Что такое DDOS и как защититься от него

Докладчик: Мажидов Саидбек.

Сначала разберемся что такое DDOS и DOS

Что такое DDoS-атака
Distributed Denial of Service, или «Распределенный отказ в обслуживании», — это перегрузка информационной системы избыточным числом запросов, блокирующая обработку обращений.

Что такое DoS-атака
Для начала важно понять, что DoS- и DDoS-атаки — не одно и то же.
Denial of Service, или «Отказ в обслуживании», — это перегрузка информационной системы, в которой работает сервисы, с помощью сетевых запросов. При этом сами запросы на сетевом уровне осуществляются с одного компьютера и нацелены на конкретный виртуальный сервер или домен.

Кроме того, что DoS-атаки используют всего один хост для перегрузки системы, есть косвенные признаки, по которым их можно отличить от DDoS. Они менее эффективны и более заметны: когда запросы приходят с одного IP-адреса источника, системному администратору становится очевидна их нелегитимность. Как следствие — DoS-атаки гораздо проще подавить, ведь достаточно использовать брандмауэр.

Потенциальные жертвы

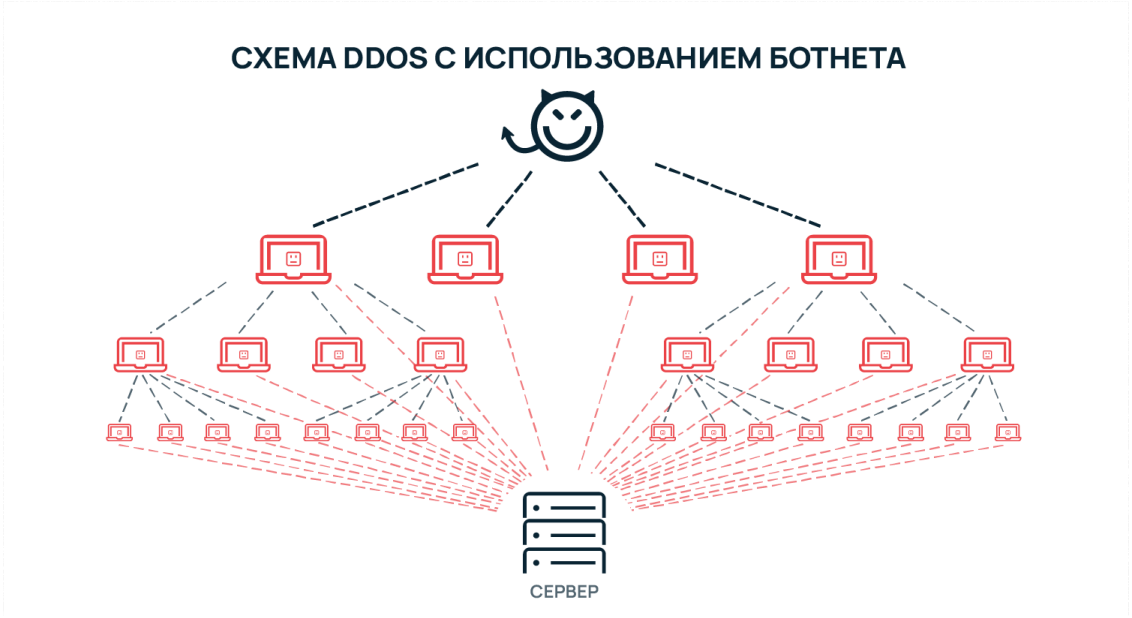
Как правило, жертвами крупных DDoS атак становятся:

- **Корпорации и государственные учреждения**: агрегаторы (маркетплейсы), сайты крупных компаний, отраслевых министерств и др.
- **Финансовые учреждения**: сайты и серверы, порталы банков, бирж, управляющих и инвестиционных компаний.
- **Медицинские учреждения**: больницы, медицинские центры и пр.
- **IoT устройства**: онлайн-кассы, системы «Умный дом» и пр.

Организация DDoS-атак

Серверы имеют ограничения на одновременную обработку запросов.

Также для оптимизации нагрузки предусмотрено ограничение пропускной способности канала связи, соединяющего сеть и сервер. Для обхода ограничений злоумышленники организуют специальную сеть с вредоносным ПО («ботнет»). Для наглядности ее схема приведена ниже.



Входящие в инфраструктуру «ботнет» компьютеры не связаны между собой. Они используются для генерации избыточного трафика, способного перегрузить атакуемую систему. Для этого на компьютеры ставится троян, который запускается удаленно. Атаке подвергается DNS сервер, пропускной канал и интернет-соединение.

Признаки DDoS-атаки

Распознать атаку можно по следующим признакам:

- **Некорректная работа серверного ПО и операционных систем**: зависания, произвольные завершения сессий и пр.
- **Пиковая нагрузка по запросам на сервер**: нагрузка на ЦП, оперативную память, диск и другие компоненты сервера, превышающая средние значения.
- **Рост числа запросов на порты**.
- **Одинаковая модель поведения**: злоумышленники пытаются маскировать вредоносный трафик, закладывая в алгоритмы симуляцию действий пользователей (скачивания файлов, просмотры страниц, использование поиска и пр.). Выявление массового совершения однотипных действий может послужить сигналом.
- **Однотипные запросы к портам и сервисам**: выявить возросшую нагрузку, однотипные запросы к службам сервера можно по анализу логов. Массовые запросы, если генерирующие их пользователи не похожи на типичную аудиторию, являются хорошим маркером.

Виды DDoS-атак

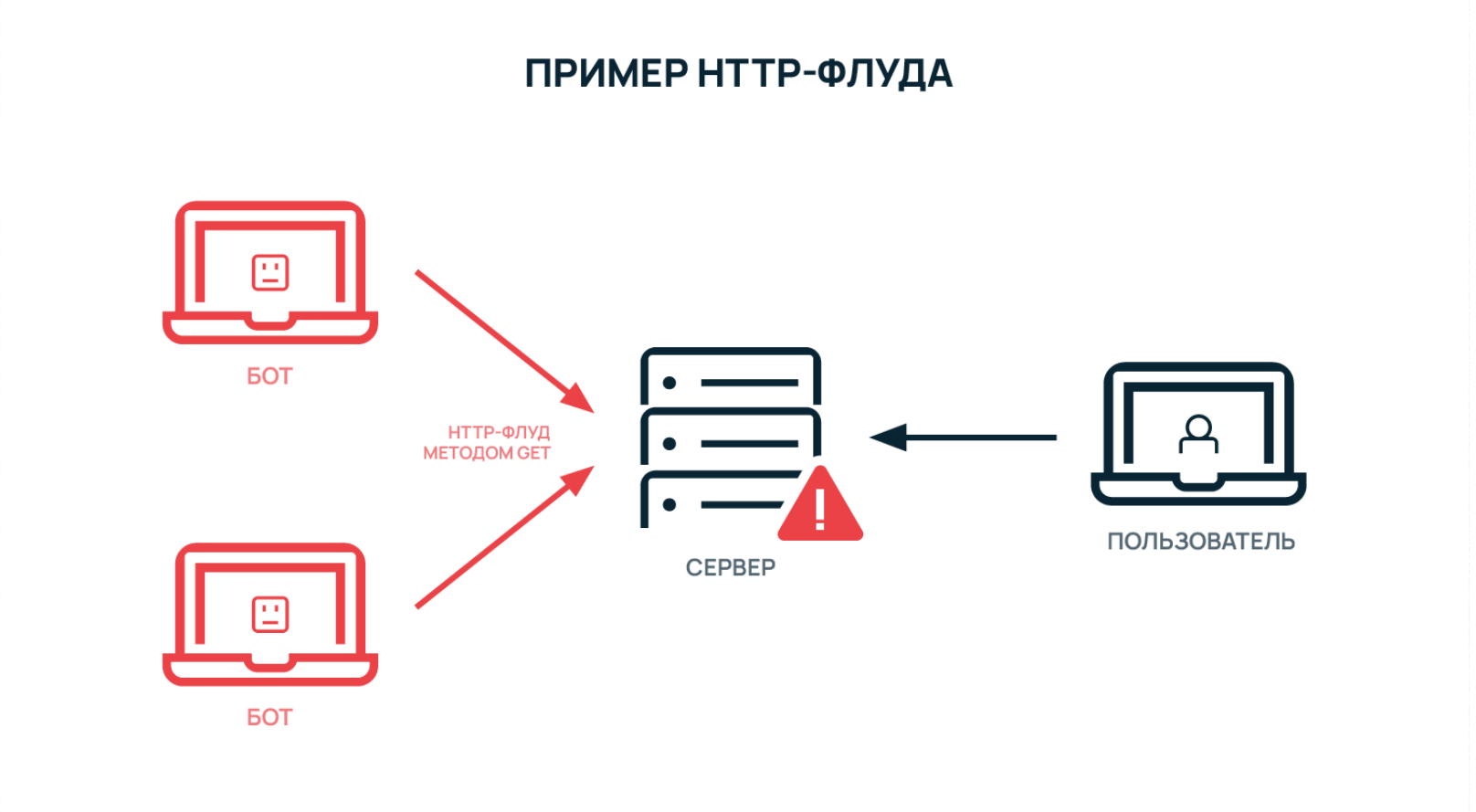
Атаки транспортного уровня

Атака направлена на перегрузку брандмауэра, центральной сети или системы, распределяющей нагрузку. При атаках такого вида распространено использование сетевого флуда, при котором генерируется масса однотипных запросов-пустышек, перегружающих канал. Основной упор здесь делается на методику обработки клиентских запросов к серверу.

Как правило, сетевая служба работает по методу FIFO, согласно которому в приоритете первое обращение. Однако, при флуде генерируется такой объем запросов, что аппаратных ресурсов сервера не хватает для завершения обработки первого запроса.

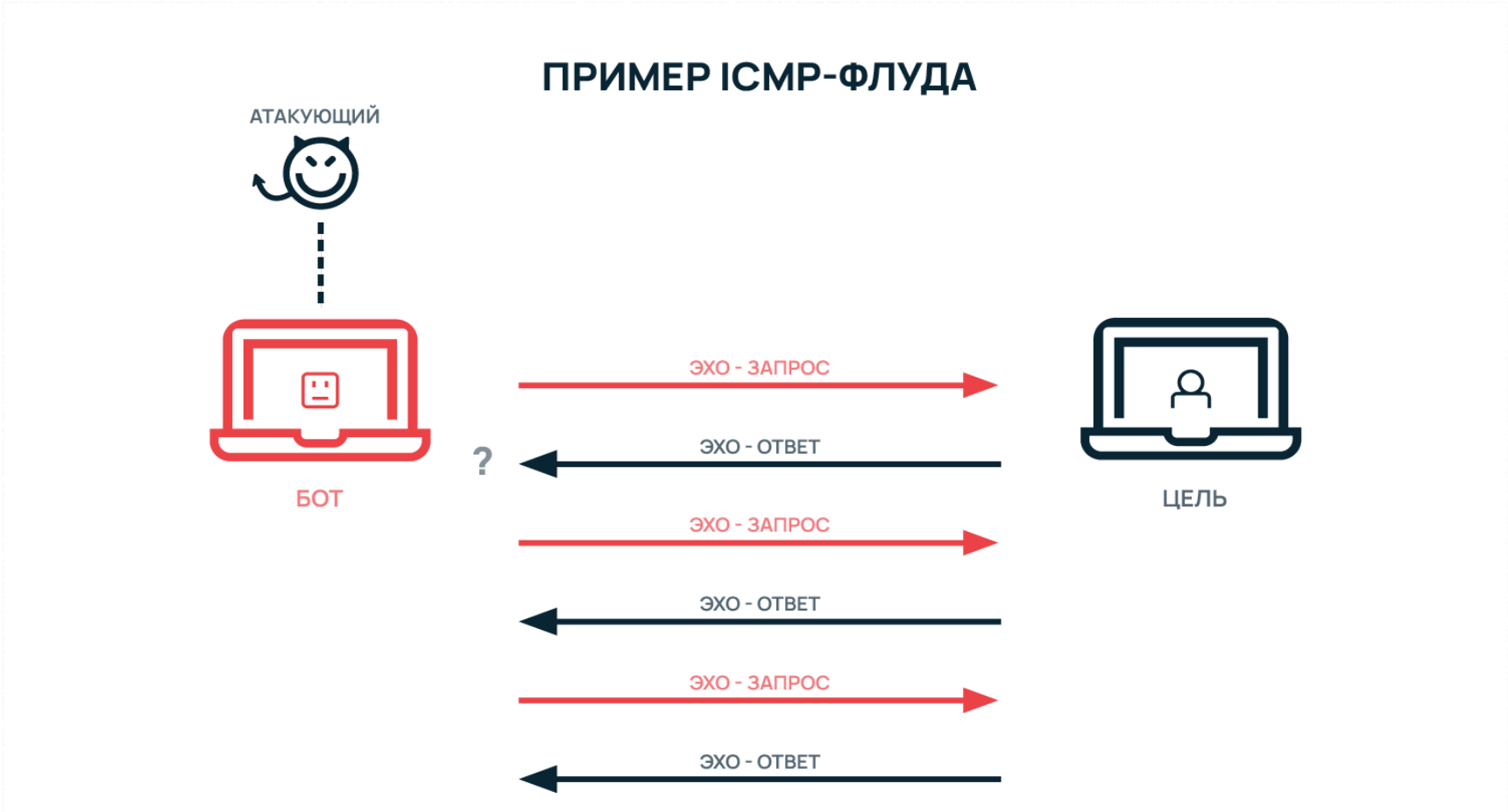
HTTP-флуд

Сервер получает избыточный объем HTTP-запросов клиентов, в результате чего все узлы связи становятся недоступными.



ICMP-флуд

Перегружает сервер жертвы служебными командами, на которые машина должна давать эхо-ответы. Классический пример DDoS-атаки — Ping-флуд, когда на сервер непрерывно отправляются ICMP-пакеты для проверки доступности узла.

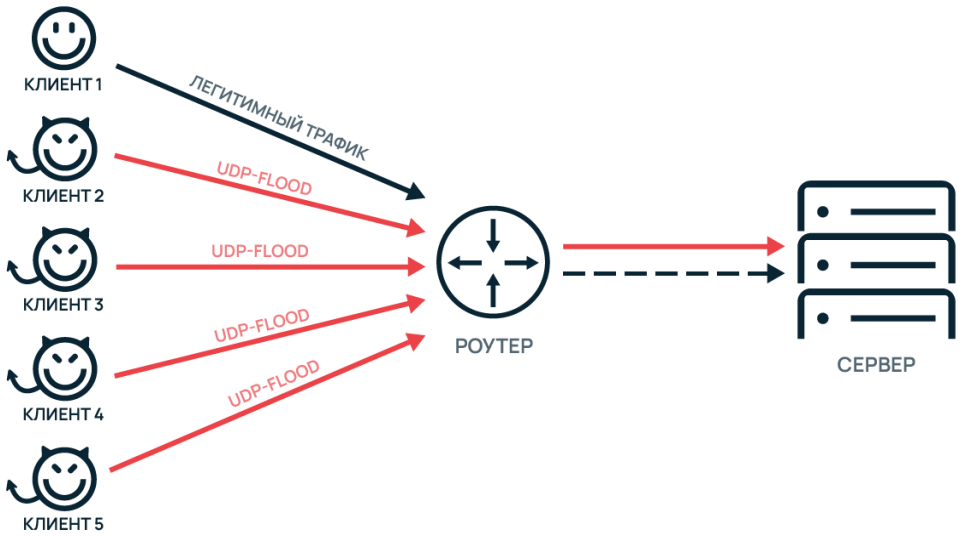


SYN-флуд

- На сервер отправляется избыточный объем SYN-запросов на TCP-подключение. Согласно алгоритму «тройного рукопожатия», сервер должен ответить на SYN-запрос клиента пакетом с флагом ACK (Acknowledge). После этого будет установлено соединение. В случае с SYN-флудом, очередь SYN-пакетов на сервере переполняется.
- При этом заголовки SYN-пакетов подделываются таким образом, чтобы ответные пакеты с сервера уходили на несуществующие адреса. Таким образом, злоумышленник создает цепочку наполовину открытых соединений, забивающих канал и делающих невозможным доступ рядовых пользователей к серверу и его службам.

UDP-флуд

- Атакуемое устройство получает множественные UDP-запросы с измененными IP-адресами источников. Так злоумышленник сохраняет анонимность паразитной сети, забивая полосу пропускания сервера. Суть атаки в следующем: из вредоносной сети на жертву направляется поток запросов по протоколу UDP. Сервер должен обработать запрос, разобрав приходящий пакет и определив для него соответствующее приложение (сервис, порт).
- Затем нужно перенаправить запрос туда и в случае успеха вернуть ответ службы. В случае отсутствия активности будет отправлено сообщение «Адресат недоступен» по протоколу ICMP. Поскольку в пакетах был изменен адрес источника инициатора запроса, то ICMP-отказы уходят на другие узлы. Тем временем, вредоносный алгоритм продолжает поддерживать очередь запросов переполненной.



Атаки уровня инфраструктуры

Атаке уровня приложения L7 модели OSI подвергаются оперативная память, процессорное время, а также подсистема хранения данных на сервере.

При этом пропускной канал не перегружается.

Существуют несколько видов таких атак.

- ***Вычисления***

Процессор получает запросы на «тяжелые» вычисления. Ввиду переизбытка запросов сервер начинает сбоить и пользователи не получают доступ к серверу, его службам и ресурсам.

- ***Переполнение диска***

Дисковое пространство сервера начинает заполняться «мусорным» содержимым с помощью вредоносного кода злоумышленников. Переполнение диска нарушает работу веб-серверов, функционал которых построен на активной работе с файловой системой (хранение, доступ и воспроизведение мультимедиа и другого контента). Для заполнения используются лог-файлы (данные о запросах и сессиях, формируемые на стороне сервера). Предотвратить умышленное заполнение диска можно ограничив размер лог-файлов.

- ***Обход системы квотирования***

Злоумышленник получает доступ к CGI-интерфейсу сервера и с его помощью использует аппаратные ресурсы машины в своих интересах.

Атаки уровня приложений

При таких атаках используются заложенные в серверное ПО упущения, создающие уязвимости. Классический пример — атака «Пинг смерти», когда на атакуемую машину направляется избыточный объем ICMP-пакетов, переполняющих буфер памяти.

DNS-атаки

Атаки этого вида направлены на:

- **Использование уязвимостей в ПО DNS-серверов**: «уязвимость нулевого дня», «Быстрый поток», «DNS-спуфинг».
- **Обрушение DNS-серверов**: из-за отключения службы DNS пользователь не сможет зайти на страницу сайта, поскольку его браузер не найдет IP-адрес нужного узла.

Предотвращение и защита от DDoS-атак

Наиболее эффективный способ защиты от DDoS-атак на сайт — это фильтрация подозрительной сетевой активности на уровне хостинг или интернет-провайдера.

Причем выполняться это может как средствами сетевых маршрутизаторов, так и с помощью специального оборудования.

Владелец же сайта, веб-сервиса или другого сетевого проекта, со своей стороны, для минимизации рисков и потерь от DDoS должен:

- **Тщательно обследовать логику своего продукта**: еще на этапе разработки и тестирования можно исключить ошибки и уязвимости.
- **Вести контроль версий ПО и сетевых служб**: необходимо своевременно обновлять программное обеспечение сетевых служб (СУБД, PHP и пр.). Также нужно поддерживать код самого продукта в актуальном и стабильном состоянии. Рекомендуется даже разворачивать проект на нескольких серверах — продуктовом (боевом), тестовом (для обкатки нового функционала) и бэкап-сервере (для хранения резервных копий и архивов исходников). Также рекомендуется использовать системы контроля версий (Git) для возможности отката проекта к предыдущей стабильной сборке.
- **Следить за доступом к сетевым службам**: делегирование прав на операции требует проработки. Необходимо обеспечить несколько уровней доступа (мастер, гостевой и пр.) к сетевым службам сервера и архиву версий проекта. Список лиц, имеющих доступ к ресурсам сервера, необходимо поддерживать в актуальном состоянии — например, своевременно отключать доступ уволившимся сотрудникам. Также нужно сбрасывать пароли и учетные записи при любом подозрении на компрометацию.
- **Контролировать панель администратора**: рекомендуется ограничить доступ к панели внутренней, либо VPN-сетью.
- **Сканировать систему на наличие уязвимостей**: в этом помогут публичные рейтинги (например, OWASP Top 10), либо инструменты разработчика.

- **Использовать брандмауэр приложений**: автоматизируйте проверку сетевого трафика и валидации запросов к портам и службам сервера.
- **Распределять трафик с помощью CDN**: за счет распределенного хранения контента нагрузка на ресурсы сервера оптимизируется, что ускоряет обработку трафика и запросов.
- **Вести списки контроля доступа (ACL)**: для персонального ограничения доступа к сетевым узлам.
- **Очищать кэш DNS**: для защиты от спуфинга.
- **Использовать защиту от спама**: один из источников уязвимостей — формы обратной связи. Злоумышленники могут направить своих ботов массово заполнять их отправлять однотипные данные на сервер. Для фильтрации такого трафика формы нужно переводить на JS-компоненты или оснащать их капчами и другими инструментами проверки;
- **Использовать контратаку**: вредоносный трафик можно перенаправить на сеть атакующего. В результате это не только сохранит доступность Вашего сервера, но и временно выведет злоумышленника из игры.
- **Использовать распределенное хранение и бэкапирование**: в случае отказа одного или нескольких серверов Вашей сети Вы сможете возобновить работу ресурса на другой машине. К этому времени там уже будет развернута функциональная копия Вашего проекта.
- **Использовать аппаратные средства защиты**: Impletec iCore, DefensePro и пр.
- **Тщательно выбирать хостинг-провайдера**: необходимо выбирать поставщика, дающего гарантии защиты от всех современных угроз. Также немаловажно иметь круглосуточную линию поддержки, панель администратора с необходимыми инструментами аналитики по конкурентным условиям.

Защита DNS

Брандмауэры и системы предотвращения вторжений на серверы

сами по себе уязвимы и рассчитывать только на их надежность не стоит.

Для TCP-трафика рекомендуется использовать облачные сервисы для фильтрации подозрительных запросов. Также рекомендуется:

- **Проводить мониторинг DNS**: подозрительную сетевую активность можно отследить. Для этого рекомендуется использовать коммерческие DNS-решения, либо open source-продукты (например, BIND). Вы сможете в режиме реального времени отслеживать сетевой трафик и запросы к DNS. Для экономии времени также рекомендуется построить базовый профиль сетевой инфраструктуры и обновлять его по мере масштабирования бизнеса.
- **Расширять аппаратные ресурсы DNS**: компромиссное решение, позволяющее защитить инфраструктуру от мелкомасштабных атак. Закупка дополнительных мощностей также сопряжена и с вложениями.
- **Использовать DNS Response Rate Limiting (RRL)**: это снижает вероятность использования Вашего DNS-сервера в атаке DDoS Reflection. RRL снижает скорость обработки повторных запросов. Этот параметр поддерживается большинством DNS;
- **Строить конфигурации высокой доступности**: DNS-служба разворачивается на HA-сервере, что позволяет восстановить работу сервиса на резервной машине в случае если основная окажется недоступной.

Географически распределенная сеть также может послужить средством защиты от DDoS. Существует два подхода к построению такой сети:

- **Anycast**: разные DNS-серверы используют общий IP-адрес, а при обработке трафика запросы направляются на ближайший сервер. Такой подход, по сравнению с описанным ниже, является более оптимальным, поскольку трафик и нагрузки распределяются между несколькими машинами. Это делает инфраструктуру более устойчивой к DDoS.
- **Unicast**: за каждым сервером DNS закрепляется уникальный IP-адрес. Служба DNS поддерживает таблицу серверов и соответствующих им адресов ресурса. При обработке запросов для балансировки трафика и нагрузок IP-адрес выбирается в случайном порядке. Такой подход к организации DNS-сети проще в реализации, однако при этом страдает устойчивость инфраструктуры. Злоумышленники могут инициировать цепочку направленных атак на DNS-серверы, последовательно выводя их из строя.

Аппаратная Защита от DDOS-атак

Аппаратная защита от DDoS-атак состоит из специализированной системы, разработанной для обнаружения, анализа и смягчения киберугроз. Она основана на использовании физических машин, способных обрабатывать массивные объемы сетевого трафика и реагировать на атаки в режиме реального времени.

Технология аппаратной защиты строится на идентификации аномальных и агрессивных сетевых потоков, которые после этого блокируются перед достижением защищаемых сетей. Таким образом достигается непрерывная работа и безопасность сетевой инфраструктуры.

Аппаратная защита состоит из программных модулей, которые устанавливаются на физические машины. Также подключаются специализированные межсетевые экраны, такие как Cisco ASA, FortiGate, Cisco FirePower, UserGate и другие защитные системы. Весь комплекс устройств обеспечивает следующие функции:

- **Обнаружение атак**

Аппаратные устройства анализируют и изучают трафик, проходящий через сеть, чтобы обнаружить признаки DDoS-атак. Он включает в себя анализ сетевых пакетов, поведенческий анализ трафика, сравнение с предварительно известными сигнатурами атак.

- **Фильтрация трафика**

Когда система обнаруживает атаку, аппаратные устройства автоматически запускают различные методы фильтрации трафика для определения вредоносного и легитимного. Для этого используются различные подходы — например, блокирование IP-адресов или применение правил доступа (ACL), фильтрация трафика с невалидной структурой пакетов, отслеживание корректности установления TCP-сессии, применение threshold порогов для выделенных сигнатур трафика.

- **Повышение пропускной способности**

В случае массированной DDoS-атаки, объем трафика значительно возрастает, что ведет к перегрузке сети и полному ее отказу. Чтобы не допустить подобной ситуации, аппаратная защита может обеспечивать дополнительную пропускную способность, чтобы обрабатывать большие объемы трафика и справляться с атакой.

Как работает аппаратная защита

Аппаратно-программный комплекс состоит из двух частей:

- аппаратные устройства
- программные модули.

Система работает следующим образом — когда любая программа пытается получить доступ к данным, она отправляет запрос к аппаратному устройству, которое обеспечивает работу ключа (токена, ридера, электронного идентификатора). После подключения этого устройства к компьютеру, оно дает разрешение на работу только в случае положительной реакции.

С точки зрения надежности, данная методика предпочтительнее, чем просто программная защита. Однако стоимость аппаратной части делает ее доступной лишь для крупных и средних компаний, а также государственных организаций.

Работа программно-аппаратной защиты состоит из следующих этапов:

1. Пользователь запускает программу и идентифицируется.

2. Программа отправляет запрос на доступ к данным, указывая требуемые разрешения.

3. Программа связывается с устройством, обеспечивающим работу ключа, таким как токен, ридер или электронный идентификатор.

4. Аппаратная часть выполняет проверку подлинности пользователя, используя предоставленную информацию. Например, пароль или биометрические данные.

5. В зависимости от результата проверки подлинности, аппаратная часть принимает решение о предоставлении или отказе в доступе к данным.

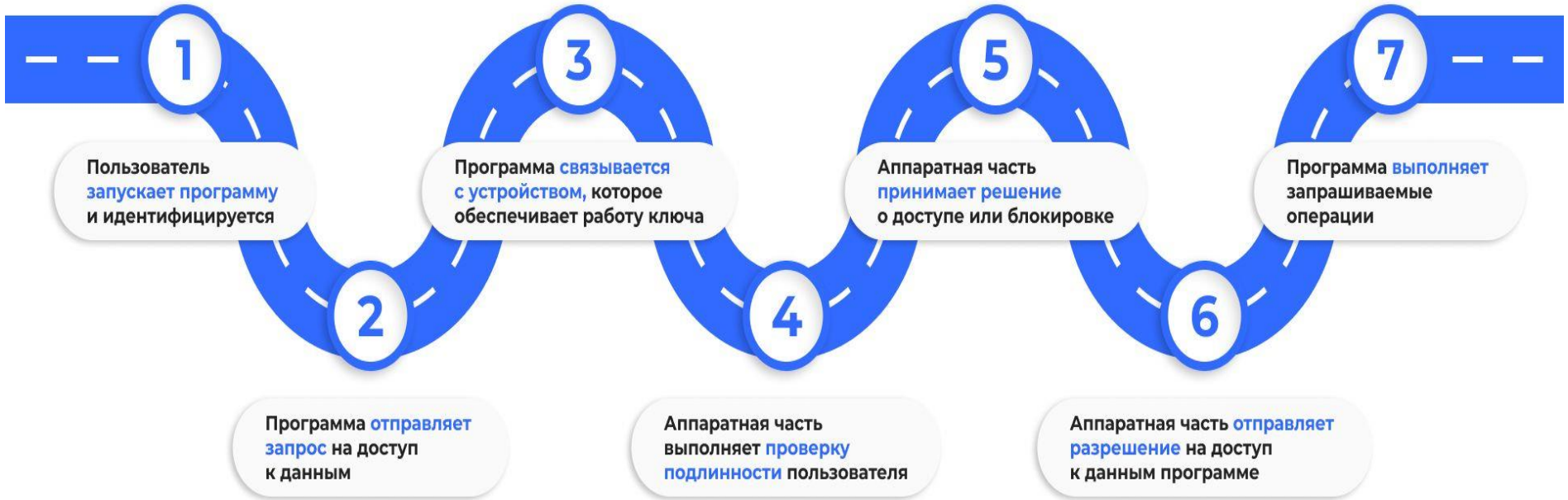
6. Если проверка подлинности успешна, аппаратная часть отправляет разрешение на доступ к данным программе.

7. При получении доступа программа выполняет запрашиваемые операции и обрабатывает информацию.

8. По завершении работы с данными или при выходе из программы, аппаратная часть отключается от компьютера.

Nihol

Работа программно-аппаратной защиты



По завершении работы с данными или при выходе из программы, аппаратная часть отключается от компьютера

Плюсы и минусы аппаратной защиты от DDoS-атак

Плюсы аппаратной защиты	Минусы аппаратной защиты
Высокая производительность и способность обрабатывать большие объемы трафика	Требует физического оборудования и инфраструктуры
Локальное размещение, обеспечивающее полный контроль над оборудованием	Большие начальные инвестиции для приобретения и обслуживания оборудования
Низкая задержка и минимальное влияние на сетевую производительность	Не такая гибкая и масштабируемая, как облачная защита
Большие возможности для настройки правил фильтрации и реализации индивидуальных решений под задачи клиента	Необходимость иметь широкие каналы для возможности утилизации высокоскоростных пакетных DDoS-атак до 400 Гбит/с
Независимость от сторонних поставщиков услуг	Ограничения географического покрытия и защита только на локальном уровне. Облачная фильтрация позволяет очищать трафик на континенте источника DDoS-атаки

Спасибо за внимание!

Узбекистан, г. Ташкент, 100187, ул. Интизор, 26,
Группа компаний NIHOL

(998-71) 208-58-44, 208-58-45, 208-58-48, 266-58-46, 266-58-47

info@nihol.uz