Не так страшен DDoS как его малюют

12 августа 2008г., Денис Батранков, консультант по информационной безопасности IBM Internet Security Systems, batrankov@ru.ibm.com

Многие считают, что защиты от DDoS атак, специально запруживающих каналы передачи данных не существует. Однако, мы в России просто про эти решения не знаем. В этой статье вы узнаете о трех типах DDoS атак и имена тех производителей и компаний, которые предлагают решения по защите от распределенных атак типа «отказ в обслуживании» направленных на заполнение пропускной способности каналов.

Источник угрозы

Представьте себе, что сейчас на ваш WEB сервер одновременно подключатся 100 тысяч человек из Интернет и попытается загрузить ее главную страницу. Хватит ли пропускной способности канала в Интернет? Как защититься от злонамеренной перегрузки ваших каналов связи?

Определения

В сети Интернет есть большое число зараженных компьютеров, которые выполняют удаленно команды, в том числе по команде могут подключаться и загружать любые страницы с любого WEB сервера. Такой управляемый компьютер называет ботом. Множество таких управляемых компьютеров называется бот сетью. Каждый такой компьютер в этой сети – зомби, который всегда готов выполнить команду своего повелителя. В составе такой бот сети может быть одновременно до нескольких сотен тысяч компьютеров.

Кто предоставляет компьютеры для бот сети

Реальные владельцы компьютеров чаще всего не подозревают, что кто-то может управлять их компьютером удаленно. Сейчас троянские программы работают незаметно и мы, не замечая этого, позволяем неизвестным людям использовать ресурсы наших компьютеров для их собственных целей. Люди, которые управляют такой большой бот сетью могут шантажировать крупные компании, владельцев интернет магазинов, интернет-казино, новостных сайтов, платежных систем и других популярных ресурсов, предлагая заплатить выкуп за то, что они не будут атаковать их при помощи своей бот сети.

Определенно, такие вычислительные ресурсы представляют явный практический интерес. Можно не только проводить DDoS атаки, но и рассылать спам или проводить распределенные вычисления, например подбор пароля. Поэтому, очень часто проводятся попытки украсть бот сеть. Чтобы зомбированный компьютер воспринял команду от хозяина нужно доказать, что ты хозяин, например при помощи пароля. Если этот пароль подобрать, то есть шанс стать хозяином небольшой стаи компьютеров. Например, это возможно для сети на основе ботов BlackEnergy, которые защищены только паролем.

Пример 1. Самые большие бот сети
Обнаружена новая бот сеть под названием Kraken, включающая порядка 400 тысяч компьютеров. Размеры бот сети превосходят всемирно известную бот сеть Storm, размер которой около 100 тысяч компьютеров. Источник: компания Damballa на конференции RSA 7.04.2008

Спросите у самого себя: а какие у меня гарантии, что мой компьютер не входит в бот сеть? Дает ли такие гарантии установленный сигнатурный антивирус? Непохоже. По статистике 40% компьютеров входящих в бот сеть имеют антивирус, который не определяет, что компьютер заражен. Дает ли гарантии установленный поведенческий антивирус или система предотвращения атак? Возможно, но многие люди даже не знают что это такое. И, слово специально, уходя с работы никогда не выключают компьютер.

Любой может стать соучастником DDoS атаки

Для того, чтобы ваш компьютер стал участником DDoS атаки совершенно необязательно, чтобы на нем была уязвимость или установлен какой-то злонамеренный код. Код для атаки может быть у вашего соседа в сети или на популярном сайте в Интернете. Так Trojan-Downloader.JS.Agent вставляет вредоносный javascript во все соседние компьютеры при помощи атаки ARP spoofing, пока они грузят странички в своим браузером из Интернет. Это может быть любой код, включая код для проведения DDoS атаки. Вот этот код в вашем браузере выполнит 10000 соединений с любым сайтом:

```
<div id="attack" style="visibility:hidden">
<script type="text/javascript">
attack_host="www.{атакуемый сайт}.com"
attack_port=80
path='index.html'
for(i=1;i<=10000;i++) { document.write('<img src="http://' + attack_host + ':' + attack_port + '/' + path + '?' + Math.random() + '">');}</script></div>
```

Если вы читаете какую-то страницу через WEB браузер, например страницу с этой статьей, и в ней будет внедрен этот javascript код, то вы становитесь соучастником DDoS атаки и 10000 раз «нападете» на выбранный автором скрипта сайт. А если эту статью прочтет 10000 человек, то на сайт уже будет осуществлено уже 100 000 000 (100 миллионов) соединений. Другой вариант, если один из пользователей вставит этот javascript в сайт, где контент сайта заполняется самими пользователями (форумы, блоги, социальные сети), то помогать в осуществлении атаки будет любой человек зашедший на сайт. Например, если это будут odnoklassniki.ru, где уже 20 миллионов пользователей, то теоретически можно осуществить атаку на сайт при помощи 200000000000 (200 миллиардов) соединений. «И это не предел». Так что вы уже представляете себе масштаб угрозы. Защищаться надо. Как владельцам сетевых ресурсов от атак, так и пользователям от того, чтобы не стать соучастниками атаки.

Пример 2: Как осуществить DoS атаку на WEB сервер при помощи двух отверток и браузера.
Запускаете Internet Explorer, вводите адрес необходимого сайта, одной отверткой фиксируете кнопку Ctrl, другой F5. Количество запросов в секунду, которые будет посылать ваш Internet Explorer может затруднить работу сайта и даже помешать другим людям посетить это же ресурс.

К DDoS атаке надо готовиться заранее

Интернет достаточно агрессивная среда, чтобы начинать в нем бизнес, не позаботившись о своей защите. Но многие компании живут в нем согласно поговорке: пока гром не грянет, мужик не перекрестится. DoS и DDoS атаки отличаются тем, что с ними невозможно бороться без предварительной подготовки. И вдобавок, и это еще хуже, с ними все равно сложно бороться, даже если вы подготовились заранее. Если сейчас страдают DNS и WEB сайты, то на подходе угроза таким все более популярным сервисам как VoIP и IPTV.

Пример 3: DDoS атака на правительственные сайты Эстонии
Атаки против эстонских правительственных сайтов начались после переноса властями статуи Бронзового солдата из центра Таллина на окраины. В результате многие правительственные сайты Эстонии перестали работать, а местная компьютерная группа быстрого реагирования была вынуждена закрыть доступ к сайтам из-за границы. Пик атак пришёлся на 8 и 9 мая 2007 года. По словам премьер-министра Эстонии, атаки представляли собой лавину запросов, иногда до 5 миллионов в секунду против обычной посещаемости 1–1,5 тыс. в день. В этой атаке обвинили Россию, тем более, что некоторые российские хакеры брали на себя ответственность за эти действия. Была ли действительно Россия источником атаки читайте в конце статьи.

К сожалению, многие сервера выставляются в Интернете даже без защиты межсетевым экраном, не говоря уже про более сложные системы защиты типа систем предотвращения атак. В итоге, в тот момент когда начинается атака, выясняется, что защищаться нечем и компании вынуждены тратить драгоценное (в момент атаки) время на простые вещи, такие как установка межсетевого экрана на сервер, установка системы предотвращения атак или переход к другому провайдеру. Но, поскольку

DDoS атаки даже с установленными системами защиты сложно остановить, а в момент атаки у вас не будет времени на выбор верного способа защиты, то вы сможете положиться только на средства защиты своего провайдера. И, как правило, в том что DDoS атака провалилась - заслуга провайдера. Именно про правильный выбор провайдера и пойдет рассказ в этой статье. Для начала давайте посмотрим более подробно какими бывают атаки типа «отказ в обслуживании».

Виды DoS атак

Существует несколько способов группирования DoS атак по типам. Одна из логичных категоризаций DoS атак находится тут http://www.niser.org.my/resources/dos_attack.pdf
Различают несколько видов DoS атак.

Разрушающие

Атаки, которые приводят к тому что устройство в сети становится полностью неработоспособно: зависает, уничтожается операционная система или конфигурация. Такие атака основаны на уязвимостях программного обеспечения атакуемых систем.

Атаки на ресурсы системы

Атаки, которые значительно снижают производительность устройств или приложений. Например к этому классу относится атака SYN Flood.

Заполнение пропускной способности каналов

В эту категорию попадают атаки, которые своей целью ставят переполнение пропускной способности каналов. Обычно для переполнения канала используются любой вид пакетов TCP, ICMP или UDP с поддельными адресами источника случайно изменяющимися в диапазоне всевозможных значений, адреса получателя в пакете точно также случайно выбирают из диапазона сети, которая находится на атакованном канале. Однако сейчас такие атаки, стали осуществляться при помощи сетей зараженных компьютеров, где адреса источников атаки настоящие, и таким образом, практически неотличимые от подключающихся компьютеров реальных пользователей.
Еще одной разновидностью DDoS атак такого типа являются DRDoS атаки (Distributed Reflection DoS), которые могут использовать как источник своей атаки любой сервер в Интернете. Идея DRDoS: любой сервер на пакет TCP с SYN флагом обязательно ответит пакетом TCP с флагами SYN+ACK. Если адресом источника в первом пакете поставить адрес жертвы, то сервер пошлет несколько TCP пакетов с флагами SYN+ACK по адресу жертвы, пока не поймет, что жертва соединения не хочет и соединения не будет. Если использовать для атаки много таких мощных серверов, отвечающих на ложные пакеты по ложному адресу, то жертва будет запружена потоком пакетов.

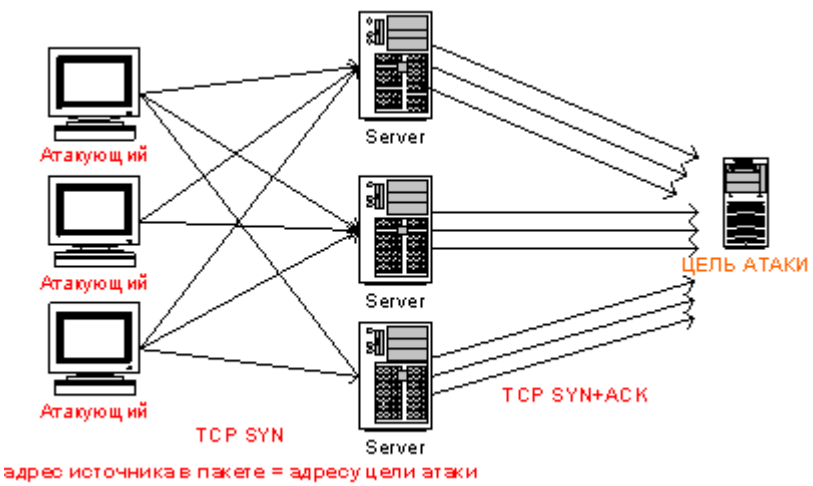


Схема работы DRDoS.

Пример 4: DDoS на Коммерсант
Генеральный директор издательского дома "Коммерсант" Демьян Кудрявцев заявил в интервью агентству "Интерфакс" 14 марта 2008 года, что финансовые потери компании, связанные с блокировкой сайта www.kommersant.ru в результате DDoS атак, исчисляются десятками или даже сотнями тысяч долларов.
Кудрявцев подчеркнул, что DDoS атаки на сайт "Коммерсанта" беспрецедентны для России: "Если известные атаки на сайты эстонского посольства, радиостанции "Эхо Москвы" представляли собой 200-300 мегабайт мусорного трафика в секунду, то вчера на наш сайт его уровень достиг 2 гигабайт в секунду", - отметил он.
Источник: securitylab.ru

Атаки 1 и 2 типа встречаются достаточно части и для борьбы с ними администраторы уже давно эффективно используют как сетевые так и хостовые системы предотвращения атак (IPS). В этой статье мы будем говорить о защите от атак 3 типа, поскольку об этих методах защиты пока еще нет информации в русскоязычном Интернете. Атака третьего типа может быть обнаружена системой обнаружения или предотвращения атак, но заблокировать такую атаку на самом канале ни одна система защиты к сожалению будет неспособна. Канал во время атаки переполнен и в защите от атак должен принимать участие вышестоящий провайдер. IPS обычно не используются для защиты от таких атак, хотя сигнатуры для защиты SYNFlood и UDPFlood помогают уменьшить влияние этих атак, разгрузив атакованные сервера. Чаще всего для атак этого типа используются бот сети, которые выполняют вполне легитимные подключения и работу с вашей сетью. Но проблема в том, что их слишком много и отличить зомбированный компьютер от реального пользователя практически невозможно. Атаки третьего типа знакомы всем дачникам, пытающимся выехать из Москвы в пятницу и вернуться в Москву в воскресенье: МКАД и все трассы в области забиты и никакими средствами избавиться от их нельзя. Все пытающиеся прорваться сквозь пробку ругаются, хотя на самом деле сами и являются частью этой пробки. Остается только ждать, когда это все кончится само.

Защита от DDoS для корпоративной сети

Если ваш провайдер не предлагает услугу по блокировании DDoS атак, то у вас есть вариант попросить кого-то еще это сделать, но не меняя провайдера. Такую услугу мы разберем на примере компании Prolexic (www.prolexic.com). Даже, если на вас в настоящий момент идет атака, то вы можете достаточно быстро блокировать ее при помощи сервиса Prolexic одним из следующих вариантов.

Перенаправление DNS и использование прокси

Вы можете прописать в DNS IP адреса сети компании Prolexic. Допустим прописать, что ваш WEB сервер стоит на IP адресах Prolexic. В итоге атака будет направляться в их сеть, трафик DDoS будет отрезаться, а нужный трафик с вашего WEB сайта при помощи обратного прокси доставляться всем клиентам. Этот вариант очень подходит Интернет банкам, Интернет магазинам, онлайн-казино или электронным журналам. Вдобавок прокси позволяет кешировать данные.

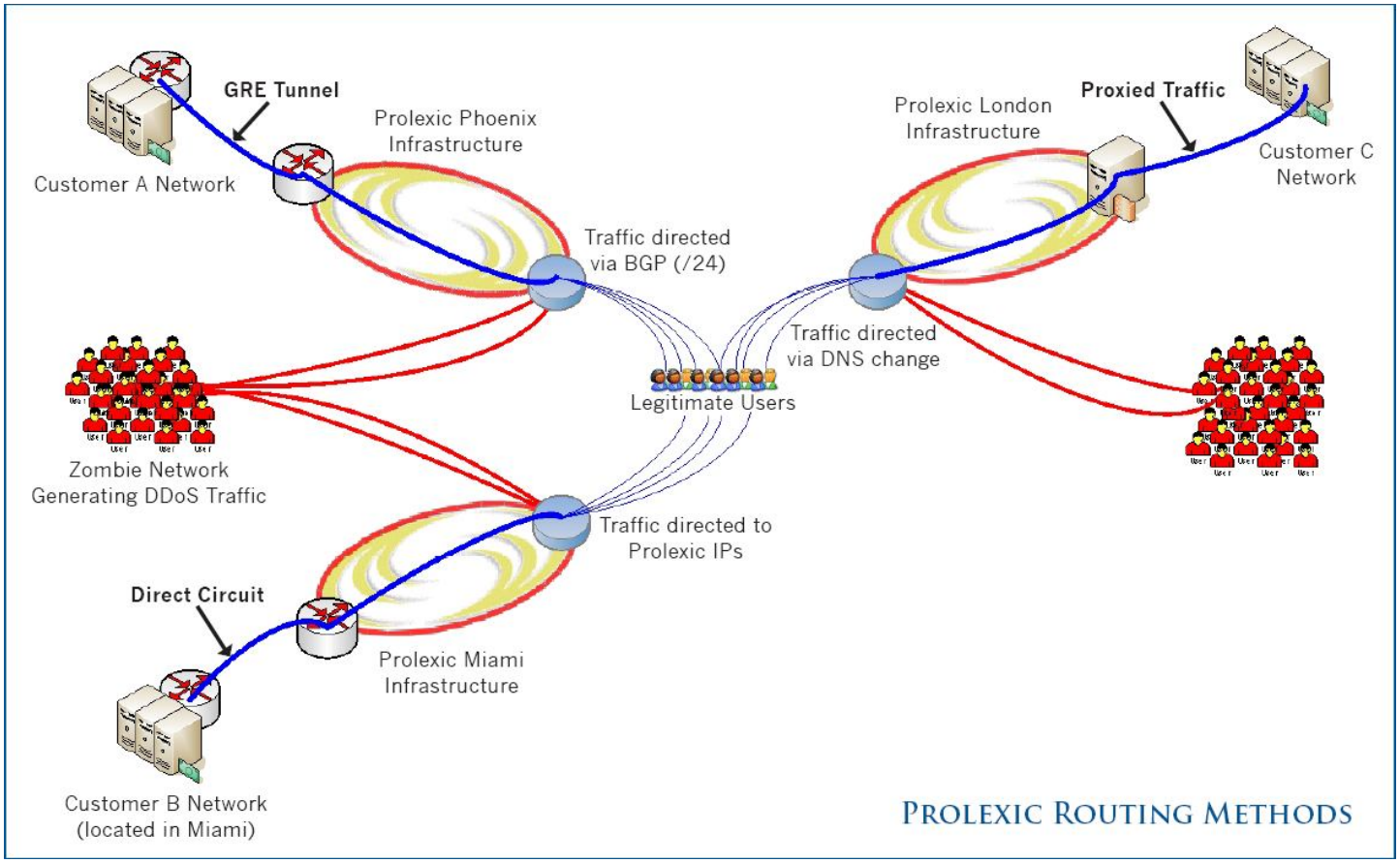
BGP маршруты и GRE туннели

Prolexic может, используя протокол маршрутизации BGP сказать всему Интернету, что ваша сеть находится в сети Prolexic и весь трафик будет перенаправляться к ним, где и будет очищаться от злонамеренного содержимого. Чистый трафик вам будет перенаправляться при помощи протокола GRE, который переносит данные в вашу сеть так, как будто никакой DDoS атаки и не было. А вы из своей сети будете отвечать на пришедшие к вам пакеты в обычном режиме, поскольку ваш канал уже не будет перегружен.

Прямое подключение к Prolexic

Можно напрямую подключить свою сеть через Prolexic и всегда быть под их защитой, но по понятным причинам это не всегда возможно. Если ваша компания международная, то часть своих ресурсов вы

можете подключить через компанию Prolexic или подобные компании. И на вас будет сложно совершить DDoS атаку.



Картинка с сайта www.prolexic.com

Как именно компания Prolexic отличает трафик зомбированных компьютеров от трафика обычных мне найти не удалось. В технической документации содержится информация о некой уникальной технологии использующей некоторые аппаратные и программные средства. Но самое главное в этой услуге, что есть к кому обратиться, если DDoS уже идет и есть возможность блокировать ее достаточно быстро.

Пример 5. Чудес не бывает. Чтобы подчеркнуть это, надо заметить, что были атаки и на сам Prolexic. В мае 2006 года появилось сообщение, что его DNS сервера перестали работать вместе с DNS серверами их клиентов. Подробнее тут www.secure64.com/ddos-news/prolexic-pharmamaster.html. Хотя потом оказалось, что атака была не на сами сети Prolexic, на защищенные технологией DNS Shield (www.ultradns.com/technology/dnsshield.html) DNS сервера компании UltraDNS, но пострадало 80% клиентов Prolexic. В общем история темная.

Сервис от **Akamai**

Большие компании, такие как IBM, Microsoft, Apple, Sony, AMD, BMW, Toyota, FedEx, NASA, NBA, MTV защищают свои WEB сайты от DDoS атак при помощи сервиса Akamai (www.akamai.com). Однако защита от DDoS, это лишь одна из возможностей сервиса Akamai. Этот сервис позволяет компаниям иметь зеркало своих сайтов в тысячах различных точек по всему земному шару, гарантируя 100% доступность в любое время. Обычно на зеркалах лежат мультимедийные данные, такие как видео, аудио и графика. Akamai использует математические алгоритмы для решения проблем с перегрузками возникающими на WEB серверах в глобальном масштабе. Эти алгоритмы были разработаны в Массачусетском технологическом институте (MIT). И именно благодаря им Akamai обеспечивает быструю и надежную передачу контента пользователям Интернет. Есть в судьбе компании и печальный

факт: один из основателей Akamai Даниель Левин был убит при попытке остановить террористов в одном из самолетов захваченных 11 сентября 2001 года в США.

Пример 6. Но даже Akamai однажды в 2004 году был выведен на час из строя. Говорят, что это была атака на DNS, но это тоже одна из темных историй. Подробнее тут www.washingtonpost.com/wp-dyn/articles/A44688-2004Jun15.html

Средства защиты от DDoS атак для провайдеров

Не пускайте к себе боты

В обычной ситуации невозможно отделить трафик ботов от трафика реальных пользователей: с виду это совершенно одинаковые запросы с разных адресов-источников. 99% этих адресов-источников могут быть ботами, и лишь 1% - реальными людьми, желающими воспользоваться вашим сайтом. И тут возникает вполне ожидаемое решение: надо просто иметь список этих зомби и блокировать их. Но как собрать такой глобальный список, ведь это затрагивает весь мир? И как выясняется для нас это элементарно.

Есть коммерческие компании, которые непрерывно собирают список адресов с зараженными компьютерами. Остается только пропустить ваш трафик через фильтр, который отрежет ненужные запросы и оставит нужные. Здесь фильтром может быть либо межсетевой экран, на который была установлена новая политика фильтрации или маршрутизатор на который был прислан новый список доступа, однако наиболее эффективным является применение специальных блокираторов. Пора уже назвать имена таких производителей (в алфавитном порядке):

- **Arbor** (www.arbornetworks.com/en/threat-management-system.html)
- **Cisco** (www.cisco.com/en/US/products/ps5888/index.html)
- **CloudShield** (www.cloudshield.com/Products/cs2000.asp)
- **Narus** (www.narus.com/products/index.html)

Компания Arbor собирает списки адресов бот сетей (http://atlas.arbor.net/summary/botnets), что используется в продуктах Arbor и ее партнеров. Такие списки адресов постоянно обновляются раз в 15 минут и, например, используются для обнаружения подключения защищаемых рабочих станций к бот сетям в продукте IBM Proventia Anomaly Detection System. В первом случае у провайдеров используется технология Peakflow SP, в другом в корпоративных сетях технология Peakflow X. Устройства производителей систем защиты от распределенных атак отличаются в первую очередь максимальными скоростями на которых они работают и числом одновременно защищаемых клиентов. Если у вас каналы передачи данных используют или планируют более одного 10Гбит соединения, то нужно уже задумываться какого производителя выбрать. Кроме того, производители отличаются различным дополнительным функционалом, временем требуемым на обнаружение атаки и включение защиты, производительностью и другими параметрами.

Автоматика против интеллекта

В случае, когда атака направлена не на сервер, а на переполнение канала, то боты подставляют в качестве адреса-источника любые адреса и трафик выглядит как поток каких-то данных со всех адресов Интернета на все адреса атакуемой сети. Это самый сложный вид атаки.

Пример 7:
30-31 мая 2007 года петербургский провайдер Infobox подвергся массированной DDoS-атаке - до 2 Гб в секунду. Атака велась с десятков тысяч адресов, расположенных по всему миру, в том числе из России, Кореи, ОАЭ, Китая. Атаке подвергались DNS сервера. В результате большая часть каналов оказалась перегружена. Сайт, размещенные у провайдера серверы и почтовые ящики были полностью или частично недоступны. Техподдержка сообщила: «Мы стараемся минимизировать ущерб, наносимый атакой, но это достаточно проблематично и может вызывать неудобства для части клиентов (блокировка доступа из сетей крупных провайдеров)». По словам генерального директора "Инфобокса" Алексея Бахтиарова, атака велась с десятков тысяч адресов, расположенных по всему миру". Источник: securitylab.ru, 03.07.07

Для атак такого типа разработаны сложные системы анализа поведения трафика в сети провайдера. Основная сложность информационных потоков в сети любого провайдера: их огромное количество. Человеку не под силу проанализировать такое количество разных соединений в секунду и тут мы вынуждены полагаться на искусственный интеллект систем анализа аномалий.

По сути в момент начала приведенной выше DDoS атаки сеть провайдера должна была прекратить принимать запросы от новых IP адресов и пускать в свою сеть только запросы с IP адресов которые приходили ранее при нормальном функционировании системы. Текущие клиенты бы даже не заметили DDoS атаки. Но для этого надо было собирать ежедневно этот «белый список». А для этого в сети должна была функционировать система анализа поведения сети, которая бы отличила своих клиентов от нежелательных.

Я конечно описываю реакцию системы анализа аномалий достаточно упрощенно. На самом деле в искусственном интеллекте таких систем кроются разработки институтов, годы практического изучения DDoS атак и результаты диссертаций. Программисты уже написали программы которые легко играют в шахматы, что было достаточно непросто – надо было обыграть человека. Точно также защита от DDoS – сложная программа требующая высокой концентрации последних достижений в области анализа трафика, чтобы в автоматическом режиме среагировать на атаку. Методы атаки могут меняться атакующими раз в полчаса и система должна это отследить и предпринять соответствующие меры.

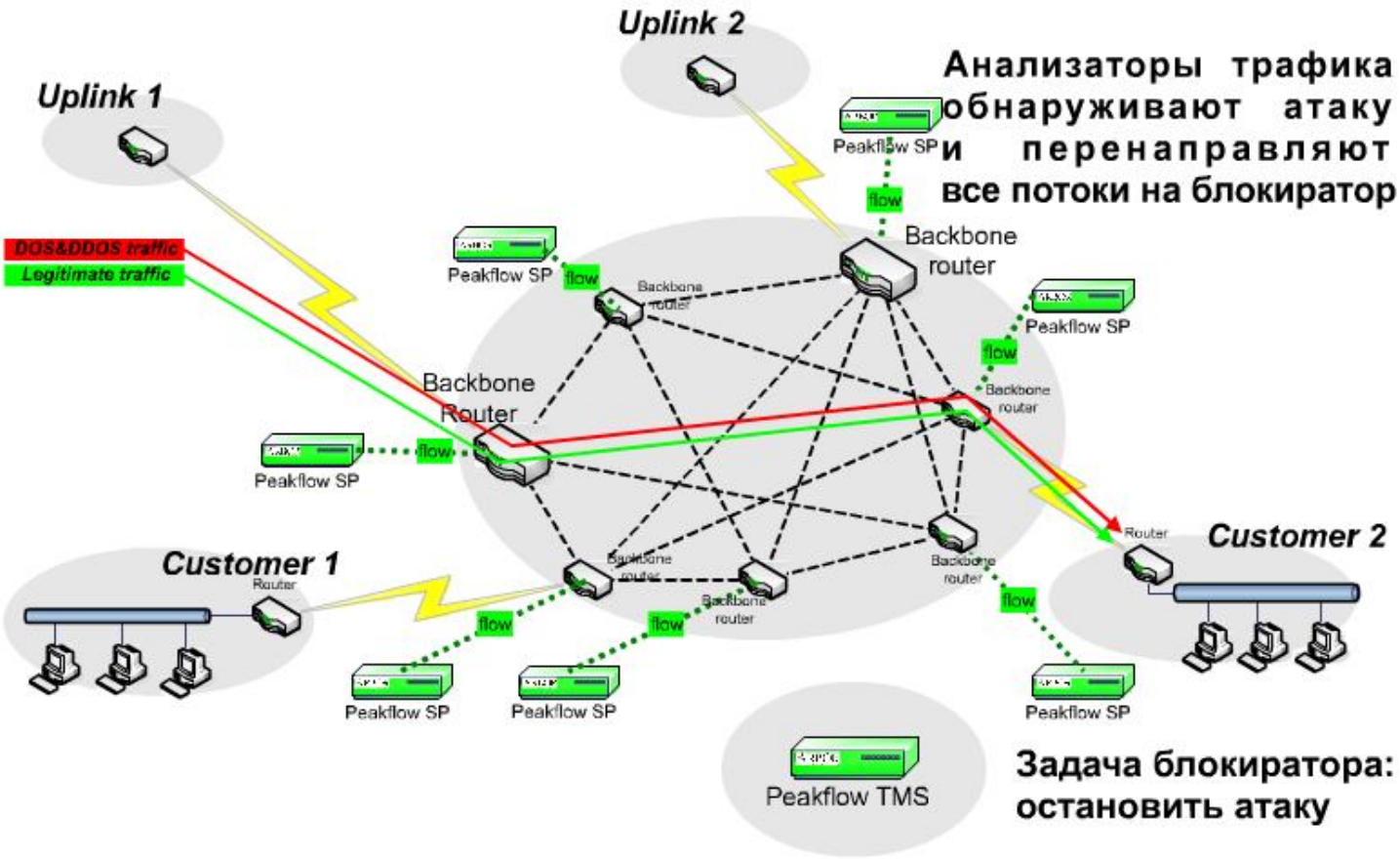
Производители таких сложных систем анализа трафика обычно рассказывают какие именно принципы заложены в механизмы защиты только при личной встрече. В этой статье мне тоже не хватит места для их подробного изложения. Попробую лишь раскрыть основные принципы работы.

Принцип работы систем защит от DDoS атак

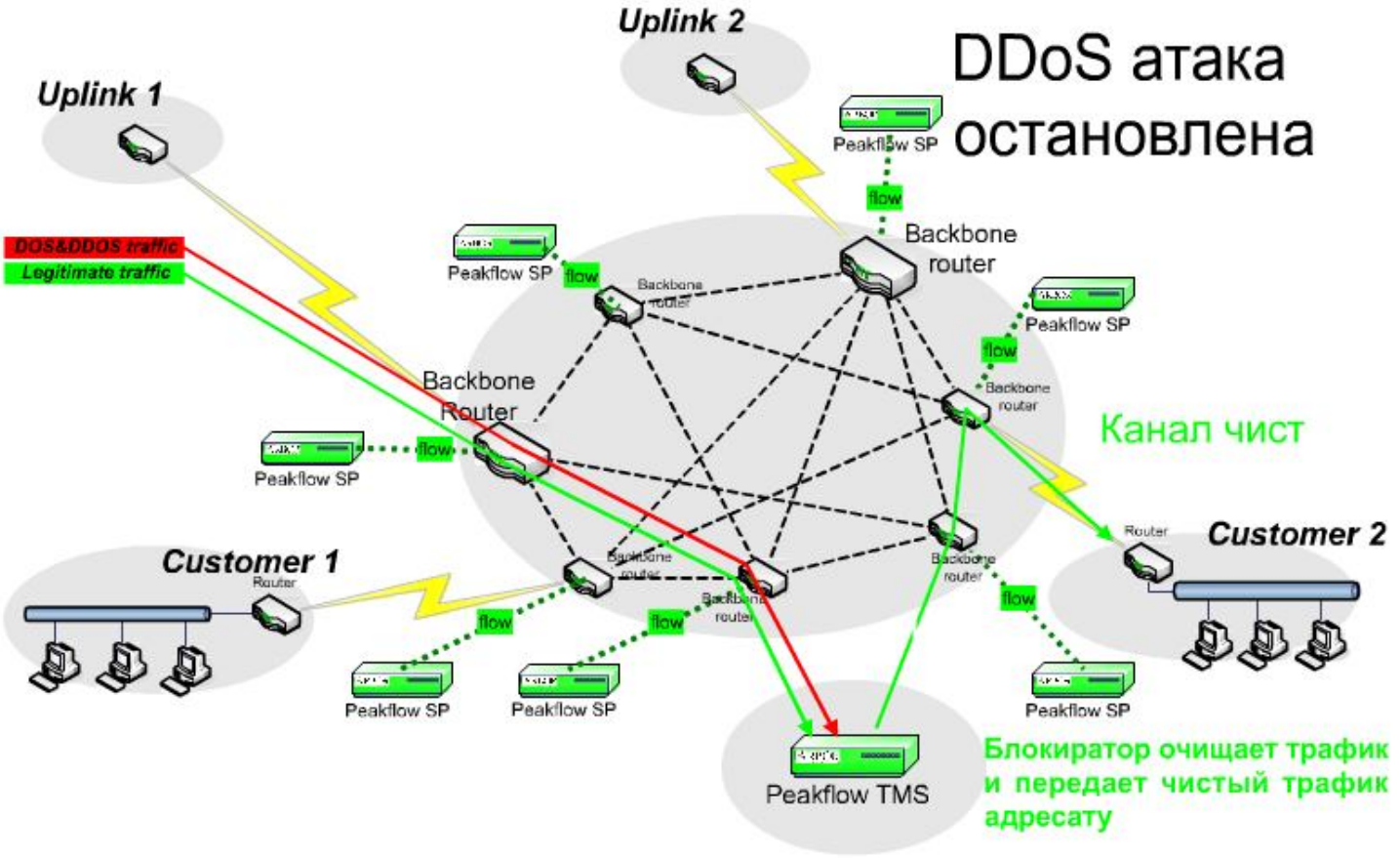
Система защиты от DDoS атак базируется на уже имеющихся в сети маршрутизаторах и добавляет в сеть свои два компонента:

- устройство для блокирования DDoS атаки. В английском языке это устройство называют mitigator. В связи с отсутствием аналогичных статей по данной теме я введу русский термин: буду называть его блокиратор;
- устройство со встроенным искусственным интеллектом для обнаружения DDoS атаки и перенаправления атаки на блокиратор, буду называть его детектор.

Надо заметить, что в задачу блокиратора входит не только блокирование трафика, но и его замедление. После обнаружения DDoS атаки на какую-то сеть анализатор трафика вставляет в таблицы динамической маршрутизации (при помощи BGP или OSPF) запись, которая говорит, что маршрут в атакуемую сеть лежит через этот блокиратор.



В результате весь трафик атаки начинает проходить через блокиратор, что дает возможность заблокировать трафик атаки, а легитимный трафик передать в защищаемую сеть. Передача в защищаемую сеть осуществляется любым доступным способом, например при помощи инкапсуляции трафика внутри GRE.



После завершения атаки, таблица маршрутизации перенастраивается, чтобы трафик проходил через конечный маршрутизатор, связанный с этой сетью.

Более подробно работу рассмотрим на конкретном примере: связка детекторов Arbor SP + с блокиратором Arbor TMS. SP здесь в названии означает Service Provider, а TMS – Threat Management System. Надо заметить, что детекторы Arbor SP часто используются совместно с блокираторами других компаний, например, они совместно работают с Cisco Guard и CloudShield CS-2000.

Принцип работы Arbor Threat Management System

Arbor TMS выполняет защиту от DDoS атак различных типов. Основным достоинством защиты на базе Arbor TMS является блокирование атак с случайных поддельных IP адресов всего Интернета на все адреса из атакуемой сети, имеющих своей целью переполнение канала. Для обнаружения DoS атаки используется детекторы Arbor SP. Устройства Arbor SP собирают информацию со всех маршрутизаторов и свитчей провайдера о трафике и анализируют его. Сбор информации собирается по любому протоколу сообщения о потоках, например при помощи Cisco NetFlow. Для перенаправления трафика атакуемой сети через устройство Arbor TMS используется протокол BGP. Управление устройством TMS осуществляется через Arbor SP контроллер, который не только управляет, но и собирает flow потоки от маршрутизаторов. Контроллер поддерживает до 5 маршрутизаторов. Каждые новые 5 маршрутизаторов обслуживаются дополнительным коллектором, который собирает flow потоки и передает в контроллер. Для передачи отфильтрованного хорошего трафика обратно в канал используется инкапсуляция GRE или MPLS. При обнаружении DoS атаки коллекторами Arbor SP по протоколу BGP добавляется подходящее устройство TMS как следующий маршрутизатор для атакуемой сети и таким образом трафик автоматически перенаправляется на фильтрующее устройство всеми маршрутизаторами.
Существует несколько этапов работы связки Arbor SP+TMS.

1. Обнаружение. Детектор Arbor SP понимает, что началась DDoS атака.
2. Активация защиты. Детектор дает необходимую информацию TMS для его работы.
3. Перенастройка маршрутизации. TMS дает маршутизаторам информацию по протоколу BGP о том какие сети он будет фильтровать. Маршрутизаторы начинают посылать ему трафик предназначенный только для этих сетей. Трафик для других сетей передается так же.
4. Фильтрация. TMS получает трафик и удаляет из него вредоносные пакеты.
5. Перенаправление. TMS перенаправляет полезный трафик клиенту провайдера. Для этого на маршрутизатор к которому подключен клиент передаются пакеты, инкапсулированные внутри GRE.

Какие именно защитные механизмы реализованы в Arbor TMS в открытом доступе я не нашел, поэтому рассматриваю эту информацию как конфиденциальную.

Пример 8: Эксперт США: Хакерские атаки на Эстонию исходили "не из Кремля"
Об этом заявил старший инженер по вопросам безопасности известной американской компании Arbor Networks Хосе Назарио. По его словам, атаки шли с огромного числа компьютеров по всему миру, в том числе из США и Вьетнама. "Ни один из источников, анализ которых мы провели по всему миру, не показывает явную линию из Москвы в Таллин. Вместо этого в Эстонию все шло со всего мира", - сказал Назарио в интервью специализированному журналу IT PRO, посвященному информационным технологиям.
По словам Назарио, хакерские атаки, из-за которых в конце апреля некоторое время был блокирован доступ, в частности, на сайты президента Эстонии, МИД, парламента и других ведомств, были глобальными и не исходили из одной страны. Они не были также результатом согласованных усилий какого-либо правительственного ведомства, сказал эксперт.
Исследование Arbor Networks показало, что нападения на эстонские интернет-сайты были организованы с использованием гигантских сетей, работающих в автоматическом режиме компьютеров, число которых могло достигать 1 миллиона.

Выводы

1. Не всегда провайдеру выгодно защищать вас от DoS атак, поскольку если трафик идет к вам, то вы платите за него, а если провайдер его заблокировал у себя, то за этот трафик платит он. Поэтому подписывая договор оговорите позицию провайдера по блокировке трафика в случае DoS, DDoS и DRDoS атак на вас.
2. Провайдеры могут использовать различные решения для защиты от DDoS атак. Спросите вашего провайдера есть ли они у него вообще и если есть, то какие.
3. Не забудьте про оповещение самих себя об атаках на ваш сервер. Это может быть какая-то автоматизированная система, это может быть собственная дежурная смена, а может быть мониторинг безопасности дежурной сменой специализированной компании.
4. Не стоит экономить на консультантах по информационной безопасности. Для сложных проблем уже найдены хорошие решения как в медицине и технике, так и в области ИБ.

12 августа 2008г., Денис Батранков, консультант по информационной безопасности IBM Internet Security Systems, batrankov@ru.ibm.com