# DDoS-атаки в 2022 и методы защиты от них

Мы в Southbridge занимаемся построением и поддержкой ИТ-инфраструктуры и в процессе работы регулярно сталкиваемся с DDoS-атаками на серверы клиентов. Поэтому мы накопили опыт в этом вопросе. Денис Чернов, DevOps-инженер Southbridge, провёл вебинар о DDoS-атаках и подготовил на его основе эту статью. Слово Денису.

Привет, Хабр! Хочу поделиться тем, что знаю о DDoS — что это за атаки, какие они бывают, как можно их предотвратить и минимизировать влияние таких атак на свой сервис.

Эта статья написана по [моему вебинару](https://www.youtube.com/watch?v=5mcWOF2EPzM). Можно посмотреть его на Youtube — там кроме теории есть практика с настройкой защиты веб-сервера и имитацией DDoS-атаки.

Что такое DDoS-атаки и зачем их устраивают

DDoS — это Distributed Denial of Service, распределённый отказ в обслуживании. По сути это хакерская атака, которая перегружает систему, чтобы конечные потребители не могли пользоваться сервисом. Атака может быть направлена на всю ИТ-инфраструктуру, конкретный сервис либо канал до этого сервиса.

Распределённая — значит, что атака выполняется одновременно с большого количества устройств, которые зачастую распределены географически. Это могут быть как специально подготовленные сервера, так и ботнеты из зараженных устройств. Ботнет — это группа устройств, на которых запущены скрипты, выполняющие нужный злоумышленнику код, в данном случае — DDoS-атаку. Зачастую ботнеты собираются из устройств, зараженных вредоносным ПО, и их владельцы даже не подозревает о «двойной жизни» своих гаджетов.

DDoS-атака может быть организована с коммерческой целью:

* Получить выкуп — обрушить систему и потребовать деньги за прекращение атаки.
* Подставить конкурента. Например, обрушить его сайт в преддверии крупного праздника, чтобы клиенты ничего не могли заказать и пошли в другой магазин.

Но бывают и некоммерческие причины атак:

* геополитические;
* просто ради развлечения;
* ради «хакерской» практики;
* из «обиды» на какой-либо сайт, сервис или бренд.

Вне зависимости от причины DDoS-атака влияет на вашу конечную инфраструктуру и делает ваш сервис или сайт недоступным. Причины у недоступности могут быть разные, например:

1. Заполнение вашего сетевого канала паразитным трафиком: пустыми запросами и пакетами.
2. Утилизация ресурсов: ваш веб-сервер или СУБД оказывается загружен обработкой ненужных запросов и не может выдать реальным клиентам нужную информацию.

**Кроме недоступности сервиса есть и другие последствия DDoS-атак:**

* Если ваши серверы в облаке, а трафик платный, вы можете понести финансовые расходы.
* Если сайт будет недоступен больше двух суток, поисковые боты станут ранжировать вас ниже. Позиции в поисковой выдаче придётся восстанавливать.
* Даже после восстановления работоспособности сервиса клиенты станут меньше вам доверять и могут уйти к конкурентам.
* Под атакой элементы ИТ-инфраструктуры могут вести себя некорректно. Например, выдавать пользователю внутреннюю информацию о СУБД, к которой не удаётся подключиться. Ещё я на практике видел ошибку коннекта к базе данных даже после того, как проблемы с DDoS были уже решены.

Какие DDoS-атаки бывают

Существует несколько классификаций DDoS-атак. Здесь я хочу поговорить о классификации по уровням модели OSI.

**Низкоуровневые.** Они происходят на L3-L4 модели OSI, то есть в районе сетевого и транспортного протокола:

* Сетевой уровень (L3): DDoS-атаки по протоколам IPv4, IPv6, ICMP, IGMP, IPsec, RIP, OSPF. Цели таких атак —  в первую очередь сетевые устройства.
* Транспортный уровень (L4): воздействие по протоколам TCP и UDP.
Цели таких атак — конечные серверы и некоторые интернет-сервисы.

Такие атаки весьма распространены. Дело в том, что стандарты интернета в делались с расчётом на то, что все участники будут добросовестно их использовать.

Например, в протоколе UDP, который работает поверх IP, информация передаётся датаграммами, и в заголовках пакета не содержится IP ни источника, ни получателя. UDP доверяет адресацию протоколу IP, поверх которого работает, а в протоколе IP эти заголовки есть, но они никак не проверяются. Соответственно, очень многие атаки основаны на том, что меняется один из IP-адресов, как правило, это IP-адрес источника. Это называется спуфингом, т.е. атакой с подменой данных одного из узлов.

Такие атаки характерны тем, что нагружают какие-то части вашей инфраструктуры, забивают канал или заполняют служебные таблицы.

**Высокоуровневые.**Они затрагивают уровень приложения, L7, и воздействуют по прикладным протоколам, например, HTTP. Цели таких атак — конечные серверы и сервисы.

Самые распространённые виды атак

Существует несколько разновидностей DDoS-атак в зависимости от того, на что и как конкретно они воздействуют. Расскажу о четырех самых популярных.

UDP Flood

UDP работает поверх протокола IP, и там нет установки соединения как такового — данные просто отсылаются безо всякого контроля целостности.  Поэтому злоумышленник может, например, подменить IP-адрес источника — рассылать пакеты со своего устройства, но делать, вид, что они приходят из других мест. Проверить это нельзя, и именно в таком виде они придут на сервер.

При такой атаке злоумышленник генерирует множество пакетов максимального размера и отправляет на сервер-жертву. Опасность в том, что даже если сервер закрыт на firewall, невозможно повлиять на фильтрацию таких данных до их получения сетевым интерфейсом. «Последняя миля» от граничного маршрутизатора до сетевого интерфейса зачастую является наиболее уязвимым местом по пропускной способности. Пакеты всё равно пойдут через ваш канал и заполнят полосу пропускания.

**Что делать.** Банить на сервере пакеты по IP неэффективно, потому что заголовки легко менять (вышеупомянутый спуфинг). А если вы ещё и слушаете что-то по UDP-порту, бороться с ситуацией становится особенно сложно.

Обычно сервисы, которые работают через UDP — потоковые: IPTV, голосовые серверы вроде Тимспика, игры. Есть вариант посчитать длину пакета, которую вы обычно получаете, например, для входа в игру. И настроить firewall так, чтобы в доверенные добавлялись только адреса, откуда пришли пакеты нужного размера с подходящим содержимым. Это можно сделать с помощью анализа дампа трафика, который генерирует легитимное клиентское приложение.

Также есть методы усиления (амплификации), позволяющие многократно усилить атаку. Злоумышленник рассылает совершенно нормальным серверам по всему миру запрос (например DNS запрос, который использует UDP порт 53), в котором подменяет свой адрес на адрес жертвы в заголовках. Соответственно все сервера, на которые пришел запрос, отправляют ответ не на адрес атакующего, а на адрес жертвы, который был указан в заголовках. Так как DNS-ответ намного больше запроса, то и объем данных, который приходит на сервер жертвы, зачастую весьма велик.

Если вы не работаете через UDP, его вообще можно закрыть — так делают многие провайдеры, размещая свои DNS-сервера внутри сети.

Кстати, сейчас активно внедряют новый протокол QUIC, который будет являться транспортным для HTTP3.  Этот протокол работает как раз поверх UDP и, скорее всего, будет подвержен таким атакам. Пока не знаю, как с ними планируют бороться. Может, разработают какие-то подходящие инструменты.

Фрагментированный UDP Flood

У него кроме описанного выше есть дополнительное действие. Атакующий присылает на сервер жертвы пакет, но говорит, что это только часть. Сервер-жертва резервирует у себя ресурс, чтобы собрать пакет, но новые фрагменты не приходят.

**Что делать.** Отбрасывать пакеты, которые по ожиданиям будут слишком большого размера, чтобы не забивать вашу оперативную память.

TCP SYN Flood

У TCP есть механизм установки соединения. Сначала источник посылает SYN-запрос о том, что хочет установить соединение. Сервер-получатель отвечает пакетом SYN+АСК о том, что готов к соединению.

Источник отвечает ACK-пакетом, подтверждая получение SYN+ACK.

Соединение устанавливается, потому что обе стороны подтвердили готовность, и начинают передаваться данные.

Здесь уже есть проверка соответствия IP-адреса, поэтому подменить его не получится. Но атакующий может генерировать SYN-пакет, инициируя новую сессию с сервером-жертвой, а соединение не установить, не отправляя АСК. Такая атака переполняет таблицу соединений, вызывая падение производительности. На настоящие запросы просто не остаётся места.

**Что делать.** Блокировать через firewall по превышению и настраивать лимиты по количеству SYN-пакетов в секунду, которые вы ожидаете для вашего сервиса.

HTTP Flood

Направлена уже не на соединение, а непосредственно на ваш сервис, и обычно воздействует на прикладной уровень модели OSI.

HTTP Flood — это просто генерация запросов. Здесь не происходит какой-то подмены, нарушений стандартов или тому подобного. Это распределённые запросы с целью вызвать недоступность вашего веб-сервера. Банально — злоумышленник отправляет миллионы запросов по генерации главной страницы вашего сайта, и сервер просто не справляется. Это как реальное обрушение в Черную пятницу, только вызванное искусственно.

Борьба с такими атаками сильно разнится в зависимости от инфраструктуры и характера атаки. Дальше расскажу об этом подробнее.

Методы предотвращения и защиты от DDoS-атак

Общий анализ инфраструктуры

1. Составить план инфраструктуры. Однозначно понять, что и где у вас расположено, какие сервисы и серверы вы используете.
2. Проанализировать, какие элементы инфраструктуры должны быть доступны извне. Все, которые не должны быть — закрыть. Например, СУБД не должна быть доступна извне. Стоит в firewall ограничить доступ и сменить порт со стандартного.
3. Убедиться, что IP-адреса инфраструктуры не скомпрометированы. Даже если вы отбили атаку на основной сервис, другой элемент вашей инфраструктуры может стать целью атаки.

Минимизация зоны атаки

1. Настроить firewall сервера. В политиках ни в коем случае нельзя оставлять настройки по дефолту. Важно закрыть все, кроме доверенных адресов и сетей.
2. Скрыть все реальные IP-адреса инфраструктуры. Периодически их менять.
3. По возможности отказаться от нешифрованного трафика. Перестать использовать HTTP и перейти на HTTPS. Это важно для безопасности в целом, но и от DDoS защищает — чтобы злоумышленники не смогли подсмотреть ваши пакеты и понять, как вы их формируете, чтобы потом подделать.
4. Проверить бизнес-логику, чтобы понять, как и куда ваш легитимный клиент должен делать запросы. Так вы научитесь распознавать нелегитимные.
5. Если на физическом сервере находится не один сервис, важно тщательно разграничить их по ресурсам. Чтобы упавший сервис не мог съесть все ресурсы и повредить другим сервисам.

Настроить мониторинг

Бывает так, что DDoS-атаки неочевидны и труднообнаружимы. Например, атаковать могут микросервис по приему заказов. Тогда главная страница будет доступна, но клиенты не смогут сделать заказ — и пока вам об этом не сообщат, вы останетесь в неведении.

Поэтому важно настроить мониторинг показателей сервиса: канал, загрузка CPU, траты памяти, работоспособности отдельных микросервисов и важных для бизнеса элементов сайта.

На что еще обратить внимание

1. После атаки IP бэкенда может остаться известен злоумышленникам. Поэтому его важно менять — ведь раз вас хотят «положить», то после отбитой атаки могут начать атаковать снова.
2. Защищать нужно все сервисы, а не только часть. Иначе эффективность защиты сильно упадет.
3. Граничные маршрутизаторы, «последняя миля» до вашего сервера, не всегда приспособлены подавлять флуд, который забивает ваш канал. Учитывайте это при выборе провайдера.
4. Определённые части кода могут быть плохо оптимизированы и уязвимы к атакам. Их нужно прорефакторить.

Мы в Southbridge достаточно часто сталкиваемся с DDoS-атаками. Последовательно выявляя характер атаки и её паттерны, не так уж сложно выработать методы противодействия и модернизировать инфраструктуру, учитывая необходимость отражения таких атак. Я сталкивался с сильной атакой только один раз, а в остальных случаях справиться всегда удавалось. Значит, и вам по силам построить инфраструктуру, устойчивую к DDoS.