УДК: 007

Защита трафика на сетях MPLS

Мануйлова И.С., Попова А.В.

Дальневосточный государственный университет путей сообщения, Хабаровск, e-mail: irinka_ma_97@inbox.ru

MPLS используется в магистральных сетях практически всех операторов и находит все большее распространение в территориальных локальных сетях. Однако при определенных условиях из-за MPLS могут возникнуть серьезные проблемы с безопасностью. Поэтому перед использованием VPN на базе MPLS или магистральных структур необходимо провести анализ рисков, в особенности в отношении передаваемого трафика.

Ключевые слова: MPLS, VPN, метка, трафик, маршрутизация, протокол, LDP, атака, инжекция, злоумышленник, internet, узел, DoS, DDos, защита сети.

Разработчики стремились избежать неэффективной маршрутизации IP, когда маршрут каждого пакета определяется по его адресу назначения посредством объемных таблиц маршрутизации Именно поэтому была разработана многопротокольная коммутация меток (Multi-Protocol Label Switching, MPLS), в которой продвижение пакетов происходит на основании так называемых «меток». Когда пакет IP достигает магистрали на базе MPLS, он в первую очередь классифицируется — по адресу назначения или по принадлежности к определенной клиентской виртуальной частной сети (Virtual Private Network, VPN), затем снабжается одной или несколькими метками и направляется дальше. На каждом транзитном узле верхняя метка заменяется на новую, после чего пакет передается следующему соседу. О метках и их значениях два соседних маршрутизатора договариваются при помощи специального протокола — в большинстве случаев протокола распределения меток (Label Distribution Protocol, LDP). Благодаря согласованию между соседними устройствами отпадает необходимость в централизованном механизме управления метками. Когда пакет покидает магистраль, он направляется дальше по традиционным механизмам маршрутизации.

При обсуждении безопасности технологии продвижения/маршрутизации пакетов в первую очередь упоминаются атаки наподобие спуфинга или инжекции, нацеленные на изменение или добавление информации о маршрутизации. Однако в описанной выше элементарной сети MPLS, в которой метки присваиваются на основании адресата назначения пакета, этот класс атак мало эффективен, поскольку метки имеют здесь значение лишь для двух соседних коммутаторов. Таким образом, атакующий не сможет повлиять на маршрут пакета за соседним транзитным узлом.

При атаках первоочередная цель злоумышленника — чтение трафика или неавторизованный доступ. Все атаки можно разделить на атаки «извне» (из клиентской сети или Internet) и атаки «изнутри» (с магистрали MPLS).

Инжекция (ввод) предварительно маркированного трафика из клиентской сети. Злоумышленник, находящийся в клиентской сети, может попытаться проникнуть в другую виртуальную частную сеть, передав «своему» устройству провайдера PE пакеты, уже содержащие метку. Однако пакеты с метками из не заслуживающих доверия источников не принимаются магистральными маршрутизаторами. С точки зрения провайдера, клиентская

сеть никогда «не заслуживает доверия», а значит, такие пакеты должны отклоняться маршрутизатором PE.

Инжекция (ввод) уже маркированного трафика из Internet. Злоумышленник может попытаться отправить на маршрутизатор PE уже маркированные пакеты из Internet, с целью передать их в клиентскую сеть. Для этого ему необходимо узнать используемые метки и IP-адреса, что вполне возможно. IP-адрес 10.1.1.1, к примеру, встречается в большинстве сетей, а кроме того, зная производителя оборудования, метки довольно легко угадать. Уже имеется инструмент, который служит для автоматического определения используемых в сети меток. Его наличие — показатель того, что атаки на MPLS попали в сферу интересов хакеров. В ближайшем будущем наверняка появятся новые средства для автоматического проведения описанных атак. Опять же, пакеты с метками из не заслуживающих доверия источников, к каковым, безусловно, относится Internet, отбрасываются. Однако такая атака на маршрутизаторы может быть успешной при использовании старых версий операционной системы IOS.

В отличие от уже перечисленных атак другие предполагают нахождение злоумышленника на магистрали. Если злоумышленник контролирует один из узлов магистрали, то у него появляется возможность для проведения целого ряда различных атак. Конечно, прежде всего весь проходящий через этот узел трафик, если он дополнительно не зашифрован, подвергается угрозе считывания. Как правило, такое шифрование обеспечить довольно просто, однако нередко от него отказываются ради экономии и простоты администрирования виртуальной частной сети MPLS. К атакам с магистрали относят:

- **Скомпрометированные провайдерские устройства.**
- **Эксплуатируемые клиентами устройства PE.** Если клиент самостоятельно эксплуатирует устройство PE, это ставит под угрозу всю модель безопасности магистрали, поскольку у него появляется потенциальная возможность доступа к виртуальным частным сетям других клиентов.
- **Взломанные станции управления.** Если сотрудник провайдерской компании входит в Internet с того же компьютера, с которого он обращается к инструментам управления с графическим интерфейсом для построения VPN, то потенциально злоумышленник может получить доступ к системе управления.
- **Атаки на транзитные узлы между провайдерами.** Для того чтобы предлагать виртуальные частные сети MPLS в мировом масштабе, многие операторы заключают между собой контракты, благодаря которым они могут строить VPN MPLS, простирающиеся за пределы их собственной сети, и одновременно обмениваться маркированными пакетами. Кроме того, в точках обмена трафика операторы часто организуют межсоединения на базе Ethernet, в результате чего создаются условия для атак на интерфейс данных на втором уровне.
- **Неправильно сконфигурированные устройства провайдеров.** В большинстве случаев устройства провайдеров обслуживаются людьми, из-за чего совершаются непредумышленные ошибки.

Также существуют разновидности атаки из ядра MPLS:

- **Модификация маршрутизации MP-BGP.** Когда злоумышленник в состоянии вмешаться в первоначальный информационный обмен в Multiprotocol BGP, он может добавлять в VPN «дополнительные филиалы», и через них получить неавторизованный доступ к системам. Причем надо не только находиться на магистрали, но и иметь в наличии

дополнительные инструменты для точечного доступа к трафику BGP, что требует значительных усилий.

- **Модификация меток на магистрали.** Этот тип атаки также предусматривает нахождение атакующего на магистрали. Если ему удается изменить метку пакета, то последний несложно перенаправить в другую виртуальную частную сеть.

Отдельно стоит выделить атаки DoS и DDoS

DoS-атака представляет собой генерацию "мусорного" трафика с одного устройства (IP-адреса) на ресурс-"жертву" (например, сайт) с целью исчерпания вычислительной и иной мощности "жертвы", чтобы заблокировать ее работу.

Поскольку интернет, компьютерная техника и сетевое оборудование развиваются стремительно, набирая мощность, то объем одной DoS-атаки очень скоро стал слишком мал, чтобы заблокировать сколько-нибудь значимый ресурс. Поэтому хакеры нашли самый очевидный способ усиления DoS-атаки: проводить ее с нескольких устройств (IP-адресов) одновременно. Так и появилась распределенная (или массивная) кибератака на отказ в обслуживании - DDoS (Distributed Denial of Service). Ее гораздо сложнее отфильтровать, а мощность может достигать 1 Tbps.

Нельзя допускать, чтобы DDoS-атаки угрожали вашим деловым операциям потерей репутации и финансовыми убытками.

По последним данным Incapsula, DDoS обходится бизнесу в 40000 долларов в час.

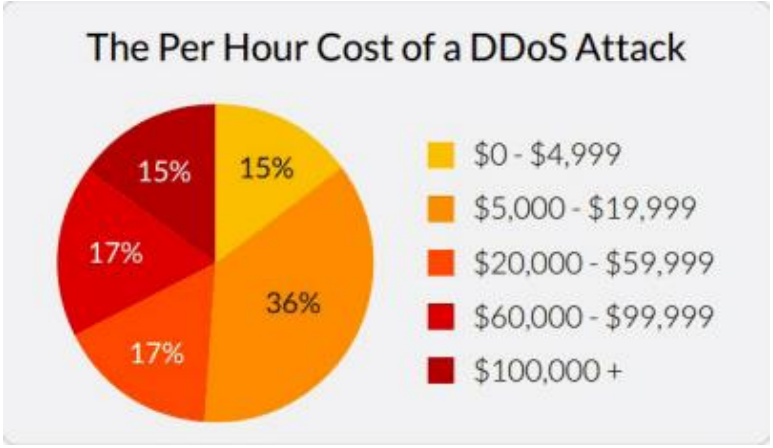

Рисунок 1. Убыток от DDoS атак в час

Хакеры прибегают к разным методикам, чтобы нанести удар по бизнесу, в том числе:

- фрагментация UDP-пакетов;
- DNS, NTP, UDP, SYN, SSPD, ACK-флуд;
- CharGEN-атака;
- аномалии TCP.

Так что нужно защищаться не только от DDoS-атак на седьмом уровне, а обеспечивать защиту на всех уровнях.

Согласно последнему отчету о безопасности AKAMAI, большинство DDoS-атак производятся из Китая.

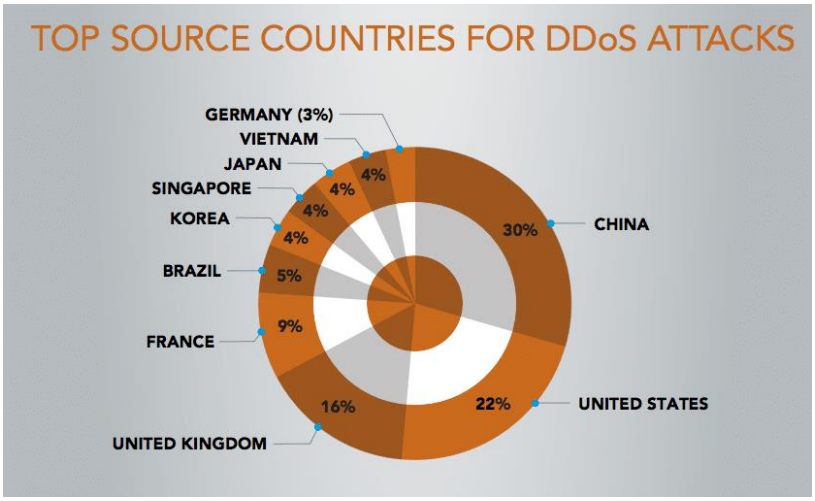

Рисунок 2. Страны, проводящие атаки DDoS

Рассмотрим облачные решения для малого и среднего бизнеса, с помощью которых можно подключить защиту от DDoS-атак за считанные минуты.

- Incapsula предлагает комплексную защиту и ограждает от любых видов DDoS-атак на 3, 4 и 7 уровнях, таких как: TCP SYN+ACK, FIN, RESET, ACK, ACK+PSH, фрагментация; UDP; спуфинг; HTTP-флуд, запуск большого числа одновременных соединений, DNS-флуд; брутфорс и другие. Защита может осуществляться в постоянном режиме или включаться вручную для поиска и устранения угроз. Сеть Incapsula состоит из 32 дата-центров с общей пропускной способностью более 3 Tbps.
- AKAMAI занимает ведущее положение на рынке в отношении услуг безопасности и CDN. Совсем недавно AKAMAI поставила рекорд, отразив атаку мощностью 620 Gbps.

Это облачное решение предохраняет от всех известных видов атак, в том числе с шифрованием трафика. AKAMAI широко представлен по всему миру: всего у AKAMAI более 1300 площадок в более чем 100 странах. AKAMAI защищает инфраструктуру всего дата-центра при помощи Prolexic Routed или Prolexic Connect.

- Cloudflare предоставляет базовую защиту от DDoS-атак в пакетах FREE и PRO. Однако для расширенной защиты от DDoS-атак на уровнях 3, 4 и 7 нужно покупать пакет Business или Enterprise. Стоимость услуг Cloudflare фиксированная, а это значит, что с какой бы масштабной атакой вы не столкнулись, одинаковая сумма взимается каждый месяц.

Сеть CloudFlare доступна в 102 дата-центрах общей пропускной способностью более 10 Tbps, то есть она справится с любыми видами DDoS-атак, в том числе: на уровнях 3, 4 и 7; DNS amplification; DNS reflection; SMURF и ACK.

- SUCURI — специализированное облачное решение для защиты самых разных сайтов. SUCURI выявляет и блокирует атаки 3,4 и 7 уровня. Стоимость обслуживания начинается от 19,88долларов в месяц.
- Anti-DDoS Pro от Alibaba поможет в защите от DDoS-атак. Anti-DDoS Pro отражает мощные атаки до 2 Tbps и поддерживает протоколы TCP/UDP/HTTP/HTTPS. Anti-DDoS можно использовать не только в случае размещения на Alibaba, но и для AWS, Azure, Google Cloud и пр.
- Myra DDoS protection — полностью автоматизированное решение для веб-сайтов, DNS-серверов, веб-приложений и инфраструктуры. Оно полностью совместимо со всеми видами CMS и системами электронной торговли.

- AWS Shield Advanced есть целый ряд преимуществ по сравнению со стандартной версией Shield, таких как: проверка сетевого потока и отслеживание трафика на прикладном уровне; передовая автоматическая защита от крупномасштабных атак, включающая блокировку вредоносного трафика; круглосуточная команда поддержки при DDoS-атаках; проведение анализа после атаки.

Описанные выше облачные решения подойдут электронным магазинам, малому и среднему бизнесу. В случае корпоративной защиты или защиты дата-центра, рекомендуются следующие сервисы: ARBOR Networks; Neustar; Rackspace; AKAMAI; F5 Silverline; Radware.

Список литературы:

1. М. Берингер М. Морроу. Безопасность виртуальных частных сетей MPLS - Индианаполис, 2005.
2. DoS и DDoS-атаки [Электронный ресурс] // 2017. URL: https://ddos-guard.net/ru/info/blog-detail/dos-i-ddos-ataki-znachenie-i-razlichiya
3. 7 лучших сервисов защиты от DDoS-атак для повышения безопасности [Электронный ресурс] // сост.: М. Козлова, 2017. URL: https://habr.com/ru/company/hosting-cafe/blog/324848/
4. Отчет по безопасности AKAMAI [Электронный ресурс] // 2016. Электрон. версия печат. публ. URL: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q3-2016-state-of-the-internet-security-report-infographic.pdf
5. Технология MPLS и сценарии нападения [Электронный ресурс] // сост.: Э. Рей, П. Фирс, 2006. URL: https://www.osp.ru/lan/2006/09/3169702/