Как финансовые организации могут максимально увеличить Безопасность, Эффективность и Надежность своего онлайн бизнеса

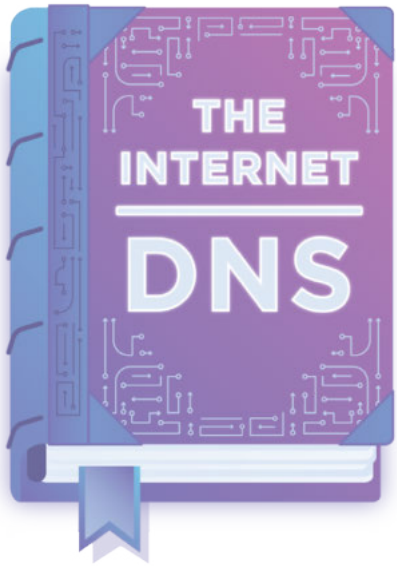
Предоставление онлайн-сервиса на высочайшем уровне становится в наши дни стандартом. Поскольку спрос на веб-сервисы и приложения растет, финансовые организации должны обеспечивать, чтобы эти веб-сайты и приложения оставались максимально безопасными, быстрыми и надежными.

Помимо этой устойчивой тенденции, как таковой, имеются еще несколько современных трендов, которые делают опыт использования онлайн-сервиса клиентом особенно актуальной проблемой для финансовых организаций в частности.
Данный сектор уже давно является главной мишенью DDoS-атак на прикладном и сетевом уровнях. Объем и сложность таких атак постоянно возрастает, создавая повышенные риски в части доступности сайта и приложений.

Кроме того, изменения и всплески интернет-трафика становятся все более экстремальными, что приводит к усилению давления как на пограничную, так и на сетевую инфраструктуру. Что могут сделать компании, чтобы обеспечить клиентам мгновенный доступ к своим деньгам и финансовым данным, независимо от перегрузки сети или скачков спроса?

Чтобы ответить на этот вопрос, надо учесть несколько аспектов. Далее приведены пять ключевых соображений, которые могут помочь любой финансовой организации начать работу.

Воспользуйтесь DNS и DNSSEC-защитой для повышения отказоустойчивости и времени полезной работы



Систему доменных имен или DNS часто называют «адресной книгой Интернета», поскольку именно она переводит доменные имена в состоящие из последовательности цифр IP-адреса и она же позволяет браузерам загружать находящиеся в Интернете ресурсы. DNS задумана и функционирует таким образом, чтобы принимать любой предоставленный ей сетевой адрес, поэтому крайне актуален вопрос о выборе грамотной стратегии защиты DNS. Отсутствие такой защиты подвергает организацию целому ряду рисков, в числе которых перехват DNS-запросов, атака посредника (man-in-the-middle), утечка и утрата конфиденциальной информации пользователей, сетевое мошенничество (фишинг) и прочие не менее серьезные виды угроз. По мере увеличения количества кибератак, мишенью которых становится DNS, многие компании начинают осознавать, что отсутствие надежной защиты делает DNS-сервер «слабым звеном» в стратегии общей безопасности их информационного онлайн-пространства.

Существуют разные подходы, которые организация может взять на вооружение для развертывания своей стратегии обеспечения отказоустойчивости DNS. Одним из вариантов является обратиться к профессиональному провайдеру услуг управляемого хостинга DNS (сервисы Managed DNS), на платформе которого могут храниться все DNS-записи, он же предложит услуги по разрешению запросов на множестве узлов в разных точках мира и обеспечит комплексную поддержку DNSSEC – модулей безопасности системы доменных имен. DNSSEC – это дополнительный уровень защиты для системы доменных имен, добавляющий к существующим DNS-записям криптографическую подпись. Дополнительный запас прочности и резервирования можно создать путем внедрения стратегии мульти-DNS: при отказе первичного сервера вторичный DNS-сервер обеспечит бесперебойное функционирование приложений. Крупные компании, предпочитающие опираться на собственную DNS-инфраструктуру, могут в сочетании с вторичным DNS-сервером использовать такой механизм как сетевой экран или DNS-файрвол. Этот механизм служит еще одним уровнем защиты для локальной инфраструктуры DNS и помогает обеспечивать резервирование всей системы DNS в целом.

Успешный опыт наших клиентов

Одна компания, занимающаяся операциями с криптовалютой и предлагающая клиентам для работы с блокчейном сетевой инструмент на базе открытого исходного кода, столкнулась с необходимостью повысить степень защиты своей системы DNS, после того как в результате изощренной кибератаки все DNS-запросы были переадресованы на подставной сайт. Хакерам удалось «убедить» один из полномочных серверов в том, что все запросы к сайту этой компании должны быть перенаправлены на новый адрес. Подставной сайт выглядел точно так же, как подлинный сайт компании, что позволило хакерам завладеть личными ключами пользователей и получить доступ к огромным суммам криптовалюты.

Подобно многим другим интернет-сайтам, эта компания стала мишенью для кибератаки в силу общей уязвимости базовой инфраструктуры Сети, в результате чего утратила доверие своих клиентов. Чтобы такого больше никогда не повторилось, эта организация воспользовалась сервисом DNS от Cloudflare. Выбор этого продукта от Cloudflare стал наиболее простым и эффективным путем внедрения DNSSEC. Компания-заказчик получила возможность управления протоколом с помощью одного простого в использовании механизма, который не только позволил ей повысить отказоустойчивость системы безопасности, но и сделал более безопасным и эффективным взаимодействие ее клиентов с сервисами сайта, от работы которых зависела безопасность их криптовалютных активов.

Чтобы более подробно ознакомиться с информацией об интеграции DNS и DNSSEC, заходите на Cloudflare DNS.

Упростите доступ к своему контенту, выбирая наименее загруженные маршруты передачи трафика

На сегодняшний день доставка большей части веб-трафика осуществляется через Сети доставки контента (CDN), по которым также проходит трафик крупнейших сайтов, в том числе Amazon и Facebook. CDN представляет собой группу географически распределенных серверов, которые обеспечивают мгновенный доступ к онлайн-контенту для множества пользователей в разных точках земного шара, а также способствуют сокращению затрат на поддержание пропускной способности.

Благодаря размещению серверов в множестве точек по всему миру CDN уменьшает расстояние между контентом и его потребителями, что, в свою очередь, сокращает неизбежно возникающие сетевые задержки и снижает время загрузки веб-страниц. Сети CDN могут извлекать статические файлы из своего сетевого кэша, что сокращает количество запросов, направляемых на размещенные в них веб-сервера, и приводит к снижению затрат на поддержание пропускной способности и на хостинг.

Успешный опыт наших клиентов

Онлайн платформа для банковских и страховых продуктов столкнулась с проблемами производительности, когда она расширила свой бизнес, ранее ограниченный домашним регионом в Сингапуре, и вышла на менее зрелые азиатские рынки. Более медленные локальные сети и нестабильная инфраструктура повлияли на качество обслуживания клиентов, что затруднило работу компании в период критического роста. Они начали искать решение, которое позволило бы сократить время загрузки для их конечных пользователей в разных географических регионах.

Сеть доставки контента (CDN) Cloudflare помогает им обеспечить превосходную производительность по всем направлениям, несмотря на различные уровни цифровой зрелости на конечных рынках. Сеть Cloudflare охватывает более 200 городов в 90 странах мира, обеспечивая быструю доставку контента компании клиентам независимо от того, где они находятся и какое устройство используют. Кроме того, решение Cloudflare Argo Smart Routing (умная маршрутизация Argo) использует ежесекундно рассчитываемые интеллектуальные данные по всей своей сети для направления контента по маршруту в обход перегруженности, изолируя компанию от проблем с локальной инфраструктурой.

Переход на Cloudflare помог компании добиться снижения затрат на пропускную способность примерно на 75% и улучшить производительность сайта на 50%.

Чтобы узнать, как CDN может ускорить доставку контента, и как это может пригодиться в вашем бизнесе, заходите на Cloudflare CDN

Сведите к минимуму риск сбоев в работе сайта с помощью глобальной балансировки нагрузки трафика

Максимизация ресурсов сервера и повышение производительности – непростая задача, требующая тщательного и сбалансированного решения. Перегруженные или находящиеся на слишком большом удалении от конечных пользователей сервера могут стать крайне негативным фактором для функционирования бизнеса, поскольку приводят к увеличению задержек в работе сети, а сбой сервера способен привести к потере прибыли, подрыву доверия со стороны клиентов и в целом больно ударить по имиджу бренда.

Облачные балансировщики нагрузки трафика занимаются распределением запросов между множеством различных серверов, что ставит целью предотвратить скачки трафика. Решение о балансировке нагрузки принимается на периферии сети, ближе к пользователям, за счет чего компания может достичь оптимального времени отклика и повысить эффективность сетевой инфраструктуры, одновременно сводя к минимуму риск сбоев на сервере. При отказе хотя бы одного сервера балансировщик нагрузки может перенаправить и перераспределить трафик между оставшимися в строю серверами, что не позволит пользователям столкнуться с ощутимыми задержками или сбоями в работе сайта. Балансировщик нагрузки служит также инструментом активной проверки функционирования сетевых серверов, в результате которой организация может выявить сервера с падающей производительностью и принять заранее меры для предотвращения их сбоя.

Успешный опыт наших клиентов

Компания, разрабатывающая программное обеспечение по подготовке налоговой документации для бухгалтерских фирм иналогоплательщиков-физических лиц уже давно использует собственное решение для балансировки нагрузки, чтобы поддерживать время безотказной работы. К сожалению, существующее у них решение не предусматривало возможность масштабирования, что затрудняло решение проблемы резких скачков трафика во время ежегодного сезона подачи налоговых деклараций. Помимо сложностей с масштабированием, управление их собственным балансировщиком нагрузки было трудоемкой задачей, с которой их технический директор часто должен был справляться самостоятельно.

Продукт Cloudflare стал идеальным решением для этой компании-разработчика налогового программного обеспечения. Используя балансировку нагрузки от Cloudflare, данная компания смогла управлять трафиком на нескольких серверах в пиковый налоговый сезон, достигнув 100% безотказной работы и превосходной производительности для своих пользователей. Кроме того, они смогли настроить решение Cloudflare с помощью нескольких щелчков мыши, что обеспечило плавный переход от их предыдущего внутреннего решения на текущее. Унифицированная и интуитивно понятная панель управления Cloudflare значительно сократила время, затрачиваемое компанией на поддержание своей инфраструктуры, высвободив инженерное и ИТ-время для более важных бизнес-задач.

«Использование балансировщика нагрузки Cloudflare позволило нам эффективно и быстро управлять нашими веб-серверами в течение активного сезона нашего бизнеса и быть уверенными, что не будет допущено никакой путаницы, всё благодаря интерфейсу Cloudflare», - отмечает технический директор компании. «Теперь я могу поручить балансировку нагрузки кому-то другому и они легко с этим справляются.»

Узнайте, как можно повысить производительность работы приложений и их готовность к работе с помощью Cloudflare Load Balancing.

Защитите веб-приложения от кибератак

Для компаний, ведущих свой бизнес онлайн, просторы глобальной сети становятся плацдармом для самых разнообразных кибератак, осуществляемых из разных мест и отличающихся уровнем сложности и опасности. При выборе системы безопасности для веб-приложений и прочих важных для функционирования бизнеса элементов может пригодиться многоуровневая стратегия защиты, работающая против самых разных видов угроз.

A. Межсетевой экран для защиты веб-приложений

Межсетевой экран (файрвол) для веб-приложений (WAF) представляет собой инструмент фильтрации и мониторинга HTTP-трафика. Имея в своем арсенале WAF, организация может обеспечить себе защиту от атак «нулевого дня» и уберечь свои веб-приложения от таких распространенных угроз, как подделка межсайтовых запросов (CSRF), межсайтовый скриптинг (XSS) и атаки с применением SQL-инъекций, которые выводят из строя сервера и приводят к хищению или порче данных.

WAF служит инструментом пристального контроля организации над реализацией политики безопасности, что достигается путем определения набора правил для защиты имеющихся в приложениях уязвимостей и выстраивания надежной системы борьбы с вновь возникающими угрозами. Облачный WAF, как правило, является наиболее гибким и экономичным с точки зрения внедрения инструментом, поскольку он может постоянно обновляться для обеспечения надежной защиты от новых видов угроз, не требуя при этом значительных дополнительных усилий или затрат со стороны пользователя.

Успешный опыт наших клиентов

Мультинациональная финансовая корпорация, входящая в список Fortune 500, столкнулась с определенными сложностями, когда зашла речь о добавлении на ее платформу дополнительных маркетинговых сайтов для каждой зоны географического присутствия. Корпорация должна была обеспечить свое глобальное присутствие онлайн, но при этом была вынуждена либо прибегать к аутсорсингу, получая в итоге систему сложной конфигурации, либо оплачивать дорогостоящие профессиональные услуги своего прошлого провайдера – все это оказалось трудоемким и затратным. Компания искала современное архитектурное решение, способное обеспечить ей точечный контроль над своими веб-ресурсами и помочь сбалансировать работу локальных дата-центров и облачных приложений в рамках мультиоблачного подхода.

Внедрив решение Cloudflare, компания получила возможность за считанные минуты обеспечить защиту свыше 700 своих веб-ресурсов, причем без дополнительных затрат. Теперь они наслаждаются результатом в виде более гибкой и самодостаточной системы, работа которой экономит время и бесценные человеческие ресурсы.

Внедрение многоуровневой стратегии безопасности является ключевым приоритетом для данной компании, поскольку многие из ее сайтов предоставляют банкам доступ к сервисам цифровых карт и прочей конфиденциальной информации. Достаточно будет одной единственной успешной кибератаки, чтобы безнадежно испортить их репутацию и нарушить доверие со стороны контрагентов и заказчиков. Продукты Cloudflare Web Application Firewall (WAF) и Advanced DDoS Protection надежно защищают каждый из сайтов компании от кибератак и угроз.

Узнайте, как можно защитить наиболее важные для бизнеса веб-приложения от кибератак с помощью Cloudflare Web Application Firewall.

B. Защита от DDoS-атак

Для большинства веб-сайтов большой объем трафика – явление положительное, поскольку означает увеличение числа клиентов, продаж и повышение коэффициента конверсии. Вместе с тем, они могут быть уязвимы к скачкам трафика вследствие кибератак, ставящих целью нарушить сетевое соединение, перегрузить сервера и не дать добросовестным пользователям попасть на сайт.

DDoS-атака представляет собой попытку киберзлоумышленников перегрузить сервера, устройства, сеть или окружающую инфраструктуру потоком «плохого» трафика. В ходе таких атак насыщается вся полоса пропускания между устройствами – объектами атаки и Сетью, что неизбежно приводит к серьезным перебоям в работе сервиса и оказывает ощутимое негативное воздействие на ход бизнес-операций, поскольку пользователи теряют возможность доступа к ресурсам, необходимым им для работы.

Успешный опыт наших клиентов

Для крупнейшей в мире торговой платформы, работающей с криптовалютой, защита часто совершаемых на ней сделок от сбоев, вызванных DDoS-атаками, представляла собой первостепенную задачу. Нарушение безопасности означало простои сервиса, каждая секунда которых приводила к потере дохода, так как миллионы сделок не могли быть выполнены. Мало того, простои влияли на удержание клиентов — если клиенты не могли торговать с помощью данной платформы, они отправлялись в другое место, чтобы завершить сделку.

Благодаря безлимитной и неограниченной защите от DDoS-атак, предоставленной Cloudflare, эта работающая с криптовалютой торговая платформа получила уверенность в том, что их платформа будет доступна всегда и не будет скомпрометирована. Со своей системой интеллектуального распознавания угроз, основанной на 26 миллионах веб-свойств, продукт Cloudflare способен защитить данную торговую платформу против большинства самых изощренных атак. Пропускная способность сети 30 Тбит/с позволяет Cloudflare обрабатывать любые современные распределенные атаки, в том числе нацеленные на DNS-инфраструктуру.

Более подробно ознакомиться с информацией о формировании многоступенчатой стратегии безопасности можно, зайдя на Cloudflare Advanced DDoS Protection. Cloudflare Advanced DDoS Protection (Cloudflare — усовершенствованная защита от DDoS-атак).

C. Нейтрализация вредоносных ботов

Для обеспечения более полной защиты клиентских данных и веб-приложений от киберугроз необходимо внедрение многоступенчатой стратегии безопасности. Помимо обычных угроз кибербезопасности сайты часто становятся мишенью для вредоносных ботов, которые перегружают веб-сервера, искажают статистику, мешают доступу пользователей к веб-страницам, похищают данные и нарушают работу важнейших бизнес-функций.

Обычные, не вредоносные боты относятся к приложениям, запрограммированным на выполнение полезных задач – от сканирования контента веб-страниц до ответа на запросы пользователей на веб-сайтах. Однако, в случае захвата хакерами контроля над ботами они становятся инструментами в руках злоумышленников и используются ими в их вредоносных целях: от атак методом credential stuffing (вид кибератаки, при которой преступник пытается авторизоваться с помощью автоматической подстановки украденных регистрационных данных), взлома конфиденциальных данных до кражи SEO-контента и нарушения бизнес-операций. Благодаря внедрению решения для управления ботами, организация получит возможность отличать действия вредоносных ботов от обычных, предотвращая нанесение ими вреда функционированию сайта.

Успешный опыт наших клиентов

Ведущая компания онлайн-сервиса для работы с личными финансами сталкивалась с постоянной угрозой от вредоносных ботов. С момента своего основания в 2011 году компания профинансировала более 40 миллиардов долларов кредитов и имела более 800 000 членов на своей платформе. В 2019 году стало понятно, что компания подвергается все большему количеству атак вредоносных ботов с вбросом учетных данных пользователей. Эти атаки представляли угрозу для бизнеса и репутации компании. Нейтрализация этих атак, чтобы сохранить качество уровня обслуживания клиентов и защитить конфиденциальные данные, стало главной заботой руководителей компании.

Продукт Cloudflare Bot Management (Управление ботами) помог этой компании, обеспечивающей работу с личными финансами, мгновенно решить проблему нейтрализации таких атак с вбросом данных. Инженеры этой компании смогли быстро построить и развернуть детализированные наборы правил и добились успеха в сокращении вредоносного трафика более чем на 60% при значительно низком уровне ложноположительных результатов. По словам их инженера по безопасности «Самое замечательное в решениях для управления ботами Cloudflare то, что мне не нужно тратить время на его тонкую настройку. Алгоритмы машинного обучения по обнаружению атак с вбросом данных просто работают, поскольку Cloudflare обладает таким огромным набором данных. Наша работа упростилась в тысячи раз, но при этом мы обеспечиваем нашим клиентам быструю и безопасную работу наших сайтов.»

Нейтрализуйте атаки ботов и управляйте «плохими» и «хорошими» ботами в режиме реального времени с продуктом Cloudflare Bot Management.

Поддерживайте свою сеть в рабочем состоянии

A. Защита сетевой инфраструктуры

Недостаточно просто обеспечить защиту для веб-серверов. Несмотря на то что зачастую компании размещают свою локальную сетевую инфраструктуру в государственных или частных дата-центрах, она по-прежнему нуждается в защите от DDoS-атак. Большинство провайдеров услуг по нейтрализации DDoS-атак применяют один или максимум 2 метода блокирования атак: скраббинг-центры или локальное сканирование и фильтрация данных аппаратными средствами. Минусами обоих методов является подразумеваемая их спецификой неизбежная задержка во времени, которая может повлечь фатальные для бизнеса последствия.

Для скраббинга требуется перенаправить сетевой трафик на централизованные скраббинг-сервера в обозначенных географических точках, где производится фильтрация или «разделение» вредоносного трафика и отделение его от «нормального». Перенаправление всего трафика в географически удаленные скраббинг-центры влечет дополнительную задержку по времени, что в большинстве случаев неприемлемо.

Другой метод нейтрализации DDoS-атак связан с использованием локально устанавливаемых аппаратных средств для сканирования трафика и фильтрации вредоносных запросов. Подобно скраббингу применение сканирующей аппаратуры привносит сетевые задержки и снижает производительность, что связано с эффектом «бутылочного горлышка», возникающим при перемаршрутизации трафика через сканеры для завершения процесса сканирования. Локальные решения для предотвращения DDoS-атак часто по умолчанию имеют определенный лимит пропускной способности, основанный на сочетании пропускной способности корпоративной сети организации и пропускной способности сканирующей аппаратуры.

Для эффективного выявления и нейтрализации DDoS-атак лучше действовать на периферии сети – как можно ближе к источнику.
Сканирование трафика в ближайшем к сети компании дата-центре в составе глобальной распределенной сети обеспечивает высокую эксплуатационную готовность даже при масштабных DDoS-атаках. Такой подход позволяет избежать задержек, возникающих в результате перенаправления подозрительного трафика в географически удаленные скраббинг-центры, а также сокращает время реагирования на атаки.

Успешный опыт наших клиентов

Когда входящая в список Fortune 500 крупная организация по предоставлению финансовых услуг стала страдать от DDoS-атак в целях вымогательства выкупа, им понадобилось решение, которое нейтрализовало бы атаки на сетевом уровне и позволяло им быстро восстановить онлайн-сервис. Этот вид атак, характеризуемый как «атака-обрушение», перегружает сервера компании нелегитимным трафиком сетевого уровня, моментально парализуя все операции.

Компания обратилась к Cloudflare с просьбой активировать продукт Magic Transit, который обеспечивает защиту от DDoS-атак для локальных сетей и дата-центров. Используя глобальную сеть Cloudflare, продукт Magic Transit обнаруживает и нейтрализует DDoS-трафик в дата-центрах Cloudflare, ближайших к источникам атак, при этом нет необходимости перенаправлять трафик на небольшое количество удаленных «скраббинг-центров».

Благодаря этой защите, компания смогла быстро нейтрализовать атаки, восстанавливать доступ к своей сети и возвращать качество обслуживания конечного клиента на нормальный уровень. В дополнение к предоставлению защиты от DDoS-атак, фиксированные цены Cloudflare (без учета количества, или масштаба атак) и ориентация на быструю маршрутизацию были главным преимуществом перед другими устаревшими продуктами вендоров.

Чтобы более подробно ознакомиться с возможностями сетевой защиты от DDoS-атак, заходите в раздел Cloudflare Magic Transit.

B. Защита TCP/UDP-приложений

На уровне транспорта сетевого трафика злоумышленники могут выбрать объектом атаки ресурсы серверов компании, перегружая все доступные порты на сервере. В результате DDoS-атаки сервер может начать медленнее обрабатывать поступающие от добросовестных пользователей запросы или вовсе перестать их обрабатывать. Для предотвращения атак на транспортном уровне необходимо решение, которое могло бы автоматически определять признаки развертывания атак и блокировать поступающий в рамках этих атак трафик.

Успешный опыт наших клиентов

Ведущий поставщик технологий для криптовалютных бирж, платежных систем и брокерских фирм столкнулся с уникальной проблемой защиты и ускорения своего трафика, направляемого по собственному протоколу TCP. Учитывая характер их бизнеса, надежность и скорость имели решающее значение — нескольких дополнительных миллисекунд было достаточно, чтобы транзакции сорвались по пути к межбанковскому рынку.

Cloudflare Spectrum стало для них решением по защите и ускорению всех видов TCP-трафика, включая таможенные протоколы. С продуктом Cloudflare Spectrum компания смогла защитить соединения с помощью протокола TLS 1.3 с нулевым временем на передачу и подтверждение, что обеспечивает быстрый и безопасный транзит.

Направляя свой TCP-трафик через Spectrum, эта компания смогла защитить свои производственные системы от DDoS-атак, одновременно обеспечивая надежность и более быстрое соединение. Компания увидела немедленное сокращение задержки более чем на 50% в некоторых регионах. Более 5 ТБ данных компании в месяц шифруются, защищаются и ускоряются с помощью Cloudflare.

Повысьте скорость доставки трафика, безопасность и надежность работы применяемых вами протоколов TCP/UDP с помощью инструмента Cloudflare Spectrum.

Заключение

Обеспечить эффективную и удобную для пользователя работу сети поможет правильный выбор стратегии защиты, которая способна не только ускорить доступ к контенту, но и обеспечить надежную защиту сети и ее эксплуатационных характеристик от перебоев в работе, хищения данных и других последствий кибератак.

Опираясь на ресурсы своей развитой сети, охватывающей более 200 городов в 90 странах мира, Cloudflare предоставляет глобальную, масштабируемую облачную платформу, с помощью которой ее клиенты могут рассчитывать на безопасную, эффективную и надежную работу всех своих локальных, облачных и SaaS-приложений. Чтобы более подробно узнать, как защитить и обезопасить свой онлайн-бизнес, заходите на Cloudflare.com.

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

РЕДАКЦИЯ: 200330