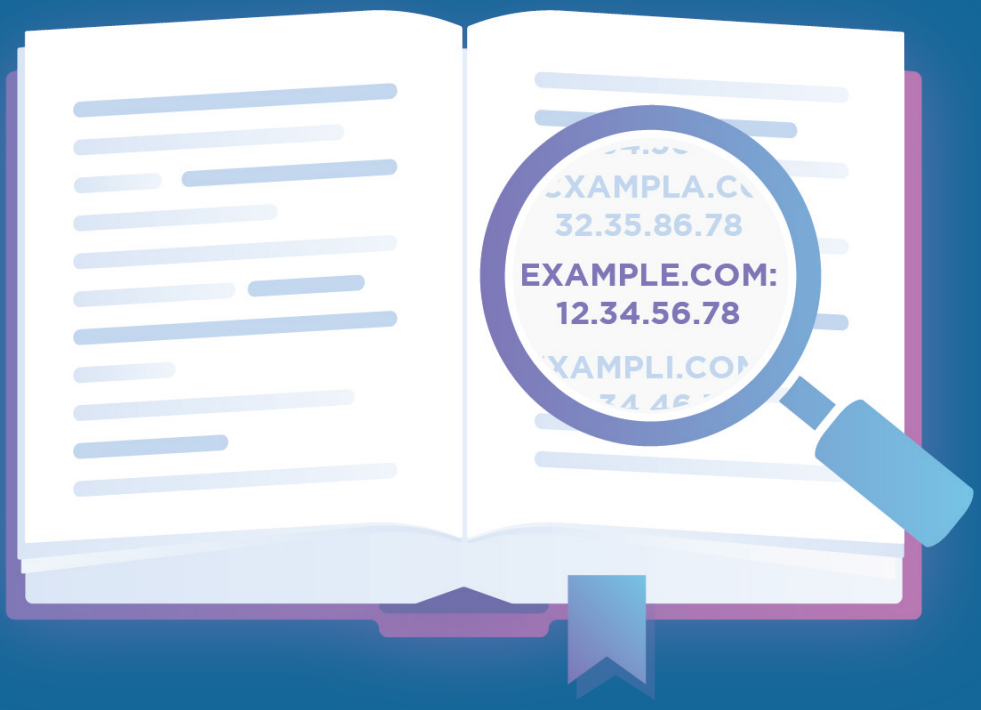
CLOUDFLARE®

Leveraging DNS to Build Reliable Digital Experiences



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

CLOUDFLARE

I. Executive Summary

Your website is only as fast as your DNS, regardless of how the site is built or where it is hosted.

When used and implemented properly, DNS can significantly improve an Internet property's security, performance, and reliability. However, the DNS infrastructure is highly vulnerable to a wide spectrum of increasingly common cyberattacks that can degrade performance or bring DNS servers down completely. These attacks, along with rising user expectations around website performance and availability, make it risky for DNS to be a single point of failure.

Achieving robust site security, performance, and reliability requires integrated DNS security and a redundant DNS infrastructure that is optimized for performance.

II. DNS security: A weak link in enterprise cybersecurity

The DNS infrastructure in use today was designed in the 1980s, when internet access was restricted to government agencies, scientists, and the military. The system's architects were concerned about reliability and functionality, not security.[1]

As a result, DNS servers in the modern world are vulnerable to a broad spectrum of attack types, including spoofing, malware, DNS tunneling, and DoS/DDoS attacks. These attacks are happening more frequently and becoming more costly. According to IDC's 2019 Global DNS Threat Report:

- 82% of organizations suffered a DNS attack in the past two years
- Significant year-over-year increases were reported across all types of attacks, from volumetric to low-signal
- The average cost per attack exceeded $1 million in 2019, up 49% from the year prior[2]

DNS attacks are frequently deployed in conjunction with other cyberattacks, often to serve as a smokescreen to distract security personnel. Verizon estimates that DNS attacks are involved in about one-third of data breaches.[3]

Optimizing DNS for security

Because the DNS threat landscape is so diverse, effectively mitigating DNS attacks requires an integrative security strategy that includes all of the following:

- **Enable DNSSEC**, a set of security protocols that verifies DNS records using cryptographic signatures. By ensuring that a site's signature matches its record, DNS resolvers can authenticate the origin of the data being sent from the DNS server, preventing spoofing.

- **Implement multilayered DDoS mitigation**, including traffic filtering measures such as rate limiting, whitelisting/blacklisting IP addresses, and connection tracking to block malicious requests while allowing legitimate traffic through. In addition to enhancing security, mitigating DDoS attacks will also improve reliability and performance by preventing malicious traffic from overwhelming DNS servers.

- **Deploy DNS firewalls** (also known as DNS filtering and DNS blocking) to block access from known malicious domains.

- **Enable DNS logging**. In addition to warning you if a hacker is trying to tamper with your DNS servers, DNS logging provides visibility into issues with DNS queries or updates.

- **Force HTTPS**. Requiring browsers to always load websites over HTTPS prevents domain spoofing by authenticating each site with an SSL/TLS certificate.

- **Keep DNS servers updated**. Updates frequently include important security patches.

III. DNS performance: Slow DNS lookups mean high latency

When users access a web asset, their devices query a DNS resolver that maps the asset's domain name to its IP address, then sends the correct IP address back to the device. Each time a user accesses a new page in their browser, it must perform at least one DNS lookup; many pages load assets from more than one domain, which requires several lookups. This process is called DNS resolution, and the time required to resolve each requested domain quickly adds up. This is why optimizing DNS resolution speed is crucial to achieving low latency.

Not all DNS providers are optimized for resolution speed. A slow DNS provider could take over 120 milliseconds to resolve each DNS query.[4] The fastest DNS providers will resolve queries in under 20 milliseconds; Cloudflare DNS, for example, resolves queries in under 12 milliseconds on average.[5]

- Today's web users demand that digital assets load instantaneously. Even small issues can have a noticeable impact on engagement and conversion rates.
- Increased site latency as small as 100-400 milliseconds has a measurable impact on consumer behavior[6]
- Just one additional second of load time can cause conversions to drop by 7%[7]
- About half of mobile users expect apps to respond in two seconds or less[8]
- Google uses page speed as a ranking factor for both desktop and mobile search[9]

Optimizing DNS for performance

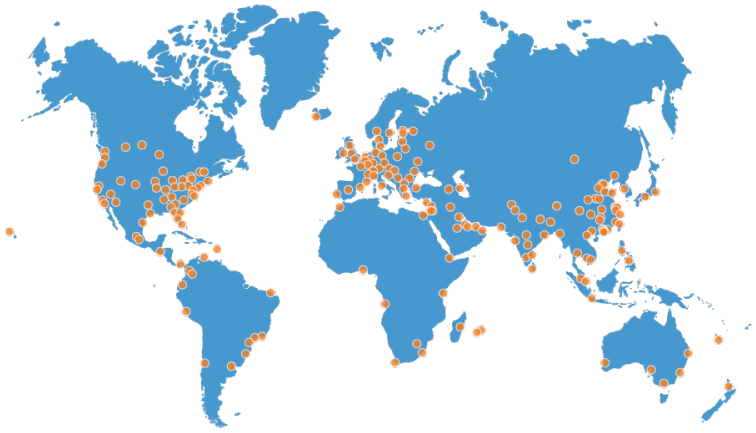
Here are some steps you can take to ensure high performance in a marketplace where every millisecond matters.

- **Use global geolocation-based routing**. Every 100 miles of geographic distance between end users and digital resources adds about 0.82 milliseconds of latency,[10] so it's important to geo-steer visitors to DNS infrastructure that is located in their part of the world.

- **Determine an optimal time to live (TTL)**. TTLs indirectly control DNS resolver caching. Low TTLs can degrade performance but can aid DNS-based load balancing. High TTLs improve performance but can cause users to be directed to a cached server that has since gone down. Since so many factors are involved, there is no universal optimal TTL value.

- **Use anycast.** Look for a DNS provider that uses anycast, which enables multiple, globally distributed DNS nameservers to advertise the same IP address. This improves DNS resolution speed and also provides seamless DNS failover protection.

Move your DNS to the Network Edge



11ms
average DNS lookup speed

<5 seconds
for worldwide DNS propagation

IV. DNS reliability: Redundancy prevents downtime

Left unchecked, latency issues result in the worst-case scenario of your website going dark altogether. The costs of downtime are high and steadily increasing. In 2010, the average per-minute cost of a data center outage was USD $5,617; by 2016, this had risen to USD $8,851.[11]

Since DNS reliability has a direct and profound impact on a company's bottom line, the goal for any business must be nothing less than 100% uptime. While that may sound lofty, it's achievable if organizations use a multi-pronged approach centered on redundancy.

Optimizing DNS for reliability

Performance and reliability are like the head and the neck; they are closely connected. one cannot exist without the other. All of the measures you take to improve reliability will also enhance performance. For example, using dual DNS providers improves page load times because resolving nameservers will default to the fastest DNS provider.

- **Dual (primary/secondary) DNS providers**. In a single-provider DNS setup, all users are answered by that provider's nameserver set, leaving sites vulnerable to provider outages. Adding a second DNS provider doubles the number of nameserver sets that are available for those domains. If the authoritative provider is unavailable, query traffic is automatically routed to the backup nameserver set.
- **Cloud-based DNS**. Few organizations have the in-house resources and expertise to manage their own DNS servers. Outsourcing to a cloud-based DNS provider lets you improve performance, reliability, and security; minimize costs; and free up in-house IT personnel to work on internal projects.
- **Nameserver segmentation**. Some DNS providers cluster many or even all of their customers in the same nameserver record. If one customer suffers a DDoS attack, all of their "neighbors" are severely impacted. Make sure your DNS provider segments their network so that only a small number of customers share nameserver records.
- **A very large, global network of DNS nodes**. Your provider's DNS network should include a large number of globally distributed DNS nodes, so if one node fails, traffic can be routed to any of the remaining nodes. A global network also allows for geo-steering, which improves performance.
- **Global and local load balancing**. In addition to ensuring that no one server is overloaded, if a server does fail, a load balancer redirects traffic to the remaining servers.

V. Conclusion

In today's fast-paced digital marketplace, a few milliseconds of load time can make or break your user experience and conversion rate. Website performance and reliability hinge on DNS resolution speed, but DNS servers are extremely vulnerable to a wide variety of cyberattacks. Ensuring a secure, high-performance DNS infrastructure with 100% uptime requires an integrated approach to security, reliability, and performance.

VI. How Cloudflare can help

Cloudflare offers an enterprise-grade authoritative DNS service that's reflective of many of these best practices, offering the fastest response time, unparalleled redundancy, and advanced security with built-in DDoS mitigation and DNSSEC. To learn more and speak to a member of our team, visit www.cloudflare.com/dns/.

Endnotes

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.