Решил написать обзорную статью на популярную в настоящее время тему, которой сам интересуюсь. Что такое современная ddos атака, как ее провести и как защитить сайт от ддос атак. Не скажу, что у меня есть какой-то большой реальный опыт в этой теме, но с небольшими атакам сталкивался и противостоял.

Содержание:

Введение

Как я уже сказал, большого опыта работы под ддос атаками у меня нет. Несколько раз я ловил ddos на свой сайт, несколько раз на сайты своих клиентов. Это были небольшие атаки, с которыми так или иначе можно было работать.

Мне интересна эта тема просто для общего развития. Я читаю статьи, смотрю доклады, знакомлюсь с сервисами по этой теме.

Что такое современная ddos атака

DDoS расшифровывается как **Distributed Denial of Service** — атака на информационную систему с целью довести ее до такого состояния, когда она не сможет обслуживать запросы клиентов, для которых она работает. Ддос атака может проводиться как на отдельный сайт, так и на сервер или сеть, обслуживающую масштабную информационную систему (например, ЦОД).

В чем же сущность ddos атаки? По своей сути это распределенная **DoS (Denial of Service)** атака. Отличие DoS от DDoS как раз в том, что DoS это просто одиночная атака, а DDoS это масштабная атака, состоящая из множества дос атак, выполняемых из разных мест.

Виды ддос атак

Для проведения ддос атак чаще всего используют ботнет. От размера ботнета зависит мощность атаки. Из определения понятно, что ddos — это когда много запросов направляют на какую-нибудь цель. А вот цели и типы запросов могут быть принципиально разные. Рассмотрю основные варианты ddos атак, которые встречаются в современном интернете. Их можно разделить на 2 основных типа:

1. Атака на уровне L7, то есть на седьмом уровне модели OSI. Нагрузка на приложение. Обычно это **HTTP Flood**, но не обзательно. Атака может быть и на открытую в мир MySQL или другую базу, почтовый сервер или даже SSH. Данная атака направлена на то, чтобы как можно меньшим трафиком напрягать наиболее тяжелое и уязвимое место сервиса. Обычно вредоносные запросы маскируются под легитимные, что осложняет отражение.
2. Уровень L3 L4, то есть сетевой и транспортный уровни модели OSI. Чаще всего это **SYN** или **UDP flood**. С помощью ддос атак этого типа стараются загрузить все каналы связи, чтобы таким образом помешать работе сервиса. Как правило, вредоносный трафик легко отличим от легитимного, но его так много, что фильтрация просто не справляется. Все входящие каналы забиваются флудом.

Рассмотрим подробнее конкретные цели для описанных выше атак. Начнем с L7 атак. В качестве цели могут использоваться следующие объекты:

- Какая-то тяжелая страница на сайте. Атакующий простым просмотром сайта с помощью DevTools определяет наиболее тяжелые страницы. Чаще

всего это поиск, большие каталоги товаров или заполняемые формы. Определив узкое место, туда направляется шквал запросов, чтобы положить сайт. Для эффективности, можно нагружать сразу все, что показалось тяжелым. С таким подходом можно и десятью запросами в секунду уронить неподготовленный сайт.
- Загрузка файлов с сайта. Если вы размещаете более ли менее крупные файлы непосредственно на веб сервере, то через них его будет очень легко положить, если не настроить ограничения на скачивание. Обычными параллельными загрузками можно так нагрузить сервер, что сайт перестанет отвечать.
- Атака на публичный API. Сейчас это очень популярный инструмент из-за его простоты и легкости использования. Защищать его сложно, поэтому он часто может быть целью ddos атак.
- Любые другие приложения, которые доступны из инетрнета. Часто это почтовые программы, ssh сервер, серверы баз данных. Все эти службы можно нагрузить, если они смотрят напрямую в интернет.

С уровня L3, L4 обычно делают следующие ддос атаки:

- **UDP-flood**. Это вообще классика. С подобными атаками сталкивались практчески все, кто держит открытыми dns и ntp сервисы. В них постоянно находят уязвимости, позволяющие использовать эти службы для ddos атак на сервера. Злоумышленники сканируют интернет, находят неправильно настроенные или уязвимые сервера, отправляют туда запросы, подделывая адрес источника. В ответ эти серверы шлют несколько запросов по поддельным адресам. Таким способом злоумышленники в несколько раз усиливают свои атаки.
- **SYN-flood**. Тоже старый вид атак типа отказ от обслуживания. Злоумышленник отправляет большое количество SYN запросов на установку соединения. В общем случае, с помощью syn запросов забивают всю очередь на подключения. В итоге легитимные трафик перестает ходить, сервис не отвечает клиентам.

На основе описания основных типов ddos атак рассмотрим простые и очевидные способы противодействия.

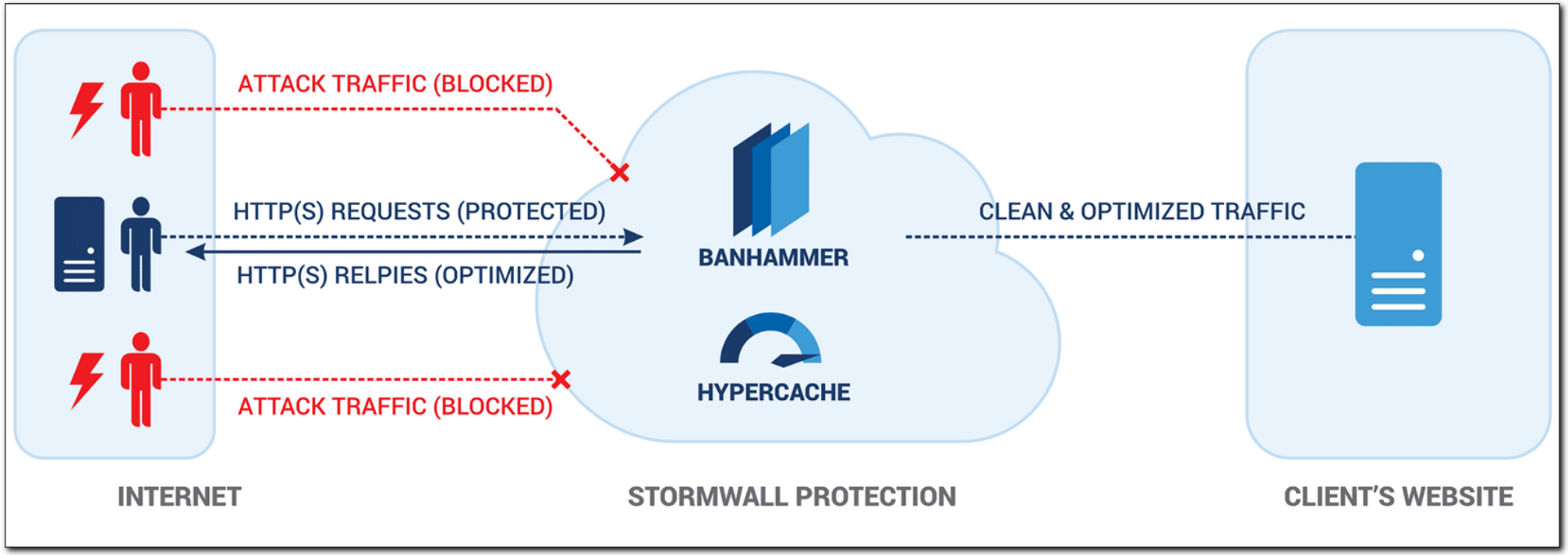
Защита от ddos атак с помощью платных сервисов

Для проведения обычной DoS атаки могут использоваться какие-то программы или скрипты. Птив таких атак не очень сложно защититься. Примеры таких программ я приведу отдельно. Если же идет масштабная ддос атака, то тут уже совсем другое дело.

Защита сайта от ddos атак может быть двух типов:

1. Профессиональная защита с помощью платных сервисов и перенаправления трафика на них.
2. Защита сервера от ддос своими силами.

Ниже я опишу различные методы защиты от ддос. Сразу скажу, что самостоятельно отбиться от серьезной атаки не получится. Вам могут тупо залить столько трафика, что все каналы связи будут загружены и хостер вас тут же отключит. Сам с этим несколько раз сталкивался. Никакие организационные меры не помогут. Но обо всем по порядку. Начнем с платных сервисов по защите.



Скрытие и защита реального ip адреса

Как же защитить свой сайт от ddos атаки? Первое и самое главное правило, если вам необходима качественная и профессиональная защита от DDoS — не раскрывайте свои прямые ip адреса. Если вас атакуют, а вам надо как можно быстрее защититься — сразу же выбирайте сервис по защите от ддос, настраивайте проксирование трафика через него, меняйте свои прямые IP адреса и ни в коем случае не светите их нигде. Иначе никакой платный сервис не поможет. Вам будут напрямую устраивать ddos атаку по ip, минуя защиту.

Простое сканирование портов по старому ip позволит определить все доступные службы на сервере и продолжить атаку на сервер напрямую по адресу, минуя защиту. Вам нужно разрешить подключения к своему серверу только с адресов службы защиты. Не забудьте закрыть и ssh службу фаерволом. Незащищенный сервер можно без проблем завалить через ssh обычным syn флудом и fail2ban не спасет. Там такой лог будет, что fail2ban сам положит сервер.

Реальный ip адрес можно определить через поддомены, которые вы забудете закрыть защитой, через заголовки писем email, если почта находится на том же сервере, где сайт, через http заголовки, если вы добавляли в них информацию об ip. Мест, где можно спалить свой реальный ip может быть много. Вам нужно потрудиться и закрыть все эти места. Пока этого не сделаете, профессиональная защита может быть неэффективной.

Также в интернете есть сервисы, которые по имени домена позволяют определить все их внешние ip адреса, которые ранее были засвечены. Если вы какое-то время были доступны в интернете под своим реальным ip адресом, он практически со 100% вероятностью уже засвечен и будет легко определен.

Какой сервис защиты от ддос атак выбирать, я не знаю. Конечно, начать проще всего с cloudflare, так как у них есть бесплатный тариф. Но там много ограничений, плюс надо немного разбираться в том, как работает этот сервис. В общем, бесплатно, без должного опыта защиты от ddos вы вряд ли что-то сделаете. Выбирайте кого-то еще. В качестве примера я уже привел **StormWall** выше. Начальный тариф там подъемный, можно начать с него.

Настройка firewall

Как я уже сказал выше, обязательно закройте фаерволом все, что только можно. Злоумышленники не должны ничего видеть на вашем реальном сервере. Просто перенести, к примеру, ssh на какой-то другой порт, отличный от 22 тут не подойдет. Закрывайте все и открывайте доступ только со своих доверенных адресов. Web трафик разрешайте только с серверов защиты. Их адреса вам предоставит поддержка.

Подробнее о настройке iptables, если используете этот фаервол, можете прочитать в моем материале по теме.

Аренда хостинга с защитой от ddos

Желательным, но не обязательным шагом по защите сервера от ddos атаки — увеличение его производительности, либо переезд на специальные виртуальные серверы, которые изначально поддерживают защиту от ддос. Это не обязательно поможет, но если есть возможность, то нарастите мощности или переедьте в другое место. Это позволит вам прожить немного дольше и расширит зону для маневра.

Когда ваш сервер и так еле тянет нагрузку, а тут еще идет атака, он очень быстро загнется. Если мощности не хватает с достаточным запасом, то атакующие могут пройти защиту очень малым объемом трафика, который невозможно будет отличить от легитимного, и этого будет достаточно, чтобы сайт стал недоступен. Специализированный хостинг учитывает эти моменты и предлагает решения.

Настройка кэширования

Кешированием стоит заниматься сразу, а не тогда, когда вас уже атакуют. Тем не менее, если у вас не оптимизирован сайт или сервис, защитить его будет очень сложно. Как я уже написал выше, защита может пропускать часть трафика, который будет очень похож на легитимный. И этого трафика может хватить, чтобы загрузить до отказа сервер.

Вопрос кэширования достаточно сложный и сходу трудно будет предложить эффективные решения. Тем не менее, если для вас важно хоть что-то отвечать пользователям, а не показывать ошибку веб сервера, то закэшируйте в статику то, что должно даваться динамически. Пусть во время атаки хотя бы сохранится видимость того, что сайт работает. Это все равно лучше, чем полная остановка работы.

Иногда ддос атака может быть вызвана вполне законными способами. К примеру, ссылку на ваш сайт опубликовали где-то в очень популярном месте. И к вам пошел шквал настоящих пользователей. Они все реальные, но по сути вы получаете ддос атаку на свой сайт, которая может привести к его отказу и вы не получите прибыль, к примеру, с показа рекламы в эти моменты.

В таком случае, лучше будет быстро закэшировать посещаемые страницы и отдавать статику, несмотря на то, что не будут работать комментарии, какая-то лента и т.д. Главное, что пользователи смогут прочитать контент, посмотреть рекламу, а вы получить прибыль. Когда нагрузка спадет, сможете проанализировать ситуацию и выработать какое-то рабочее решение на будущее.

Вынести smtp на отдельный сервер

Не используйте web сервер в качестве почтового серврea. По возможности, выносите функции отправки email сообщений куда-то на сторону. Это может быть как специальный почтовый сервис, так и ваш собственный, но настроенный отдельно. Это полезная практика не только во время ddos атак, но и в общем случае. Как настроить почтовый сервер можете прочитать в моих статьях.

Мало того, что через почтовый сервер можно легко узнать ваши реальные ip адреса, так это дополнительные точки для поиска уязвимостей и отказа. Лучше перестраховаться и минимизировать риски.

Я рассказал, как может быть настроена защита от ddos атак с помощью платных сервисов. В качестве примера привел компанию StormWall. Она достаточно известна, цены доступны, русская поддержка. Они выступают на различных мероприятиях и делятся знаниями. Вот пример отличного выступления, которое я сам в свое время с удовольствием посмотрел и взял их на примету.

Защита сайта от ддос своими силами

Давайте теперь рассмотрим, что мы сможем сделать сами, чтобы защитить свой сайт от распределенной атаки. Сразу скажу, что не очень много. Я немного разбирал эту тему в отдельной статье по защите web сервера от ddos. Там описано несколько простых и эффективных действий, которые позволят вам защититься от простенькой атаки, которую будет выполнять какой-то любитель или школьник из небольшого количества мест.

Если атака будет распределенная и масштабная, то своими силами вы ничего не сможете сделать. Вас просто будет отключать хостер, если вы используете обычный VPS или выделенный срервер, без защиты от ддоса. Я сам с этим несколько раз сталкивался. Что бы ты не делал, ничего не помогает. Как только трафика приходит слишком много, вас отключают, даже если сервер еще вполне себе тянет нагрузку. Необходимо обращаться в специализированные сервисы, переправлять весь трафик туда и проксировать его к себе уже очищенным.

Как сделать ддос атаку самому

Рассмотрим на примерах, как в принципе можно провести ddos атаку. *«Чтобы поймать преступника, нужно думать как преступник»*. По понятным причинам, я расскажу только немного теории, без практических примеров, во избежание, так сказать. Хотя у меня и примеров то нет. Я сам никогда всерьез не занимался ddos атаками.

У Яндекса есть отличный инструмент для нагрузочного тестирования — Яндекс.Танк. Когда я с ним знакомился, решил нагрузить несколько первых попавшихся под руку сайтов. К моему удивлению, я положил все сайты, которые пробовал нагрузить :) Сразу скажу, что это были небольшие блоги таких же любителей блоггинга, как и я.

Для того, чтобы сделать ddos атаку самому на неподготовленный сайт достаточно из 3-5 разных мест запустить Яндекс.Танк и указать в качестве целей набор наиболее тяжелых страниц. Обычному динамическому сайту сразу станет плохо. Когда владелец спохватится и начнет разбираться, он достаточно

быстро забанит ваши ip адреса сам, либо с помощью хостера и на этом ваша ддос атака закончится.

Вам придется искать новые ip адреса для проведения очередной ддос атаки, что весьма хлопотно, а вот блокировать их будет легко. Дальше уже нужно включать голову и думать, как оперативно и легко менять ip адреса. В голову приходят готовые списки с прокси, скрипты, curl, python и т.д. Не буду дальше развивать эту мысль. В общем и целом, самому научиться ддосить на начальном уровне не так сложно. Достаточно базовых знаний linux и скриптинга.

Сразу скажу, что профессиональные службы по защите от ддос, наподобии StormWall или CloudFlare, такие ваши атаки отметут, даже не заметив. Это может быть интересно только в качестве саморазвития. Все современные и эффективные ddos атаки делают с помощью ботнет сетей.

Программы для ddos атак

Я решил сделать раздел с описанием программ для ддос вот с какой целью. Если вам это интересно, то наверняка вы будете искать в интернете подобные программы, как это делал я в свое время. Сразу предупреждаю, что сами эти программы и сайты, которые их распространяют, набиты вирусами и прочими вредоносами. Будьте очень внимательны и осторожны при поиске программ.

Подобные программы рекомендуется использовать, чтобы проверить, как ваш сайт будет работать под их натиском. Если вам будут организовывать ddos, то возможно начнут именно с таких простых средств. Так что имеет смысл после настройки защиты посмотреть, а как она реально работает.

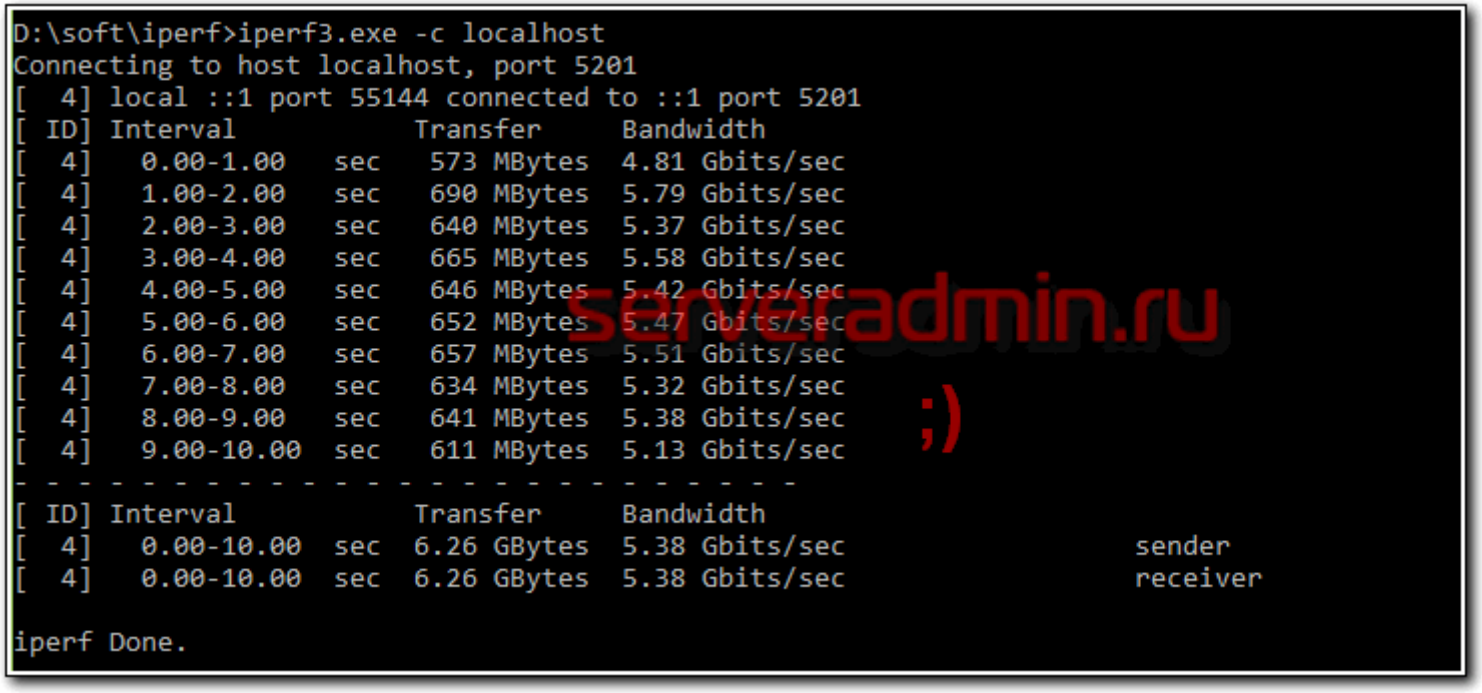
Ddos программы делятся на 3 типа:

1. Программы для проведения syn и udp флуда.
2. Программные комплексы для создания своего ботнета.
3. Stresser сервисы.

Программы для проведения syn и udp флуда

Из первых наиболее популярны:

- **Server Flooder**. Простая программа, которая может долбить запросами конкретный ip адрес и порт. Защита от такой программы очень простая — баним ip адрес при большом количестве запросов от него. Где скачать нормальный Server Flooder не знаю. В большинстве мест вместо него в архивах будут вирусы, так что аккуратнее.
- **Loic**. Программа старая. Умеет спамить http запросами, а так же флудить tcp и udp пакетами. Скачать loic можно на sourceforge.
- **MummyDDOS**. Такой же tcp флудер, как и первые два.



Программные комплексы для создания своего ботнета

В публичный доступ попадают какие-то старые поделки, которые потеряли актуальность из-за того, что их детектят все современные антивирусы. Использовать их можно только в каких-то академических целях на подконтрольных вам машинах. Реально собрать свой ботнет для проведения мощных ddos атак с помощью публичных бесплатных программ невозможно.

К таким ботнетам относятся **Zemra Botnet**, **Dirt Jumper**, **Solar** и т.д. Все это есть в свободном доступе. Можете для общего развития установить и посмотреть, как все это работает.

Stresser панели

Современные, удобные, функциональные инструменты для проведения ddos атак. К сожалению :(Stresser — это некий сервис с web панелью, личным кабинетом. Вы оплачиваете услугу по доступу к ddos панели и можете использовать ее некоторое оплаченное время. Стоимость для простых атак невысокая. Буквально за 3-5 долларов в день вы можете два-три раза устраивать сайту достаточно мощный ддос на 3-5 минут каждый день. Иногда этого времени достаточно, чтобы хостер снял сайт с обслуживания.

В бэкенде у таких панелей обычный ботнет. Есть панели с тестовым доступом для проведения мощной ддос атаки полностью бесплатно. Да, она будет кратковременная, но все равно может навредить ресурсу. Работают такие панели вполне легально, предоставляя свой доступ якобы для тестирования надежности ресурсов. А то, что их используют для ddos атак, это уже их не касается.

Заключение

> Не понравилась статья и хочешь научить меня администрировать? Пожалуйста, я люблю учиться. Комментарии в твоем распоряжении. Расскажи, как сделать правильно!

На этом у меня все по теме ddos атак. Как обычно, хотелось написать больше и с примерами, но получилось и так длинная статья. Думаю, конкретные примеры по проведению ddos своими силами и противодействию им опишу отдельно.

Если у вас есть замечания, дополнения, интересные ссылки на доклады, видео, сервисы по защите, делитесь в комментариях.

Помогла статья? Есть возможность отблагодарить автора