CLOUDFLARE

Безопасность и производительность для Вашей платформы Google Cloud.

Располагая центрами обработки данных в более чем 180 городах на территории 80 стран, Cloudflare предлагает полный набор услуг по обеспечению безопасности и производительности.

Программа CDN Interconnect в Google Cloud Platform оптимизирует соединение между сетью Google и центрами обработки данных Cloudflare, экономя до 76% на оплате исходящего трафика*

Сокращение расходов на исходящий трафик и обеспечение пропускной способности

Подключите Cloudflare к своим серверам Google Cloud с CDN Interconnect, для ежемесячной экономии в 75% на исходящем трафике Google Cloud и 76% на пропускной способности

Улучшенная производительность

Наша сеть доставки содержимого (CDN) и веб-оптимизация могут двукратно увеличить скорость загрузки на вашем веб-сайте или приложении, размещенном в Google Cloud.

Продвинутая защита от DDOS-атак

Усовершенствованная защита от DDoS-атак Cloudflare имеет пропускную способность сети 56 Тбит/с что в 10 раз превышает возможности самой крупной из когда-либо зарегистрированных DDoS-атак

FIREWALL для Веб-приложений (WAF)

WAF от Cloudflare блокирует самые изощренные атаки уровня 7, защищая от топ-10 уязвимостей по версии OWASP и уязвимостей в популярных приложениях и языках

*Исходящий трафик - это трафик, покидающий центры обработки данных Google Cloud и направляющийся в центры обработки данных Cloudflare. Цены и скидки на исодящий трафик CDN Interconnect доступны по ссылке: cfl.re/egress-pricing

DISCORD

"Используя Cloudflare мы сохранили деньги, серверы и душевное равновесие."

JAKE HEINZ

Разработчик ПО, Discord

Discord ежемесячно экономит $100,000 на исходящем трафике при использовании Google Cloud.

cfl.re/discord-case-study

Quizlet

"Причина, по которой мы используем Cloudflare, заключается в превосходных функциях безопасности, высокой производительности сети CDN, и действительно удобно, что эти решения объединены вместе. Это упрощает управление всем и позволяет нам сосредоточиться на нашем основном бизнесе."

PETER BAKKUM

Руководитель Платформы в Quizlet

Quizlet экономит 50% расходов на исходящий трафик в сети Google Cloud и сокращает ежедневную загрузку пропускной способности на 76% (более 10 ТБ).

cfl.re/quizlet-case-study

Регистрация в Cloudflare
cloudflare.com/plans

Остались вопросы? Напишите нам: google@cloudflare.com

Безопасность и производительность с Cloudflare

Миссия Cloudflare - помочь в создании лучшего Интернета. Обладая глобальной сетью центров обработки данных в более чем 200 городах и общей пропускной способностью 56 Тбит/с, Cloudflare защищает и ускоряет работу более 25 миллионов Интернет-ресурсов. Предсказуемая фиксированная цена означает, что плата за использование пропускной способности не взимается даже в случае реальных скачков трафика или атаки. С каждым новым веб-сайтом сеть Cloudflare становится умнее. Наша проактивная система безопасности автоматически определяет новые угрозы и блокирует их до того, как они достигнут исходных серверов. Клиенты Cloudflare являются крупнейшими пользователями IPv6, HTTP2 и SSL / TLS по всему миру. По мере появления новых стандартов Cloudflare упрощает их использование.

Десятки тысяч клиентов Google Cloud Platform используют преимущества производительности, безопасности и экономии от Cloudflare.

Полная интеграция с Cloud Security Command Center

Центр Управления Безопасностью в Облаке от Google Cloud (CSCC) - основополагающая база данных по безопасности и рискам с данными для платформы Google Cloud.

CSCC объединяет в одном месте активы, ресурсы, политики, политики IAM, изыскания, аннотации по рискам и безопасности, обеспечивает понимание сути безопасности и рисков данных, объединяет управление и рекомендации. Cloudflare - один из первых провайдеров систем безопасности включенная в CSCC. Посредством панели управления CSCC, анализ актуальных угроз, типов угроз и события межсетевого экрана Cloudflare отображаются вместе с другими показателями безопасности приложений для целостного представления о состоянии безопасности веб-приложений.

CDN Interconnect для платформы Google Cloud

Клиенты Cloudflare с интернет-приложениями и API, размещенными на платформе Google Cloud, могут получить выгоду от сокращения расходов на пропускную способность и до 75% экономии на исходящем трафике, при этом устанавливая более быстрые соединения между Cloudflare и исходными серверами Google Cloud. В то время как CDN Cloudflare уже обеспечивает минимальную задержку, кэшируя содержимое как максимально близко к вашим пользователям, Google Cloud CDN Interconnect оптимизирует соединение между сетью Google и подключением Cloudflare, используемым для восполнения потерь кеша. Чтобы узнать больше, посетите https://cfl.re/cdn-interconnect-program

Узнать больше об использовании Cloudflare с платформой Google Cloud Cloudflare.com/google/

CLOUDFLARE

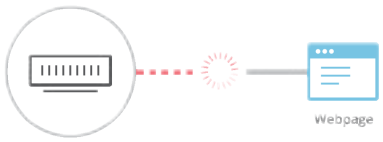
Сервисы для увеличения производительности от Cloudflare

Сервисы по увеличению производительности Cloudflare ускоряют работу приложений, улучшают мобильную доставку и обеспечивают доступность интернет-приложений.

Ускорьте работу интернет-приложений

Тяжелые страницы и большое расстояние от исходного сервера замедляют работу интернет-приложений. Обеспечьте быстрый и богатый пользовательский опыт для интернет-приложений, это оптимизирует время ожидания, увеличивает конверсию и сокращает расходы.

Модель инфраструктуры



СЕРВИСЫ

- Anycast Network
- CDN
- DNS
- Балансировка нагрузки
- Оптимизация веб-содержимого
- Умная маршрутизация Argo
- Сеть в Китае
- Потоковая передача (Stream)

Улучшите опыт для мобильных устройств

Мобильные клиенты связаны с ограничениями производительности и доставки содержимого, а это ухудшает пользовательский опыт. Обеспечьте быструю работу с мобильными устройствами, что поможет улучшить взаимодействие и увеличить конверсию независимо от расстояния до исходных серверов, типов устройств или состояния сети.

Модель инфраструктуры

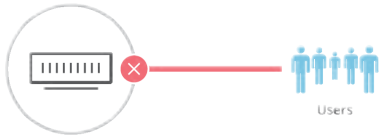
СЕРВИСЫ

- Anycast Network
- DNS
- CDN
- Оптимизация веб-содержимого
- Умная маршрутизация Argo
- Мобильные оптимизации (Mirage)
- AMP
- Пакет разработчика для мобильных устройств
- Сеть в Китае

Гарантированная доступность приложения

Перегруженная или недоступная инфраструктура препятствует доступу пользователей к приложениям. Обеспечьте быстродействие, доступность и масштабируемость интернет-приложений даже во время неожиданных скачков трафика или сбоев инфраструктуры.

Модель инфраструктуры



СЕРВИСЫ

- Anycast Network
- Сеть доставки содержимого (CDN)
- Балансировка нагрузки
- Web Application Firewall (WAF)
- Ratel Limiting

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

Сервисы для увеличения производительности от Cloudflare

Anycast Network

Обладая центрами обработки данных в более чем 200 городах и 100 странах с общей пропускной способностью 56 Тбит/с, Cloudflare Anycast Network кэширует статический контент на периферии, сокращая задержку за счет предоставления ресурсов, максимально близких географически к посетителю.

DNS

DNS от Cloudflare экономит миллисекунды на каждом запросе к DNS. Поскольку запрос DNS может возникать при каждом запросе, задержка от DNS-серверов может замедлить работу целого сайта. По данным DNSPerf.com, DNS Cloudflare - это самый быстрый в мире управляемый DNS-провайдер.

Поддержка веб-стандартов

TLS 1.3 с нулевым временем на передачу и подтверждение приёма экономит время на каждом периоде кругового обращения сообщения при установке безопасного соединения. HTTP/2 сжимает заголовки, делая размер полезных данных меньше, позволяет одному соединению передавать несколько запросов параллельно, снижая общую «стоимость» производительности, связанной с полным циклическим обменом данными.

CDN

Позволяет приложениям продолжать работать со статичным контентом, даже если их исходные серверы недоступны. Снижает риск простоя за счет перераспределения запросов на статический контент от исходного сервера.

Оптимизация веб-содержимого

Cloudflare включает набор веб-оптимизаций для повышения производительности интернет-ресурсов. Оптимизация включает новейшие веб-стандарты, такие как HTTP / 2 и TLS 1.3, а также собственные наработки для изображений и посетителей с мобильных устройств.

Умная маршрутизация Argo

Умная маршрутизация находит самый быстрый и наименее загруженный путь от посетителя до исходного сервера и ускоряет передачу трафика в сети Cloudflare. Измеряя время прохождения туда и обратно в сети Cloudflare, Argo интеллектуально маршрутизирует трафик, чтобы обеспечить эффективную доставку динамического содержимого из источника.

Сеть в Китае

Обладая центрами обработки данных в 18 городах Китая, Cloudflare ускоряет и защищает доставку контента клиентам в Китае, где почти 1,5 миллиарда мобильных пользователей, 75% из которых выходят в Интернет через свои мобильные устройства.

Балансировка нагрузки

Использует глобальные проверки работоспособности для определения отключенного исходного сервера с целью перенаправления трафика на другой работающий сервер или центр обработки данных для обеспечения доступности приложения. Автоматическое переключение при отказе сводит к минимуму время простоя, а предупреждения об отключении сервера ускоряют обнаружение проблем и устранение сбоев.

Оптимизация для мобильных устройств (Mirage)

Улучшает оптимизацию веб-контента Cloudflare для мобильных пользователей за счет «виртуализации» изображений - их отправка изначально с более низким разрешением - и их объединения в один запрос.

Stream

Cloudflare Stream упрощает потоковую передачу видео за счет управления хранением данных, кодированием мультимедиа, внедрением и воспроизведением контента, доставкой с ближайшего сервера и аналитикой.

Mobile SDK

Пакет разработки предоставляет разработчикам метрики сети, которые позволяют им оценить влияние перегрузки сотовой сети и задержек на производительность мобильного приложения. Собственный протокол Cloudflare «ASAP», встроенный в Mobile SDK, обеспечивает быструю работу для пользователей мобильных устройств.

CLOUDFLARE

Преимущество Cloudflare

ANYCAST NETWORK и логические функции

Глобальная сеть центров обработки данных по технологии Anycast от Cloudflare в более чем 200 городах в 100 странах сокращает задержки и время до получения первого байта за счет набора функций по улучшению производительности, **интегрированного** в каждом центре обработки данных.

ПРОСТОТА ИСПОЛЬЗОВАНИЯ

Настройка Cloudflare занимает всего 5 минут. Простая в использовании панель управления позволяет быстро и точно настроить функции для улучшения производительности интернет-приложений.

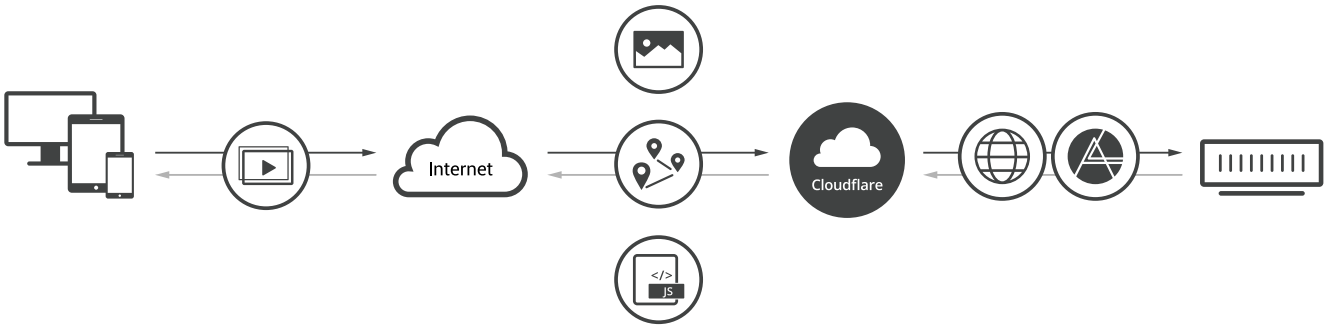
ВСТРОЕННАЯ ЗАЩИТА И ПРОИЗВОДИТЕЛЬНОСТЬ

Cloudflare включает интегрированные службы безопасности для защиты от DDoS-атак, утечки данных клиентов и ботов-мошенников, сохраняя при этом бескомпромиссную производительность.

REV: 190909

Сервисы увеличения производительности Cloudflare

Cloudflare - это глобальная облачная сеть, которая ускоряет и защищает все, что подключено к Интернету. Веб-сайты, API и приложения SaaS работают быстрее, безопаснее и надежнее с Cloudflare.



Сервисы увеличения производительности Cloudflare

Cloudflare доставляет ваши интернет-ресурсы по самым быстрым и надежным ссылкам - независимо от типа содержимого или устройства конечного пользователя.

CDN. Кэшируйте статический контент в любом центре обработки данных Cloudflare чтобы уменьшить задержку при подключении к вашему веб-хосту.

- Архитектура API First для бесшовной интеграции
- Встроенная неограниченная защита от DDoS атак.
- Настраиваемое управление кэшем и возможность наращивания граничных вычислений с **Cloudflare Workers** для увеличения интенсивности обращения к кэшу
- Доставляйте подписанные обмены для средства просмотра Google AMP (ускоренных мобильных страниц), позволяя издателям сохранять означивание URL путем развертывания Cloudflare AMP Real URL.
- Поддержка таких новых веб-стандартов TLS 1.3 и HTTP/3
- Снижение затрат на исходящий трафик с хостинг-партнерами Bandwidth Alliance

Умная маршрутизация Argo. Сеть Cloudflare направляет более 10 триллионов глобальных запросов в месяц, предоставляя умной маршрутизации Argo уникальную точку обзора для обнаружения перегрузок в реальном времени и маршрутизации трафика по самым быстрым и надежным сетевым путям.

Ускорьте доставку динамического контента между любыми двумя точками земного шара. В среднем веб-ресурсы работают на 30% быстрее при включенной интеллектуальной маршрутизации Argo.

Глобальная балансировка нагрузки. Уменьшите задержку и улучшите доступность приложений, направляя трафик от неисправных исходных серверов и динамически распределяя его по наиболее доступным и быстро реагирующим пулам серверов.

Оптимизация изображений. Создает высококачественные варианты изображения, используя одно эталонное изображение из вашего источника. Измените размер, кадрируйте, сжимайте или конвертируйте изображения в WebP, чтобы снизить затраты на пропускную способность и повысить производительность.

Потоковая передача. Поддерживайте свою инфраструктуры доставки видео в актуальном состоянии за счет перехода на онлайн видео платформу со встроенным кодированием, хранением, распространением и проигрывателем HTML5. Сокращает время и усилия для публикации видеоконтента по запросу на веб-страницах.

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

Преимущество Cloudflare

Всемирный масштаб
Cloudflare снижает ваши затраты на пропускную способность и продление, обеспечивая при этом огромный масштаб, с помощью набора интегрированных решений для повышения производительности и безопасности, которые были разработаны с нуля.

Увеличенная гибкость
Расширенная интеграция API и настраиваемые бессерверные функции позволяют разработчикам легко интегрировать наши сервисы в ваши текущие рабочие процессы.

Интегрированная защита
Cloudflare объединяет службы безопасности в сети и в инфраструктуре для защиты от самых крупных и изощренных DDoS-атак, утечек данных и злонамеренных ботов. И все это без потери производительности.

"Мы кэшируем 80% нашего трафика в Cloudflare, и наблюдали снижение времени загрузки страниц как для настольных, так и для мобильных клиентов в среднем на 50%, и это было потрясающе!"

DAVID O'BRIEN
Digital and eCommerce Manager, YPO

"Мы в Discord находимся в постоянном поиске способов улучшить опыт использования нашего продукта … Argo позволила нам сократить времена загрузки в среднем на 33 миллисекунды без каких-либо усилий по разработке со стороны нашей команды."

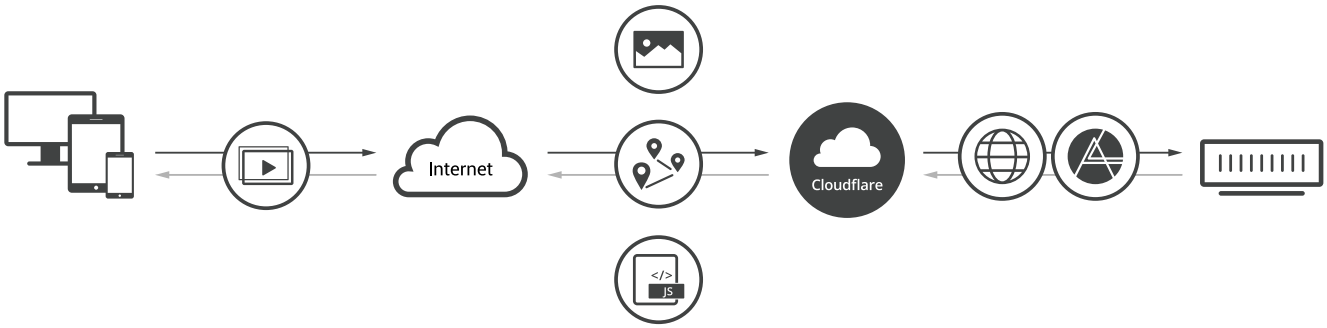
STANISLAV VISHNEVSKIY
CTO, Discord

"Когда мы развернули Балансировщик нагрузки от Cloudflare для маршрутизации трафика через наши WebSocket серверы, мы сразу получили сообщения от клиентов из Азии и Океании с благодарностями за улучшение.."

VALÉRIAN SALIOU
CTO, Crisp

Сервисы увеличения производительности Cloudflare

Cloudflare - это глобальная облачная сеть, которая ускоряет и защищает все, что подключено к Интернету. Веб-сайты, API и приложения SaaS работают быстрее, безопаснее и надежнее с Cloudflare.



Сервисы увеличения производительности Cloudflare

Cloudflare доставляет ваши интернет-ресурсы по самым быстрым и надежным ссылкам - независимо от типа содержимого или устройства конечного пользователя.

CDN. Кэшируйте статический контент в любом центре обработки данных Cloudflare чтобы уменьшить задержку при подключении к вашему веб-хосту.

- Архитектура API first для бесшовной интеграции
- Встроенная неограниченная защита от DDoS атак
- Настраиваемое управление кэшем и возможность наращивания граничных вычислений с работниками Cloudflare для увеличения интенсивности обращения к кэшу
- Доставляйте подписанные обмены для средства просмотра Google AMP (ускоренных мобильных страниц), позволяя издателям сохранять означивание URL путем развертывания Cloudflare AMP Real URL.
- Поддержка новых веб-стандартов TLS 1.3 и HTTP/3
- Снижение затрат на исходящий трафик с хостинг-партнерами Bandwidth Alliance

Умная маршрутизация Argo. Сеть Cloudflare направляет более 10 триллионов глобальных запросов в месяц, предоставляя умной маршрутизации Argo уникальную точку обзора для обнаружения перегрузок в реальном времени и маршрутизации трафика по самым быстрым и надежным сетевым путям.

Ускорьте доставку динамического контента между любыми двумя точками земного шара. В среднем веб-ресурсы работают на 30% быстрее при включенной умной маршрутизации Argo.

Глобальная балансировка нагрузки. Уменьшите задержку и улучшите доступность приложений, направляя трафик от неисправных исходных серверов и динамически распределяя его по наиболее доступным и быстро реагирующим пулам серверов.

Оптимизация изображений. Создает высококачественные варианты изображения, используя одно эталонное изображение из вашего источника. Измените размер, кадрируйте, сжимайте или конвертируйте изображения в WebP, чтобы снизить затраты на пропускную способность и повысить производительность.

Потоковая передача. Поддерживайте свою инфраструктуры доставки видео в актуальном состоянии за счет перехода на онлайн видео платформу со встроенным кодированием, хранением, распространением и проигрывателем HTML5. Сокращает время и усилия для публикации видеоконтента по запросу на веб-страницах.

REV: 191118

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

Преимущество Cloudflare

Всемирный масштаб
Cloudflare снижает ваши затраты на пропускную способность и продление, обеспечивая при этом огромный масштаб, с помощью набора интегрированных решений для повышения производительности и безопасности, которые были разработаны с нуля.

Увеличенная гибкость
Расширенная интеграция API и настраиваемые бессерверные функции позволяют разработчикам легко интегрировать наши сервисы в ваши текущие рабочие процессы.

Интегрированная защита Cloudflare объединяет службы безопасности в сети и в инфраструктуре для защиты от самых крупных и изощренных DDoS-атак, утечек данных и злонамеренных ботов. И все это без потери производительности.

"Мы кэшируем 80% нашего трафика в Cloudflare, и наблюдали снижение времени загрузки страниц как для настольных, так и для мобильных клиентов в среднем на 50%, и это было потрясающе!"

DAVID O'BRIEN
Digital and eCommerce Manager, YPO

"Мы в Discord находимся в постоянном поиске способов улучшить опыт использования нашего продукта … Argo позволила нам сократить времена загрузки в среднем на 33 миллисекунды без каких-либо усилий по разработке со стороны нашей команды."

STANISLAV VISHNEVSKIY
CTO, Discord

"Когда мы развернули Балансировщик нагрузки от Cloudflare для маршрутизации трафика через наши WebSocket серверы, мы сразу получили сообщения от клиентов из Азии и Океании с благодарностями за улучшение.."

VALÉRIAN SALIOU
CTO, Crisp

Cloudflare CDN

С легкостью ускоряйте доставку больших файлов с помощью параллельного ускорения потоковой передачи.

Обслуживание больших файлов для конечных пользователей часто приводит к высокой сквозной задержке и чрезмерным затратам на поддержание пропускной способности для издателей контента. Ускорение параллельной потоковой передачи в сети Cloudflare позволяет значительно ускорить доставку больших файлов с меньшими накладными расходами.

Это достигается путем передачи частично кэшированного содержимого нескольким клиентам одновременно, а также путем объединения нескольких клиентских запросов в один запрос к исходному серверу. Наблюдаемое улучшение сквозной задержки особенно заметно для клиентов, отдающих файлы размером более 500 МБ.

Испытание большими файлами и передача видео в реальном времени

Сети CDN повышают производительность за счет кэширования файлов максимально близко к конечным пользователям. Если файл недоступен в кэше, CDN должна взять его с исходного сервера. Сети CDN обычно требуют, чтобы контент был полностью записан в кэш, прежде чем его можно будет передавать по запросу клиентам.

В случае нескольких одновременных запросов на контент, который еще не кэширован, обычная CDN работает следующим образом:

1. Или задерживает запросы до тех пор, пока файл не будет полностью кэширован, увеличивая время загрузки.
2. Или отправляет несколько запросов на исходный сервер, увеличивая расходы на пропускную способность

Одним из вариантов решения этой проблемы является «предварительный прогрев» кеша: это означает, что файл загружается в ближайшие ЦОД CDN до запросов клиентов. Хотя это гарантирует более высокую частоту попаданий в кэш и более быстрый отклик для пользователя, это также требует тщательного планирования со стороны издателя и заблаговременного знания того, какой контент станет популярным.

Отличие Cloudflare

Сеть Cloudflare оптимизирована для доставки больших файлов за счет использования ускорения параллельной потоковой передачи (CSA - Concurrent Streaming Acceleration) двумя способами. Во-первых, CSA обеспечивает потоковую передачу файлов запрашивающей стороне, даже если части файлов все еще загружаются с исходного сервера. Это резко сокращает время ожидания первого байта (TTFB) и сокращает задержки, связанные с ожиданием загрузки содержимого из кэша.

Во-вторых, при сжимании запросов Cloudflare преобразовывает несколько запросов к исходному серверу в один комплексный «свернутый» запрос HTTPS. Это гарантирует, что несколько клиентов могут одновременно получать доступ к контенту, не дожидаясь других пользователей в очереди. Многоуровневое кэширование Cloudflare также гарантирует, что несколько запросов на некэшированный контент могут обрабатываться ЦОД 1 уровня Cloudflare, что сокращает количество запросов к исходному серверу.

Доставка больших файлов в Cloudflare

Примеры использования

Хотя CSA работает с любым кэшируемым контентом, самые большие улучшения увидят клиенты, которые передают большие (> 500 МБ) файлы одновременно нескольким пользователям, что часто может вызывать задержку. Часто эти файлы популярны (много одновременных запросов) и еще не кэшируются в CDN.

Общие примеры успешного использования CSA, - это загрузка игр, обновления программного обеспечения, популярное видео в интернете и видео-сервис по запросу (VoD).

Резюме

Технология Concurrent Streaming Acceleration (CSA) в Cloudflare значительно сокращает сквозную задержку и загруженность исходного сервера при отдаче больших файлов. Это улучшает опыт для конечных пользователей и снижает затраты на поддержание пропускной способности исходного сервера.

"В нашем тесте Cloudflare показала самую лучшую производительность по всему миру, а команда Cloudflare работала с нами чтобы гарантировать скорейшую доставку наших больших файлов пользователям."

Robert Cope
Инженер инфраструктуры, компания National Instruments

CLOUDFLARE®

Работа быстрее: Узнайте о Вашем веб-сайте, а также том, что замедляет его работу

Цифры не лгут: Пользователи предпочитают более быстрые сайты и приложения.

На скорость вашего сайта влияет множество факторов. Некоторые из них вы контролируете, другие нет. В этом документе рассматриваются различные факторы, влияющие на производительность сети, и шаги, которые компании могут предпринять для оценки и повышения производительности своих веб-ресурсов.

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

ЧАСТЬ 1

Почему так важна производительность?

Производительность Вашего сайта напрямую затрагивает Ваши возможности привлекать прибыль.

Производительность влияет как на общее впечатление пользователя, так и на уровень конверсии. Веб-сайты и приложения должны быстро загружаться и быстро реагировать на действия пользователей, чтобы поддерживать заинтересованность пользователей и увеличивать конверсию. Производительность также является важным фактором в поисковой оптимизации (SEO) в значении её влияния на естественный трафик.

Заинтересованность пользователя

Исследования показывают, что пользователи очень охотно отказываются от приложений и веб-сайтов, которые загружаются медленно или вообще не загружаются:

- BBC обнаружила, что в каждую дополнительную секунду, потраченную на загрузку их веб-страниц, уходило на 10% больше посетителей.[1]
- 39% пользователей переставало интересоваться сайтом если на загрузку изображений уходило слишком много времени.[2]
- На мобильных устройствах 53% посещений веб-страниц, вероятно, будут прерваны, если страницы загружаются дольше 3 секунд.[3]

И наоборот, за счет повышения скорости загрузки страницы на мобильных устройствах количество уходов с сайта U.S. Express снизилось на 15,65%[4]

Конверсия

Страницы, которые загружаются быстрее, превращают больше посетителей в покупателей, то же самое справедливо и для приложений, которые быстрее реагируют. Это так просто, анализ результатов исследований показывает это:

- Конверсии снижаются на 7% уже при одной дополнительной секунде времени на загрузку.[5]
- Walmart зафиксировал резкое падение конверсии, когда время загрузки увеличилось с 1 до 4 секунд.[6]
- В случае с Pinterest сокращение на 40% воспринимаемого времени загрузки увеличило количество регистраций сайте на 15%.[7]
- Даже тысячные доли секунды имеют значение: Mobify обнаружила, что сокращение времени загрузки их домашней страницы на 100 миллисекунд привело к увеличению конверсии на 1,11%.[8]

Неудивительно, что повышение конверсии приводит к увеличению дохода: средний годовой доход Mobify увеличился почти на 380000 долларов США в результате увеличения коэффициента конверсии.[8]

Оптимизация поиска и естественный трафик

Поисковая оптимизация или SEO - это практика, позволяющая сделать какой-либо интернет-ресурс более заметным за счет улучшения размещения в выдаче поиска, что приводит к увеличению количества кликов пользователей и увеличению естественного трафика. Скорость сайта - важная часть оптимизации сайта для поиска. Google включил скорость сайта в качестве фактора в поисковом рейтинг по крайней мере с 2010 года.[9] В связи с распространением мобильных устройств во всем мире, с 2018 году Google также начал использовать производительность на мобильных устройствах в качестве фактора ранжирования.[10]

Быстродействие на мобильных устройствах

Поскольку мобильные устройства предлагают особые задачи по сравнению с настольными компьютерами, их следует рассматривать как отдельный аспект производительности: веб-сайт или приложение должны быть специально разработаны для мобильных устройств, чтобы гарантировать, что они будут хорошо работать на портативных устройствах.

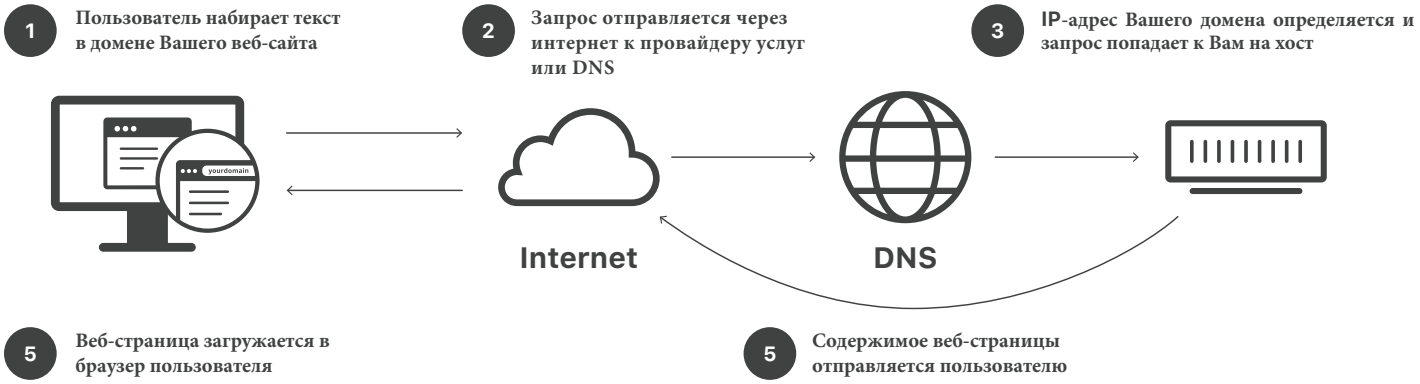
Мобильные устройства обогнали настольные компьютеры по количеству подключений к Интернету в 2016 году: в октябре того же года на мобильные устройства и планшеты приходилось 51,3% использования Интернета.[11] Опрос, проведенный венчурной компанией Kleiner Perkins в 2017 году, показал, что в среднем пользователи проводят в сети 3,1 часа в день с мобильных устройств и 2,2 часа с компьютеров.[12]

Следовательно, производительность с мобильных устройств очень важна для бизнеса:

- 40% платежей в интернете происходит с мобильных устройств.[13]
- Пользователи склонны уходить с 52% сайтов для мобильного устройства, если их загрузка занимает более 3 секунд.[14]

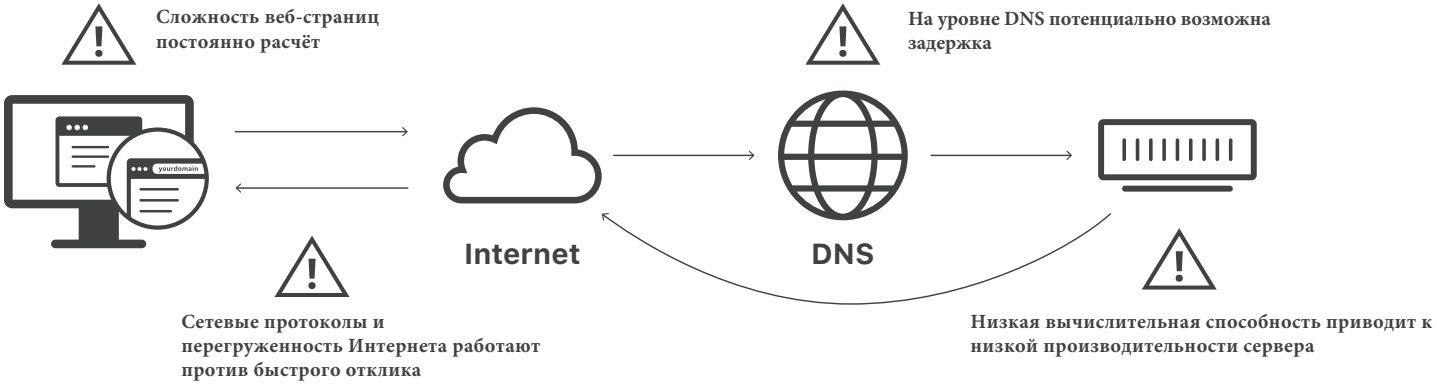
ЧАСТЬ 2

Что влияет на производительность?



Интернет сегодня уже не тот, что был даже пять лет назад. Веб-страницы и веб-приложения стали тяжелее и больше зависят от внешних ресурсов и служб. Серверные части приложений становятся более сложными благодаря развитию облачных технологий и изменениям в интернет-протоколах. Пользователи выходят в Интернет с более разнообразных устройств, чем когда-либо прежде.

Как следствие, поддержание производительности стало более сложной задачей, чем когда-либо. И все же производительность, вероятно, никогда ещё не была столь важна для бизнеса. Давайте подробно рассмотрим тенденции, влияющие на производительность сегодня.



Разнообразие веб-содержимого

Размер веб-страниц растёт

В 2016 году средний размер веб-страницы составлял 2,3 МБ, что больше, чем исходная версия классической компьютерной игры «Doom» на момент ее первого выпуска[15]. С тех пор веб-сайты становились только тяжелее.

По мере совершенствования технологий пользователи ожидают более богатого и персонализированного пользовательского опыта, охватывающего различные типы содержимого. Простой HTML больше не справляется.
В результате, сегодня в среднем одна страница сегодня больше, чем классическая видеоигра.

Чтобы оставлять пользователей заинтересованными, приложения и веб-сайты сегодня имеют у себя все больше и больше:

- **Мультимедийный контент**, например видео и высококачественные изображения.
- **Каскадные таблицы стилей:** Таблицы стилей, влияющие на внешний вид и восприятие страницы
- **JavaScript:** Динамические веб-страницы и персонализированный контент являются нормой. В результате разработчики добавляют все больше JavaScript, который необходимо отобразить.
- **Вызовы API**: увеличение числа сетевых вызовов API, которые доставляют контент или дополнительные функции из нескольких сторонних источников.

Хотя эти изменения направлены на более богатый и персонализированный опыт, для пользователей[16], они затрудняют построение Интернета, который бы эффективно загружаться и быстро реагировал.

Возросшие ожидания потребителей и широкое использование мобильных устройств

Сегодняшние потребители подключены к Интернету больше, чем когда-либо, и это увеличивает потребность в серверной инфраструктуре, поддерживающей веб-сайты и приложения. Пользователи подключаются к приложениям и веб-сайтам со всего мира с любых устройств. Опрос Nielsen 2016 года показал, что 57% респондентов, совершивших покупки в Интернете за последние шесть месяцев, покупали у зарубежных розничных продавцов.[17]

Мобильные устройства - это новый эталон производительности в Интернете. Однако разработка инфраструктуры для мобильных устройств представляет собой новый набор трудностей. Производительность на мобильных устройствах ограничивается возможностью подключения к сети и ее доступностью. Несмотря на широкую доступность сетей 4G и 5G в некоторых странах, 60% мобильных подключений во всем мире используют 2G.[18] А в некоторых регионах провайдеры мобильных сетей ограничивают пропускную способность до определенного уровня.[19] Адаптация веб-страниц для мобильных устройств также означает проблему восприятия на маленьком дисплее. Веб-страницы должны быть разработаны таким образом, чтобы их можно было по-прежнему читать и использовать на мобильных устройствах.

Несмотря на эти вызовы для разработчиков, пользователи мобильных устройств имеют высокие требования производительности для своих приложений: одно исследование, проведенное Dimensional Research, показало, что 49% пользователей ожидают, что приложения ответят в течение 2 секунд или меньше, 55% не удаляют приложение с проблемами производительности, и 80% указали, что они будут пытаться использовать проблемное приложение только три раза или меньше.[20]

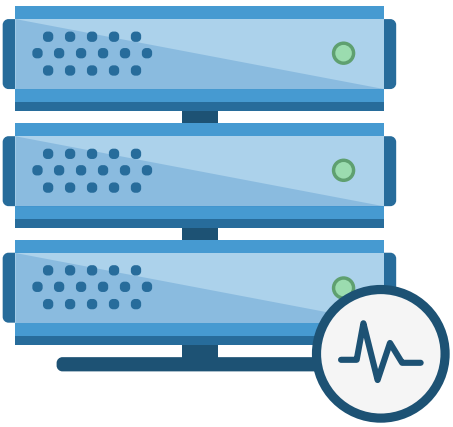
DNS

Прежде чем пользовательские устройства смогут подключаться к Интернет-ресурсам, пользовательское имя этого ресурса - доменное имя - должно быть преобразовано в машиночитаемый IP-адрес, аналогично тому, как вы должны найти номер телефона организации перед тем, как связаться с ней. Для этого пользовательское устройство должно запросить сопоставитель DNS, который сопоставит доменное имя с IP-адресом и отправит устройству правильный IP-адрес. Этот процесс требует времени, поэтому оптимизация DNS является важной частью оптимизации производительности.

В дополнение к поиску DNS для основного доменного имени, могут потребоваться другие DNS-запросы для загрузки других ресурсов на каждой веб-странице. Например, если изображения размещены не в Вашем домене, то загрузка веб-страницы будет включать запрос всех этих доменов для загрузки изображений. В некоторых случаях многократный поиск DNS может привести к задержке загрузки до нескольких секунд.

Поставщики DNS могут не быть оптимизированы по скорости. Если пользовательский запрос сначала остановится у медленного DNS-провайдера, находящегося далеко от него, то загрузка вашего сайта займет больше времени.

Многим поставщикам DNS требуется более 50 миллисекунд для обработки каждого запроса DNS, в то время как самые быстрые поставщики DNS обрабатывают запросы менее чем за 20 миллисекунд - Cloudflare DNS, например, обрабатывает запросы в среднем менее чем за 12 миллисекунд.[21]



Работоспособность исходного сервера

Производительность начинается с исходных серверов: основных серверов, которые обрабатывают входящие клиентские запросы и отвечают на них. По мере того, как приложения и веб-сайты становятся более сложными, они увеличивают нагрузку на исходные серверы. Низкая производительность исходного сервера приводит к снижению производительности в целом, даже если остальная часть инфраструктуры и содержимое веб-ресурса оптимизированы.

Исследование, проведенное Nielsen Norman Group, показывает, что время отклика не должно превышать 1 секунды, чтобы не прерывать ход мыслей пользователя[22]. Если сервер не может обработать хотя бы 1 запрос в секунду, пользователь будет воспринимать приложение как медленное.

Неравномерно распределенные нагрузки на сервер

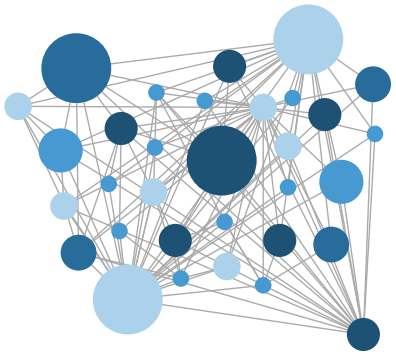
Перегруженные серверы будут работать медленнее, увеличивая ненужную задержку и сказываясь на пользовательском опыте. Если некоторые серверы имеют слишком большую рабочую нагрузку, а другие серверы используются недостаточно, рабочая нагрузка должна распределяться между серверами более равномерно, чтобы максимизировать производительность.

Различия между приложением с эффективной балансировкой нагрузки и приложением без нее могут быть существенными. Одна компания SaaS отметила уменьшение времени загрузки страницы на 2-3 секунды после развертывания Балансировщика Нагрузки Cloudflare.[23]

Сбои на сервере

Как и все компьютеры, серверы иногда выходят из строя. Исследование, проведенное ITIC Corp в 2017 году, показало, что некоторые серверы в среднем незапланированно простаивают до 37 минут в год, в то время как самые надежные серверы - IBM Z Systems с Linux - простаивают всего на 0,9 минуты в год.[24]

Если стратегия отказоустойчивости отсутствует, простой сервера может привести к замедлению обслуживания пользователей или к его полной потере.



Сетевые факторы

Интернет состоит из больших взаимосвязанных сетей. Когда данные перемещаются из одной точки в другую, они могут проходить через любое количество маршрутизаторов, коммутаторов и сетей, прежде, чем достигнут места назначения. Следовательно, ряд сетевых факторов может замедлить или повлиять на производительность. Некоторые из этих факторов находятся вне вашего контроля, но вы можете предпринять шаги для оптимизации многих из них.

Интернет-протоколы, влияющие на производительность.

Сетевые протоколы, используемые в Интернете, не были созданы для нынешнего Интернета с его огромным масштабом, гигантской пользовательской базой и терабайтами данных, передаваемых туда и обратно по всему миру.

TCP (Transmission Control Protocol) (протокол управления передачей) - это основной протокол, используемый в Интернете. Этот транспортный протокол включает в себя двустороннее подтверждение для открытия соединения между клиентом и сервером. Как только соединение открыто, TCP гарантирует надежность передачи, проверяя, что все данные поступают и находятся в порядке. Этот упор на надежность означает, что TCP не самый быстрый из доступных транспортных протоколов, однако большая часть вашего веб-сайта будет достигать пользователей через TCP.

UDP (User Datagram Protocol) (протокол датаграмм пользователя) - это гораздо более быстрый транспортный протокол, чем TCP, но он также намного менее надежен. В отличие от TCP, UDP не открывает выделенное соединение между устройствами перед передачей данных и не гарантирует, что все пакеты данных будут доставлены и находятся в порядке. UDP очень полезен для потоковой передачи видео, голосовых вызовов и других сценариев, когда скорость важнее надежности, но его использование ограничено только этими вариантами использования.

HTTP - это протокол уровня приложения, что означает, что этот протокол, работает непосредственно внутри веб-приложений. Все действия пользователя преобразуются в HTTP-запросы, которые отправляются на исходный сервер, и все ответы сервера также приходят на HTTP. Новые версии HTTP работают быстрее и эффективнее: HTTP/2, выпущенный в 2015 году, работает быстрее, чем HTTP/1.1. Если ваш веб-сайт по-прежнему обслуживается через HTTP/1.1, пользователи могут испытывать более низкую производительность, чем через HTTP/2.

TLS или Transport Layer Security - это протокол для шифрования интернет-трафика и гарантии того, что устройство подключается к реальному серверу. В то время как TLS необходим для обеспечения безопасности, особенно с учетом того, что потребители больше зависят от Интернета, использование старых версий протокола TLS может увеличивать время загрузки. В последней версия TLS, TLS 1.3, устранено несколько этапов для более быстрого соединения. (TLS также известен как SSL, это было первоначальным названием протокола в 1990-х годах.)

Сеть между сервером и клиентом (включая мобильные сети)

Пользователи получают доступ к интернет-ресурсам из всех типов сетей, и состояние сети играет огромную роль в том, насколько хорошо работает ваш сайт или приложение.

Задержка в сети частично вызвана расстоянием. Чем дальше физически пользователь находится от исходного сервера, тем ощутимее задержка. Скорость света - это жесткое ограничение того, насколько быстро могут перемещаться данные, и перемещение данных от пользователя к серверу и обратно может занять от нескольких миллисекунд до почти секунды. (Влияние сетевой задержки можно несколько уменьшить, используя CDN - сеть доставки контента - для кэширования контента ближе к пользователям.)

Перегрузка сети возникает, когда объём сетевого трафика превышает пропускную способность в определенной точке сети, будь то точка обмена интернет-трафиком (IXP), центр обработки данных или домашний роутер. Возникающая перегрузка приводит к снижению скорости Интернета для всех, кто подключен к данной сети. Перегрузка сети может быть свойственна определенной географической области, в которой недостаточно развита инфраструктура, или может затронуть всю сеть Интернет-провайдера.

Мобильные сети часто ненадежны, хотя пользователи все больше используют их для доступа в Интернет. Качество доступа в мобильной сети зависит от местоположения пользователя, пропускной способности сети, предлагаемой оператором сотовой связи, и многих других факторов. Хотя мобильные сети во всем мире развиваются, в некоторых регионах все еще возникают проблемы с надежностью сотовой связи и доступностью подключения.[18]

ЧАСТЬ 3

Что можно предпринять для оценки и улучшения производительности?

Тест скорости сайта

То, как работает сайт в локальной тестовой среде, не является хорошим показателем того, как он будет работать для пользователей в разных сетях.

Тестирование скорости веб-сайта направлено на моделирование реальных условий и демонстрацию того, насколько хорошо веб-сайт на самом деле работает. Лучшие тесты скорости веб-сайтов должны дать вам представление не только о том, насколько быстрым является сайт или приложение, но и о том, какие его свойства снижают производительность.

Тесты скорости могут дать множество показателей:

- **Время загрузки:** сколько времени требуется браузеру для завершения загрузки и отображения веб-страницы
- **Время до первого байта (TTFB):** сколько времени требуется браузеру для получения первого байта данных от веб-сервера
- **Запросы:** количество HTTP-запросов, которые делает браузер для полной загрузки страницы

Для получения дополнительной информации об измерении производительности с помощью теста скорости см. **Приложение: «О показателях производительности».**

WebPageTest.org одна из уважаемых и при этом бесплатная платформа для тестирования. Google PageSpeed Insights также может помочь Вам в оценке веб-сайта.

Дополнительно, Cloudflare предлагает инструмент simple testing для оценки времени загрузки, TTFB, и общего количества запросов.

Оценка состояния и загруженности исходного сервера

Мониторинг состояния сервера

Производительность сервера может снижаться по разным причинам: например, может выйти из строя серверное оборудование или серверное программное обеспечение может устареть. Средний срок службы сервера составляет около 5 лет.[25] За серверами следует постоянно наблюдать, чтобы гарантировать их работоспособность и доступность.

Проверка загруженности сервера

Если исходные серверы перегружены, они будут работать медленно. Проверьте использование памяти ваших серверов. Возможно некоторые машины работают интенсивнее, чем другие? Некоторые серверы используют всю свою вычислительную мощность, а другие - нет? Чтобы получить максимальную производительность от ваших серверов и эффективно использовать серверные ресурсы, важно сбалансировать рабочие нагрузки между несколькими серверами.

Разгрузка некоторых запросов контента посредством кеширования

Если каждый запрос пользователя выполняется на исходном сервере, он может быть перегружен. Посредством реализации кэширования - в браузере, на границе сети (с использованием CDN) или в обоими способами - можно исключить многие, если не большинство, циклические запросы на всем пути к исходному серверу.

Определите, откуда приходит трафик сайта

Одна из основных причин задержки в сети - расстояние, поэтому местоположение пользователей имеет большое значение.

Например, интернет-трафику, чтобы преодолеть почти 16000 километров от Нью-Йорка до Сиднея (80 мс) требуется больше времени, чем чтобы преодолеть 4000 километров от Нью-Йорка до Сан-Франциско (21 мс)[26]. Если хостинг веб-сайта в США, но большинство его пользователей находятся в Сиднее, тогда у большинства пользователей будет низкая производительность.

Google Analytics - полезный инструмент для определения географического расположения пользователей. Определив, откуда поступает трафик на сайт, вы сможете определить, настроена ли инфраструктура вашего веб-ресурса для эффективного обслуживания этих местоположений.

Аудит и оптимизация изображений для сайта.

Браузеру пользователя необходимо загрузить изображения, прежде чем они могут быть отображены. Чем больше изображение (с точки зрения размера файла, а не размеров), тем больше времени требуется для загрузки. Большие изображения часто увеличивают время загрузки веб-страницы необоснованно, поскольку многие устройства не имеют достаточно хорошего разрешения экрана или экрана достаточного размера, чтобы иметь потребность в изображениях с очень высоким разрешением.

Прежде чем изображения можно будет оптимизировать, вы должны с помощью аудита изображений определить, сколько изображений есть на вашем веб-сайте и где они расположены. После аудита необходимо оптимизировать как можно больше изображений - то есть сжать, изменить размер и преобразовать в формат файла, допускающий потери, такой как JPEG. Оптимизированные изображения загрузятся намного быстрее.

Moz.com содержит пошаговые инструкции по проверке всех изображений на вашем веб-сайте, определению того, какие из них необходимо оптимизировать, и их оптимизации. Сканер на SEO веб-сайте Screaming Frog помогает проверять изображения на веб-сайтах.

В Интернете доступно множество бесплатных инструментов для оптимизации изображений. Adobe Photoshop также может сжимать изображения и преобразовывать их в различные форматы.

Cloudflare Image Resizing, Mirage и Polish - лучшие варианты для компаний, которые уже развернули Cloudflare CDN для кэширования изображений и более быстрой доставки. Cloudflare Polish можно активировать на вкладке «Скорость» на панели инструментов Cloudflare.

Проверьте текущую производительность Вашего провайдера DNS

Определите своего DNS-провайдера, а затем выясните, обеспечивает ли ваш провайдер максимально возможную производительность.

Один из лучших ресурсов для измерения производительности DNS это DNSPerf. DNSPerf регулярно тестирует всех авторитетных поставщиков DNS и общедоступные сопоставители DNS. Их результаты и рейтинги доступны бесплатно на сайте dnsperf.com.

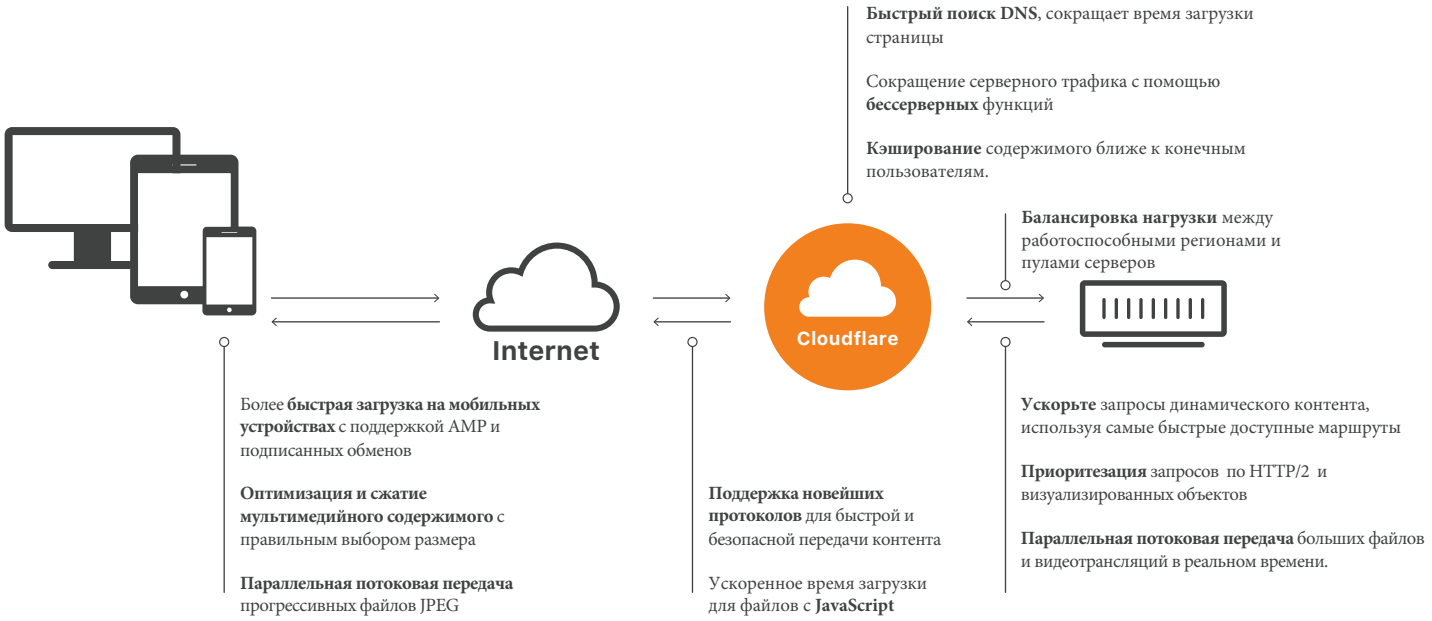
Чтобы еще больше улучшить пользовательский опыт работы с DNS, они могут настроить работу с бесплатной службой распознавания DNS Cloudflare 1.1.1.1 для более быстрой работы с акцентом на конфиденциальность.[14]

ЧАСТЬ 4

Как проблемы производительности решаются в Cloudflare

Сеть центров обработки данных Cloudflare охватывает города по всему миру. Каждый центр обработки данных поддерживает полный набор сервисов производительности и безопасности Cloudflare для оптимизации скорости внутри сети.

Cloudflare ускоряет трафик в ключевые моменты жизненного цикла запроса - от поиска веб-адресов до ускоренной доставки на исходный сервер.



Возможные проблемы с DNS и интернет-провайдером

DNS Cloudflare: Cloudflare - самый быстрый и надежный доверенный DNS-провайдер в мире.[21] Cloudflare предоставляет быстрый и безопасный управляемый DNS в качестве встроенного сервиса в своей сети. Cloudflare также предлагает 1.1.1.1 - общедоступный сервер DNS, который сохраняет конфиденциальность DNS-запросов.

Для пользователей, **Cloudflare Warp** ускоряет доступ в Интернет с мобильных устройств. **Cloudflare Speed Test** на speed.cloudflare.com помогает пользователям оценить производительность сети своего интернет-провайдера.

Сеть

CDN Cloudflare охватывает глобальную сеть центров обработки данных, которые кэшируют контент близко к пользователям, чтобы запросы не преодолевали большие расстояния до исходных серверов.

Cloudflare оптимизирует скорость сетевого трафика несколькими способами

Cloudflare Argo Smart Routing: Argo доставляет динамический веб-контент посредством самых быстрых доступных ссылок, что значительно ускоряет доставку и улучшает опыт конечного пользователя.

Cloudflare поддерживает **новейшие веб-стандарты и протоколы**, включая HTTP/2 и QUIC (HTTP/3) для более быстрой передачи данных на уровне приложений, TLS 1.3 для более эффективного шифрования SSL.

Cloudflare поддерживает **использование подписанных обменов с Google AMP**, обеспечивая определение собственного URL-адреса при просмотре в средстве просмотра AMP.

Для мобильных приложений **Cloudflare Mobile SDK** предоставляет аналитику производительности мобильной сети, которую можно интегрировать в любое приложение.

Оптимизация содержимого

Cloudflare предлагает ряд функций **оптимизации изображений**, включая изменение размера изображения, Polish и Mirage. Изменение размера изображения позволяет клиентам оптимизировать изображения путем изменения размера, обрезки, сжатия или преобразования их в WebP, новый формат изображений, созданный для быстрой загрузки. Cloudflare также позволяет **параллельную потоковую передачу изображений** в современных форматах для ускорения загрузки нескольких изображений на странице.

Видео очень важно для привлечения пользователей, и Cloudflare предлагает несколько продуктов и функций для оптимизации видео. **Cloudflare Stream** - это онлайн видеоплатформа для потоковой передачи мультимедиа, а **Stream Delivery** обеспечивает максимально быструю потоковую передачу видео. Cloudflare также предлагает **Concurrent Streaming Acceleration** - ускорение одновременной потоковой передачи для трансляции содержимого в реальном времени.

Приоритезация или порядок, в котором загружаются объекты на веб-странице, имеет огромное значение для скорости загрузки. **Rocket Loader** от Cloudflare оптимизирует порядок загрузки для любых ресурсов, которые необходимо загрузить, до выполнения JavaScript на странице. Cloudflare также поддерживает **приоритезацию HTTP/2**, для управления порядком загрузки объектов страницы, избегая более медленной установки порядка по умолчанию в большинстве браузеров. Cloudflare поддерживает **BinaryAST для JavaScript**, для ускорения синтаксического анализа JavaScript и его более быстрого выполнения, что имеет решающее значение для производительности динамических или персонализированных веб-страниц.

Состояние и доступность сервера

Балансировщик нагрузки в Cloudflare обеспечивает локальное и глобальное распределение нагрузки для уменьшения задержки либо путем балансировки трафика между несколькими серверами, либо путем направления трафика через ближайший регион. Он также включает в себя проверки работоспособности с возможностью быстрого переключения на резервные мощности, чтобы предотвратить сбои на стороне посетителей.

Бессерверные вычисления имеют огромный потенциал при создания самых быстрых и адаптивных приложений. **Cloudflare Workers** позволяет разработчикам создавать бессерверные приложения, которые работают в сети Cloudflare, ближе к вашим пользователям. Приложения, созданные с помощью Cloudflare Workers, всегда доступны с низкой задержкой отклика.

Вывод

Сегодня пользователи хотят более быстрого и персонализированного взаимодействия при регистрации запуске приложения. Этого можно добиться, если использовать подходящие инструменты. Cloudflare помогает ускорить работу более 18 миллионов интернет-ресурсов, давая компаниям возможность предлагать своим клиентам наилучший опыт.

О Cloudflare

Cloudflare, Inc. (www.cloudflare.com / @cloudflare) ставит своей целью сделать Интернет лучше. Сегодня компания управляет одной из крупнейших в мире сетей, в которой почти 10 процентов компаний из списка Fortune 1000 и примерно 19 процентов из 10 000 крупнейших веб-сайтов используют по крайней мере один продукт Cloudflare. Платформа Cloudflare защищает и ускоряет работу любого интернет-приложения в сети без установки дополнительного оборудования, программного обеспечения или изменения хотя бы одной строки кода. Интернет-ресурсы, управляемые Cloudflare, направляют весь веб-трафик через продвинутую глобальную сеть, которая развивается с каждым запросом. В результате они видят значительное увеличение производительности и снижение спама и других атак. Cloudflare вошла в список лучших корпоративных культур 2018 по версии журнала Entrepreneur Magazine и вошла в число самых инновационных компаний мира по версии Fast Company в 2019 году. Cloudflare имеет штаб-квартиру в Сан-Франциско, Калифорния, а также офисы в Остине, Техас, Шампейн, Иллинойс, Нью-Йорк, Нью-Йорк, Сан. Хосе, Калифорния, Вашингтон, округ Колумбия, Лондон, Мюнхен, Пекин, Сингапур и Сидней.

Сноски

1. Clark, Matthew. “How the BBC builds websites that scale." CreativeBloq, https://www.creativebloq.com/features/how-the-bbc-builds-websites-that-scale. Accessed 22 July 2019.

2. “The State of Content: Expectations on the Rise." Adobe, https://blogs.adobe.com/creative/files/2015/12/Adobe-State-of-Content-Report.pdf. Accessed 24 July 2019.

3. “The need for mobile speed: How mobile latency impacts publisher revenue." Think with Google, https://www.thinkwithgoogle.com/intl/en-154/insights-inspiration/research-data/need-mobile-speed-how-mobile-latency-impacts-publisher-revenue/. Accessed 22 July 2019.

4. “Cloudflare Case Study: US Xpress." Cloudflare, https://www.cloudflare.com/case-studies/us-xpress/. Accessed 22 July 2019.

5. Rodman, Tedd. “Marketing & Web Performance: How Site Speed Impacts Metrics" Yottaa, https://www.yottaa.com/marketing-web-performance-101-how-site-speed-impacts-your-metrics/. Accessed 24 July 2019.

6. Everts, Tammy. “How Does Web Page Speed Affect Conversions? [INFOGRAPHIC]." Radware Blog, https://blog.radware.com/applicationdelivery/wpo/2014/04/web-page-speed-affect-conversions-infographic/. Accessed 24 July 2019.

7. Meder, Sam et al. “Driving user growth with performance improvements." Pinterest Engineering (Medium), https://medium.com/@Pinterest_Engineering/driving-user-growth-with-performance-improvements-cfc50dafadd7. Accessed 22 July 2019. h/t https://developers.google.com/web/fundamentals/performance/why-performance-matters/

8. “2016 Q2 Mobile Insights Report." Mobify, https://resources.mobify.com/2016-Q2-mobile-insights-benchmark-report.html. Gated. Accessed 22 July 2019. Secondary source: Runkevicius, Dainius. “Your Bottom Line Literally Depends on Milliseconds: 5 Advanced Techniques to Optimize Your Page Load Speed." The Mission (Medium), https://medium.com/the-mission/your-bottom-line-literally-depends-on-milliseconds-5-advanced-techniques-to-optimize-your-page-6b2350a98501. Accessed 22 July 2019.

9. Singhal, Amit, and Matt Cutts. “Using site speed in web search ranking." Google Webmaster Central Blog, https://webmasters.googleblog.com/2010/04/using-site-speed-in-web-search-ranking.html. Accessed 22 July 2019.

10. Wang, Zhiheng, and Doantam Phan. “Using page speed in mobile search ranking." Google Webmaster Central Blog, https://webmasters.googleblog.com/2018/01/using-page-speed-in-mobile-search.html. Accessed 22 July 2019.

11. “Mobile and tablet internet usage exceeds desktop for first time worldwide." StatCounter, http://gs.statcounter.com/press/mobile-and-tablet-internet-usage-exceeds-desktop-for-first-time-worldwide. Accessed 22 July 2019.

12. Meeker, Mary. “Internet Trends 2017 - Code Conference." Kleiner Perkins, https://www.kleinerperkins.com/perspectives/internet-trends-report-2017/. Accessed 24 July 2019. Presentation.

13. “Online mobile transaction statistics." Think with Google, https://www.thinkwithgoogle.com/data/online-mobile-transaction-statistics/. Accessed 22 July 2019.

14. An, Daniel. “Find out how you stack up to new industry benchmarks for mobile page speed." Think with Google, https://www.thinkwithgoogle.com/marketing-resources/data-measurement/mobile-page-speed-new-industry-benchmarks/. Accessed 24 July 2019. h/t https://www.marketingdive.com/news/google-53-of-mobile-users-abandon-sites-that-take-over-3-seconds-to-load/426070/

15. Finley, Klint. “The Average Webpage Is Now the Size of the Original Doom." Wired, https://www.wired.com/2016/04/average-webpage-now-size-original-doom/. Accessed 17 July 2019.

16. Laurinavicius, Tomas. “Top Web Design Trends To Watch In 2017." Forbes, https://web.archive.org/web/20170128171620/https://www.forbes.com/sites/tomaslaurinavicius/2017/01/25/web-design-trends-2017/#1afde0b41521. Archived Version Accessed 18 July 2019.

17. “Global Connected Commerce: Is e-tail therapy the next retail therapy?" Nielsen, https://www.nielsen.com/bd/en/insights/report/2016/global-connected-commerce/. Accessed 23 July 2019.

18. Schwarz, Ben. “Beyond the Bubble: Real world performance." Calibre (Medium), https://building.calibreapp.com/beyond-the-bubble-real-world-performance-9c991dcd5342. Accessed 24 July 2019.

19. O'Donoghue, Ruadhán. “You've been throttled, but don't stop browsing!" mobiForge, https://mobiforge.com/news-comment/youve-been-throttled-dont-stop-browsing. Accessed 24 July 2019.

20. “Failing to Meet Mobile App User Expectations: A Mobile App User Study." Dimensional Research, https://techbeacon.com/sites/default/files/gated_asset/mobile-app-user-survey-failing-meet-user-expectations.pdf. Accessed 24 July 2019. h/t http://thinkapps.com/blog/post-launch/mobile-app-performance-tips/

21. “DNS Performance Analytics and Comparison." DNSPerf, https://www.dnsperf.com/. Accessed 23 July 2019.

22. Nielsen, Jakob. “Response Times: The 3 Important Limits." Nielsen Norman Group, https://www.nngroup.com/articles/response-times-3-important-limits/. Accessed 26 July 2019.

23. “Cloudflare Case Study: Crisp." Cloudflare, https://www.cloudflare.com/case-studies/crisp/. Accessed 26 July 2019.

24. “ITIC 2017 – 2018 Global Server Hardware, Server OS Reliability Report." Information Technology Intelligence Consulting (ITIC) Corp, https://cloud.kapostcontent.net/pub/3dee045e-4b09-48e3-9077-8b126a9f2093/itic-2017-2018-global-server-hardware-server-os-reliability-report.pdf. Accessed 26 July 2019.

25. “Server FAIL: 3 signs your server is on the brink." Spiceworks, https://www.spiceworks.com/it-articles/3-signs-server-about-to-fail/. Accessed 26 July 2019.

26. Указанные временные значения получены на основе скорости света, проходящего через оптоволокно.

Приложение: показатели производительности, которые необходимо знать

Время загрузки: время, необходимое веб-браузеру для завершения загрузки и отображения веб-страницы (обычно измеряется в миллисекундах).

Время до первого байта (TTFB): сколько времени требуется браузеру для получения первого байта данных от веб-сервера. (измеряется в миллисекундах).

Запросы: количество HTTP-запросов к ресурсам, которые браузер должен выполнить для полной загрузки страницы.

DOMContentLoaded (DCL): измеряет время, необходимое для загрузки полного HTML-кода страницы; изображения, файлы CSS и другие ресурсы загружать не нужно

Время загрузки страницы, видимой без прокрутки: «Видимый без прокрутки» относится к области веб-страницы, которая умещается в окне браузера без необходимости прокрутки страницы вниз.

Первое существенное отображение (FCP): время, когда контент впервые начинает «рисоваться» или отображаться браузером. Это может быть любое содержимое страницы, включая текст, изображения или не белые цвета фона.

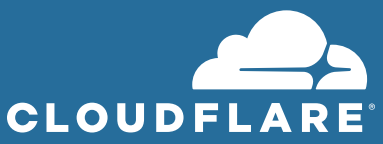
Размер страницы: общий размер файлов всего содержимого и ресурсов, отображаемых на странице.

Круговые обходы: этот показатель подсчитывает количество круговых обходов, необходимых для загрузки веб-страницы. Когда HTTP-запрос проходит весь путь от браузера к исходному серверу, а HTTP-ответ сервера возвращается обратно, это представляет собой круговой обход.

Круговые обходы блокирующие рендеринг: подкатегория круговых обходов. «Блокирующие рендеринг» относится к ресурсам, которые необходимо загрузить, прежде чем что-либо еще может быть загружено.

Круговая задержка (Время приема-передачи): количество времени, которое занимает выполнение одного кругового обхода

Ресурсы, блокирующие рендеринг: определенные ресурсы, такие как файлы CSS, блокируют загрузку других частей страницы, если они еще не загружены. Чем больше у веб-страницы ресурсов, блокирующих рендеринг, тем больше шансов, что браузер не сможет загрузить страницу.



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

REV: 200315

CLOUDFLARE®

5 Способов максимально повысить безопасность, производительность и надежность Вашего онлайн-бизнеса

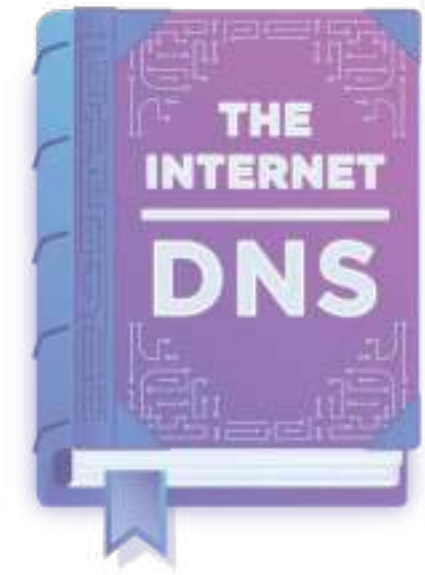
Интернет быстро меняется, а вместе с ним меняется и характер современных предприятий. Обеспечение наилучшего онлайн-опыта для ваших клиентов больше не является необязательной опцией; по мере роста спроса на веб-службы и приложения, предприятия обязаны удовлетворять потребности клиентов, обеспечивая при этом максимальную безопасность, скорость и надежность своих веб-сайтов и приложений.

С постепенным переходом в "онлайн", предприятия сталкиваются с новыми вызовами и возможностями для роста - от прогнозирования и удовлетворения цифровых потребностей клиентов до создания надежной защиты от веб-атак, а также с преодолением проблем с задержками (пингом), предотвращением сбоев в работе сайтов, поддержанием доступности и высокой производительности сети.

При оптимизации взаимодействия с клиентами в Интернете предприятиям необходимо принять чёткую стратегию, объединяющую в себе безопасность, производительность и надежность сайта. Хотя эта стратегия включает в себя множество компонентов, вот пять ключевых моментов, которые могут помочь предприятиям удовлетворить потребности клиентов и обеспечить безопасный и бесперебойный пользовательский опыт.

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

Используйте поддержку DNS и DNSSEC, чтобы максимально увеличить доступность и время безотказной работы



DNS (система доменных имен), которую часто называют «телефонной книгой Интернета», преобразует доменные имена в числовые IP-адреса и позволяет браузерам загружать Интернет-ресурсы. Поскольку DNS предназначен для приема любого адреса, предоставленного ему, выбор правильной стратегии безопасности DNS имеет решающее значение. Пренебрегая безопасностью, компании подвергаются нескольким рискам, в числе которых - перехват DNS, атаки типа «атака посредника», раскрытие и потеря конфиденциальной информации пользователей, фишинг и другие серьезные угрозы. По мере того как DNS атаки становятся все более распространенными, компании начинают понимать, что отсутствие отказоустойчивого DNS создает уязвимость в их общей стратегии безопасности.

Есть несколько подходов, которые компании могут использовать для развертывания отказоустойчивой стратегии DNS. Например, они могут начать использовать поставщика управляемых DNS, который размещает у себя все записи DNS, предлагает обработку запросов DNS на нескольких узлах по всему миру и обеспечивает интегрированную поддержку DNSSEC. DNSSEC добавляет уровень безопасности к системе доменных имен, путем добавления криптографических подписей к существующим записям DNS. Компании также могут создать дополнительную избыточность, развернув стратегию нескольких DNS - даже если первичный DNS выходит из строя, вторичный DNS помогает поддерживать приложения в сети. Крупные предприятия, которые предпочитают поддерживать свою собственную инфраструктуру DNS, могут внедрить DNS firewall в сочетании со вторичным DNS. Эта надстройка добавляет уровень безопасности к локальной инфраструктуре DNS и помогает обеспечить общую избыточность DNS.

Истории успеха клиентов

Перед компанией, которая занимается криптовалютой и разработкой клиентского инструмента с открытым исходным кодом для работы с блокчейн, после сложной DNS-атаки, перенаправляющей все запросы на фишинговый сайт, встала задача повышения безопасности их DNS. Хакерам удалось заставить один из авторитетных серверов, перенаправлять все запросы к веб-сайту компании в новое место назначения. Фишинговый веб-сайт выглядел идентично сайту фирмы, но использовался для передачи хакерам личных ключей пользователей, давая злоумышленникам доступ к огромному количеству криптовалюты.

Как и многие другие компании, они стали жертвами из-за серьезной уязвимости в базовой инфраструктуре Интернета и в результате потеряли доверие своих клиентов. Чтобы этого никогда не повторилось, они внедрили Cloudflare DNS. Переход на Cloudflare был самым простым способом внедрения DNSSEC, поскольку они смогли подготовить протокол и управлять им с единой, простой в использовании административной панели, что не только повысило отказоустойчивость их среды безопасности, но и обеспечило более безопасный и эффективный пользовательский опыт для их клиентов, которые полностью полагались на них в вопросе сохранности своих криптоактивов.

Для получения дополнительной информации о DNS и DNSSEC посетите наш веб-сайт Cloudflare DNS.

Ускорьте доставку контента за счет маршрутизации трафика по наименее загруженным маршрутам

Сегодня большая часть веб-трафика проходит через сети доставки содержимого (CDN), включая трафик с таких крупных сайтов, как Amazon и Facebook. CDN — это географически распределенная сеть серверов, которая помогает обеспечить быстрый доступ к интернет содержимому для аудитории по всему миру, а также уменьшить расходы на обеспечение производительности.

Располагая серверами в нескольких точках по всему миру, CDN может размещать контент ближе к посетителям веб-сайта и тем самым сокращать естественную задержку в сети и уменьшать время загрузки страницы. CDN также обрабатывает статические ресурсы из кеша по всей своей сети, уменьшая количество запросов, отправляемых на веб-сервера, что приводит к улучшению пропускной способности и снижению затрат на хостинг.

История успеха клиента

С этой проблемой, столкнулась одна из крупнейших в мире служб доставки еды. Работая с партнерами в тысячах городах США и оказывая услуги "доставка до двери", которая полностью зависит от их онлайн-платформы и приложений для смартфонов. Компании очень важно постоянно обеспечивать быстрый и надёжный клиентский опыт. Это не только помогает поддерживать растущую базу пользователей, но и укрепляет их партнерские отношения с местными ресторанами и торговцами.

Изначально компания столкнулась с несколькими проблемами производительности. У них не было надежного CDN, а также решения для изменения размера изображений, что являлось ключевым пунктом для обеспечивания надлежащего пользовательского опыта для их клиентов. Клиенты, посещающие сайт, должны были иметь возможность просматривать фотографии различных вариантов продуктов в высоком разрешении. К тому же, по мере роста компании, количество пунктов меню, которые они предлагали своим пользователям, постоянно увеличивалось. Поиск решения для оптимизации изображений и уменьшения времени загрузки был жизненно важным, тем более, что их предыдущее решение по изменению размера изображений обходилось им в тысячи долларов в месяц.

CloudFlare помогает компании по доставке еды ускорить взаимодействие с пользователеми с помощью внедрения Cloudflare Content Delivery Network (CDN). Cloudflare CDN, поддерживается глобальной сетью, которая охватывает более 25 миллионов Интернет-ресурсов. Сервис кэширует статический контент как можно ближе к конечным пользователям и работает в тандеме с Argo Smart Routing для интеллектуальной маршрутизации запросов контента по наиболее быстрому пути. А благодаря Cloudflare Image Resizing, позволяющему компании кэшировать изображения и уменьшать задержку, загрузка их ЦП снизилась на 20%.

Чтобы узнать, как CDN может ускорить доставку контента для вашего бизнеса, посетите Cloudflare CDN.

Минимизируйте риск простоя сайта за счет глобальной балансировки нагрузки трафика

Максимизация ресурсов и в то же время увеличение эффективности сервера это тонкий баланс. Перегруженные сервера или сервера, которые находятся слишком далеко от конечных пользователей географически, могут пагубно сказаться на бизнесе, поскольку увеличенная задержка, а также сбои в работе сервера могут привести к потере дохода, потере доверия клиентов и ухудшению качества бренда.

Облачные балансировщики нагрузки распределяют запросы между несколькими серверами, чтобы справляться с пиковым трафиком. Балансировка нагрузки принимается на границе сети, ближе к конечным пользователям, что позволяет предприятиям увеличить время отклика и эффективно оптимизировать свою инфраструктуру, сводя к минимуму риск отказа сервера. Даже если один сервер выходит из строя, балансировщик нагрузки может перенаправлять и перераспределять трафик между оставшимися серверами, гарантируя, что клиенты никогда не испытают значительных задержек или не увидят сбой сайта. Балансировщик нагрузки также позволяет проводить активные проверки работоспособности, что позволяет предприятиям выявлять неэффективные серверы и принимать превентивные меры до того, как произойдет сбой.

История успеха клиента

Когда крупной платформе электронной коммерции со штаб-квартирой в Канаде, работающей в 175 странах по всему миру, потребовалось интегрированное решение для повышения производительности и безопасности, они искали поставщика, который обеспечил бы простоту внедрения и помог бы сократить расходы на инфраструктуру. Во время перехода компании на Cloudflare им требовалось, чтобы этот процесс был непрерывным и не мешал работе более 1 миллиона предприятий, зависящих от их платформы. Разместив каждый из сайтов в глобальной сети Cloudflare, компания электронной коммерции обеспечила своим клиентам более быстрый отклик , что помогло увеличить продажи на платформе.

Центральное место в увеличении производительности занимает балансировщик нагрузки Cloudflare, использование которого позволило компании применить динамическое управление - другими словами, направлять трафик на самый быстрый пул исходных серверов для данного пользователя, уменьшая задержку и еще больше ускоряя трафик. Теперь у компании есть детальный контроль над тем, как их трафик распределяется между исходными серверами в добавок к преимуществам в производительности и точности, обеспеченными вычислениями в пределах досягаемости конечных устройств.

Узнайте, как повысить производительность и доступность приложений с помощью Cloudflare Load Balancing.

Защитите веб-приложения от злонамеренных атак

Интернет подвергает бизнес, основанный на работе в сети, широкому спектру рисков, связанных с атаками из разных мест с разными уровнями сложности. Многоуровневая стратегия безопасности может помочь защитить Ваш бизнес и веб-приложения от множества различных видов угроз.

Защита с помощью файрвола веб-приложения

Файрвол веб-приложений, или WAF, защищает веб-приложения, фильтруя и отслеживая HTTP-трафик. С помощью WAF предприятия могут защитить свои приложения от уязвимости нулевого дня, а также от наиболее распространенных угроз, таких как: межсайтовая подделка запросов.
(CSRF), межсайтовый скриптинг (XSS) и внедрение SQL-кода. Эти атаки могут поставить под угрозу серверы и сделать возможным кражу или подделку данных.
WAF также позволяет компаниям поддерживать детальный контроль над своими политиками безопасности, устанавливая правила, которые могут устранить уязвимости в их приложениях и обеспечить защиту от возникающих угроз. Облачные WAF, как правило, являются наиболее гибким и экономичным решением, так как их можно постоянно обновлять для защиты от новых угроз без значительных дополнительных усилий или затрат со стороны пользователя.

История успеха клиента

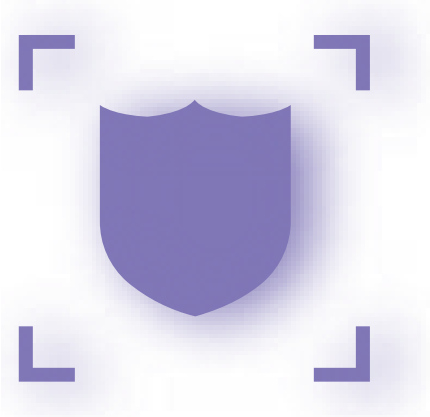
Для транснациональной финансовой корпорации из списка Fortune 500 создание дополнительных маркетинговых веб-сайтов для каждого географического местоположения было сложной задачей. Корпорации необходимо было обеспечить глобальное присутствие в сети, но она была вынуждена передать сложную инфраструктуру на аутсорсинг или оплачивать дорогостоящие профессиональные услуги у своего предыдущего поставщика, что оказалось трудоемким и непомерно дорогостоящим решением. Им требовалось решение, современное по своей архитектуре, которое предоставило бы им более детальный контроль над своими веб-ресурсами и помогло бы сбалансировать их мультиоблачную веб структуру с локальными центрами обработки данных и облачными приложениями.

После перехода на Cloudflare компания смогла защитить более 700 собственных веб-ресурсов за считанные минуты - без каких-либо дополнительных затрат. Теперь они могут воспользоваться преимуществами более гибкой самообслуживаемой среды, сэкономив и время, и драгоценные внутренние ресурсы.
Поскольку многие веб-сайты компании позволяют банкам получать доступ к данным платежных карт и обрабатывать другие конфиденциальные данные, внедрение многоуровневой стратегии безопасности является главным приоритетом для организации. Даже единичная успешная атака может поставить под угрозу репутацию их бренда и подорвать их доверие со стороны поставщиков и клиентов. Благодаря файрволу веб-приложений от Cloudflare (WAF) и расширенной защите от DDoS-атак каждый их сайт теперь защищен от внешних атак и вредоносных угроз.

Узнайте, как защитить критически важные для бизнеса веб-приложения от вредоносных атак с помощью Cloudflare Web Application Firewall.

Защита от DDoS атак

Для большинства веб-сайтов большой объем веб-трафика может быть хорошим фактором, ведущим к большему количеству конверсий, клиентов и продаж. Однако всплески веб-трафика также могут быть вызваны кибератаками, которые направлены на обрыв сетевых подключений, перегрузку серверов и таким образом на предотвращение доступа к сайту реальных пользователей.



DDoS-атака - это злонамеренная попытка перегрузить серверы, устройства, сети или окружающую инфраструктуру потоком ложного интернет-трафика. Занимая всю доступную полосу пропускания между целевыми устройствами и Интернетом, эти атаки не только вызывают серьезные сбои в обслуживании, но и оказывают ощутимое и негативное влияние на бизнес, поскольку клиенты не могут получить доступ к ресурсам компании.

История успеха клиента

Клиентская база крупнейшей в Индии компании по продаже билетов насчитывает более 60 миллионов клиентов. Объем трафика - около пяти миллиардов посещений в месяц и объём продаж - свыше 200 миллионов билетов ежегодно. Обеспечение быстрого и безопасного взаимодействия с пользователем имеет первостепенное значение для продажи их услуг, поскольку негативный опыт может увести клиентов к конкуренту. Когда компания подверглась масштабной DDoS-атаке, это поставило под угрозу весь бизнес.

Благодаря Cloudflare Advanced DDoS Protection им удалось избежать работы в авральном режиме, чтобы устранить последствия атаки. Обладая сетью с пропускной способностью более 56 Тбит/с, механизм защиты от DDoS-атак от Cloudflare разработан для простоты использования и управления. Cloudflare блокирует атаки на границе сети, чтобы поддерживать исходные серверы в рабочем состоянии и доступности - независимо от того, находятся ли они в локальной гибридной, или в мультиоблачной среде.

Cloudflare мгновенно начал блокировать вредоносный трафик со скоростью до 50 гигабайт в секунду и эффективно предотвратил DDoS-атаку, которая нарушила бы работу или замедлила работу сайта. Это позволило компании не только повысить уровень безопасности, но и обеспечить полную надежность и возрастающую операционную эффективность.

Для получения дополнительной информации о применении многоуровневого подхода к безопасности посетите Cloudflare Advanced DDoS Protection.

Защита от вредоносных ботов

Полная защита данных клиентов и веб-приложений от киберугроз требует многоуровневого подхода. Помимо других распространенных угроз кибербезопасности, сайты могут стать целью вредоносной активности ботов, что может привести к перегрузке веб-серверов, искажению аналитики, блокировке доступа пользователей к веб-страницам, краже пользовательских данных и поставить под угрозу критически важные бизнес-функции.

"Хорошие" боты относятся к программным приложениям, которые запрограммированы для выполнения полезных задач, от сканирования контента на веб-страницах до ответа на запросы клиентов на веб-сайте. Однако боты также могут быть скомпрометированы хакерами и использованы для выполнения злонамеренных действий, от кражи учетных данных и взлома конфиденциальных данных до кражи SEO-контента и нарушения бизнес-операций. Внедряя решение для управления ботами, компании смогут различать полезные и вредоносные действия ботов и предотвращать злонамеренное влияние ботов на работу конечных пользователей.

История успеха клиента

Компания лидер отрасли в области программного обеспечения для автоматизации маркетинга столкнулась с атакой спамерскими ботами на веб-формы размещенные на сайте. Боты периодически атаковали веб-формы и затрудняли доступ к форме настоящих пользователей, что ставило под угрозу способность компании обеспечивать бесперебойную работу по обслуживанию своих клиентов

Компания обратилась к Cloudflare за решением для защиты от ботов, которое позволило бы им блокировать злонамеренные запросы не ухудшая опыт конечного пользователя. Cloudflare Bot Management использует машинное обучение для обнаружения аномалий в веб-трафике, блокирования атак ботов и вредоносного трафика, при этом пропуская хороших ботов и запросы реальных пользователей. Сегодня Cloudflare помогает им отфильтровать более 1 миллиона вредоносных запросов ботов в день, позволяя пользователям использовать программное обеспечение без риска сбоев или потери конфиденциальных данных.

Нивелируйте атаки ботов и управляйте "хорошими" и "плохими" ботами в реальном времени с Cloudflare Bot Management.

Поддерживайте вашу сеть в рабочем состоянии

Защитите свою сетевую инфраструктуру

Недостаточно просто защитить веб-серверы. Предприятия зачастую обладают аппаратной сетевой инфраструктурой, размещённой в общественных или частных ЦОДах, которые также нуждаются в защите от DDoS-атак. Многие поставщики средств защиты от DDoS-атак полагаются на один из двух методов остановки атаки: центры очистки или локальное сканирование и фильтрация через аппаратные блоки. Проблема обоих методов заключается в том, что их использование увеличивает время загрузки, что может отрицательно повлиять на бизнес.

Очистка требует перенаправления сетевого трафика на централизованные сервера по очистке в определенных географических точках в попытке отфильтровать или «очистить» вредоносный трафик от не вредоносного. Перенаправление всего трафика в географически удаленный центр очистки влечет за собой дополнительно увеличение времени отклика, что часто неприемлемо для большинства приложений.

Другой метод защиты от DDoS-атак использует локальные аппаратные блоки для сканирования трафика и фильтрации вредоносных запросов. Подобно очистке, сканирующее оборудование вызывает задержку в сети и снижает производительность из за принципиальной необходимости пропускать весь трафик через единый блок для сканирования. Локальные устройства защиты от DDoS-атак часто имеют ограниченную пропускную способность, которая зависит и от пропускной способности сети организации и от аппаратной мощности устройства.

Лучший способ обнаружить и подавить DDoS-атаки - сделать это на границе сети, в пределах досягаемости конечных устройств.
Благодаря сканированию трафика в географически ближайшем центре обработки данных, обеспечивается высокая доступность услуг даже во время серьезных DDoS-атак. Такой подход снижает увеличение времени загрузки страницы при атаке, вызванное из-за маршрутизации подозрительного трафика в географически удаленные центры очистки. Он также позволяет быстрее начать реагировать на атаку.

История успеха клиента

Когда некоммерческая организация, управляющая одним из 10 лучших веб-сайтов (по рейтингу Alexa), начала испытывать серьезные проблемы с временем отклика и сбоями, им потребовалось решение, которое смягчило бы атаки на сетевом уровне и позволило бы им быстро вернуться в онлайн.

Атака, характеризуемая как ‘takedown attack’ - это злонамеренная атака, которая приводит к перегрузке серверов компании и останавливает все операции. Атака переполнила сервера ложным сетевым и HTTP-трафиком. Компания обратилась в Cloudflare с просьбой подавить атаку и восстановить доступ к своему сайту, а также реализовать защиту от DDoS-атак на сетевом уровне, чтобы предотвратить подобные атаки в будущем.

Cloudflare Magic Transit обеспечивает защиту от DDoS-атак для локальных сетей и центров обработки данных в постоянном режиме или по в режиме по требованию. Cloudflare Magic Transit использует глобальную сеть Cloudflare для обнаружения и подавления DDoS-трафика в центрах обработки данных Cloudflare, ближайших к источникам атак. Благодаря крупномасштабной сети Cloudflare и надёжной защите от DDoS атак, компания смогла быстро обойти эффекты атаки, вернув для конечных пользователей работу на привычном уровне.

Посетите Cloudflare Magic Transit, чтобы узнать больше о защите от DDoS-атак в сети

Защита приложений TCP / UDP

На транспортном уровне злоумышленники могут выбрать своей целью ресурсы бизнес-сервера, подавляя все доступные порты на сервере. Эти DDoS-атаки могут привести к тому, что сервер будет медленно реагировать на настоящие запросы - или вообще перестанет отвечать. Предотвращение атак на транспортном уровне требует решения безопасности, которое может автоматически обнаруживать шаблоны атак и блокировать их трафик.

История успеха клиента

Это была одна из проблем, с которыми столкнулся лидер киберспортивной индустрии и разработчик игр - компания, которая может похвастаться более чем 200 миллионами пользователей по всему миру - когда она выявила многочисленные DDoS-атаки и обнаружила, что некоторые из их пользователей в удаленных частях земного шара получают негативный пользовательский опыт использования их TCP-приложения. В игровой индустрии это представляет собой значительную проблему, поскольку любая задержка в обслуживании может привести к серьёзной потере клиентов и дохода.

Инфраструктура игрового провайдера работает по проприетарному сетевому протоколу, разработанному для специально для геймеров, для которых важна низкая задержка, поэтому, когда дело доходит до DDoS-атак, обычные продукты безопасности не могут защитить данные протоколы.

Для повышения производительности и смягчения DDoS-атак на транспортном уровне компания обратилась за помощью к Cloudflare. Cloudflare Spectrum - защита от DDoS-атак для любых протоколов TCP / UDP позволила им защищать свой критически важный протокол связи, не снижая сквозной производительности, успешно предотвращая попытки замедлить их работу. Кроме того, Cloudflare Spectrum также использует оптимизацию TCP и интеллектуальную маршрутизацию Argo для ускорения TCP-трафика в сети Cloudflare.

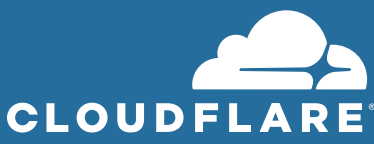
Повысьте скорость, безопасность и надежность приложения TCP / UDP вашего бизнеса с Cloudflare Spectrum.

Заключение

Для создания отличного пользовательского опыта в Интернете требуется правильная стратегия безопасности и производительности - стратегия, которая не только позволяет предприятиям ускорить доставку контента, но и обеспечивает надежность сети и защищает их веб-ресурсы от сбоев сайтов, кражи данных и других критических атак.

Располагая сетью, которая охватывает более 200 городов в более чем 90 странах по всему миру, Cloudflare предоставляет масштабируемую интегрированную глобальную облачную платформу, которая помогает предприятиям обеспечивать безопасность, производительность и надежность своих локальных, облачных и SaaS-приложений.

Чтобы узнать, как защитить и обезопасить свой бизнес в Интернете, посетите Cloudflare.com.



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

REV: 200330

Балансировка нагрузки Cloudflare

Максимизируйте доступность и производительность приложений

Для любой организации сложно привлечь новых клиентов, а еще сложнее их удержать. Потеря клиентов из-за простоев приложений или медленного отклика может стать дорогостоящей ошибкой - ошибкой, которой можно легко избежать.

Балансировщик нагрузки Cloudflare повышает доступность и производительность приложений, направляя запросы от неисправных исходных серверов и динамически распределяя их по ближайшим и наиболее быстро реагирующим пулам серверов.

Преимущества Cloudflare

ЕДИНАЯ ПАНЕЛЬ УПРАВЛЕНИЯ

Распределяйте трафик без перебоев между центрами обработки данных и облачными провайдерами из одного места - Cloudflare Dashboard.

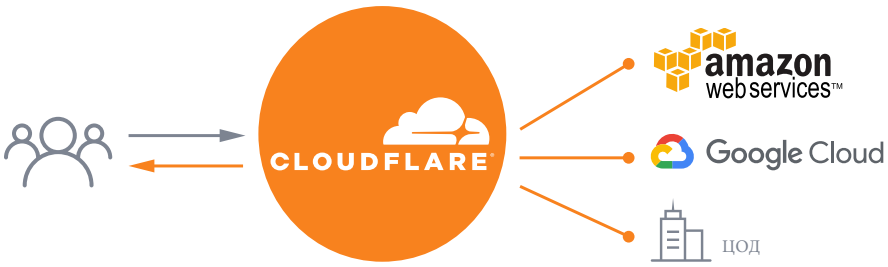
ИНТЕЛЛЕКТУАЛЬНЫЙ КОНТРОЛЬ ТРАФИКА

Управляйте глобальным и локальным трафиком в зависимости от географии, времени отклика и доступности. Поддерживает HTTP / S и TCP / UDP.

АНАЛИТИКА В РЕАЛЬНОМ ВРЕМЕНИ

Получите детальное представление о своем трафике и проанализируйте скорость отклика исходных серверов, где бы они ни находились

Независимый от провайдера балансировщик нагрузки в виде услуги



Cloudflare Load Balancing легко вписывается в любую среду - локальную, мультиоблачную или гибридную.
Повысьте отказоустойчивость ваших приложений, защитив их от сбоев по вине провайдера.

Ключевые особенности

Активные проверки работоспособности и быстрое переключение при отказе

Следите за состоянием своих пулов, чтобы обнаруживать сбои и устранять потенциальные простои. Как только источник или пул выходит из строя, запросы, проксированные через Cloudflare, мгновенно перенаправляются - без ожидания истечения срока жизни запроса. Проверки работоспособности могут проводиться каждые 5 секунд, а отчеты доставляются с помощью уведомлений по электронной почте или REST API.

Неограниченная защита от DDoS-атак

Получите неограниченную защиту от DDoS-атак. Наша глобальная сеть Anycast в 15 раз больше, чем самая крупная когда-либо зарегистрированная DDoS-атака, обеспечивает маршрутизацию трафика даже в условиях продолжающейся атаки.

Подробная аналитика трафика

Получите детальный отчет по своему трафику - определите, какие исходные серверы и пулы выбираются для вашего трафика и почему. Просматривайте визуализацию вашего трафика по балансировщикам нагрузки, пулам и исходным серверам в различных временных диапазонах.

Карты времени отклика в реальном времени

Создавайте карты времён отклика в реальном времени для анализа скорости реагирования всех ваших ресурсов по всему миру, независимо от того, где они размещены - локально, в облаке или в гибридной среде. Определяйте регионы, в которых запросы обрабатываются медленно, чтобы вы могли своевременно исследовать причину сбоев.

Привязка сессии к определённому серверу

Привяжите сеанс пользователя к определенному исходному серверу. Обеспечьте бесперебойную работу, сохраняя критически важную информацию о сеансах.

Легкая настройка

Настройте полнофункциональный балансировщик нагрузки за считанные минуты с помощью Cloudflare Dashboard или REST API. Добавляйте или удаляйте исходные серверы для балансировщиков нагрузки по мере масштабирования вашего трафика. Никакого дополнительного оборудования или программного обеспечения не требуется.

Комбинация возможностей управления геолокацией Балансировки нагрузки и кэширования в Cloudflare гарантируют, что клиенты получают максимально быстрое время загрузки

NIGEL HEPWORTH
Managing Director, Active Solutions

active solutions

Аналитические функции Балансировщика нагрузок от CloudFlare дают нашей команде точное понимание того, как идет наш трафик, через несколько исходных серверов и географических местоположений».

BOBBY SAMANIAN
Director, System Operations
8x8

8x8

CLOUDFLARE®

Балансировка нагрузки для высокой производительности и доступности в облаке

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

I. Основные выводы

Ежегодно предприятия теряют миллионы долларов из-за медлительности и простоя сайтов, в основном в форме упущенных сделок. Медленные или недоступные сайты и приложения также негативно влияют на внутреннюю производительность и ухудшают рейтинг в поисковых системах. Проблемы с задержкой и доступностью могут быть вызваны множеством факторов, в том числе перегруженными или неисправными серверами, географическим расстоянием между конечными пользователями и серверами, долгой работой сопоставителя DNS, DDoS-атаками и даже типом устройства, которое посетитель использует для доступа в Интернет.

Балансировщики нагрузки уменьшают задержки и проблемы с доступностью ресурса, равномерно распределяя веб-трафик по сети серверов, гарантируя, что ни один отдельный сервер не будет перегружен, и что веб-ресурсы будут по-прежнему доступны, даже если один из серверов выйдет из строя. Традиционно компании развертывали аппаратные балансировщики нагрузки в центрах обработки данных, но по мере того, как вычисления переходят в облако, предприятия переходят на более гибкие, менее дорогостоящие и простые в использовании облачные решения для балансировки нагрузки .

Однако не все облачные решения для балансировки нагрузки одинаковы. Надежное решение должно быть интегрировано с глобальной сетью доставки контента (CDN) и должно предлагать такие функции, как глобальная маршрутизация на основе геолокации, устойчивость к DDoS-атакам, функцию балансировки нагрузки уровней 3 и 4, а также расширенную аналитику и аварийное переключение в реальном времени. Решение также должно легко интегрироваться в мультиоблачные и гибридные облачные среды данных, которые сегодня есть у большинства предприятий.

II. Понимание балансировки нагрузки

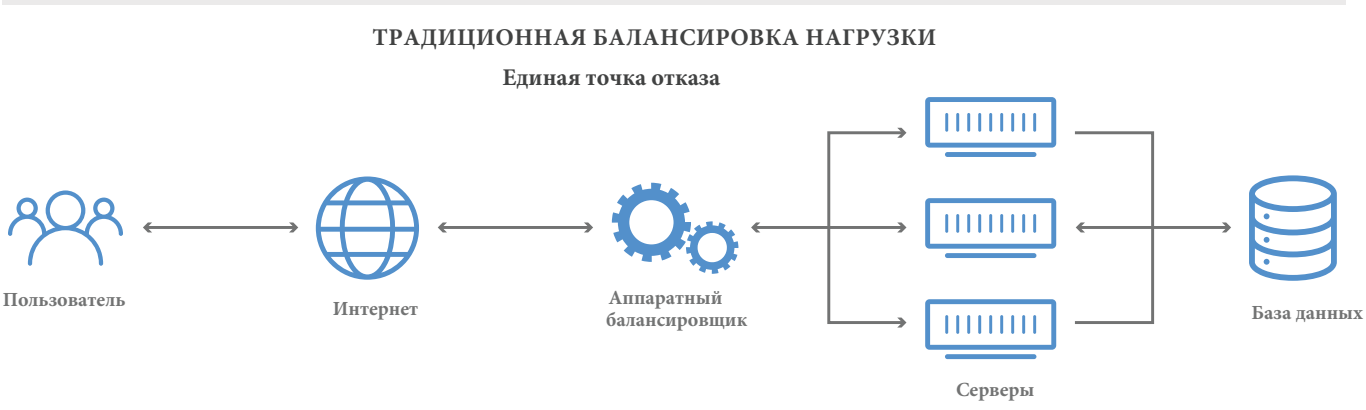
Балансировщик нагрузки - это уровень, располагающийся между сетью серверов и Интернетом, который управляет потоком информации между серверами и конечными пользователями. Целью балансировки нагрузки является равномерное распределение рабочих нагрузок между несколькими серверами. Это гарантирует надежность, эффективность и скорость отклика приложений, гарантируя, что отдельные серверы не будут перегружены во время пиков трафика. Балансировка нагрузки также обеспечивает аварийное переключение в случае сбоя сервера. Балансировщики нагрузки контролируют работоспособность сервера, и если один из серверов выходит из строя, балансировщик нагрузки просто направляет трафик через исправные серверы.

Традиционные балансировщики нагрузки

Традиционные балансировщики нагрузки - это аппаратные устройства, развернутые в локальных центрах обработки данных. Обычно они развертываются парами, чтобы обеспечить резерв на случай выхода из строя одного устройства.

- Аппаратные балансировщики нагрузки имеют множество недостатков.
- Их необходимо приобретать заранее, а их стоимость может быть существенной.
- Они не масштабируются. Чтобы определить, сколько балансировщиков нагрузки необходимо приобрести, предприятие должно рассчитать, какой объем трафика они ожидают от своего веб-сайта или приложения. Если трафик меньше, чем ожидалось, предприятие не использует избыточную пропускную способность, Если объем трафика превышает ожидаемый, конечные пользователи будут испытывать задержки или простои, пока не будут куплены, настроены и установлены новые устройства.
- Они работают на специализированных операционных системах, их довольно сложно настроить и обслуживать, что увеличивает их совокупную стоимость владения (TCO)
- Их можно использовать только в дата-центрах, а для развертывания приложений в облаке требуется виртуальное устройство, которое должно быть уникально настроено для каждого облака или центра обработки данных, в котором оно будет работать.

Облачные балансировщики нагрузки менее дороги, проще в использовании и больше подходят для современных вычислительных сред, в условиях, когда уже 94% предприятий перешли в облако, а 84% используют многооблачные среды[1]. Благодаря использованию гибкой сети серверов облачные балансировщики нагрузок дают предприятиям достаточную гибкость и мастабируемость для оперативного реагирования как на сезонные пики трафика, так и на долгосрочные планы нагрузок.

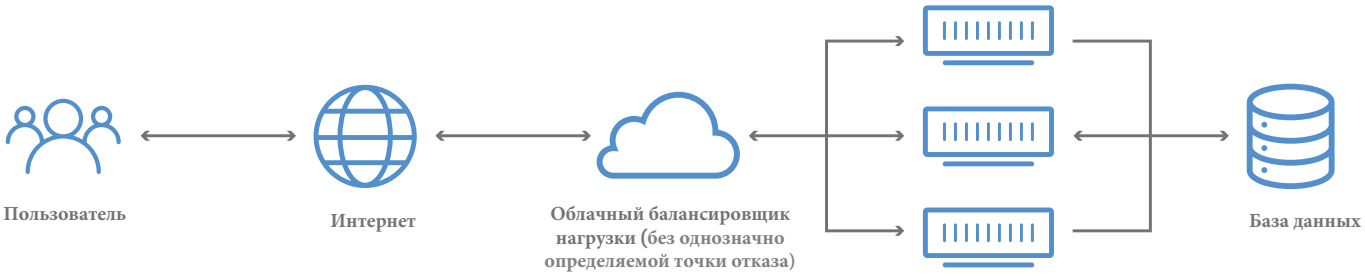


Облачные балансировщики нагрузки нового поколения

Хотя все поставщики общедоступных облачных ресурсов и предлагают балансировщики нагрузки, они остаются зависимыми от платформы. Они встроены в облако провайдера и могут использоваться только с приложениями, работающими в среде этого провайдера. Если предприятие хочет переместить приложение к другому облачному провайдеру или запустить его локально, балансировщик нагрузки не будет перемещаться вместе с ним, вынуждая предприятие перенастраивать балансировку нагрузки каждый раз, когда они хотят переместить приложение. Ситуация еще более осложняется для 58% организаций, которые пользуются гибридными облачными средами[2] и используют традиционные аппаратные балансировщики нагрузки.

Надежный автономный облачный балансировщик нагрузки можно использовать в сочетании с традиционными аппаратными решениями в гибридных средах, а также со штатными балансировщиками нагрузки, характерными для общедоступных облачных сервисов. Автономный балансировщик нагрузки - это нейтральный, независимый от поставщика уровень, который располагается поверх балансировщиков общественных облачных сервисов и аппаратных решений для балансировки внутри организации. Предприятие выбирает основного провайдера, через которого будет направлен весь трафик. Когда балансировщик нагрузки обнаруживает сбой, он автоматически направляет трафик через резервных провайдеров или другой регион. Если на предприятии возникают перебои в сети или подключение становится неустойчивым через общедоступное облако или в собственной инфраструктуре, автономный облачный балансировщик нагрузки автоматически переключается на исправных провайдеров или серверы.

ОБЛАЧНАЯ БАЛАНСИРОВКА НАГРУЗКИ НОВОГО ПОКОЛЕНИЯ



III. Проблемы, решаемые облачными балансировщиками нагрузки

У Предприятий, которым нужен облачный балансировщик нагрузки, есть выбор из нескольких опций. Выбор правильного решения для нужд вашего предприятия требует понимания проблем, которые решают балансировщики нагрузки - это проблемы со временем отклика временем простоя ресурса.

Стоимость на задержки отклика и времени простоя

На заре тысячелетия продолжительность концентрации внимания человека составляла 12 секунд; сегодня это всего восемь секунд[3]. Это имеет серьезные последствия для онлайн-бизнеса любого размера и в любой отрасли. Современные потребители в цифровом информационном пространстве нуждаются в веб-сайтах, приложениях и API, которые загружаются мгновенно и всегда доступны онлайн по первому требованию. Понимая это, Google использует скорость страницы в качестве фактора ранжирования как для настольного, так и для мобильного поиска.[4]

Даже крошечные задержки могут заметно повлиять на вовлеченность и коэффициент конверсии. Задержка становится заметной для среднего пользователя через 30 миллисекунд,[5] а задержки от 100 до 400 миллисекунд оказывают заметное влияние на поведение потребителей.[6] Всего одна дополнительная секунда времени загрузки может привести к снижению конверсии на 7%.[7] Задержка также вредит и операционной деятельности компании. В среднем сотрудник ежегодно тратит одну неделю в год на ожидание отклика от сети своей компании[8].

При отсутствии контроля задержка может привести к тому, что веб-сайты и приложения вообще становятся недоступными. Стоимость простоя резко возрастает. В 2010 году средняя стоимость минуты простоя центра обработки данных составила 5 617 долларов США. К 2016 году эта сумма выросла до 8 851 долларов США. Большая часть этих затрат связана с активностью пользователей, упущенной выручкой и сбоями в работе.[9]

Ожидание в сетях

В среднем сотрудник ежегодно тратит одну неделю в год на ожидание отклика от сети своей компании.

Причины задержки и простоя

Поскольку многие факторы влияют на скорость загрузки веб-ресурсов, предприятия постоянно сталкиваются с проблемой достижения низкой задержки и высокой доступности. Среди прочих факторов, на задержку и доступность ресурса влияют:

НЕРАВНОМЕРНО РАСПРЕДЕЛЕННАЯ ЗАГРУЗКА СЕРВЕРА

Чрезмерно загруженные серверы работают медленнее, что может привести к замедлению работы веб-сайтов и приложений или даже к их полной одновременной остановке. Равномерное распределение рабочих нагрузок по сети серверов максимизирует производительность и предотвращает простои. Эффективная балансировка нагрузки может значительно повысить производительность; одна компания SaaS отметила уменьшение времени загрузки страницы на 2-3 секунды после развертывания Балансировщика нагрузки от Cloudflare.[10]

ГЕОГРАФИЧЕСКОЕ РАССТОЯНИЕ

Интернет стремительно растет. В 2019 году 57% населения мира были подключены к Интернету, и более миллиона человек в день выходили в Интернет впервые.[11]

Это влияет на скорость и доступность двумя способами. Больше людей в сети означает меньшую пропускную способность, а расстояние между пользователями и серверами мешает компаниям взаимодействовать с клиентской базой. По оценкам, каждые 100 миль географического расстояния между ресурсами приложения или веб-сайта и конечным пользователем добавляют 0,82 миллисекунды задержки.[12]

СЛОЖНОСТЬ САЙТОВ И ПРИЛОЖЕНИЙ

Интернет-контент становится богаче и сложнее, что делает современные веб-сайты , более громоздкими, чем когда-либо. Общий размер страницы неуклонно увеличивался с 2011 года[13]. Приложения, богатые контентом, которые используются для игр, виртуальной реальности и приложения дополненной реальности широко используются повсеместно, а видеоигры сейчас являются самым популярным развлечением в мире.[14]

Размер страницы

Общий размер страницы неуклонно растет как минимум с 2011 года.

Когда-то размеры игр были ограничены размером физических носителей, таких как диски CD-ROM. Благодаря широкому распространению высокоскоростного доступа в Интернет, современные игры ограничены только пропускной способностью канала конечного пользователя и пространством на жестком диске. Видео с высоким разрешением, объемный звук 5.1 и замысловатые текстуры, используемые для создания современных игр, привели к увеличению размеров файлов. В середине 2000-х Red Orchestra 1 считался довольно большим - 2,6 ГБ. Но Forza Motorsport 7, выпущенная в 2017 году, имеет колоссальный размер в 96,5 ГБ.[15]

ТИП УСТРОЙСТВА

Оптимизация сайтов и приложений для мобильных устройств теперь обязательна. Почти 60% запросов в поисковиках выполняются с мобильных устройств,[16] и около половины мобильных пользователей ожидают, что приложения ответят за две секунды или меньше.[17] Достижение постоянной доступности и низкой задержки на мобильных устройствах связано с собой особый набором трудностей. Производительность мобильной связи ограничивается возможностью подключения к сети и ее доступностью. Несмотря на широкую доступность сетей 4G и 5G в некоторых странах, 60% мобильных подключений во всем мире осуществляются по 2G.[18] В некоторых регионах провайдеры мобильных сетей ограничивают пропускную способность сверх определенной величины.[19]

МЕДЛЕННОЕ СОПОСТАВЛЕНИЕ DNS

Когда пользователи получают доступ к веб-ресурсу, их устройства должны запрашивать DNS, который сопоставит доменное имя ресурса с его IP-адресом, а затем отправит правильный IP-адрес обратно на устройство. Это называется сопоставлением DNS, и его оптимизация является важной частью оптимизации производительности. Не все DNS-провайдеры оптимизированы по скорости - многим DNS-провайдерам требуется более 50 миллисекунд для обработки каждого DNS-запроса. Самые быстрые поставщики DNS обрабатывают запросы менее чем за 20 миллисекунд; Например, Cloudflare DNS обрабатывает запросы в среднем менее чем за 12 миллисекунд.[20]

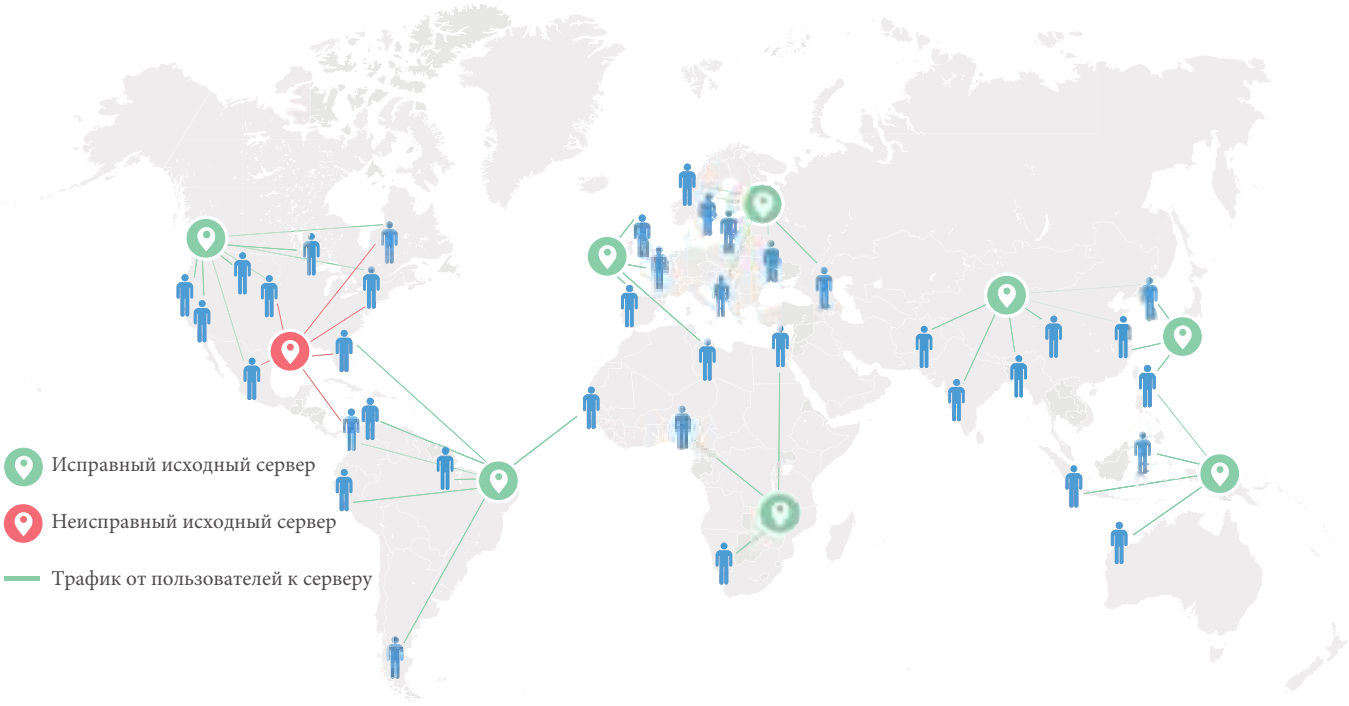
60 секунд

многим DNS-провайдерам требуется более 60 миллисекунд для обработки каждого DNS-запроса

РАБОТОСПОСОБНОСТЬ СЕРВЕРА

Как и на всех компьютерах, на серверах могут возникать проблемы. Мониторинг работоспособности серверов и приложений имеет решающее значение для уменьшения задержки и обеспечения доступности приложений в случае сбоя. Решения для балансировки нагрузки, которые не могут отслеживать состояние сервера, могут непреднамеренно направлять трафик на сервер, на котором возникают проблемы, что приводит к длительным задержкам и отключениям для пользователей.

ПРОСТОИ ПО ПРИЧИНЕ НЕИСПРАВНОСТИ ИСХОДНОГО СЕРВЕРА



Распределённые атаки на отказ в обслуживании (DDOS-атаки)

DDoS-атаки представляют собой серьезную угрозу для здоровья серверов, а их частота, размер и критичность возрастают. В период с первого квартала 2019 года по первый квартал 2018 года количество атак размером 100 Гбит/с и выше резко возросло на 967%, и более трех четвертей атак были направлены на более чем один вектор.[21] Во многих DDoS-атаках используются «армии зомби» захваченных устройств IoT, как это было в случае с ботнет-атаками Mirai против DNS-провайдера Dyn в 2016 году[22]

Помимо того, что DDoS-атаки вызывают задержки и простои, они иногда используются как дымовая завеса для других кибератак. Вывод из строя веб-сайта или приложения - хороший способ отвлечь ИТ-команду компании во время утечки данных

IV. На что обращать внимание при оценке облачных решений для балансировки нагрузки

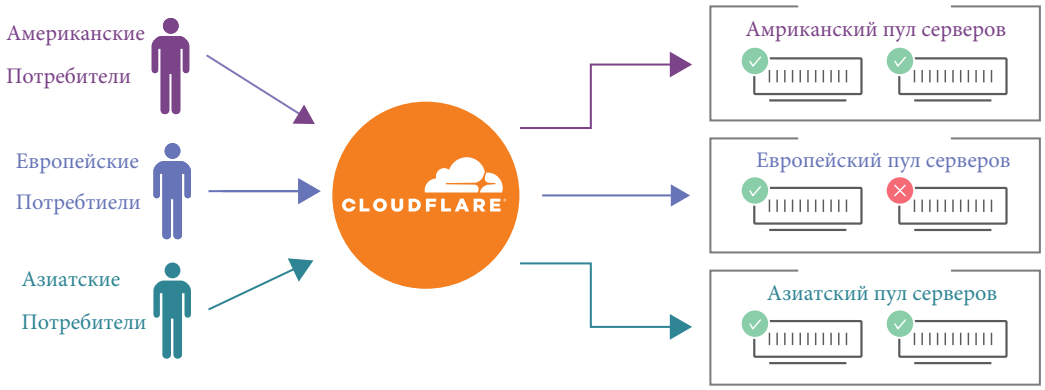
Крайне важно выбрать решение для балансировки нагрузки, которое не только соответствует требованиям вашего бизнеса сегодня, но и может легко масштабироваться в соответствии с вашими будущими потребностями. Решение также должно быть достаточно надежным, чтобы соответствовать современным уровням объема трафика, сложности приложений и размеру DDoS-атак. Вот список функций, на которые стоит обратить внимание.

Интеграция с глобальной сетью доставки контента (CDN)

Балансировка нагрузки и CDN работают вместе, чтобы решить проблемы с задержкой и доступностью. CDN кэширует статический контент на границе сети, чтобы его можно было получать с ближайшего к конечному пользователю сервера. Это значительно повышает производительность и минимизирует нагрузку на канал за счет уменьшения количества запросов, отправляемых на исходный сервер.

Глобальная маршрутизация на основе геолокации

Поскольку географическое расстояние между сервером и конечным пользователем играет такую важную роль в борьбе с задержками, современный балансировщик нагрузки должен иметь возможность подключать посетителей к инфраструктуре, которая находится в той же части мира. Например, трафик из Великобритании следует направлять в центр обработки данных в Лондоне, а не в Нью-Йорк.



Устойчивость к DDoS-атакам

Чем меньше емкость глобальной CDN, тем больше вероятность того, что DDoS-атака сможет вывести её из строя. В связи с быстрым ростом масштабов DDoS-атак сеть CDN должна иметь возможность противостоять даже самой крупной DDoS-атаке и иметь свободное место, чтобы балансировщик нагрузки всегда мог направлять трафик на исправные серверы даже в условиях продолжающейся атаки.

Функциональность балансировки нагрузки уровней 3 и 4

Злоумышленники могут напрямую отправлять объёмный DDoS-трафик на настраиваемые протоколы связи TCP и UDP, используемые для настраиваемых игровых протоколов, удаленного доступа к серверу (SSH), служб безопасной передачи файлов (SFTP) и электронной почты (SMTP). Они также могут использовать эти порты для перехвата незашифрованных данных при передаче. Защита этих портов и протоколов без ущерба для производительности требует дополнительных ресурсов. Убедитесь, что ваш балансировщик нагрузки поддерживает защиту от DDoS-атак уровней 3 и 4, а также защиту TLS / SSL для шифрования данных клиентов.

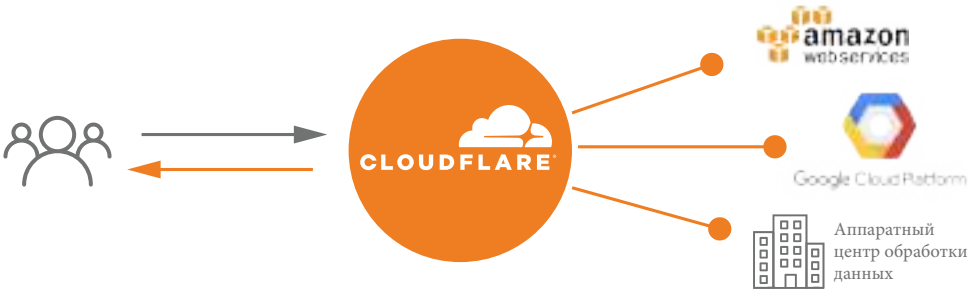
Отработка отказа в режиме, близком к реальному

Облачные балансировщики нагрузки часто полагаются на общедоступный DNS, который обладает низкой пропускной способностью, задерживая отработку отказа в случае проблем. Убедитесь, что ваш балансировщик нагрузки основан на DNS с коротким временем жизни (TTL), что гарантирует, что переключение при отказе может произойти за считанные секунды.

Поддержка мультиоблака и гибридного облака

Чтобы избежать привязки к поставщику, снизить сложность и свести к минимуму неправильные конфигурации в мультиоблачных и гибридных средах, убедитесь, что балансировщик нагрузки является нейтральным уровнем, который может работать как локально, так и в любом общедоступном облаке. Независимый от поставщика балансировщик нагрузки не заменит встроенные балансировщики нагрузки поставщиков облачных услуг или традиционные аппаратные устройства, а скорее будет работать в тандеме с ними, чтобы всё работало вместе без сбоев.

Независимый от поставщика балансировщик



Легкость использования

Время, потраченное на настройку вашего решения для балансировки нагрузки, - это время, которое вы не можете потратить на управление своим бизнесом. Хороший облачный балансировщик нагрузки может быть настроен за считанные минуты и требует минимального управления. Должна присутствовать поддержка графического пользовательского интерфейса и мощных API-интерфейсов, а решение должно легко перенастраиваться по мере изменения потребностей вашего бизнеса.

Аналитика

Поскольку решения для балансировки нагрузки расположены между конечными пользователями и приложениями, они находятся в идеальном положении для сбора эффективной бизнес-аналитики, касающейся поведения клиентов, производительности приложений, состояния безопасности и других операционных данных. Убедитесь, что ваше решение для балансировки нагрузки собирает эту аналитику, а также интегрируется с Вашим существующим поставщиком аналитических данных.

Заключение

Современные веб-сайты и приложения не будут работать должным образом или оставаться в сети без использования балансировщика нагрузки. Надежный облачный балансировщик нагрузки - гораздо лучший выбор, чем традиционное аппаратное решение. Помимо того, что автономный облачный балансировщик нагрузки менее дорогой, простой в использовании и масштабируемый, он дополняет как традиционные аппаратные балансировщики нагрузки, так и проприетарные решения, предлагаемые поставщиками общедоступного облака, гарантируя, что веб-ресурсы всегда остаются доступными и высокопроизводительными.

Ссылки

1. Flexera, "Cloud Computing Trends: 2019 State of the Cloud Survey," https://www.flexera.com/blog/cloud/2019/02/cloud- computing-trends-2019-state-of-the-cloud-survey/. Accessed October 10, 2019.
2. Ibid.
3. The Human Attention Span [Infographic], Digital Information World, https://www.digitalinformationworld.com/2018/09/the-human-attention-span-infographic.html. Accessed August 6, 2019.
4. "Using page speed in mobile search ranking," Google Webmaster Central Blog, https://webmasters.googleblog.com/2018/01/using-page-speed-in-mobile-search.html. Accessed August 6, 2019.
5. Rouse, Margaret. "What Is Latency?" TechTarget. https://whatis.techtarget.com/definition/latency. Accessed October 10, 2019.
6. Brutlag, Jake. "Speed Matters," Google AI Blog, https://ai.googleblog.com/2009/06/speed-matters.html. Accessed August 6, 2019.
7. Rodman, Tedd. "Marketing & Web Performance: How Site Speed Impacts Metrics," Yottaa, https://www.yottaa.com/marketing-web-performance-101-how-site-speed-impacts-your-metrics. Accessed August 6, 2019.
8. Hastreiter, Nick. "Why Slow Internet Costs Companies Money," HuffPost, https://www.huffpost.com/entry/why-slow-internet-costs-companies-money_b_5801a4b2e4b0985f6d1570e5. Accessed October 10, 2019.
9. Priceonomics Data Studio. "Quantifying the Staggering Cost of IT Outages," https://priceonomics.com/quantifying-the-staggering-cost-of-it-outages/. Accessed October 10, 2019.
10. "Cloudflare Case Study: Crisp." Cloudflare, https://www.cloudflare.com/case-studies/crisp/. Accessed July 26, 2019.
11. Kemp, Simon. "Digital 2019: Global Internet Use Accelerates," We Are Social, https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates. Accessed October 10, 2019.
12. Sherman, Fraser. "Network Latency Milliseconds Per Mile," Techwalla, https://www.techwalla.com/articles/network-latency-milliseconds-per-mile. Accessed 6 August 2019.
13. Report: State of the Web, HTTP Archive. http://beta.httparchive.org/reports/state-of-the-web#bytesTotal. Accessed August 6, 2019.
14. D'Argenio, Angelo M. "Statistically, Video Games Are Now the Most Popular and Profitable Form of Entertainment." https://www.gamecrate.com/statistically-video-games-are-now-most-popular-and-profitable-form-entertainment/20087. GameCrate. Accessed 27 August 2019.
15. Wilde, Tyler. "How game sizes got so huge, and why they'll get even bigger." https://www.pcgamer.com/how-game-sizes-got-so-huge-and-why-theyll-get-even-bigger/. PCGamer. Accessed 27 August 2019.
16. Sterling, Greg. "The mobile, desktop split may have stabilized at roughly 60% – 40%," Search Engine Land, https://searchengineland.com/mobile-desktop-search-traffic-split-may-have-stabilized-at-roughly-60-40-317091. Accessed August 6, 2019.
17. Dimensional Research. "Failing to Meet Mobile App User Expectations: A Mobile App User Survey," https://techbeacon.com/sites/default/files/gated_asset/mobile-app-user-survey-failing-meet-user-expectations.pdf. Accessed August 6, 2019.
18. Schwarz, Ben. "Beyond the Bubble: Real world performance." Calibre (Medium), https://building.calibreapp.com/beyond-the-bubble-real-world-performance-9c991dcd5342. Accessed October 10, 2019.
19. O'Donoghue, Ruadhán. "You've been throttled, but don't stop browsing!" mobiForge,https://mobiforge.com/news-comment/youve-been-throttled-dont-stop-browsing. Accessed October 10, 2019.
20. "DNS Performance Analytics and Comparison." DNSPerf, https://www.dnsperf.com/. Accessed 23 July 2019.
21. Rayome, Alison DeNisco. "Major DDoS attacks increased 967% this year," TechRepublic, https://www.techrepublic.com/article/major-ddos-attacks-increased-967-this-year/. Accessed August 6, 2019.
22. Dignan, Larry. "Dyn confirms Mirai botnet involved in distributed denial of service attack," ZD Net, https://www.zdnet.com/article/dyn-confirms-mirai-botnet-involved-in-distributed-denial-of-service-attack/. Accessed August 6, 2019.