

DDoS-атаки и как от них защищаться. Систематизация мирового и российского опыта

Автор: Илья Яблонко, CISSP, ведущий инженер отдела систем и методов обеспечения информационной безопасности департамента системной интеграции компании Микротест.

Статья опубликована в рамках конкурса "Формула связи".

Введение

Сразу оговорюсь, что когда я писал данный обзор, я прежде всего ориентировался на аудиторию, разбирающуюся в специфике работы операторов связи и их сетей передачи данных. В данной статье излагаются основные принципы защиты от DDoS атак, история их развития в последнее десятилетие, и ситуация в настоящее время.

Что такое DDoS?

Наверное, о том, что такое DDoS-атаки, сегодня знает если не каждый "пользователь", то уж во всяком случае – каждый "АйТишник". Но пару слов всё же необходимо сказать.

DDoS-атаки (Distributed Denial of Service – распределённые атаки класса "отказ в обслуживании") – это атаки на вычислительные системы (сетевые ресурсы или каналы связи), имеющие целью сделать их недоступными для легитимных пользователей. DDoS-атаки заключаются в одновременной отправке в сторону определенного ресурса большого количества запросов с одного или многих компьютеров, расположенных в сети Интернет. Если тысячи, десятки тысяч или миллионы компьютеров одновременно начнут посылать запросы в адрес определенного сервера (или сетевого сервиса), то либо не выдержит сервер, либо не хватит полосы пропускания канала связи к этому серверу. В обоих случаях, пользователи сети Интернет не смогут получить доступ к атакуемому серверу, или даже ко всем серверам и другим ресурсам, подключенным через заблокированный канал связи.

Некоторые особенности DDoS-атак

Против кого и с какой целью запускаются DDoS-атаки?

DDoS-атаки могут быть запущены против любого ресурса, представленного в сети Интернет. Наибольший ущерб от DDoS-атак получают организации, чей бизнес непосредственно связан с присутствием в Интернет – банки (предоставляющие услуги Интернет-банкинга), интернет-магазины, торговые площадки, аукционы, а также другие виды деятельности, активность и эффективность которых существенно зависит от представительства в Интернет (турфирмы, авиакомпании, производители оборудования и программного обеспечения, и т.д.) DDoS-атаки регулярно запускаются против ресурсов таких гигантов мировой IT-индустрии, как IBM, Cisco Systems, Microsoft и других. Наблюдались массированные DDoS-атаки против eBay.com, Amazon.com, многих известных банков и организаций.

Очень часто DDoS-атаки запускаются против web-представительств политических организаций, институтов или отдельных известных личностей. Многим известно про массированные и длительные DDoS-атаки, которые запускались против web-сайта президента Грузии во время грузино-осетинской войны 2008 года (web-сайт был недоступен в течение нескольких месяцев, начиная с августа 2008 года), против серверов правительства Эстонии (весной 2007 года, во время беспорядков, связанных с переносом Бронзового солдата), про периодические атаки со стороны северокорейского сегмента сети Интернет против американских сайтов.

Основными целями DDoS-атак являются либо извлечение выгоды (прямой или косвенной) путём шантажа и вымогательства, либо преследование политических интересов, нагнетание ситуации, месть.

Каковы механизмы запуска DDoS-атак?

Наиболее популярным и опасным способом запуска DDoS-атак является использование ботнетов (BotNets). Ботнет – это множество компьютеров, на которых установлены специальные программные закладки (боты), в переводе с английского ботнет – это сеть ботов. Боты как правило разрабатываются хакерами индивидуально для каждого ботнета, и имеют основной целью отправку запросов в сторону определенного ресурса в Интернет по команде, получаемой с сервера управления ботнетом – Botnet Command and Control Server. Сервером управления ботнетом управляет хакер, либо лицо, купившее у хакера данный ботнет и возможность запускать DDoS-атаку. Боты распространяются в сети Интернет различными способами, как правило – путем атак на компьютеры, имеющие уязвимые сервисы, и установки на них программных закладок, либо путем обмана

пользователей и принуждения их к установке ботов под видом предоставления других услуг или программного обеспечения, выполняющего вполне безобидную или даже полезную функцию. Способов распространения ботов много, новые способы изобретаются регулярно.

Если ботнет достаточно большой – десятки или сотни тысяч компьютеров – то одновременная отправка со всех этих компьютеров даже вполне легитимных запросов в сторону определённого сетевого сервиса (например, web-сервиса на конкретном сайте) приведет к исчерпанию ресурсов либо самого сервиса или сервера, либо к исчерпанию возможностей канала связи. В любом случае, сервис будет недоступен пользователям, и владелец сервиса понесет прямые, косвенные и репутационные убытки. А если каждый из компьютеров отправляет не один запрос, а десятки, сотни или тысячи запросов в секунду, то ударная сила атаки увеличивается многократно, что позволяет вывести из строя даже самые производительные ресурсы или каналы связи.

Некоторые атаки запускаются более "безобидными" способами. Например, флэш-моб пользователей определенных форумов, которые по договоренности запускают в определенное время "пинги" или другие запросы со своих компьютеров в сторону конкретного сервера. Другой пример – размещение ссылки на web-сайт на популярных Интернет-ресурсах, что вызывает наплыв пользователей на целевой сервер. Если "фейковая" ссылка (внешне выглядит как ссылка на один ресурс, а на самом деле ссылается на совершенно другой сервер) ссылается на web-сайт небольшой организации, но размещена на популярных серверах или форумах, такая атака может вызвать нежелательный для данного сайта наплыв посетителей. Атаки последних двух типов редко приводят к прекращению доступности серверов на правильно организованных хостинг-площадках, однако такие примеры были, и даже в России в 2009 году.

Помогут ли традиционные технические средства защиты от DDoS-атак?

Особенностью DDoS-атак является то, что они состоят из множества одновременных запросов, из которых каждый в отдельности вполне "легален", более того – эти запросы посылают компьютеры (зараженные ботами), которые вполне себе могут принадлежать самым обычным реальным или потенциальным пользователям атакуемого сервиса или ресурса. Поэтому правильно идентифицировать и отфильтровать именно те запросы, которые составляют DDoS-атаку, стандартными средствами очень сложно. Стандартные системы класса IDS/IPS (Intrusion Detection / Prevention System – система обнаружения / предотвращения сетевых атак) не найдут в этих запросах "состава преступления", не поймут, что они являются частью атаки, если только они не выполняют качественный анализ аномалий трафика. А если даже и найдут, то отфильтровать ненужные запросы тоже не так просто – стандартные межсетевые экраны и маршрутизаторы фильтруют трафик на основании четко определяемых списков доступа (правил контроля), и не умеют "динамически" подстраиваться под профиль конкретной атаки. Межсетевые экраны могут регулировать потоки трафика, основываясь на таких критериях, как адреса отправителя, используемые сетевые сервисы, порты и протоколы. Но в DDoS-атаке принимают участие обычные пользователи Интернет, которые отправляют запросы по наиболее распространенным протоколам – не будет же оператор связи запрещать всем и всё подряд? Тогда он просто прекратит оказывать услуги связи своим абонентам, и прекратит обеспечивать доступ к обслуживаемым им сетевым ресурсам, чего, собственно, и добивается инициатор атаки.

Многим специалистам, наверное, известно о существовании специальных решений для защиты от DDoS-атак, которые заключаются в обнаружении аномалий в трафике, построении профиля трафика и профиля атаки, и последующем процессе динамической многостадийной фильтрации трафика. И об этих решениях я тоже расскажу в этой статье, но несколько попозже. А сначала будет рассказано о некоторых менее известных, но иногда достаточно эффективных мерах, которые могут приниматься для подавления DDoS-атак существующими средствами сети передачи данных и её администраторов.

Защита от DDoS-атак имеющимися средствами

Существует довольно много механизмов и "хитростей", позволяющих в некоторых частных случаях подавлять DDoS-атаки. Некоторые могут использоваться, только если сеть передачи данных построена на оборудовании какого-то конкретного производителя, другие более или менее универсальные.

Начнем с рекомендаций Cisco Systems. Специалисты этой компании рекомендуют обеспечить защиту фундамента сети ([Network Foundation Protection](#)), которая включает защиту уровня администрирования сетью (Control Plane), уровня управления сетью (Management Plane), и защиту уровня данных в сети (Data Plane).

Защита уровня администрирования (Management Plane)

Термин "уровень администрирования" охватывает весь трафик, который обеспечивает управление

или мониторинг маршрутизаторов и другого сетевого оборудования. Этот трафик направляется в сторону маршрутизатора, или исходит от маршрутизатора. Примерами такого трафика являются Telnet, SSH и http(s) сессии, syslog-сообщения, SNMP-трапы. Общие best practices включают:

- обеспечение максимальной защищенности протоколов управления и мониторинга, использование шифрования и аутентификации:

- протокол [SNMP v3](#) предусматривает средства защиты, в то время как SNMP v1 практически не предусматривает, а SNMP v2 предусматривает лишь частично--установленные по умолчанию значения Community всегда нужно менять;
- должны использоваться различные значения для public и private community;
- протокол telnet передает все данные, в том числе логин и пароль, в открытом виде (если трафик перехватывается, эта информация легко может быть извлечена и использована), вместо него рекомендуется всегда использовать протокол ssh v2;
- аналогично, вместо http используйте https для доступа к оборудованию; строгий контроль доступа к оборудованию, включая адекватную парольную политику, централизованные аутентификацию, авторизацию и аккаунтинг (модель AAA) и локальной аутентификации с целью резервирования;

- реализацию ролевой модели доступа;

- контроль разрешенных подключений по адресу источника с помощью списков контроля доступа;

- отключение неиспользуемых сервисов, многие из которых включены по-умолчанию (либо их забыли отключить после диагностики или настройки системы);

- мониторинг использования ресурсов оборудования.

На последних двух пунктах стоит остановиться более подробно.

Некоторые сервисы, которые включены по умолчанию или которые забыли выключить после настройки или диагностики оборудования, могут быть использованы злоумышленниками для обхода существующих правил безопасности. Список этих сервисов ниже:

- [Cisco Discovery Protocol](#);
- Directed Broadcasts;
- Finger;
- Maintenance Operations Protocol;
- IP BOOTP Server;
- IP Redirects;
- IP Source Routing;
- PAD (packet assembler/disassembler);
- Proxy ARP;
- [TCP and UDP small services](#);

Естественно, перед тем как отключать данные сервисы, нужно тщательно проанализировать отсутствие их необходимости в вашей сети.

Желательно осуществлять мониторинг использования ресурсов оборудования. Это позволит, во первых, вовремя заметить перегруженность отдельных элементов сети и принять меры по предотвращению аварии, и во вторых, обнаружить DDoS-атаки и аномалии, если их обнаружение не предусмотрено специальными средствами. Как минимум, рекомендуется осуществлять мониторинг:

- загрузки процессора
- использования памяти
- загрузки интерфейсов маршрутизаторов.

Мониторинг можно осуществлять "вручную" (периодически отслеживая состояние оборудования), но лучше конечно это делать специальными системами мониторинга сети или мониторинга информационной безопасности (к последним относится Cisco MARS).

Защита уровня управления (Control Plane)

Уровень управления сетью включает весь служебный трафик, который обеспечивает функционирование и связность сети в соответствии с заданной топологией и параметрами. Примерами трафика уровня управления являются: весь трафик, генерируемый или предназначенный для процессора маршрутизации (route processor – RR), в том числе все протоколы маршрутизации, в некоторых случаях – протоколы SSH и SNMP, а также ICMP. Любая атака на функционирование процессора маршрутизации, а особенно – DDoS-атаки, могут повлечь существенные проблемы и перебои в функционировании сети. Ниже описаны best practices для защиты уровня управления.

Control Plane Policing

Заключается в использовании механизмов QoS (Quality of Service - качество обслуживания) для предоставления более высокого приоритета трафику уровня управления, чем пользовательскому трафику (частью которого являются и атаки). Это позволит обеспечить работу служебных протоколов и процессора маршрутизации, то есть сохранить топологию и связность сети, а также собственно маршрутизацию и коммутацию пакетов.

IP Receive ACL

Данный функционал позволяет осуществлять фильтрацию и контроль служебного трафика, предназначенного для маршрутизатора и процессора маршрутизации.

IP Receive ACL:

- применяются уже непосредственно на маршрутизирующем оборудовании перед тем, как трафик достигает процессора маршрутизации, обеспечивая "персональную" защиту оборудования;
- применяются уже после того, как трафик прошел обычные списки контроля доступа – являются последним уровнем защиты на пути к процессору маршрутизации;
- применяются ко всему трафику (и внутреннему, и внешнему, и транзитному по отношению к сети оператора связи).

Infrastructure ACL

Обычно, доступ к собственным адресам маршрутизирующего оборудования необходим только для хостов собственной сети оператора связи, однако бывают и исключения (например, eBGP, GRE, туннели IPv6 over IPv4, и ICMP). Инфраструктурные списки контроля доступа:

- обычно устанавливаются на границе сети оператора связи ("на входе в сеть");
- имеют целью предотвратить доступ внешних хостов к адресам инфраструктуры оператора;
- обеспечивают беспрепятственный транзит трафика через границу операторской сети;
- обеспечивают базовые механизмы защиты от несанкционированной сетевой активности, описанные в RFC 1918, RFC 3330, в частности, защиту от спуфинга (spoofing, использование поддельных IP адресов источника с целью маскировки при запуске атаки).

Neighbour Authentication

Основная цель аутентификации соседних маршрутизаторов – предотвращение атак, заключающихся в отсылке поддельных сообщений протоколов маршрутизации с целью изменить маршрутизацию в сети. Такие атаки могут привести к несанкционированному проникновению в сеть, несанкционированному использованию сетевых ресурсов, а также к тому, что злоумышленник перехватит трафик с целью анализа и получения необходимой информации.

Рекомендуется всегда, когда это возможно, обеспечивать аутентификацию хостов, с которыми производится обмен служебными данными либо трафиком управления.

Настройка BGP

При работе с протоколом BGP рекомендуется использовать следующие механизмы защиты:

- фильтрация префиксов BGP (BGP prefix filters) – используется для того, чтобы информация о маршрутах внутренней сети оператора связи не распространялась в Интернет (иногда эта информация может оказаться очень полезной для злоумышленника);
- ограничение количества префиксов, которые могут быть приняты от другого маршрутизатора (prefix limiting) – используется для защиты от DDoS атак, аномалий и сбоя в сетях пиринг-партнеров;
- использование параметров BGP Community и фильтрация по ним также могут использоваться для ограничения распространения маршрутной информации;
- мониторинг BGP и сопоставление данных BGP с наблюдаемым трафиком является одним из механизмов раннего обнаружения DDoS-атак и аномалий;
- фильтрация по параметру TTL (Time-to-Live) – используется для проверки BGP-партнёров.

Если атака по протоколу BGP запускается не из сети пиринг-партнера, а из более удаленной сети, то параметр TTL у BGP-пакетов будет меньшим, чем 255. Можно сконфигурировать граничные маршрутизаторы оператора связи так, чтобы они отбрасывали все BGP пакеты со значением TTL < 255, а маршрутизаторы пиринг-партнеров наоборот – чтобы они генерировали только BGP-пакеты с параметром TTL=255. Так как TTL при каждом хопе маршрутизации уменьшается на 1, данный нехитрый приём позволит легко избежать атак из-за границ вашего пиринг-партнера.

Защита уровня данных в сети (Data Plane)

Несмотря на важность защиты уровней администрирования и управления, большая часть трафика в сети оператора связи – это данные, транзитные или же предназначенные для абонентов данного оператора.

Unicast Reverse Path Forwarding (uRPF)

Нередко атаки запускаются с использованием технологии спуфинга (spoofing) – IP-адреса источника фальсифицируются с тем, чтобы источник атаки невозможно было отследить. Фальсифицированные IP-адреса могут быть:

- из реально используемого адресного пространства, но в другом сегменте сети (в том сегменте, откуда была запущена атака, данные поддельные адреса не маршрутизируются);
- из неиспользуемого в данной сети передачи данных адресного пространства;
- из адресного пространства, не маршрутизируемого в сети Интернет.

Реализация на маршрутизаторах механизма uRPF позволит предотвратить маршрутизацию пакетов с адресами источника, несовместимыми или неиспользуемыми в сегменте сети, из которого они поступили на интерфейс маршрутизатора. Данная технология позволяет иногда достаточно эффективно отфильтровать нежелательный трафик наиболее близко к его источнику, то есть наиболее эффективно. Многие DDoS-атаки (включая известные Smurf и Tribal Flood Network) используют механизм спуфинга и постоянной смены адресов источника для того, обмануть стандартные средства защиты и фильтрации трафика.

Использование механизма uRPF операторами связи, предоставляющим абонентам доступ в Интернет, позволит эффективно предотвратить DDoS-атаки с применением технологии спуфинга, направленные со стороны собственных абонентов против Интернет-ресурсов. Таким образом, DDoS-атака подавляется наиболее близко к её источнику, то есть наиболее эффективно.

Remotely Triggered Blackholes (RTBH)

Управляемые черные дыры (Remotely Triggered Blackholes) используются для "сбрасывания" (уничтожения, отправления "в никуда") трафика, поступающего в сеть, путем маршрутизации данного трафика на специальные интерфейсы Null 0. Данную технологию рекомендуется использовать на границе сети для сброса содержащего DDoS-атаку трафика при его поступлении в сеть. Ограничением (причем существенным) данного метода является то, что он применяется ко всему трафику, предназначенному для определенного хоста или хостов, являющимися целью атаки. Таким образом, данный метод может использоваться в случаях, когда массовой атаке подвергается один или несколько хостов, что вызывает проблемы не только для атакуемых хостов, но также и для других абонентов и сети оператора связи в целом.

Управление черными дырами может осуществляться как вручную, так и посредством протокола BGP.

QoS Policy Propagation Through BGP (QPPB)

Управление QoS через BGP (QPPB) позволяет управлять политиками приоритета для трафика, предназначенного определенной автономной системе либо блоку IP-адресов. Данный механизм может оказаться очень полезен для операторов связи и крупных предприятий, в том числе и для управления уровнем приоритета для нежелательного трафика или трафика, содержащего DDoS-атаку.

Sink Holes

В некоторых случаях требуется не полностью удалять трафик с использованием черных дыр, а отводить его в сторону от основных каналов или ресурсов для последующего мониторинга и анализа. Именно для этого и предназначены "отводные каналы" или Sink Holes.

Sink Holes используются чаще всего в следующих случаях:

- для отвода в сторону и анализа трафика с адресами назначения, которые принадлежат адресному пространству сети оператора связи, но при этом реально не используются (не были выделены ни оборудованию, ни пользователям); такой трафик является априори подозрительным, так как зачастую свидетельствует о попытках просканировать или проникнуть в вашу сеть злоумышленником, не имеющим подробной информации о её структуре;
- для перенаправления трафика от цели атаки, являющейся реально функционирующим в сети оператора связи ресурсом, для его мониторинга и анализа.

Защита от DDoS с использованием специальных средств

Концепция Cisco Clean Pipes - родоначальник отрасли

Современную концепцию защиты от DDoS-атак разработала (да, да, вы не удивитесь! :)) компания Cisco Systems. Разработанная Cisco концепция получила название Cisco Clean Pipes ("очищенные каналы"). В детально разработанной уже почти 10 лет назад концепции довольно подробно описывались основные принципы и технологии защиты от аномалий в трафике, большая часть которых используется и сегодня, в том числе другими производителями.

Концепция Cisco Clean Pipes предполагает следующие принципы обнаружения и подавления DDoS-атак.

Выбираются точки (участки сети), трафик в которых анализируется на предмет выявления аномалий. В зависимости от того, что мы защищаем, такими точками могут являться пиринг-соединения оператора связи с вышестоящими операторами, точки подключения нижестоящих операторов или абонентов, каналы подключения центров обработки данных к сети.

Специальные детекторы анализируют трафик в этих точках, строят (изучают) профиль трафика в его нормальном состоянии, при появлении DDoS-атаки или аномалии – обнаруживают её, изучают и динамически формируют её характеристики. Далее, информация анализируется оператором системы, и в полуавтоматическом или автоматическом режиме запускается процесс подавления атаки. Подавление заключается в том, что трафик, предназначенный "жертве", динамически перенаправляется через устройство фильтрации, на котором к этому трафику применяются фильтры, сформированные детектором и отражающие индивидуальный характер этой атаки. Очищенный трафик вводится в сеть и отправляется получателю (потому и возникло название Clean Pipes – абонент получает "чистый канал", не содержащий атаку).

Таким образом, весь цикл защиты от DDoS-атак включает следующие основные стадии:

- Обучение контрольным характеристикам трафика (профилирование, Baseline Learning)
- Обнаружение атак и аномалий (Detection)
- Перенаправление трафика с целью его пропуска через устройство очистки (Diversion)
- Фильтрация трафика с целью подавления атак (Mitigation)
- Ввод трафика обратно в сеть и отправка адресату (Injection).

Одновременно с этим рекомендуется использовать предусмотренные концепцией Network Foundation Protection механизмы защиты инфраструктуры сети, что позволит повысить уровень защищенности в целом.

Cisco DDoS Protection Solution	Detection	Diversion / Injection	Mitigation
	Идентифицировать и классифицировать атаки на основании характеристик трафика	Перенаправить весь трафик, предназначенный определенной цели; вернуть очищенный трафик обратно в сеть чтобы он достиг цели	Анализ трафика и удаление пакетов DDoS-атаки
Network Foundation Protection Защита фундамента сети			

Несколько особенностей.

В качестве детекторов могут использоваться два типа устройств:

- Детекторы производства Cisco Systems – сервисные модули Cisco Traffic Anomaly Detector Services Module, предназначенные для установки в шасси Cisco 6500/7600.
- Детекторы производства Arbor Networks – устройства Arbor Peakflow SP CP.

Ниже приведена таблица сравнения детекторов Cisco и Arbor.

Параметр	Cisco Traffic Anomaly Detector	Arbor Peakflow SP CP
Получение информации о трафике для анализа	Используется копия трафика, выделяемая на шасси Cisco 6500/7600	Используется Netflow-данные о трафике, получаемые с маршрутизаторов, допускается регулировать выборку (1 : 1, 1 : 1 000, 1 : 10 000 и т.д.)
Используемые принципы выявления	Сигнатурный анализ (misuse detection) и выявление аномалий (dynamic profiling)	Преимущественно выявление аномалий; сигнатурный анализ используется, но сигнатуры имеют общий характер
Форм-фактор	сервисные модули в шасси Cisco 6500/7600	отдельные устройства (сервера)
Производительность	Анализируется трафик до 2 Гбит/с	Практически неограниченна (можно уменьшать частоту выборки)
Масштабируемость	Установка до 4 модулей Cisco Detector SM в одно шасси (однако модули действуют независимо друг от друга)	Возможность использования нескольких устройств в рамках единой системы анализа, одному из которых присваивается статус Leader
Мониторинг трафика и маршрутизации в сети	Функционал практически отсутствует	Функционал очень развит. Многие операторы связи покупают Arbor Peakflow SP из-за глубокого и проработанного функционала по мониторингу трафика и маршрутизации в сети

Предоставление портала (индивидуального интерфейса для абонента, позволяющего мониторить только относящуюся непосредственно к нему часть сети)	Не предусмотрено	Предусмотрено. Является серьезным преимуществом данного решения, так как оператор связи может продавать индивидуальные сервисы по защите от DDoS своим абонентам.
Совместимые устройства очистки трафика (подавления атак)	Cisco Guard Services Module	Arbor Peakflow SP TMS; Cisco Guard Services Module.
Рекомендуемые сценарии использования	Защита центров обработки данных (Data Centre) при их подключении к Интернет Мониторинг downstream-подключений абонентских сетей к сети оператора связи	Обнаружение атак на upstream-подключениях сети оператора связи к сетям вышестоящих провайдеров Мониторинг магистрали оператора связи

В последней строке таблицы приведены сценарии использования детекторов от Cisco и от Arbor, которые рекомендовались Cisco Systems. Данные сценарии отражены на приведенной ниже схеме.

В качестве устройства очистки трафика Cisco рекомендует использовать сервисный модуль Cisco Guard, который устанавливается в шасси Cisco 6500/7600 и по команде, получаемой с детектора Cisco Detector либо с Arbor Peakflow SP CP осуществляется динамическое перенаправление, очистка и обратный ввод трафика в сеть. Механизмы перенаправления – это либо BGP апдейты в сторону вышестоящих маршрутизаторов, либо непосредственные управляющие команды в сторону супервизора с использованием проприетарного протокола. При использовании BGP-апдейтов, вышестоящему маршрутизатору указывается новое значение пех-хор для трафика, содержащего атаку – так, что этот трафик попадает на сервер очистки. При этом необходимо позаботиться о том, чтобы эта информация не повлекла организацию петли (чтобы нижестоящий маршрутизатор при вводе на него очищенного трафика не пробовал снова завернуть этот трафик на устройство очистки). Для этого могут использоваться механизмы контроля распространения BGP-апдейтов по параметру community, либо использование GRE-туннелей при вводе очищенного трафика.

Такое положение дел существовало до тех пор, пока Arbor Networks существенно не расширил линейку продуктов Peakflow SP и не стал выходить на рынок с полностью самостоятельным решением по защите от DDoS-атак.

Появление Arbor Peakflow SP TMS

Несколько лет назад, компания Arbor Networks решила развивать свою линейку продуктов по защите от DDoS-атак самостоятельно и вне зависимости от темпов и политики развития данного направления у Cisco. Решения Peakflow SP CP имели принципиальные преимущества перед Cisco Detector, так как они анализировали flow-информацию с возможностью регулирования частоты выборки, а значит не имели ограничений по использованию в сетях операторов связи и на магистральных каналах (в отличие от Cisco Detector, которые анализируют копию трафика). Кроме того, серьезным преимуществом Peakflow SP явилась возможность для операторов продавать абонентам индивидуальный сервис по мониторингу и защите их сегментов сети.

Ввиду этих или других соображений, Arbor существенно расширил линейку продуктов Peakflow SP. Появился целый ряд новых устройств:

Peakflow SP TMS (Threat Management System) – осуществляет подавление DDoS-атак путем многоступенчатой фильтрации на основе данных, полученных от Peakflow SP CP и от лаборатории ASERT, принадлежащей Arbor Networks и осуществляющей мониторинг и анализ DDoS-атак в Интернете;

Peakflow SP BI (Business Intelligence) – устройства, обеспечивающие масштабирование системы, увеличивая число подлежащих мониторингу логических объектов и обеспечивая резервирование собираемых и анализируемых данных;

Peakflow SP PI (Portal Interface) – устройства, обеспечивающие увеличение абонентов, которым предоставляется индивидуальный интерфейс для управления собственной безопасностью;

Peakflow SP FS (Flow Sensor) – устройства, обеспечивающие мониторинг абонентских маршрутизаторов, подключений к нижестоящим сетям и центрам обработки данных.

Принципы работы системы Arbor Peakflow SP остались в основном такими же, как и Cisco Clean Pipes, однако Arbor регулярно производит развитие и улучшение своих систем, так что на данный момент функциональность продуктов Arbor по многим параметрам лучше, чем у Cisco, в том числе и по производительности.

На сегодняшний день, максимальная производительность Cisco Guard может быть достигнута путем создания кластера из 4-х модулей Guard в одной шасси Cisco 6500/7600, при этом полноценная кластеризация этих устройств не реализована. В то же время, верхние модели Arbor Peakflow SP TMS имеют производительность до 10 Гбит/с, и в свою очередь могут кластеризоваться.

После того, как Arbor стал позиционировать себя в качестве самостоятельного игрока на рынке систем обнаружения и подавления DDoS-атак, Cisco стала искать партнера, который бы обеспечил ей так необходимый мониторинг flow-данных о сетевом трафике, но при этом не являлся бы прямым конкурентом. Такой компанией стала Narus, производящая системы мониторинга трафика на базе flow-данных (NarusInsight), и заключившая партнерство с Cisco Systems. Однако серьезного развития и присутствия на рынке это партнерство не получило. Более того, по некоторым сообщениям, Cisco не планирует инвестиции в свои решения Cisco Detector и Cisco Guard, фактически, оставляя данную нишу на откуп компании Arbor Networks.

Некоторые особенности решений Cisco и Arbor

Стоит отметить некоторые особенности решений Cisco и Arbor.

1. Cisco Guard можно использовать как совместно с детектором, так и самостоятельно. В последнем случае он устанавливается в режим in-line и выполняет функции детектора анализируя трафик, а при необходимости включает фильтры и осуществляет очистку трафика. Минус этого режима заключается в том, что, во-первых, добавляется дополнительная точка потенциально отказа, и во-вторых, дополнительная задержка трафика (хотя она и небольшая до тех пор, пока не включается механизм фильтрации). Рекомендуются для Cisco Guard режим – ожидания команды на перенаправление трафика, содержащего атаку, его фильтрации и ввода обратно в сеть.
2. Устройства Arbor Peakflow SP TMS также могут работать как в режиме off-ramp, так и в режиме in-line. В первом случае устройство пассивно ожидает команды на перенаправление содержащего атаку трафика с целью его очистки и ввода обратно в сеть. Во втором пропускает через себя весь трафик, вырабатывает на его основе данные в формате Arborflow и передает их на Peakflow SP CP для анализа и обнаружения атак. Arborflow – это формат, похожий на Netflow, но доработанный компанией Arbor для своих систем Peakflow SP. Мониторинг трафика и выявление атак осуществляет Peakflow SP CP на основании получаемых от TMS данных Arborflow. При обнаружении атаки, оператор Peakflow SP CP дает команду на её подавление, после чего TMS включает фильтры и очищает трафик от атаки. В отличие от Cisco, сервер Peakflow SP TMS не может работать самостоятельно, для его работы требуется наличие сервера Peakflow SP CP, который производит анализ трафика.
3. Сегодня большинство специалистов сходятся во мнении, что задачи защиты локальных участков сети (например, подключение ЦОДов или подключение downstream-сетей) эффек