электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 621.391

Анализ созданных при проектировании угроз информационной безопасности VPN на базе третьего уровня сети MPLS и рекомендации по способам защиты

Петрухин И.С., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Бельфер Р.А.,к.т.н., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
v.a.matveev@bmstu.ru

Введение. Ведущими провайдерами услуг в нашей и других странах виртуальные частные сети VPN третьего уровня строятся на базе сетей MPLS [1]. Это объясняется их преимуществом перед VPN на базе протокола IPSec.

(Такие VPN иногда называют виртуальными частными маршрутизируемыми сетями– VPRN, Virtual Private Routed Network. Такое обозначение VPN третьего уровня на основе MPLS мы будем использовать далее в некоторых случаях для отличия от VPN второго уровня на основе MPLS. В тексте данной статьи эти сети будем также называть VPN, а в приведенных в статье примерах – сервисами).

Приведём основные преимущества VPRN по сравнению с сетями VPN на базе IPSec.

- VPRN обеспечивает такой же высокий уровень информационной безопасности, не прибегая к шифрованию. В случае требований заказчика по повышению ИБ технология VPRN использует криптографию в области ядра сети MPLS с помощью протокола IPSec.
- VPRN в отличие от VPN на IPSec обеспечивает пользователю затребованное им качество обслуживания соединения. Технология MPLS реализует модель дифференцированного обслуживания DiffServ, позволяющая обеспечить требуемое пользователем качество обслуживания QoS путем разделения трафика соединений на классы обслуживания (до 8 классов обслуживания). Технология MPLS позволяет перераспределять потоки, перемещая нагрузку с чрезмерно используемых частей сети в мало загруженные. Маршрутизация с перераспределением потоков и резервированием ресурсов позволяет провайдерам в максимальной степени использовать сетевые ресурсы,

обеспечить высокое качество обслуживания QoS и добиться оптимальной работы сети. При этом достигается оптимизация недостаточно загруженных каналов и более эффективная маршрутизация.

- VPRN в отличие от VPN на IPSec обладает возможностью большей масштабируемости.

Отмеченный в работе [1] высокий уровень информационной безопасности VPRN относится к корректно спроектированной сети. Настоящая работа посвящена анализу одних из распространенных угроз и способам защиты от них, которые могут создаваться при конфигурировании таблиц маршрутизации VPRN.

Архитектура информационной безопасности VPRN. В архитектуру ИБ сети связи входит понятие плоскости безопасности (Security Plane), под которой понимается определенная функция сети связи, защищенная определенным способом. В Рекомендации ITU-T X.805 [2] по общим положениям архитектуры сетей связи, определено 3 типа плоскости безопасности.

1. Плоскость безопасности Management Security Plane по управлению сетью, к которой относится защита функций администрирования, эксплуатации и обслуживания сети OAM&P (Operation Administration Maintenance&Provision).

2. Плоскость безопасности Control Security Plane по обеспечению безопасности транспортной сети, к которой относится защита функций и передаваемой по сети информации, например, по установлению и разъединению соединения, по маршрутизации сообщений. Согласно документу по RFC 4364 [3] понимается то, что в VPRN сообщения протоколов LDP, BGP по обеспечению маршрутизации должны быть аутентифицированы. В этом документе RFC 4364 в качестве механизма защиты рекомендуется протокол аутентификации MD5.

3. Плоскость безопасности оконечного пользователя (End-User Security Plane). Плоскость безопасности оконечного пользователя относится к безопасности сети доступа и пользования абонентами сетью поставщика услуг. К этой плоскости безопасности относится также защита потоков данных оконечного пользователя. В документе RFC 4364 эта плоскость безопасности называется плоскостью безопасности данных (data plane). Под этим понимается защита от случаев нарушения политики безопасности, когда пакеты из данной VPN поступают в другие VPN или наоборот.

Зоны доверия VPRN. Для разных корпоративных VPRN характерны определенные схемы взаимодействия виртуальных частных сетей в ее окружающей среде с устройствами других зон сети.

В настоящем разделе приводятся примеры взаимодействия VPRN с некоторыми из

них.

На рисунке 1 приведена базовая модель VPRN. Здесь VPN A состоит из двух сайтов, VPN B – из трех сайтов и VPN C - из четырех сайтов.

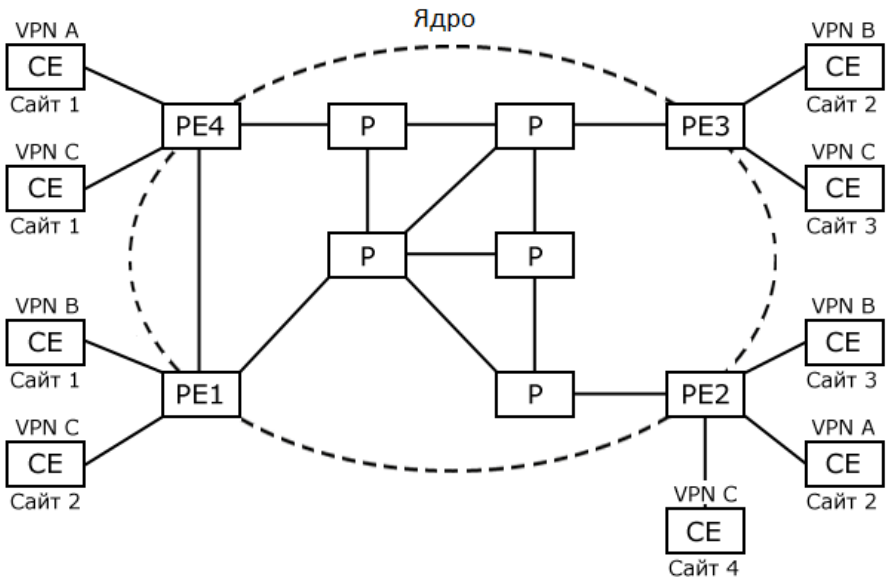

Рис. 1. Базовая модель VPRN

Здесь показано, что ядро сети MPLS включает внутренние маршрутизаторы провайдера P (Provider router) и граничные маршрутизаторы провайдера PE (Provider Edge router). Граничный маршрутизатор клиента CE (Customer Edge router) является оборудованием абонентского доступа к ядру сети MPLS. Для приведенной базовой модели безопасности недопустимо передавать сообщения из одной VPN в другую, из VPN – абонентам ядра сети (не в VPN), принимать в VPN сообщения от абонентов ядра сети. На практике модель безопасности более сложная, чем приведенная базовая модель. Например, многие VPN могут взаимодействовать с Internet или другими VPN (Extranet). При взаимодействии VPN с Internet ядро сети остается изолированным от этого взаимодействия. Для анализа угроз ИБ в таких случаях вводится понятие “безопасной” или “доверенной” зоны [4]. В приведенном примере такой зоной является ядро сети. Для защиты ядра сети в этом случае между VPN и ядром сети устанавливается межсетевой экран (брандмауэр).

На рисунке 2 приведен пример взаимодействия VPRN с двумя зонами доверия, каждое из которых является ядром сети MPLS. Каждое ядро является автономной системой AS (Autonomous System) и может обслуживаться одним или разными провайдерами услуг.

Взаимодействие между AS осуществляется через граничные маршрутизаторы автономной системы ASBR (Autonomous System Border routers). Здесь имеет место

взаимодействие сайтов VPN между собой через два ядра сети MPLS.

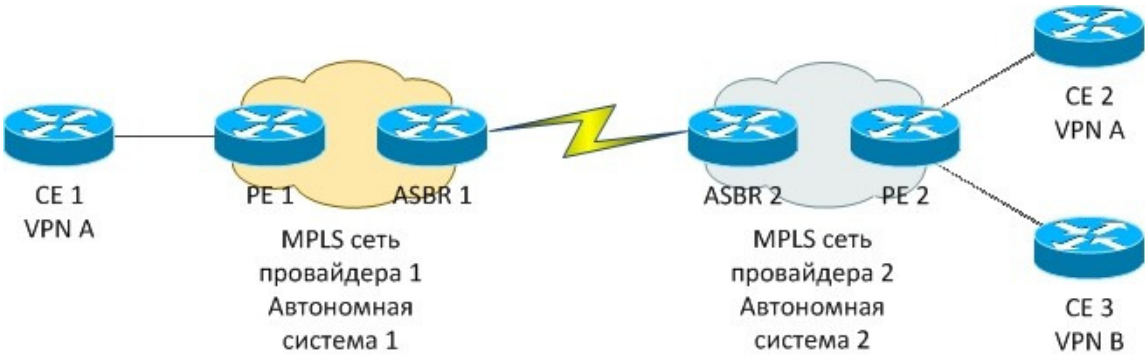

Рис. 2. Пример взаимодействия VPRN с двумя зонами доверия

При взаимодействии VPN оба ядра сети остаются изолированными. Защита ядер сети в этом случае между VPN и ядром сети обеспечивается также с помощью брандмауэра. Приведенная на этом рисунке архитектура VPRN с двумя зонами доверия относится к одноуровневой технологии [5].

Источники угроз ИБ при проектировании VPRN и способы защиты. Одной из характеристик угроз ИБ является описание источника угроз. Все эти угрозы могут исходить из разных источников: из самих VPN, из сети Интернет, от провайдера услуг и др. угрозы могут различаться по способу воздействия на VPN: вторжения, отказ в обслуживании DoS (Denial of Service). В настоящей работе приводится анализ моделей угроз ИБ VPRN, созданных при проектировании сети MPLS провайдера услуг. При этом приводятся примеры потенциальных источников угроз информационной безопасности VPRN. Все нижеприведенные примеры, относятся к плоскостям безопасности управления или данных.

Угроза 1 и ее последствия. Рассмотрим одну из самых распространенных угроз ИБ VPRN, вызванных случайной или преднамеренной ошибкой, внесенной администратором, настраивающим граничное оборудование провайдера услуг.

Суть данной угрозы состоит в некорректной конфигурации граничного маршрутизатора PE, что может повлечь вторжение в VPRN.

В приведенном ниже примере показана корректная конфигурация маршрутизатора PE. На нем настроены два VPRN сервиса (с числовыми идентификаторами 1 и 2), соответственно существуют две различные таблицы маршрутизации VRF, каждая со своей маршрутной целью RT [6]. CE подключены к этим сервисам через гигабитные интерфейсы (1/1/1 и 1/1/2).

В данной топологии RT определяют, каким образом будут обрабатываться маршруты из каждой VRF: при разных значениях RT маршруты будут находиться в соответствующих VRF.

Пример. Корректная настройка сервисов VPRN.

1. PE# ***configure service***

2. PE>config>service# ***vprn 1 customer 1 create***

3. PE>config>service>vprn# ***route-distinguisher 65530:1***

4. PE>config>service>vprn# ***vrf-target target:65530:1***

5. PE>config>service>vprn# ***interface “access” create***

6. PE>config>service>vprn>if# ***address 192.168.1.1/24***

7. PE>config>service>vprn>if# ***sap 1/1/1 create***

8. PE>config>service>vprn>if# ***exit***

9. PE>config>service>vprn# ***no shutdown***

10. PE>config>service>vprn# ***exit***

11. PE>config>service# ***vprn 2 customer 1 create***

12. PE>config>service>vprn# ***route-distinguisher 65530:2***

13. PE>config>service>vprn# ***vrf-target target:65530:2***

14. PE>config>service>vprn# ***interface “access” create***

15. PE>config>service>vprn>if# ***address 192.168.2.1/24***

16. PE>config>service>vprn>if# ***sap 1/1/2 create***

17. PE>config>service>vprn>if# ***exit***

18. PE>config>service>vprn# ***no shutdown***

19. PE>config>service>vprn# ***exit all***

Комментарии к командам конфигурации:

1) Войти в режим конфигурации сервисов (общий для всех возможных сервисов, как второго, так и третьего уровней).

2) Создать сервис VPRN 1 для клиента 1 (в данном примере используется один клиент для сервисов VPRN 1 и VPRN 2).

3) Задать RD для сервиса VPRN 1.

4) Задать RT для VRF сервиса VPRN 1.

5) Создать логический интерфейс.

6) Задать IP-адрес на вышеуказанном интерфейсе (в некоторых конфигурациях данный IP-адрес абонент может использовать как шлюз по умолчанию) [7].

http://sntbul.bmstu.ru/doc/622420.html

7) Осуществить привязку физического порта (к которому будет подключаться оборудование CE абонента для сервиса VPRN 1) к логическому интерфейсу с настроенным IP-адресом.

8) Выйти из режима конфигурации интерфейса.

9) Включить сервис VPRN 1.

Строки конфигурации с 11 по19 дублируют вышеуказанные, за исключением того, что все они применяются к сервису VPRN 2 и содержат уникальные для данного сервиса атрибуты, такие как: идентификатор сервиса, RD, RT, IP-адрес интерфейса (данные значения могут быть идентичны для обоих сервисов, т.к., технология MPLS подразумевает полное разделение клиентских маршрутов посредством протокола MP-BGP), номер физического порта [7].

Так же стоит заметить, что в этой конфигурации не присутствуют ссылки на транспортные туннели (spoke-sdp) т.к. настраиваемые сервисы VPRN являются локальными для маршрутизатора PE (в сети провайдера не существуют других PE, на которые должны распространяться эти сервисы) [8].

Теперь допустим, что сетевой администратор при настройке RT задал неправильную команду: *PE>config>service>vprn#* ***vrf-target target:65530:1*** вместо команды *PE>config>service>vprn#* ***vrf-target target:65530:2*** в строке конфигурации № 13.

Последствием этой нелегитимной команды будет являться то, что сайт, который подключен к VPRN 2 будет логически принадлежать к VPRN 1.

Опасность данной ситуации заключается в том, что сайт сервиса VPRN 1 становится потенциально подвержен вторжениям с сайта сервиса VPRN 2. В результате сайт VPRN 2 становится логически принадлежать сайту VPRN 1. Потенциальной угрозой данной ошибки в конфигурации является то, что появившееся связь между двумя сайтами может быть не сразу замечена на сайте VPRN 1 (если на сайтах VPRN 1 и VPRN 2 нет перекрытия диапазонов используемых IP-адресов). Даже если данная команда была непреднамеренна, то угроза для сайта VPRN 1 остается серьезной, т.к. теперь различные вирусы могут перейти в VPRN 1 из VPRN 2.

Угроза 2 и ее последствия. Рассмотрим ещё одну распространенную угрозу ИБ, вызванную нелегитимной конфигурацией PE. Данная угроза обуславливается переполнением таблицы VRF, атакой отказ в обслуживании DoS граничного маршрутизатора PE.

Максимальный объем любой таблицы маршрутизации (в том числе и VRF) характеризуется производительностью самого маршрутизатора (объем памяти, производительность процессора). Даже самые производительные маршрутизаторы не

могут обработать все возможные маршруты из сети Интернет, не говоря уже о менее производительном граничном оборудовании PE.

В результате при достижении некоторого критического количества маршрутов в одной из VRF, заполняется вся доступная память на самом PE, снижается производительность PE, вплоть до полной прекращения передачи данных через это устройство [9]. Со стороны абонента данная ситуация может выглядеть как потеря связи с другими сайтами или сетью Интернет, если данная услуга предоставляется провайдером.

Поэтому, если на PE для связи с абонентом запущен любой динамический протокол маршрутизации (или если через данный сервис осуществляется подключение к Интернет), необходимо явно ограничивать максимальное возможное количество маршрутов в VRF. Сделать это можно выполнив следующую команду на PE в режиме конфигурирования желаемого сервиса (см. пример 1.):

PE>config>service>vprn# ***maximum-routes*** *X* [9]

Где X – любое целое значение в интервале от 1 до 2147483647 (для маршрутизатора Alcatel-Lucent модификации SR7750-12). После достижения значения X новые маршруты не будут устанавливаться в таблицу маршрутизации VRF для конкретного сервиса. Максимальное возможное значение X определяется производительностью маршрутизатора PE.

Угроза 3 и ее последствия. Так же существует потенциальная возможность реализации угрозы вторжения в VPN при распределенном ядре сети (рис. 2), когда ядро сети образуют два и более провайдера связи и эти провайдеры не могут доверять друг другу.

При такой топологии оба маршрутизатора PE могут видеть друг друга посредством протокола MP-BGP и обмениваться всей информацией, касающейся VPN (VPN-IPv4 NLRI, метки и т.д.). Данная связь не затрагивает ASBR, это означает, что ASBR не нужно знать информацию о VPN. Им нужно только обмениваться маршрутами к граничным маршрутизаторам PE, участвующих в VPN.

Так как туннель LSP строится от PE в AS 1 к PE в AS 2 с использованием системных адресов самих PE, то ASBR должны функционировать как обычные P маршрутизаторы, за исключением того, что они не будут добавлять свою транспортную метку на пути движения пакета.

С учетом вышеуказанной схемы возникает возможность реализации следующий атаки: из AS 1 может передавать трафик с любой меткой VPN в AS 2 (т.к. на ASBR метки не могут проверяться).

Эта потенциальная атака на приведенной топологии сети реально остается на настоящий момент незащищенной. Избежать такую уязвимость ИБ можно следующим образом:

либо не проектировать такую топологию, если провайдеры, отвечающие за разные AS, не могут доверять друг другу, либо следует распространять информацию о VPN до ASBR маршрутизаторов (в последнем варианте для этого между ними необходимо настроить MP-eBGP сессии, что ухудшает масштабируемость всей сети в целом).

При этом следует учесть, что если злоумышленнику неизвестна сервисная VPN метка и BGP-IPv4 адрес (IP адрес + RD), то ему необходимо будет находить эти параметры случайным перебором, что потребует очень много времени.

Выводы. Приведенный анализ источников угроз ИБ при проектировании VPRF позволяет использовать предложенный способ защиты от них. При конфигурировании таблиц маршрутизации нескольких корпоративных VPRN эти предложения были успешно реализованы.

Список литературы

1. Оливейн В. Структура и реализация современной технологии MPLS. М. Вильямс, 2004. 480с.
2. ITU-T Recommendation X.805. Security architecture for System providing end-to-end communication, 2003
3. Michael H. Behringer, Monique J. Morrow, MPLS VPN Security Cisco Press, 2005, p.312
4. E. Rosen, Y. Rekhter. RFC 4364, BGP/MPLS IP Virtual Private Networks (VPNs), 2006
5. Бельфер Р.А. Сети и системы связи (технологии, безопасность): учебное пособие по дисциплине «Сети и системы связи»: электронное учебное издание: ФГБОУ ВПО МГТУ им. Н. Э. Баумана, 2012, 738 с.
6. Kent Hudley. Alcatel-Lucent Virtual Private Routed Networks. 2010. p. 453
7. Alcatel-Lucent 7750 Services. 2011. p. 1568
8. Glenn Warnock, Amin Nathoo. Alcatel-Lucent Network Routing Specialist II (NRS II) Self-Study Guide: Preparing for the NRS II Certification Exams. 2011. p. 1488
9. Alcatel-Lucent 7750 SR OS Router Configuration Guide. 2011. p. 498