных от CE-маршрутизаторов, и любые такие пакеты данных будут отбрасываться. Поэтому реализовать атаки через подмену меток в сетях MPLS невозможно.

3 Особенности MPLS VPN

По сравнению с обычными IP-услугами и частными сетевыми услугами услуги VPN обладают характеристиками безопасной связи, масштабируемости, простоты управления, низкой стоимости и гарантированного качества обслуживания.

Безопасность: MPLS VPN использует различные методы, такие как изоляция адресов, изоляция маршрутов, сокрытие информации и двойные метки, чтобы противостоять атакам и подделке меток, но это не решает общие проблемы несанкционированного доступа к защищенным элементам сети и ошибок во всех управляемых общих сетях. Проблемы безопасности, такие как конфигурация и внутренние (в том числе основные) атаки, не обеспечивают такие службы безопасности, как шифрование и аутентификация, а передаваемые данные представляют собой обычный текст, поэтому его безопасность находится на среднем уровне.

Масштабируемость: MPLS VPN принимает одноранговый режим и структуру без установления соединения третьего уровня, поддерживает многопротокольную инкапсуляцию и единый механизм пересылки, поэтому он может поддерживать пересылку нескольких типов услуг в одной сети одновременно. , и имеет сильную масштабируемость.

Простота управления: для MPLS VPN, поскольку нет необходимости устанавливать и поддерживать соединения между участниками одной и той же VPN, когда присоединяется новый участник, поставщик интернет-услуг сообщает устройству на стороне пользователя, как подключиться к сети, и настроить PE для идентификации соединения с CE. Члены VPN, BGP (протокол пограничного шлюза) автоматически обновят соответствующую конфигурацию, и пользователям не нужно менять свои собственные пограничные устройства. Этот метод централизованного управления и унифицированная платформа для бизнес-настройки и планирования снижают нагрузку на пользователей.

Стоимость: в основном управляется и обслуживается интернет-провайдерами и операторами связи. Пользователям не нужно предоставлять техническую и аппаратную поддержку для создания сетей MPLS VPN, а нужно лишь предоставить небольшой объем пользовательской информации о сети. Единовременные инвестиции невелики, но долгосрочные инвестиции относительно высоки.

QoS: интегрируя технологию коммутации канального уровня (ATM, Frame Relay)

и технологию маршрутизации сетевого уровня, он идеально сочетает маршрутизацию уровня 3 с коммутацией уровня 2, решает проблему масштабируемости Интернета и обеспечивает плавность передачи данных. Производительность QoS. С помощью этого механизма QoS поставщики услуг могут предоставлять пользователям различные дополнительные услуги, соответствующие соглашениям об уровне обслуживания.

4 Анализ и решение

4.1 Анализ

В зависимости от того, участвуют ли маршрутизаторы PE в маршрутизации клиентов, MPLS VPN делится на MPLS VPN уровня 3 и MPLS VPN уровня 2. Среди них MPLS VPN уровня 3 соответствует стандарту RFC2547bis, использует BGP (протокол пограничного шлюза) для распределения маршрутной информации между PE-маршрутизаторами и использует технологию MPLS для передачи данных между сайтами VPN, поэтому его также называют BGP/MPLS VPN. В этой трехуровневой MPLS BGP VPN MP-iBGP используется между одноранговыми узлами PE для обмена маршрутной информацией. PE-маршрутизаторы обеспечивают распространение информации о маршрутизации на все PE-маршрутизаторы, поддерживая ячеистые соединения iBGP или используя отражатели маршрутов. Когда входной PE-маршрутизатор распространяет информацию о маршрутизации, он также будет нести RD таблицы VRF, в которой находится маршрутизация, то есть преобразовывать адрес IPv4 маршрутизации в адрес VPN-IPv4. Кодировка адреса VPN-IPv4 показана на рис. 2. Распространяемая конкретная маршрутная информация включает в себя префикс адреса VPN-IPv4 маршрута, адрес BGP VPN-IPv4 следующего перехода входного PE-маршрутизатора (где RD=0), Метка VPN, назначенная маршруту, и экспорт RT. Мы называем эту информацию о маршрутизации информацией о маршрутизации VPN-IPv4. С учетом приведенного выше анализа информация о маршрутизации VPNv4, которой обмениваются узлы PE с помощью BGP/MPLS VPN, основана только на достижении маршрутизатора назначения без соответствующей защиты безопасности, особенно расширенные атрибуты сообщества, переносимые MP-BGP, должны быть прозрачными для любой третьей стороны. кроме сверстника [6].

В этом случае вы можете использовать систему открытого ключа PKI (инфраструктура открытых ключей) для подачи заявки на сертификат и настройки пары открытый ключ-закрытый ключ для каждой VPN, а также использовать закрытый ключ VPN для шифрования вывода маршрута VPNv4 с помощью каждый участник VRF VPN. , узлы PE используют открытый ключ VPN для расшифровки маршрутов VPNv4 после их получения. В настоящее время маршруты VPNv4 представляют собой зашифрованную передачу между одноранговыми узлами PE, а также предоставляется функция проверки маршрутов VPNv4, чтобы гарантировать, что маршруты VPNv4 исходят от правильных участников VPN. Без открытого ключа VPN узел PE не сможет

расшифровать этот маршрут VPNv4. Система PKI генерирует пару открытого ключа и закрытого ключа для каждой группы VPN. Члены группы, у которых есть открытый ключ и закрытый ключ группы, по умолчанию имеют взаимный доступ, а участники, имеющие доступ между группами, могут распространять открытый ключ группы VPN для доступа. Информация о маршрутизации VPN, реализуемая функцией зашифрованной аутентификации на основе криптосистемы с открытым ключом, повышает безопасность BGP/MPLS VPN.
Структура данных, используемая в этом методе:

```
typedef struct Key_Table {
int key_pub[4]; //Открытый ключ для группы VPN, длина ключа 128 бит.int
key_pri[4];       //Открытый ключ для группы VPN, длина ключа 128 бит.
}Key_Table;
```

4.2 Эксперимент по моделированию

Используйте платформу моделирования OPNET Modeler для проведения экспериментов по моделированию улучшенной модели VPN для проверки безопасности VPN. Топология имитационного эксперимента показана на рис. 2. Два пользователя VPN, Enterprise A и Enterprise B, имеют сервисные функции BGP/MPLS VPN. И Enterprise A, и Enterprise B состоят из штаб-квартиры и двух филиалоSite2.

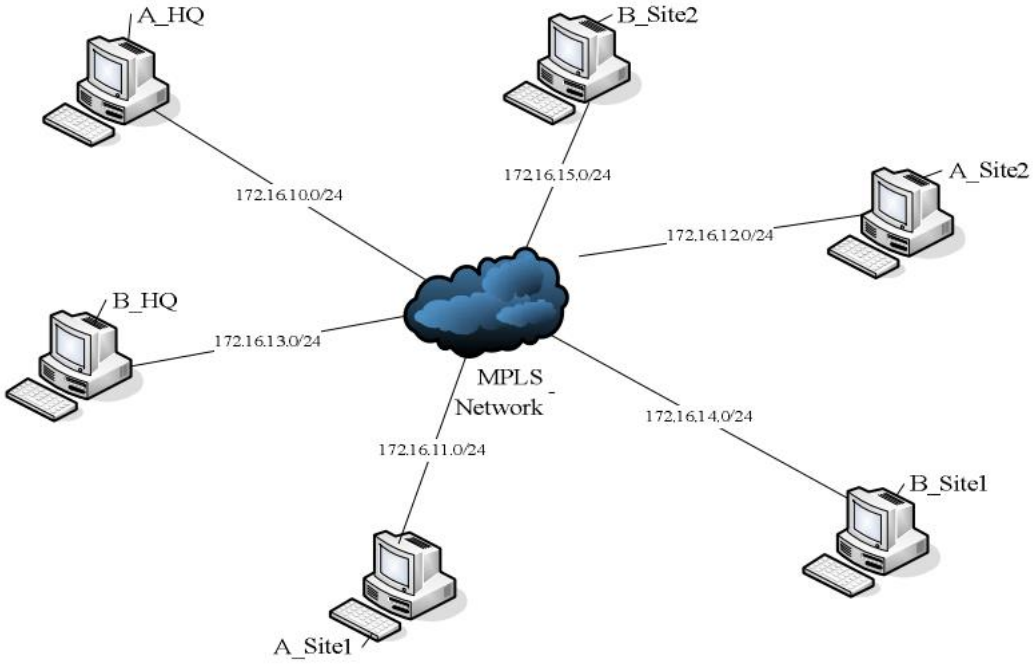

Рис. 2 Топология эксперимента по моделированию

Топология базовой сети показана на рис. 3, включая 3 LSR основного оборудования провайдера (P1, P2, P3), 3 граничных оборудования LER провайдера (PE1, PE2, PE3), область Server_Farm, включая инфраструктуру PK1 и сервер управления VPN. Полносвязный динамический LSP устанавливается между PE1, PE2 и PE3.

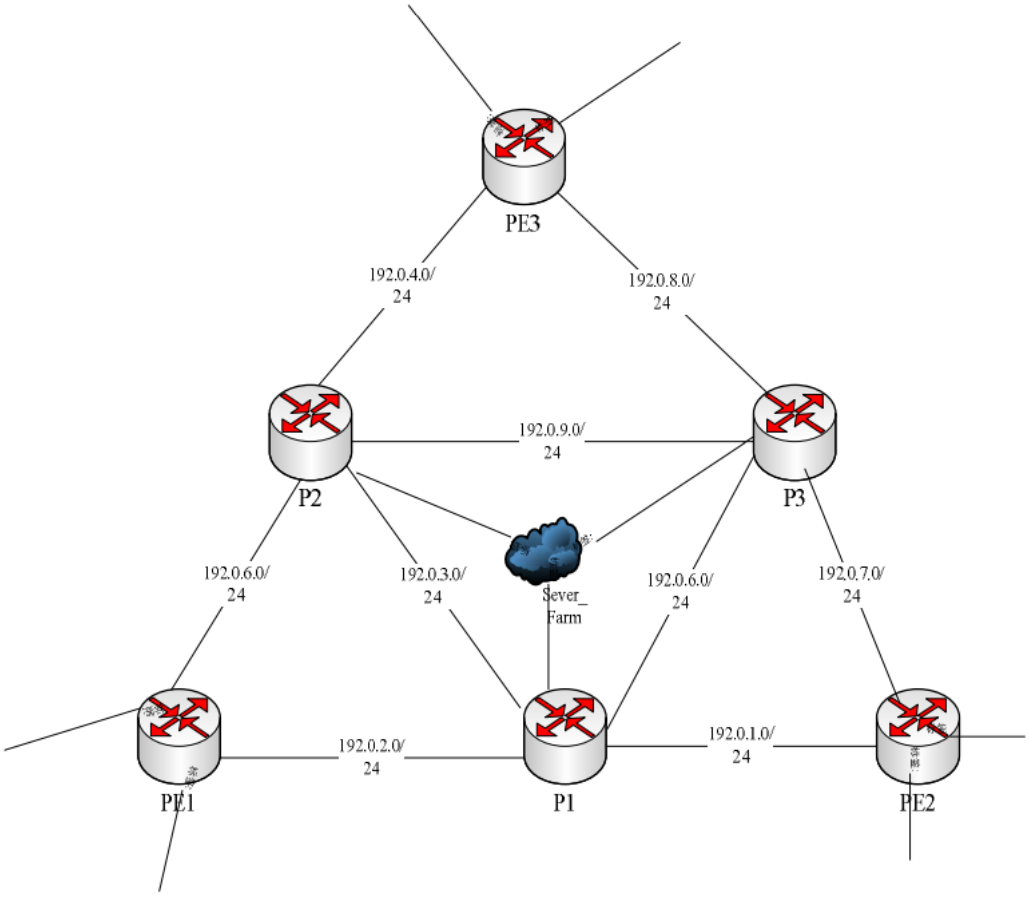

Рис. 3 Топология базовой сети

Предположим, что RT импорта и экспорта VRF, связанный со штаб-квартирой A на PEL, неправильно настроен на RT B: 100:2 (должно быть 100:1). И заставьте сайт B обнаружить, имитировать атаку site2 B на сайт HQ A, настроить поток Traceroute от B_Site2.Site2_Wkstn1 до A_HQ.Web Server соответственно в двух сценариях VPN. В сценарии, где используется групповое шифрование PKI, выходные данные таблицы VRF сайта штаб-квартиры A показывают, что он был добавлен в B, стал членом B, имеет маршрут B, но не имеет маршрутов sitel A и site2, в результате чего sitel и site2 этой VPN не может связываться со штаб-квартирой, и все сайты B смогут беспрепятственно получить доступ к сайту HQ A. Однако в BGP/MPLS VPN без шифрования выходные данные таблицы VRF HQ сайта A показывают только маршруты этого сайта, ни маршруты sitel, ни site2, ни маршруты B, ни таблица VRF сайта B-2. site A HQ Маршрут сайта, поэтому поток Traceroute, отправленный Wkstnl на сайте, не имеет ответа, и сообщение об ошибке, выводимое симуляцией:
ОШИБКА(-Ы): В таблице IP-маршрутизации на этом узле нет маршрута к месту назначения 192.168.1.1. Приведенный выше IP-адрес назначения соответствует интерфейсу на следующем узле: [Корпоративная сеть．EnterpriseA_HQ．Веб-сервер]

Результаты тестирования показывают, что для обеспечения взаимных посещений между сайтами-членами двух групп VPN необходимо сначала получить открытый ключ группы участников, к которой принадлежит другой сайт VPN. Неавторизованная третья сторона не может атаковать целевой сайт VPN, даже если угадывает RT, потому что открытый ключ Ключ и идентификатор группы VPN другой стороны назначаются оператором, что полностью прозрачно для пользователей VPN. Стратегия распределения маршрутов, основанная на двойном факторном контроле RT и группового ключа VPN, может эффективно повысить безопасность маршрутизации VPN и гарантировать, что только авторизованные сайты VPN могут получить взаимный доступ.

Несмотря на то, что перспективы развития относительно оптимистичны, для дальнейшего развития технологии MPLS VPN необходимо дальнейшее улучшение текущей проблемы QoS, усиление проблемы безопасности и дальнейшее повышение степени стандартизации для решения проблемы. Проблема совместимости мультивендорного оборудования. Считается, что благодаря постоянному совершенствованию и развитию технологии MPLS VPN в будущем она будет прекрасно сочетаться с IP-сетью, предоставлять пользователям более качественные и богатые услуги и станет основным направлением технологии VPN.

Рекомендации

[1] Гао Хайин, Сюэ Юаньсин, Синь Ян, Технология VPN [M], Пекин: Издательство машиностроительной промышленности, 2004.
[2] Ван Да Сущность виртуальной частной сети (VPN) [M], Пекин: Издательство Университета Цинхуа, 2006.
[3] Лу Цзэсинь, Чжу Пэйдун, Ци Нин, Архитектура MPLS и VPN (Том 2) [M], Пекин: Народная почта и телекоммуникационная пресса, 2004.
[4] Тянь Вей, Исследование и сравнение виртуальных частных сетей на основе MPLS и IPSec [J], Computer Age, 2004, (6): 11～13.
[5] He Baohong, Tian Hui, Технология виртуальной частной сети IP (второе издание) [M], Пекин: People's Posts and Telecommunications Press, 2008.
[6] Фэн Цзин, Технология многопротокольной коммутации по меткам, Пекин:

Народная почта и телекоммуникации, 2002.
[7] Орман Х. Протокол определения ключа OAKLEY [S], RFC2401, 1998-11.