CLOUDFLARE®

Пять способов сделать функционирование вашего онлайн-бизнеса максимально безопасным, эффективным и надежным

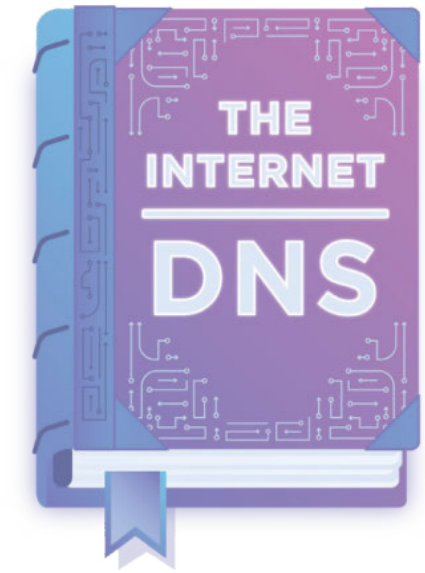
Сфера Интернет-технологий претерпевает стремительные изменения, а вместе с ней меняется и сама природа ведения бизнеса современными компаниями. Обеспечение высочайшего уровня удовлетворенности клиентов по всему миру при взаимодействии с вашим онлайн-бизнесом больше не является факультативным требованием. По мере роста спроса на веб-услуги и приложения компании должны стремиться не только выполнить текущие запросы клиентов, но и одновременно обеспечить максимальную безопасность, оперативность и надежность своих сайтов и приложений.

В процессе этой цифровой трансформации компании не только сталкиваются с новыми проблемами, но и открывают для себя интересные перспективы: от оперативного прогнозирования и удовлетворения потребностей клиентов в сфере цифровых технологий до создания механизмов мощной защиты от веб-атак, решения проблем с операционными задержками, предотвращения сбоев в работе сайта и поддержания необходимой производительности и стабильного соединения с Сетью.

Для повышения удовлетворенности клиентов от взаимодействий в интернете компаниям необходимо внедрить стратегию, позволяющую обеспечить высокий уровень безопасности, производительности и надежности при работе с сайтом.
Хотя подобная стратегия включает в себя множество элементов, мы выделили и хотим представить вашему вниманию пять наиболее важных из них, которые могут помочь вашей компании удовлетворить потребности клиентов и обеспечить им высокую степень удовлетворенности при безопасном и удобном взаимодействии с вашим онлайн-бизнесом.

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

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 обращение 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 со 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 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 хостинг.

Успешный опыт наших клиентов

От этих проблем страдала одна из крупнейших мировых компаний, оказывающих услуги по доставке продуктов на дом. Наличие развитой партнерской сети в тысячах городов на территории США и система доставки «до двери», работа которой полностью зависела от функционирования онлайн-платформы и мобильных приложений, требовали оперативной и надежной работы онлайн-системы этой компании. Такая система должна не только обеспечивать прирост клиентской базы, но и укреплять партнерские связи с местными ресторанами и торговыми точками.

Изначально компания столкнулась с несколькими проблемами, связанными с работой ее онлайн-системы. Не хватало надежной CDN и отсутствовал механизм для масштабирования размеров изображений на сайте, а именно эта функция являлась ключевым фактором, от которого зависело удобство пользователя. Было необходимо дать пользователям сайта возможность просмотра множества фотографий в высоком разрешении с изображением предлагаемой продукции. Кроме того, по мере расширения компании, соответственно, расширялся и ее ассортимент. При наличии большого количества изображений высокого разрешения, загружаемых с платформы этой компании, было крайне важно найти решение, позволяющее оптимизировать их загрузку и отображение и сократить время задержки при загрузке, учитывая, что ранее использовавшееся решение для масштабирования изображений обходилось фирме недешево — несколько тысяч долларов в месяц.

Cloudflare помогла фирме по доставке продуктов питания наладить быстрый и удобный для пользователя процесс для работы с графической частью сайта — решением проблемы стал продукт Cloudflare Content Delivery Network (CDN). Функционирующий на базе глобальной сети, насчитывающей более 25 миллионов веб-ресурсов, Cloudflare CDN кэширует статический контент как можно ближе к конечным пользователям и работает совместно с Argo Smart Routing, что позволяет оптимизировать путь отправки запросов контента. Благодаря инструменту Cloudflare Image Resizing, позволяющему кэшировать изображения и сокращать задержку при загрузке, коэффициент использования ЦП у этой компании сократился на 20%.

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

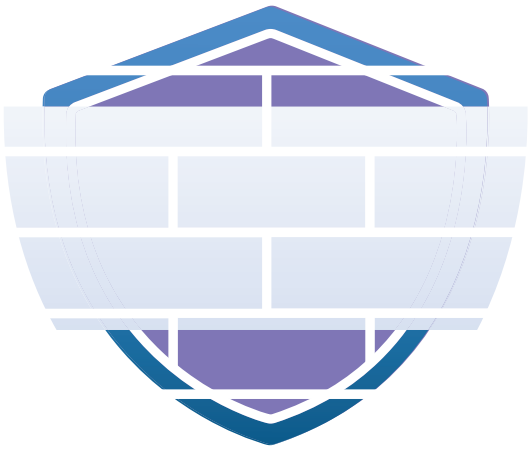
Крупная платформа онлайн-торговли (со штаб-квартирой в Канаде и сетью, охватывающей 175 стран мира) нуждалась в комплексном решении для обеспечения безопасности и высокой производительности своей сети и искала провайдера, способного предложить простое для внедрения решение и вместе с тем снизить расходы на обслуживание инфраструктуры. Сделав выбор в пользу Cloudflare, компания поставила условием сделать процесс внедрения максимально плавным и незаметным, чтобы ни один из более миллиона их клиентов, чей бизнес функционировал на базе их платформы, не столкнулся со сбоями или перерывами в ее работе. Перенеся все свои сайты в глобальную сеть Cloudflare, эта компания смогла улучшить условия для своих фирм-продавцов и скорость их работы со своими клиентами, что, в свою очередь, привело к росту продаж на базе данной платформы.

В эпицентре этих достижений находился балансировщик нагрузки Cloudflare Load Balancing, внедрение которого обеспечило компании возможность динамического управления нагрузкой трафика — иными словами, способность направлять трафик на менее загруженные и быстрее работающие сервера для конкретного пользователя, что позволило сократить сетевые задержки и ускорить доставку трафика. Теперь эта компания может с ювелирной точностью контролировать свой трафик и его распределение между серверами-источниками, увеличив производительность и точность работы за счет принятия решений на периферии сети.

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.



А. 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 кибер-злоумышленников 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

Крупнейшая в Индии компания-оператор по продаже билетов имеет в своем активе более 60 миллионов клиентов, около 5 млрд просмотров экранов в месяц, а объем ее продаж превышает 200 млн билетов в год. Ключевым фактором ее успеха является обеспечение пользователям возможности быстрой и безопасной работы с ее онлайн-сервисами, поскольку в противном случае клиенты просто уйдут к конкурентам.
Став жертвой масштабной DDoS-атаки, компания столкнулась с серьезной угрозой функционированию своей платформы.

Однако установленный продукт Cloudflare Advanced DDoS Protection позволил им смягчить и устранить последствия этой атаки, не входя в авральный режим. Благодаря пропускной способности сети более 35 Тбит/с, Cloudflare Advanced DDoS Protection предназначен для упрощения использования и управления сетью, позволяя блокировать атаки еще на периферии сети и поддерживать сервера-источники в рабочем состоянии с высоким уровнем эксплуатационной готовности — независимо от их размещения — локального, в гибридной или мультиоблачной среде.

Инструмент от Cloudflare немедленно начал блокировать вредоносный трафик — до 50 Гб/с — и не дал злоумышленникам добиться желаемого результата DDoS-атаки — снизить скорость работы сайта или вызвать перебои в его работе. Применение этого инструмента позволило компании не только укрепить безопасность своей сети, но даже повысить надежность и эффективность ее функционирования.

Более подробно ознакомиться с информацией о формировании многоступенчатой стратегии безопасности можно, зайдя на Cloudflare Advanced DDoS Protection.

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

Один из лидеров отрасли по разработке ПО для автоматизации маркетинговых операций столкнулся с этой проблемой, когда разработанные им веб-формы были наводнены спам-ботами. Веб-формы часто становились мишенью вредоносных ботов, которые сделали практически невозможным доступ к формам для добросовестных пользователей, до предела усложнив и замедлив процесс, что крайне отрицательно сказывалось на способности компании обеспечить своим клиентам удобный процесс онлайн-взаимодействия с веб-формами.

Компания обратилась к Cloudflare в поисках решения для нейтрализации вредоносных ботов, которое позволило бы блокировать исходящие от «плохих» ботов запросы без ущерба скорости и качеству функционирования ее онлайн-сервисов. В продукте Cloudflare Bot Management реализованы технологии машинного обучения для выявления аномалий в поведении веб-трафика с последующим блокированием атак ботов и вредоносного трафика, параллельно пропуская «хороших» ботов и полезный трафик. На текущий момент продукт от Cloudflare помогает этой организации нейтрализовать более 1 миллиона запросов от «плохих» ботов в день, что дает возможность клиентам использоваться маркетинговое ПО без угрозы сбоев в его работе и не рискуя потерять важные данные.

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

Некоммерческая организация — владелец сайта, входящего в первую десятку рейтинга Alexa, столкнулась с проблемой значительных сетевых задержек и перебоев в работе сайта. Ей требовалось решение, способное нейтрализовать атаки при прохождении сетевой периферии и обеспечивать скорейшее восстановление работы сети.

Этот вид атак, характеризуемый как «атака-обрушение», перегружает сервера компании нелегитимными протоколами сетевого уровня и HTTP-трафиком, моментально парализуя все операции. Компания обратилась к Cloudflare с целью поиска решения для нейтрализации атак и восстановления доступа к сайту, параллельно планируя внедрить дополнительный уровень DDoS-защиты для предотвращения атак в будущем.

Продукт Cloudflare Magic Transit обеспечивает защиту от DDoS-атак для локальных сетей и дата-центров, работая как в режиме постоянной защиты, так и в режиме защиты по требованию. Продукт работает на базе ресурсов глобальной сети Cloudflare, обеспечивая выявление и нейтрализацию DDoS-трафика через дата-центры Cloudflare, расположенные ближе всего к источнику атаки. Опираясь на возможности глобальной сети Cloudflare и надежные механизмы защиты от DDoS-атак, компания смогла быстро устранить последствия атак и восстановить до нормального уровня эффективность и удобство работы сети.

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

Именно такое решение искала компания, являющаяся разработчиком компьютерных игр и одним из лидеров в индустрии киберспорта с заявленной аудиторией более 200 млн пользователей по всему миру. Компания выявила большое количество DDoS-атак на свои сервера, а также обнаружила, что ряд пользователей в удаленных уголках земного шара сталкиваются с проблемами при работе с их приложениями на базе протоколов TCP. В индустрии компьютерных игр это очень серьезная проблема, поскольку любые сбои в работе сервиса могут вызвать массовый отток пользователей и потерю доходов.

Сетевая инфраструктура данной организации функционирует на базе протокола собственной разработки, основной задачей которого является обеспечение минимальных задержек для удобства геймеров. Поэтому, когда речь идет о масштабных DDoS-атаках, стандартные продукты для обеспечения безопасности не будут совместимы с этим протоколом.

Для повышения производительности сети и нейтрализации DDoS-атак на транспортном уровне компания обратилась к помощи Cloudflare. Cloudflare Spectrum — инструмент защиты от DDoS-атак для любых видов протоколов TCP/UDP — позволяет организации обеспечить надежную защиту ее критичного с точки зрения функционирования сети протокола передачи данных, не влияя на производительность на всех участках сети и успешно предотвращая попытки организации сбоев в работе, тем самым защищая репутацию этой организации. Помимо вышеперечисленных функций, в Cloudflare Spectrum применяются механизмы оптимизации работы протоколов TCP и Argo Smart Routing для ускорения доставки трафика по всей сети 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, зайдите на Cloudflare.com.

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

РЕДАКЦИЯ: 200330