EBU

OPERATING EUROVISION AND EURORADIO

R 141

MITIGATION OF DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACKS

RECOMMENDATION

SOURCE: SP-MCS

Geneva
June 2015

EBU
OPERATING EUROVISION AND EURORADIO

R 141
MITIGATION OF DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACKS

Внимание!
Данный перевод **НЕ** претендует на аутентичность
и может содержать отдельные неточности.
Оригинал документа на сайте https://tech.ebu.ch

УСТРАНЕНИЕ ПОСЛЕДСТВИЙ РАСПРЕДЕЛЕННЫХ АТАК ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ» (DDoS)

РЕКОМЕНДАЦИЯ

ИСТОЧНИК: SP-MCS

Женева
Июнь 2015

Устранение последствий распределенных атак типа «отказ в обслуживании» (DDoS) на медиа компании

Комитет EBU	*Первый выпуск*	*Переработка*	*Переиздание*
SP-MCS	2015		

Ключевые слова: Кибербезопасность, DDoS, Бот-сети, IP, Киберугроза, Кибератака.

Рекомендация

EBU, учитывая, что:

1. Медиа компании все чаще имеют услуги в интернете (традиционные веб-сайты, блоги, сайты сообществ и потоковые услуги для распространения радио- и телепрограмм).
2. Киберугроза атак DDoS присутствует и особенно растет в отношении медиа и вещательных организаций.
3. DDoS – один из самых распространенных и часто встречающихся типов кибератак, совершенных на медиа компании.
4. Атаки DDoS часто коррелируются по контенту телерадиопрограмм и имеют экономическую или политическую основу.
5. С точки зрения взломщиков, атаки DDoS осуществлять проще и дешевле, чем большинство типов кибератак.
6. Атаки DDoS обычно провоцируют перегрузку в критической инфраструктуре медиа компаний, что ведет к недоступности их услуг (веб-сайтов, радио- и телепрограмм).

Рекомендует:

Предпринять в каждой медиа компании следующие меры безопасности.

1. **Детективная безопасность** в форме непрерывного мониторинга пропускной способности (нагрузка на системный ЦП, нагрузка входного трафика и т.д.), типа трафика и любой критической инфраструктуры и службы (например, файрволы и т.д.) в целях улучшения функций обнаружения кибератак.
2. **Превентивные меры безопасности,** например:
   a. Сегментация внутренних сетей во внешние и любой сети, содержащей критические системы вещания.
   b. Сканирование (предпочтительно автоматическое) и корректировка потенциальных мест уязвимости DOS в службах с выходом в интернет.
   c. Балансировка нагрузки.
   d. Наличие надлежащих инструментов и процедур для реагирования на атаки.
   e. Определение соглашения об уровне защиты DDoS со своим ISP ***(ISP- Internet Service Provider – провайдер интернет услуг – прим. переводчика)***.
3. **Корректирующие меры безопасности** (минимум одна, желательно больше), например:
   a. Службы защиты DDoS, позволяющие очистку трафика (могут на базе внешнего ISP или сторонней организации).
   b. IШлюзы безопасности внутреннего фронта, которые защищают каждую систему, доступную из интернета. Сам шлюз должен включать возможности обнаружения (и защиты DDoS).
   c. Можно рассматривать контрмеры на базе дополнительной сети, например:

      Blackholing.
      Блокировка IP адресов взломщиков.
      Остановка IP оповещений.
      Реконфигурация DNS.
      Изоляция (отключение доступа в интернет internet access) – как крайняя мера.

Примечание: Решения безопасности, имеющие защиту DDoS, обычно содержат и детективные, и корректирующие меры. В некоторых решениях могут быть и превентивные методы.

[Информативное приложение на следующей странице]

Приложение: Справочная информация об атаках DDoS и потенциальных контрмерах

Это приложение содержит высокоуровневые описания всех контрмер (детективных, превентивных и корректирующих).

1. Справка

DDoS (распределенная атака типа «отказ в обслуживании») – это сетевая попытка сделать веб-сайт, службу или всю инфраструктуру недоступными, обычно путем одновременной атаки жертвы из нескольких систем, поставленных под угрозу. Типы атак разные; самые распространенные описаны в § 3.

Медиа компании все чаще основаны на IP-производстве и часто предлагают свои услуги в интернете, что подвергает их потенциальных атакам.

Осуществлять атаки DDoS становится все дешевле и проще с технической точки зрения; и они становятся серьезной угрозой.

2. Потенциальные последствия для деятельности

Для медиа компаний, предлагающих интернет-услуги (например, веб-сайты, заказные услуги, гибридные ТВ технологии), атаки DDoS являются серьезной угрозой, поскольку, в зависимости от архитектуры инфраструктуры, успешная атака DDoS может повредить услуги, а также лежащие в их основе или подключенные инфраструктуры (например, внутренние сети).

В худшем случае атака DDoS на веб-сайт может привести к поломке внутреннего радио и ТВ оборудования, если эти системы не отделены надлежащим образом или при передаче таких услуг как DNS, AD или DHCP.

Несколько членов EBU уже испытали большой диапазон атак DDoS, которые привели к критическим повреждениям инфраструктуры и сделали интернет-услуги недоступными.

3. Тип атак DDoS (Общая часть)

DDoS включает несколько методов атаки, направленных на сетевой, сеансовый или прикладной уровень. Атаки DDoS можно грубо разделить на симметричные и асимметричные, в зависимости от симметричности генерирования и распространения нагрузки в обоих концах атаки.

При симметричных атаках взломщики должны сгенерировать полную нагрузку с собственными ресурсами и передать ее жертве. Этот тип атаки часто включает бот-сети (большое количество подключенных к интернету систем, поставленных под угрозу и работающих совместно).

При асимметричных атаках взломщик оптимизирует асимметричный характер некоторых интернет-протоколов, которые могут запускать большой ответ (количество данных) из маленького запроса (количества данных). Это ведет к малой нагрузке со стороны взломщика, но дает огромную нагрузку при отказе или потреблении критических ресурсов со стороны жертвы.

Симметричные атаки:

В зависимости от текущего вещательного контента медиа компании являются весьма уязвимыми жертвами для этой формы атак DDoS из-за малых (финансовых и технических) усилий, необходимых для их запуска. Публике доступны «инструменты хактивизма», такие как “Low Orbit Ion Canon” и другие, которые облегчают атаку; а многие веб-сайты предлагают крупномасштабные атаки DDoS на базе бот-сетей за относительно низкие суммы денег (60 Gbit/s за 25$/час).

Асимметричные атаки:

а) Отражающие / усиливающие атаки:

Эти виды атак используют тот факт, что передача небольших или деформированных запросов любому адресату приведет к ответу с гораздо большим пакетом, чем исходный запрос. Путем искажения адреса источника ответ отправляется реальному адресату хакера. Обычно такие виды атак требуют большого количества систем, которые одновременно выполняют запросы с общим искаженным адресом источника, чтобы ответы перегружали службу или сеть жертвы. Эти системы были взломаны ранее и образуют «бот-сеть», которую можно арендовать или использовать «как сервис» для атак.

b) Синхронные атаки:

При этой весьма популярной атаке взломщик посылает большой объем SYN-запросов TCP одному IP-адресату для заполнения его таблицы соединений полуоткрытых сеансов, что относительно легко выполнить. После этого поврежденный хост не может принимать новые сеансы.

c) Низкоскоростные атаки:

Эти виды атак основаны на концепции потребления множества или всех ресурсов в веб-сервере или приложении запуском регулярного запроса, например, HTTP POST, и затем работы на крайне низкой скорости (например, 1 байт /110 секунд) для завершения запроса. При таком подходе ресурсы веб-сервера будут исчерпаны за очень короткий период an времени и с очень малыми усилиями со стороны взломщика. Известные атаки этого типа – Slowloris, SLOW post и RUDY (R-U-Dead-Yet?).

d) Атаки с фрагментацией:

Лавинное заполнение систем-адресатов множеством небольших IP фрагментов, пакетами TCP-окна нулевой длины или искаженными IP фрагментами (каплями) – также популярные атаки DoS, увеличивающие потребление ЦП системы. В этом сценарии внутренние буферы и таблицы исчерпывают пределы памяти, что ведет к поломке системы, если в системе-адресате не приняты внутренние меры защиты.

e) Атаки IPv6:

С появлением IPv6 появилась и масса атак на его доступность, включая атаки “long-presumed-dead”, например, Ping-of-Death или Landattack. См. *THC IPv6 Attack Toolkit*.

f) Специализированные атаки:

Странное или неопределенное поведение протоколов или программного обеспечения – также популярная отправная точка для атак DDoS. Поскольку возможных атак великое множество, перечислим лишь несколько самых популярных в этой категории:

- **DNS NXDOMAIN**: Лавинное заполнение DNS сервера произвольно сгенерированными несуществующими именами хостов, что ведет к колоссальной рабочей нагрузке на DNS интерпретатор, делая весь сервер недоступным.
- **SSL Renegotiation DoS**: Ведет к большой нагрузке на SSL-сервер, когда включено повторное согласование SSL, инициированное клиентом.
- **HashDoS**: Чрезвычайно эффективная и умная атака. Один специально изготовленный HTTP-POST может дезорганизовать уязвимый веб-сервер на несколько часов. Проблема состоит в том, что веб-структуры, например, PHP и многие другие, генерируют и организуют свои внутренние словари как хеш-таблицы. Эту атаку очень трудно обнаружить!
- **Apache Killer**: Уязвимые версии Apache потребляют большую часть ЦП, пытаясь вычислить специально созданные specially crafted запросы в байтовом диапазоне в HTTP 1.1.
- **HTTP Pipelining**: Неправильное применение свойств этого протокола ведет к полному насыщению веб-сервера. Несколько вредоносных клиентов, используя конвейерный режим, могут заполнить буферы сервера HTTP запросами без необходимости дожидаться ответа от сервера.
- **ReDoS**: Использует тот факт, что большинство реализаций регулярных выражений могут достигать крайних ситуаций, в результате чего работают очень медленно (что экспоненциально связано с размером входных данных).

4. Потенциальные решения

4.1 Общие решения

Есть несколько вариантов устранения последствий атаки DDoS. Некоторые из предложенных корректирующих мер безопасности могут успешно помешать атаке DDoS дойти до службы, на которую она нацелена. К сожалению, вместе с вредоносным трафиком отбрасываются и легитимные пакеты, поэтому служба недоступна для внешнего мира и атака типа «отказ в обслуживании» проходит успешно.

Если цель – сохранить доступность услуги для легитимных пользователей во время атаки, система должна точно обнаружить атаку, отличить легитимный трафик от трафика DDoS и передать в службу-адресат только легитимный трафик. Есть пара вариантов для успешного удаления трафика DDoS при сохранении приема легитимного трафика:

1. Компании с хостом или «как сервис» могут активировать свои анти-DDoS службы, при необходимости работающие «извне».
2. Локальное «внутреннее» обнаружение и устранение последствий с использованием оборудования в сети компании, которое может обнаружить и успешно устранить последствия атак DDoS.

Со вторым вариантом возможно больше решений:

- **Обнаружение с помощью информации OSI layer 4 или layer 7 information**: Для обнаружения атаки DDoS необходимо проанализировать все пакеты, назначенные для внутренней сети. Это можно сделать с помощью данных Netflow, которые дают только информацию до OSI layer 4 (*src/dst* IP и *src/dst* port) или с помощью SPAN или сбора внутренних данных, которые дают информацию до OSI layer 7 (включая, например, HTTP команды в пакете).
- **Внутриполосное или внеполосное**: Одно оборудование должно работать в полосе, что означает, что физически оно находится в канале между двумя маршрутизаторами. Другое оборудование может использоваться вне полосы. Оно собирает данные с помощью Flow или SPAN и может выделить из них потенциально вредный трафик.

Все эти варианты имеют плюсы и минусы («за» и «против») и различаются в разных сетевых дизайнах и решениях.

4.2. Примеры опробованных решений для медиа компаний

4.2.1 Решение 1 – на базе внешнего ISP

Многие ISP (провайдеры интернет-услуг) обеспечивают функции защиты или обнаружения DDoS как добавки к свои интернет-услугам. Следующее высокоуровневое решение основано на типичной платформе защиты DDoS, которая состоит из двух основных систем:

1) Коллектор Netflow

Контролирует внутриполосный и внеполосный трафик на основе данных Netflow. Путем настройки на подходящую частоту дискретизации коллектор может создавать типичный базовый профиль трафика, который использует для создания оповещений при обнаружении отличающегося трафика.

2) Система управления угрозами (TMS - The Threat Management System)

TMS использует несколько технологий фильтрации для «отмывки» трафика. (Например, передача определенных типов сообщений ICMP или искаженных пакетов http).

Рис. 1: Решение на базе внешнего ISP

Для вещательной сети базовый трафик может быть слишком неспецифическим, т.к. загрузка большого фильма в файле может быть ошибочно обнаружена как DoS, или в случае прямой спортивной трансляции передача потока может потреблять гораздо больше трафика, чем указано в базовом профиле трафика.

Поэтому лучшим решением является мониторинг конечных устройств и систем. Эти системы могут быть маршрутизаторами, файрволами, а также http серверами. Если потребление ЦП или таблицы маршрутов выглядят подозрительно, основной причиной может быть атака DoS или DDoS.

В процессе решения проблем и инцидентов Netflow Collector – лишь дополнительный источник информации. Если исследование показывает присутствие атаки DDoS, менеджер инцидентов может обратиться к TMS и активировать специальные меры для фильтрации трафика.

В случае двойной установки (с использованием более одного ISP) весь входящий и выходящий трафик необходимо перемаршрутизировать через сеть ISP, который является хостом системы TMS, для устранения последствий атаки.

Рис. 2: Устранение последствий атаки в сценарии с двумя провайдерами

Шаблоны устранения последствий могут быть предопределены для повышения эффективности фильтрации для сценария атаки. Когда устранение последствий активно, сеть вещателя принимает и передает чистый трафик.

Перед активацией такого устранения последствий необходимо учесть, что может отфильтровываться и хороший трафик и что сама система TMS имеет ограничение полосы пропускания. Общее решение лучше считать решением «непрерывности услуг», т.к. оно поддерживает и сеть, и услуги, которые находятся внутри сети вещателя онлайн. Постоянно активировать TMS невозможно.

«За»:

Решение осуществляется так, что вредоносный трафик можно изолировать и отфильтровать, прежде чем он войдет в периметр внутренней сети. Кроме того, внешний партнер может больше знать о защите DDoS, т.к. услуга обычно предлагается нескольким абонентам. Это помогает снизить расходы на эксплуатацию и персонал.

«Против»:

Поскольку медиа трафик всегда разный, решения на базе ISP часто производят огромное количество ложных результатов. Необходим мониторинг самой службы. В зависимости от решения он не может быть активирован все время, а активируется только для поддержания услуг в случае инцидента. В случае долговременного поражения сети вещателя DDoS необходимо разработать и применить дополнительные контрмеры.

4.2.2 Решение 2 – Внутри организации

Это решение основано на локальном устранении последствий DDoS. Весь процесс обнаружения и очистки трафика производится внутри сети вещателя. Установка состоит из одного устройства, которое находится вне полосы на уровне сети Internet Edge:

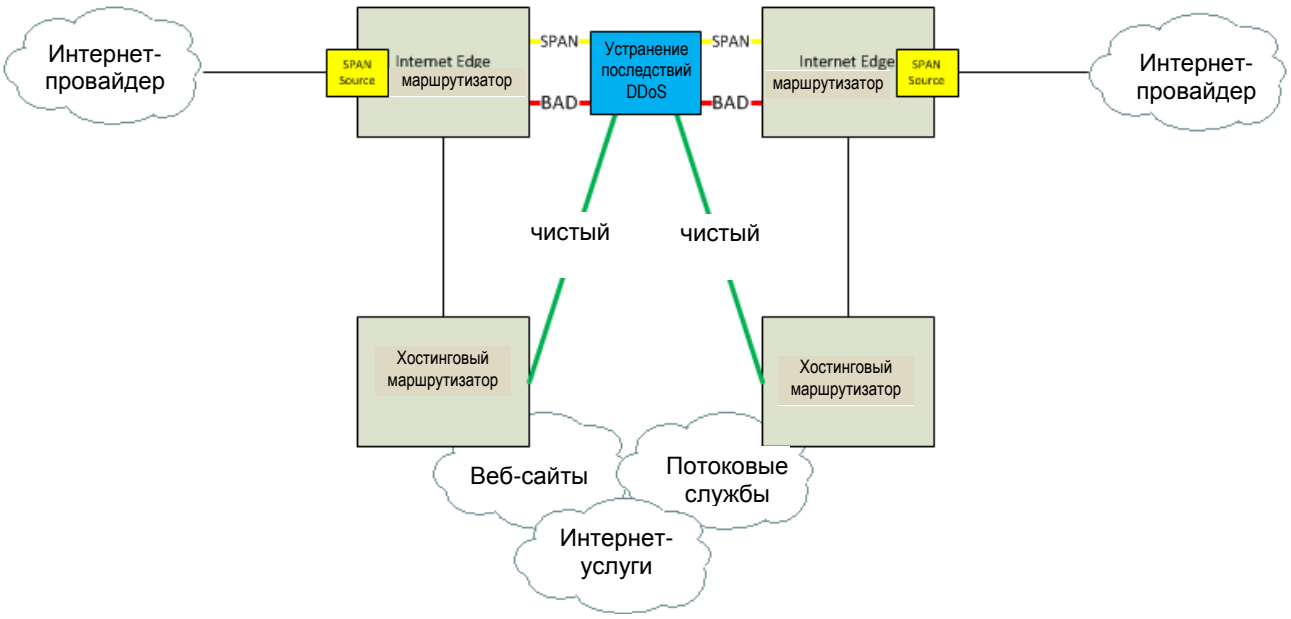

Рис. 3: Решение внутри организации с маршрутизаторами internet Edge

Обнаружение:

Устройство принимает информацию трафика через порты SPAN. Весь входящий трафик дублируется в механизме Detection устройства устранения последствий DDoS. Исходящий трафик дублировать не нужно, т.к. входящие пакеты содержат достаточно информации для определения, идет ли в данный момент атака DDoS.

Прибор сохраняет профиль каждого IP адреса, который он защищает. С помощью такой информации как «максимум новых соединений в секунду» или «максимум HTTP GET в секунду» он создает базу для определенной услуги. Пока трафик ниже базы, атаки нет. Прибор также проверяет определенные шаблоны трафика для выявления низкоскоростных атак.

Нормальная работа:

Поскольку трафик дублируется только в прибор, весь трафик продолжает идти обычным путем. Это значит, что устройство устранения последствий некритично к повседневным операциям сети и легко в обслуживании.

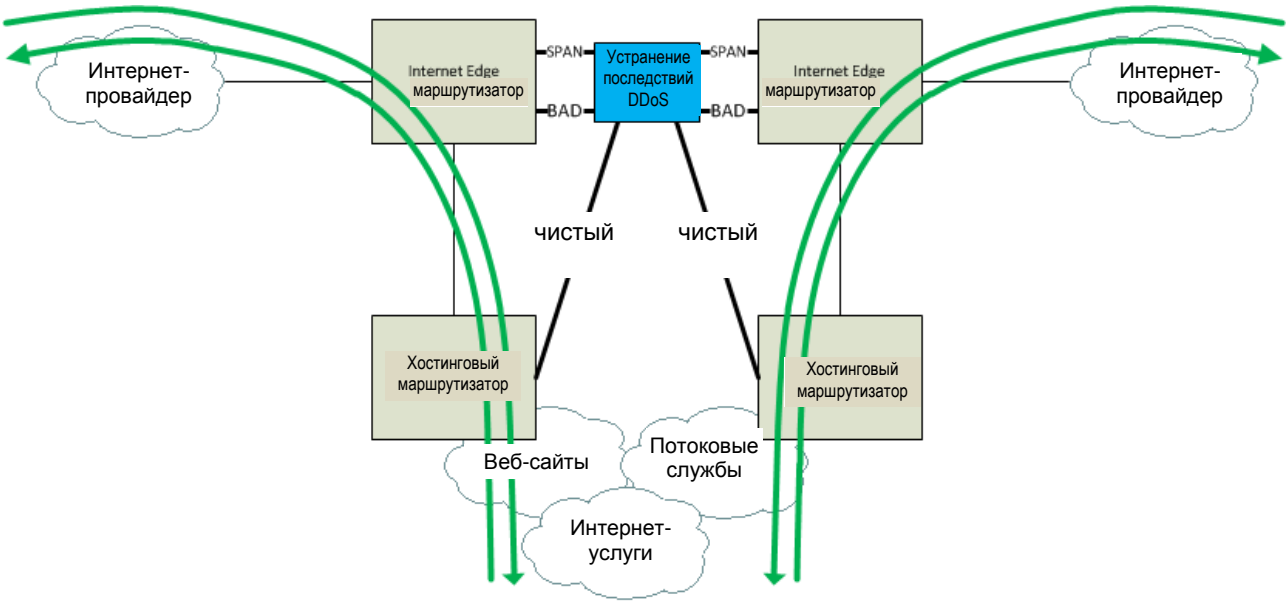

Рис. 4: Нормальная маршрутизация трафика с устройством мониторинга дублированных данных

DDoS:

Если прибор обнаружит (возможную) атаку DDoS, он определяет атакуемый IP адрес и передает обновление маршрута для данного IP адреса в маршрутизаторы Internet Edge через BGP (Border Gateway Protocol). Весь трафик для этого IP адреса (и DDoS, и легитимный) направляется из маршрутизатора Internet Edge в чистящий механизм прибора. Пакеты DDoS отбрасываются, а чистый трафик направляется в службу-адресат по отдельным выделенным каналам.

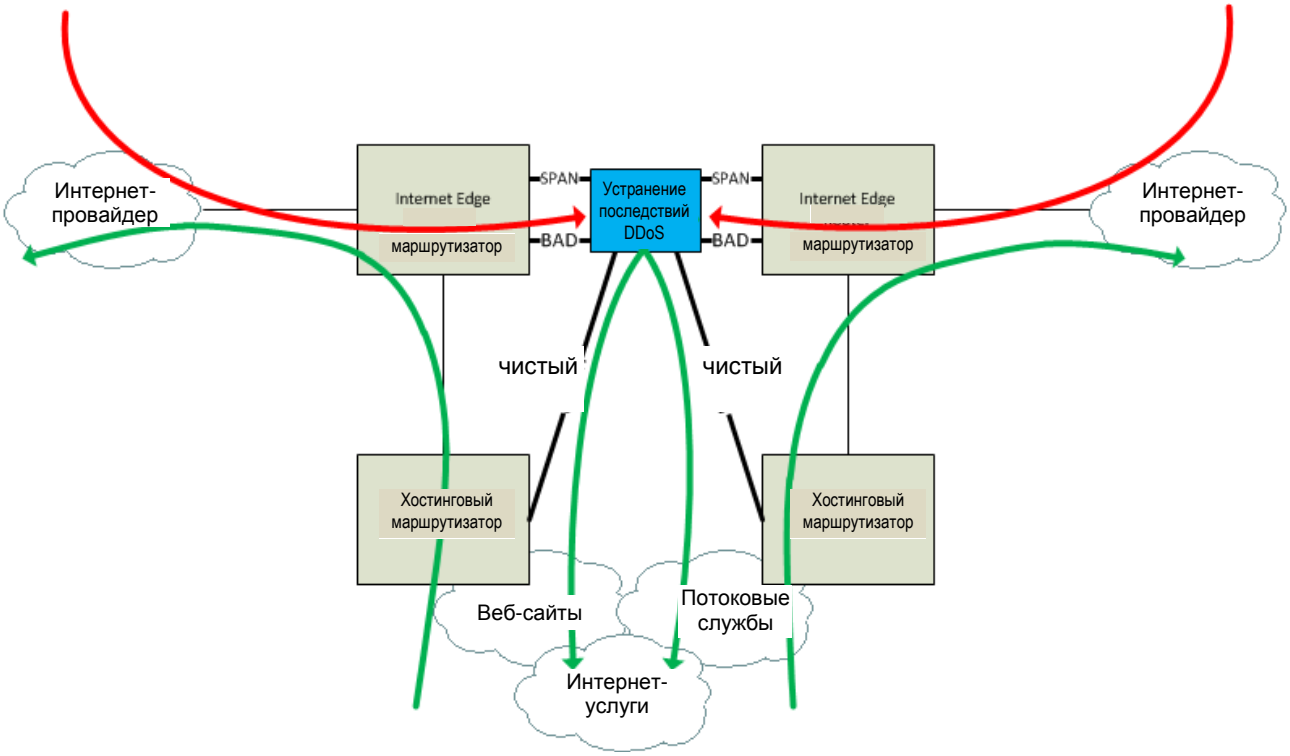

Рис. 5: Маршрутизация трафика через устройство во время атаки DDoS

Если прибор определяет, что IP адрес уже не атакуется (определенные пороги уже не превышены), он аннулирует обновление маршрута, и трафик возвращается на обычный тракт.

«За»:

- В этой установке инженеры имеют полный контроль над настройками, порогами и трактами в сети.
- Поскольку весь трафик внутренний, инженеры могут специально направить через устройство один IP адрес. Решения на базе внешних BGP должны направлять всю подсеть из 255 или более адресов для приема трафика для одного IP адреса. Это свойственно для обмена префиксами между ISP в Интернете.
- Размещение вне полосы облегчает обслуживание устройства.
- Ложные результаты атак DDoS (прибор обнаруживает атаку, но на самом деле весь трафик легитимный) направляются через механизм очистки и в службы-адресаты без особого снижения производительности, т.к. весь трафик внутренний.

«Против»:

- Потенциальный DDoS все равно направляется на уровень Internet Edge вещателя. Полоса пропускания на этом уровне должна быть больше самого большого потенциального DDoS.

Гибридная установка, например, с использованием данной локальной установки для ежедневных атак и решения на базе внешнего ISP или третьей стороны для более серьезных атак может помочь в устранении последствий крупных атак.

4.2.3 Решение 3 – на базе третьей стороны

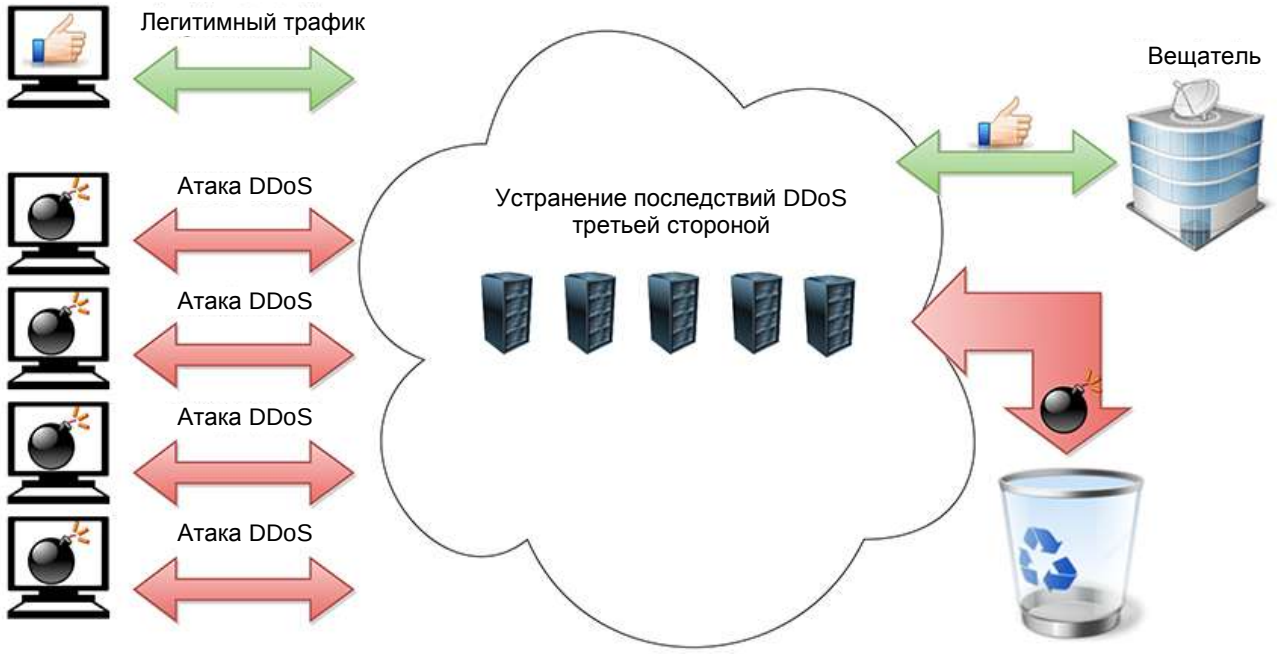

Рис. 6: Устранение последствий третьей стороной

Еще одно решение может включать аренду службы устранения последствий DDoS у стороннего провайдера с облачными центрами очистки в магистральной сети. Атаки DDoS пытаются сделать службу или сетевой ресурс недоступными, оптимизируя скоординированные действия бот-сетей из поврежденных компьютеров. Такой провайдер может устранить большой объем потоков DDoS в собственной базовой сети и гарантировать сохранение нормального трафика. Вещатели уязвимы, когда атаки вредоносного трафика поглощают полосу пропускания, т.к. это влияет на способность публикации.

Центр безопасности поставщика обнаруживает аномалии сетевого трафика поиском типичных сигнатур при мониторинге трафика. Атаки DDoS можно устранить на каждом сетевом уровне или обычно на 3-7уровнях ISO, в зависимости от поставщика.

Абонент может определить, какие IP-диапазоны или подсети надо контролировать. Также важно определить уровни трафика, откуда идут аварийные сигналы. В соглашении должно быть четко указано, когда следует уведомлять вещателя и контакты для передачи оповещений. Также можно согласовать, чтобы устранение последствий начиналось автоматически при определенных порогах.

«За»:

Это решение с «платой за устранение последствий» может быть экономичным по сравнению с покупкой или арендой оборудования. Некоторые атаки такие слабые, что нет смысла справляться с ними такими средствами. Однако некоторые объемные атаки DDoS могут быть слишком серьезными для устранения на предприятии.

«Против»:

Недостаток арендования службы в том, что это коллективный ресурс, не предназначенный для эксклюзивного пользования одним абонентом. Отдельное локальное или внутреннее устройство очистки дает больше контроля. Устранение последствий также может начаться быстрее, если вещатель займется обнаружением самостоятельно.