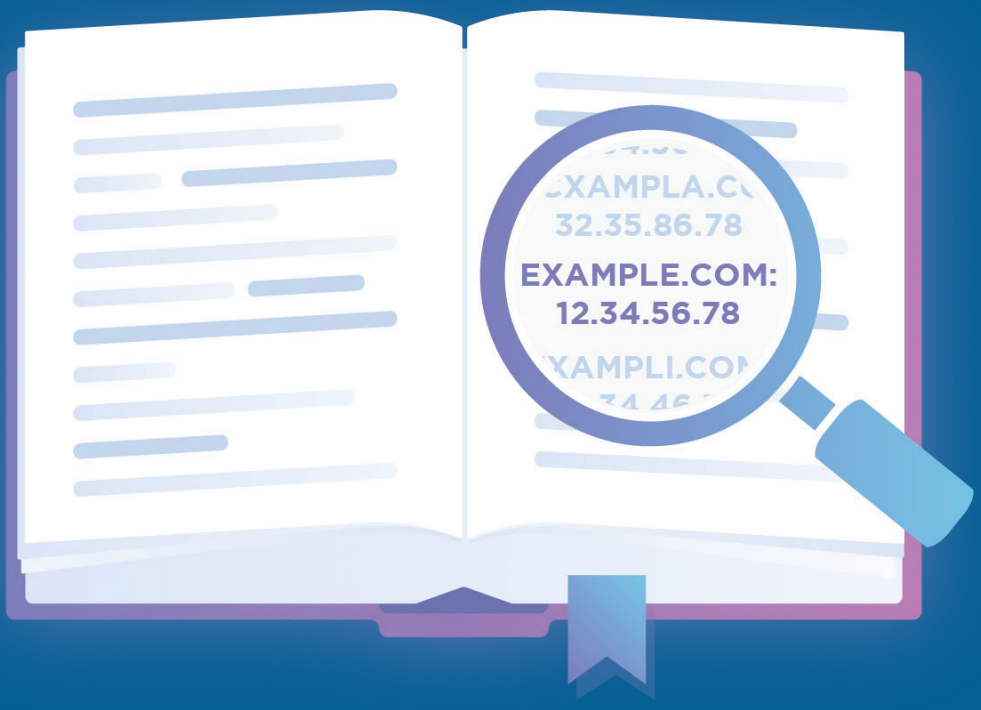
CLOUDFLARE®

Оптимизация DNS для формирования надежной среды функционирования сети



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

CLOUDFLARE

I. Краткий обзор

Скорость работы вашего сайта напрямую зависит от настроек системы DNS, а характеристики дизайна и хостинг не являются при этом определяющими факторами.

При грамотном внедрении и использовании система DNS способна обеспечить не только безопасность ваших Интернет-ресурсов, но и повысить надежность и качество функционирования сети. Однако, DNS-инфраструктура является крайне уязвимой перед широким спектром кибератак, постепенно становящихся повседневным явлением, но при этом способных существенно нарушить работу системы или даже полностью вывести из строя DNS-серверы. Угроза подобных кибератак, наряду с возрастающими ожиданиями пользователей в отношении качества и скорости работы сайта, делают недопустимой ситуацию, в которой система DNS может являться единственным «слабым звеном».

Для обеспечения безопасности сайта, его эффективной и надежной работы потребуется интегрированная система безопасности и DNS-инфраструктура с высокой степенью резервированности, оптимизированная для выполнения этих задач.

II. Безопасность системы DNS: Слабое звено в системе кибербезопасности предприятия

DNS-инфраструктура, на которую мы опираемся сегодня, была разработана еще в 1980-е, когда доступ к глобальной Сети был лишь у правительственных структур, научных и военных ведомств. На тот момент разработчиков системы беспокоили в первую очередь ее надежность и функциональность, а не безопасность.[1]

В результате современные DNS-серверы остались незащищенными от огромного количества кибератак — чего стоят, например, спуфинг-атаки, постоянный поток вредоносных программ, DNS-тунелирование и DoS/DDoS-атаки. Все это становится крайне распространенным, а также все более дорогостоящим явлением. По данным Global DNS Threat Report компании IDC за 2019 год:

- за прошедшие 2 года DNS-атакам подверглись 82% предприятий
- значительный ежегодный прирост наблюдается по всем типам кибератак, от так называемых DDoS-атак с усилением до атак типа low-signal
- средний объем убытков, который предприятие несет в результате кибератак, в 2019 году превысил 1 млн.долларов, что на 49% выше по сравнению с предыдущим годом[2]

DNS-атаки часто разворачиваются на фоне других видов кибератак, зачастую выполняя функцию «дымовой завесы», под прикрытием которой действуют злоумышленники, пока специалисты по безопасности занимаются устранением проблем. По оценке экспертов Verizon, примерно в одной трети инцидентов, связанных с утечкой данных, были задействованы именно DNS-атаки.[3]

Оптимизация системы DNS для удовлетворения требований безопасности

Разнообразие спектра угроз, которым подвержена система DNS, делает наличие интегрированной стратегии безопасности непременным условием эффективного отражения DNS-атак, подобная стратегия должна отвечать следующим требованиям:

- **обеспечивать поддержку DNSSEC/модулей безопасности системы доменных имен**, представляющих собой набор протоколов безопасности для проверки записей в системе DNS с использованием криптографических подписей. Путем проверки соответствия цифровой подписи сайта и записи в системе DNS, модули безопасности могут достоверно установить происхождение данных, отправляемых с DNS-сервера, позволяя таким образом предотвратить спуфинг-атаки.

- **обеспечивать многоуровневую систему нейтрализации DDoS-атак**, в том числе за счет применения мер по фильтрации трафика, в частности — ограничения скорости передачи, использования методов создания «белого» и «черного списка» IP-адресов, а также отслеживания соединений для блокирования вредоносных запросов, одновременно пропуская легитимный трафик. Помимо увеличения степени защищенности сети, нейтрализация DDoS-атак также повысит надежность и эффективность ее функционирования при одновременном предотвращении перегрузки DNS-серверов вредоносным трафиком.

- **Внедрение DNS-файрволов** (также известно как DNS-фильтры или DNS-блокировка) для блокирования доступа с доменов, известных в качестве источников вредоносных запросов.

- **Ведение журнала учета DNS-запросов**. Помимо генерации системой предупреждений в случае, если хакер пытается нарушить работу ваших DNS-серверов, журнал учета DNS-запросов обеспечивает возможность последующего анализа истории DNS-запросов или их обновления.

- **Усиленное применение протокола HTTPS**. Настройка браузеров таким образом, чтобы сайты всегда загружались через HTTPS, позволяет предотвратить угрозу спуфинг-атак на домены путем обеспечения механизма аутентификации для каждого сайта в виде сертификата SSL/TLS.

- **Регулярное обновление настроек DNS-серверов**. В объеме обновления настроек часто производится установка патчей безопасности.

III. Скорость работы системы DNS: Медленная обработка запросов системой DNS означает задержки в работе сети

Когда пользователь пытается получить доступ к веб-ресурсу, его устройство отправляет запрос на DNS-резолвер, который устанавливает соответствие доменного имени и IP-адреса, отправляя затем правильный IP-адрес обратно на устройство пользователя. Всякий раз, когда пользователь через свой браузер заходит на новую веб-страницу, обработка запроса (DNS-поиск) проводится минимум один раз, учитывая, что многие веб-страницы опираются на ресурсы нескольких доменов, таких DNS-поисков может понадобиться несколько. Этот процесс называется обработкой DNS-запросов, при этом время, необходимое на каждый просмотр в процессе обработки, имеет свойство суммироваться. По этой причине оптимизация скорости обработки запросов системой DNS, по сути скорости работы этой системы, является крайне важным для обеспечения низких сетевых задержек.

Не все DNS-провайдеры способны решить проблему оптимизации скорости обработки запросов системой DNS. «Медленному» DNS-провайдеру может понадобиться более 120 миллисекунд для обработки каждого DNS-запроса.[4] Более быстрым достаточно будет и 20 миллисекунд. Обработка запросов с помощью Cloudflare DNS, к примеру, в среднем занимает 12 миллисекунд.[5]

- Сегодня пользователи Интернета ожидают моментальной загрузки нужных им ресурсов. Даже небольшие задержки могут оказать значительное влияние на приверженность пользователей и коэффициент конверсии
- Увеличение задержки при загрузке сайта всего лишь на 100-400 миллисекунд может оказать весьма ощутимый эффект на поведение пользователей[6]
- При возрастании времени загрузки на 1 секунду уровень конверсии может упасть на 7%[7]
- Более половины пользователей мобильных устройств ожидают, что на загрузку интересующего их приложения потребуется не более 2 секунд[8]
- Компания Google использует скорость загрузки страницы как один из факторов при формировании рейтинга сайтов для загрузки как с мобильных устройств, так и с обычных настольных ПК[9]

Оптимизация системы DNS для повышения производительности

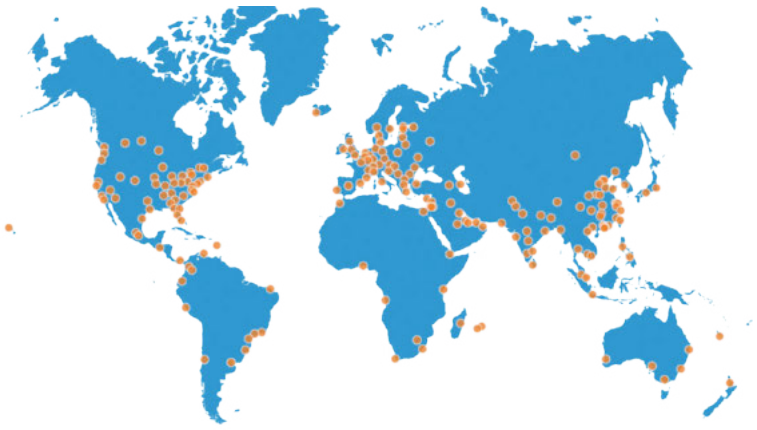
Ниже перечислены шаги, которые можно предпринять для обеспечения высокой производительности системы в мире современных маркетплейсов, где важна каждая миллисекунда.

- **Использование механизмов маршрутизации на базе глобальной геолокации**. Каждые 100 миль географического расстояния между конечным пользователем и интересующим его интернет-ресурсом добавляют 0,82 миллисекунды задержки,[10] поэтому крайне важно обеспечить географическую привязку пользователей к тем объектам DNS-инфраструктуры, которые расположены в их регионе земного шара.

- **Определение показателя TTL — времени жизни пакета в момент перехода от начального узла к конечному**. Показатель TTL косвенно влияет на возможности кэширования у DNS-резолвера. В частности, низкий TTL может отрицательно сказаться на производительности, но будет способствовать выравниванию нагрузки. Высокий TTL улучшает производительность, но может привести к перенаправлению пользователя на кэшируемый сервер, который больше не существует. Учитывая широкий разброс факторов, нельзя точно определить, какое значение TTL является оптимальным.

- **Используйте модель «anycast».** Старайтесь найти DNS-провайдера, использующего модель «anycast» для рассылки пакетов, она позволяет множеству глобально распределенных DNS-серверов анонсировать одинаковый префикс IP-адресов. Таким образом повышается скорость обработки запросов системой DNS и обеспечивается бесперебойная защита системы от сбоя.

Доведите скорость работы вашей DNS-системой на периферии сети



до 11 милли-секунд
при обработке DNS-запросов

менее 5 секунд
на обновление DNS по всему миру

IV. Надежность системы DNS: Резервирование помогает избежать простоев системы

При отсутствии должного внимания проблемы, связанные с задержками, могут обернуться в худшем из сценариев полным выходом из строя вашего сайта. Убытки в результате такого события составляют значительные суммы и имеют тенденцию к увеличению. В 2010 году средняя стоимость минуты простоя ЦОДа составляла 5 617 долларов, а уже в 2016 году эта сумма выросла до 8 851,11 долларов.[11]

Надежность функционирования системы DNS определяет и конечный финансовый результат компании, поэтому целью любого бизнеса должно быть обеспечение 100% рабочего времени для своих интернет-ресурсов. Хотя данный показатель может выглядеть несбыточно, добиться этого можно при использовании предприятием многоуровневого подхода, в основе которого лежит принцип резервирования систем.

Оптимизация системы DNS для повышения надежности

Понятия «производительности» и «надежности» — это как голова и шея, не могут существовать друг без друга. Все, что вы делаете для повышения степени надежности системы, также повысит и ее производительность. К примеру, при работе в системе с двумя DNS-провайдерами существенно улучшаются показатели времени загрузки страниц, поскольку серверами по умолчанию используется самый быстрый DNS-провайдер.

- **Система двух DNS-провайдеров (первичный/ вторичный DNS)**. При работе в системе с одним DNS-провайдером все пользовательские запросы обрабатываются исключительно доменными серверами этого провайдера, что ставит функционирование сайтов под угрозу в случае сбоя в работе этого провайдера. Включение в систему второго DNS-провайдера удваивает количество серверов, доступных для обработки пользовательских запросов. Если серверы имен полномочного (первичного) провайдера недоступны, трафик из пользовательских запросов автоматически перенаправляется на резервные серверы.
- **Облачная система DNS**. Немногие предприятия располагают достаточным количеством собственных ресурсов и знаний для содержания DNS-серверов и управления ими. Аутсорсинг этой функции облачному DNS-провайдеру позволит вам повысить производительность, надежность и безопасность работы вашей системы, сократить издержки и высвободить человеческие ресурсы в виде IT-специалистов для работы над внутренними проектами.
- **Сегментация доменных серверов**. Некоторые DNS-провайдеры группируют многих или даже всех своих клиентов в особые группы (кластеры), каждой из которых присваивается одна и та же запись доменного сервера. Если один из клиентов в таком кластере подвергается DDoS-атаке, все его «соседи» также испытывают последствия этой атаки. Убедитесь, что выбранный вами DNS-провайдер при сегментации своей сети помещает в состав одного кластера под одной записью доменного сервера не слишком большое количество клиентов.
- **Масштабная глобальная сеть DNS-узлов**. DNS-сеть выбранного вами провайдера должна включать в себя большое количество глобально распределенных DNS-узлов, в случае сбоя одного узла трафик может быть перенаправлен на оставшиеся. Глобальные масштабы такой сети также обеспечивают возможность привязки пользователей на основе данных геолокации к ближайшим к ним узлам, что способствует повышению производительности.
- **Выравнивание нагрузки на серверы в локальном и глобальном масштабе**. Помимо всего прочего, для предотвращения перегрузки серверов предусмотрен балансировщик нагрузки, позволяющий перенаправить трафик на оставшиеся сервера в случае сбоя одного из них.

V. Заключение

Современное цифровое пространство для бизнеса отличается высокой степенью динамичности, даже несколько миллисекунд при загрузки веб-страницы могут стать либо залогом успеха, либо фактором неудовлетворенности пользователя от работы с вашим сайтом. Качество и надежность работы сайта во многом зависят от скорости обработки запросов системой DNS, при этом серверы системы крайне уязвимы перед широким спектром кибер-атак. Формирование такой DNS-инфраструктуры, которая отвечала бы требованиям безопасности и имела высокую производительность, обеспечивая 100% готовность к работе, требует применения комплексного подхода к безопасности, надежности и производительности.

VI. Как может помочь в этом компания Cloudflare

Cloudflare предлагает продукт корпоративного уровня — систему DNS-хостинга, отвечающую всем вышеперечисленным требованиям и разработанную с использованием самого передового опыта. Она обеспечивает не только минимальное время отклика, но и отличное резервирование и высокий уровень безопасности благодаря встроенным механизмам DDoS-защиты и DNSSEC/модулей безопасности системы доменных имен. Если вы хотите получить более подробную информацию об этой системе или пообщаться со специалистом из нашей команды, заходите на www.cloudflare.com/dns/.

Примечания

1. ICANN, “DNSSEC — What Is It and Why Is It Important?” https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en. Accessed January 27, 2020.
2. IDC, “2019 Global DNS Threat Report,” https://www.efficientip.com/resources/idc-dns-threat-report-2019/. Accessed January 26, 2020.
3. Global Cyber Alliance, “The Economic Value of DNS Security,” https://www.globalcyberalliance.org/wp-content/uploads/Economic-Value-of-DNS-Security-GCA-2019.pdf. Accessed January 27, 2020.
4. Mann, Bill. “The Best DNS Servers for Speed and Privacy in 2019.” Blokt, https://blokt.com/guides/best-dns-servers. Accessed January 27, 2020.
5. “DNS Performance Analytics and Comparison.” DNSPerf, https://www.dnsperf.com/. Accessed 23 July 2019.
6. Brutlag, Jake. “Speed Matters,” Google AI Blog, https://ai.googleblog.com/2009/06/speed-matters.html. Accessed January 27, 2020.
7. Rodman, Tedd. “Marketing & Web Performance: How Site Speed Impacts Metrics,” Yotta, https://www.yottaa.com/marketing-web-performance-101-how-site-speed-impacts-your-metrics. Accessed January 27, 2020.
8. 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 January 27, 2020.
9. “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 January 27, 2020.
10. Sherman, Fraser. “Network Latency Milliseconds Per Mile,” Techwalla, https://www.techwalla.com/articles/network-latency-milliseconds-per-mile/ Accessed January 27, 2020.
11. Priceonomics Data Studio. “Quantifying the Staggering Cost of IT Outages,” https://priceonomics.com/quantifying-the-staggering-cost-of-it-outages/. Accessed January 27, 2020.