



Cloudflare DNS

Overview

DNS is a mission-critical component for any online business, yet this component is often overlooked and forgotten until something breaks. With DNS-based attacks on the rise, enterprises are realizing the importance of building resiliency and redundancy in their DNS setup. Organizations are scaling their DNS infrastructure — moving away from on-premise DNS servers to a managed DNS provider to multiple DNS vendors — in order to increase redundancy against the possibility of a DDoS attack taking down one of their providers.

How Cloudflare protects DNS infrastructure

Cloudflare offers an enterprise-grade DNS to improve the resilience and redundancy of DNS infrastructure. Whether deployed as an authoritative or secondary DNS, Cloudflare offers the fastest response time (as per dnsperf.com), unparalleled redundancy, and advanced security.

Our DNS network is the fastest and largest in the world. Our global anycast network allows DNS resolution at the network edge in each of our data centers across 200+ cities, resulting in a resolution speed of 13ms on average and worldwide DNS propagation in less than 5 seconds.

To ensure the highest level of security against DNS-based attacks, we offer unlimited and unmetered DDoS protection. Our network capacity is 15x bigger than the largest DDoS attack ever recorded. Also, unlike other DNS providers in the industry, we offer built-in DNSSEC to protect users from on-path attacks that can spoof or hijack DNS records. The best part is that you can easily deploy DNSSEC at the click of a single button.

Key integrations with Cloudflare's security and performance suite

Cloudflare DNS integrates seamlessly with all our core offerings, allowing businesses to make their applications and networks more secure and performant from a unified control plane. Using our DNS truly allows our customers to enable additional products and services from Cloudflare at the click of a button. Our customers often use our Load Balancing solution along with our DNS to steer requests away from unhealthy origins and dynamically route them to the closest and most responsive server pools, thereby improving application performance and availability.

Get the most out of Cloudflare DNS

Cloudflare DNS can be deployed in any setup — primary-secondary, hidden primary, or multi-DNS setup. Whether deployed as primary or secondary DNS, we offer in-depth, real-time analytics into the health of your DNS traffic — all easily accessible from the Cloudflare Dashboard. Detailed reports for DNS queries can be generated by response codes, record types, geography, domains, etc. Raw log files are also available via API and can be integrated with SIEM/parsing tools.

Above all, we make DNS easy. All your DNS records can be migrated in bulk within minutes, with zero downtime. Just upload your DNS records in BIND format using the Cloudflare Dashboard, and that's it. Terraform integration further automates DNS management and configuration.

Real-world applications

Learn how companies like yours are leveraging our platform

- FastMail, a premium email hosting service in Australia, sought out Cloudflare DNS after an attempted DDoS attack surfaced the need for a security partner that would deliver greater peace of mind. With DNS Firewall, Cloudflare's network acts as a reverse proxy for FastMail's DNS infrastructure. Traffic aimed at FastMail's DNS servers is first routed through one of Cloudflare's global data centers, where malicious requests are blocked and clean traffic is then directed to FastMail's masked origin servers. DNS Firewall is especially helpful to FastMail because it means that their DNS is always on, and thus their mail will always get delivered.
- When AutoTrader, the largest automobile classifieds service in the United Kingdom and Ireland, began their migration from on-premise infrastructure to cloud-based services, they chose Cloudflare. With a single unified interface that managed their DNS, performance, and security needs, they saw a 50% increase in DNS performance and greater operational efficiency across their team.

How to implement Cloudflare DNS

To use Cloudflare as authoritative DNS:

1. Follow the steps outlined when you click 'Add a Site'. This will include changing your nameservers to the Cloudflare pair assigned.

To keep you current DNS provider and use Cloudflare to proxy a subdomain:

1. Create an account. Let your Solutions Engineer know that you will be doing a partial setup. We will convert your zone into a partial setup mode. A TXT record will appear in the Overview page of your Dashboard.
2. Add this TXT record to your current authoritative DNS provider.
3. In the Cloudflare DNS tab, create a record for this subdomain pointing to origin. For example:

Type	Name	Content	TTL	Proxy status
A	subdomain	1.2.3.4	Auto	 Proxied

4. In your authoritative DNS console, create a CNAME record pointing your subdomain to Cloudflare. It should look like this:

CNAME **Subdomain** → subdomain.example.com.cdn.cloudflare.net