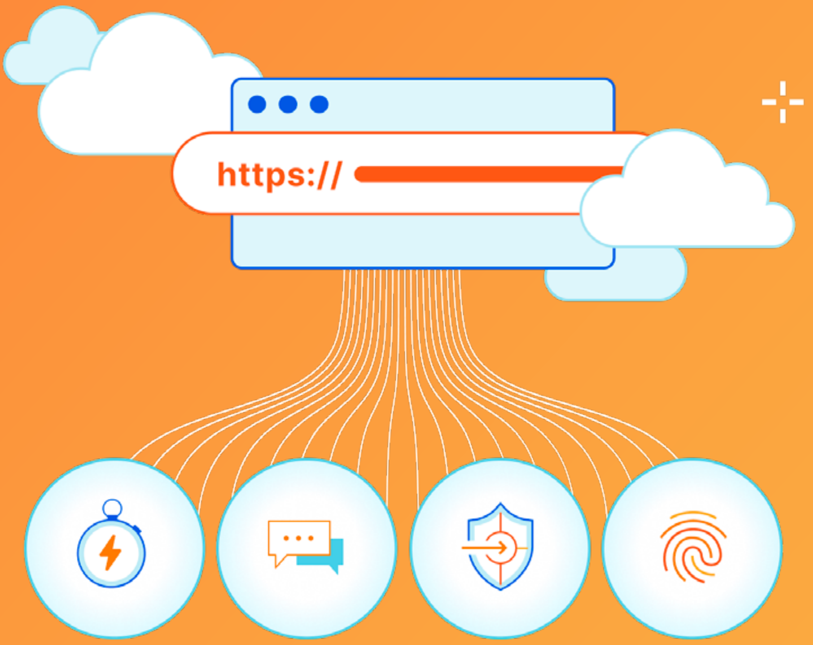
CLOUDFLARE

WHITEPAPER

Securing DNS: How to protect your business against security and performance pitfalls



Content

Executive Summary

Websites and mobile applications are only as secure as their weakest components. As DNS is one of the core services that all web applications rely on, how can you ensure that vulnerabilities in your DNS infrastructure do not compromise your business?

From its inception, DNS has been susceptible to a wide spectrum of common cyber attacks. Since DNS infrastructure was not built with security in mind, it can be easily exploited by attackers, making it a key vector in attacks that can degrade performance or bring servers down completely.

These attacks, along with rising user expectations around website performance and reliability, make it risky for DNS to be a single point of failure.

Achieving robust site security, performance, and reliability requires both integrated DNS security and a redundant DNS infrastructure. This paper explores different strategies and tools designed to help secure your DNS and achieve those benefits.

DNS security: A weak link in enterprise cybersecurity

DNS was designed in the 1980s, when Internet access was restricted to a small number of computers operated by different government agencies, science organizations, and military services. The system's early architects were primarily concerned with its reliability and functionality, but failed to take security measures into account. As a result, malicious parties were able to leverage weaknesses in DNS infrastructure to carry out a variety of cyber attacks.

Over the years, DNS attacks steadily increased in frequency and remediation costs. According to IDC's 2022 Global DNS Threat Report, sponsored by EfficientIP[1]:

- 88% of organizations suffered one or more DNS attacks
- 24% of these attacks resulted in sensitive data being stolen
- On average, these attacks cost $942,000 in damages

Types of DNS attacks

Modern DNS servers make an appealing target for attackers, who often leverage those servers to amplify attacks against a target or use them to distract security personnel from more advanced attacks against other targets.

While these tactics vary according to the motive of the attacker — and the level of ease with which each attack can be launched, they are typically variants of common **distributed denial-of-service (DDoS) attacks**. In a DDoS attack, a high volume of traffic is sent to a targeted machine so that legitimate traffic cannot get through. This can slow down services for end users and, in extreme cases, take down servers completely, costing organizations significant time and money to bring their services back online.

Here are three common DNS attack methods that your organization should be aware of:

DNS amplification

DNS amplification attacks are a subset of DDoS attacks that uses a compromised endpoint to send UDP packets with spoofed IP addresses to a DNS recursor. Each one of the UDP packets makes a request to a DNS resolver, often passing an argument (such as "ANY") in order to receive the largest response possible. After receiving the requests, the DNS resolver sends a large response to the spoofed IP address. The IP address of the target receives the response and the surrounding network infrastructure becomes overwhelmed with the deluge of traffic, resulting in a denial of service.

These attacks are particularly potent as a relatively smaller number of requests can generate massive attack traffic volumes, depending on the amplification factor of the protocol being exploited (for instance, DNS amplification can generate attack traffic up to 54x the size of the request traffic).

Amplification attacks in the real world

In one DNS amplification attack, middleboxes — network devices used for packet inspection and content filtering — were exploited and used to amplify DDoS attacks by a factor of 65x.[2] Attackers identified security vulnerabilities in these devices, then configured them to carry out TCP and UDP reflection abuse, in which each reflection triggered increasingly larger responses. Due to the prevalence of these devices, amplification attacks like these hit a wide range of industries and organizations, spanning travel, banking, and gaming sectors, among others.

DNS water torture

DNS water torture attacks are another form of DDoS attack designed to interrupt service to a DNS server. A standard DNS water torture attack works by generating random strings (i.e. random fake subdomain names) to make DNS servers attempt to resolve the IP address for subdomains that do not exist.

For example, an attack might generate a fake subdomain called **xxyyzz.foo.com.** As a result, foo.com must respond to the query even though **xxyyzz.foo.com** does not exist. If enough of these queries are sent, the authoritative server can be overwhelmed, resulting in a denial-of-service (DoS) attack that can either take down the server or the entire zone.

DNS water torture attacks in the real world

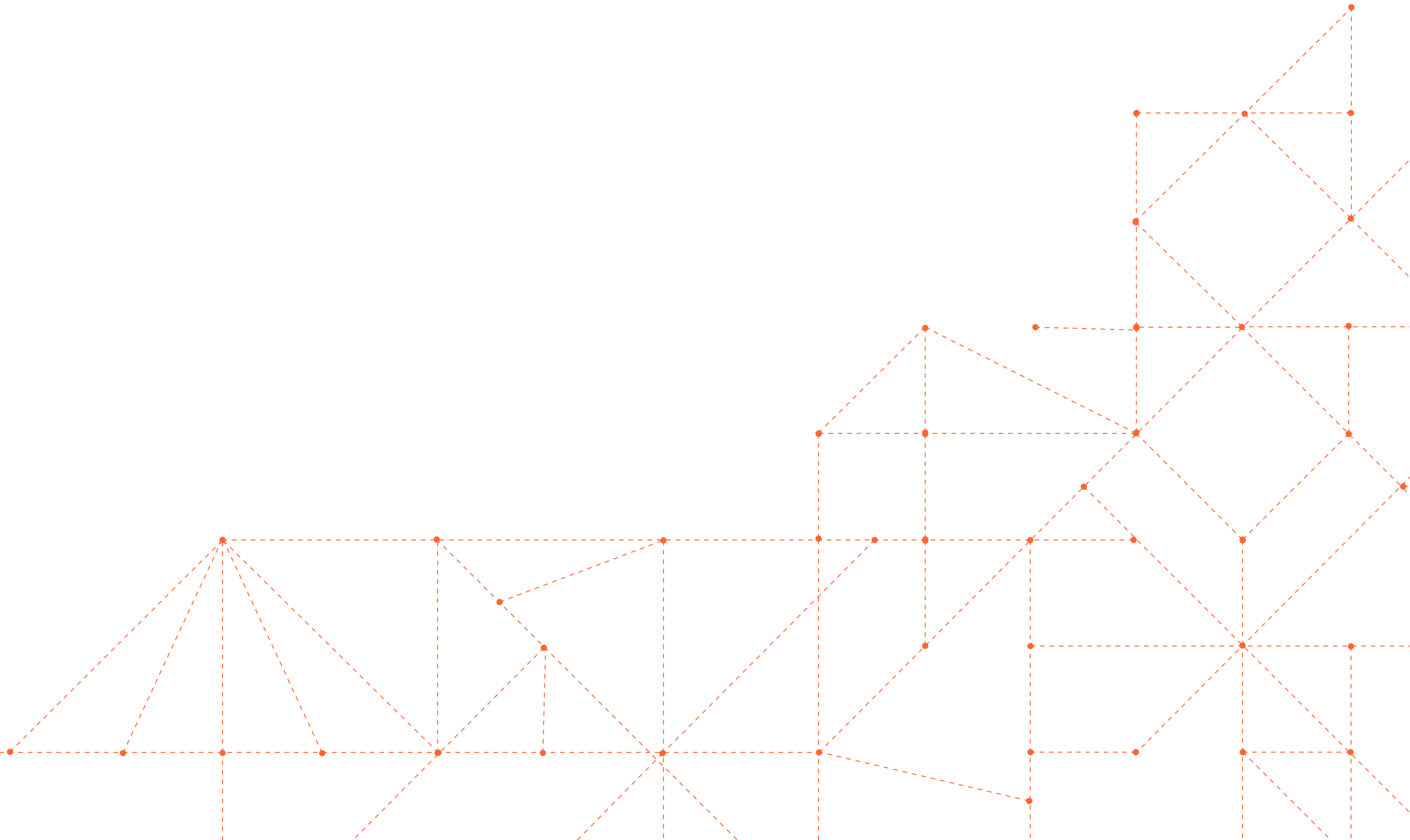
One of the most infamous DNS water torture attacks originated from the Mirai botnet, which flooded DNS servers with fraudulent requests for the victims' domains. Although the real target of the attack was the authoritative DNS server hosted by the victim's service provider, the large volume of queries consumed significant memory resources and caused major disruptions to the victims' services.[3]

DNS spoofing

A spoofing attack, while not a type of DDoS attack, is still a highly effective method of compromising a DNS server. These attacks (sometimes called “cache poisoning”) introduce forged DNS data into a DNS resolver’s cache. As a result, the resolver returns an incorrect IP address for a domain. Hence, instead of going to the correct website, traffic can be diverted to a malicious machine or anywhere else the attacker desires; often this will be a replica of the original site that is then used for malicious purposes, such as distributing malware or collecting login information.

Spoofing attacks in the real world

While a spoofing attack often targets one website or organization, it can have ripple effects across a large number of end users and devices. In one spoofing attack, attackers compromised the target’s external DNS infrastructure, then pointed the DNS records to a cloned web server. The results were severe: due to the malicious redirect, the target lost more than $573,000 USD in the attack.[4]



Optimizing DNS for security

Organizations can make their DNS infrastructure more resilient to attacks by implementing tools that address its core weaknesses. Here are some strategies designed to help secure DNS against common attacks:

Enable DNSSEC

DNSSEC is 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, thereby preventing spoofing attempts.

Implement multi-layered DDoS mitigation

Incorporate traffic filtering measures — such as rate limiting, allowlisting/blocklisting IP addresses, and connection tracking — to block malicious requests while allowing legitimate traffic through.

Deploy DNS filtering

Use filtering tools to block access from known malicious domains or IP addresses.

Enable DNS logging

Get visibility into issues with DNS queries or updates, and receive timely notifications whenever hackers attempt to tamper with DNS servers.

Force HTTPS

Require browsers to always load websites over HTTPS, which helps prevent domain spoofing by authenticating each site with an SSL/TLS certificate.

Opt for DNS-over-HTTPS (DoH)

Use DoH to encrypt DNS queries and responses, stopping attackers from forging or altering DNS traffic.

Use multi-node resolution

Hand off the DNS lookup process to multiple servers — which are often maintained by multiple vendors or hosted on alternative networks — to create redundancy in case of an attack.

DNS performance: A potential roadblock for website performance

Optimizing DNS resolution speed is crucial to achieving low latency — and ensuring lightning-fast DNS performance.

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.

Not all DNS providers are optimized for resolution speed. A slow DNS provider could take over 120 milliseconds to resolve each DNS query.[5] The fastest DNS providers will resolve queries in under 20 milliseconds; Cloudflare DNS, for example, resolves queries in under 9 milliseconds on average.[6]

Today's web users demand that digital assets load instantaneously. Even small issues can have a noticeable impact on engagement and conversion rates:

- 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 loading performance as a ranking factor for both desktop and mobile search[9]

Optimizing DNS for performance

In a marketplace where every millisecond matters, here are some steps you can take to provide high DNS performance:

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 is important to steer traffic to DNS infrastructure that is located as close as possible to end users.

Determine an optimal time to live (TTL)

TTLs indirectly control DNS resolver caching. Low TTLs can degrade performance while simultaneously aiding DNS-based load balancing. High TTLs improve performance while causing users to be directed to a cached server that has since gone down. Since so many factors are involved, optimal TTL value often varies from organization to organization.

Use Anycast DNS

Anycast enables multiple, globally-distributed DNS nameservers to advertise the same IP address. This improves DNS resolution speed and also provides seamless DNS failover protection.

DNS reliability: An essential requirement for business continuity

Downtime — the amount of time during which a website or application is non-functional — can have a critical impact on your business, from decreased conversion rates and reputational damage to high remediation costs for hardware failure or data center outages.

There are several factors that may lead to downtime, including system or network malfunctions, latency, and targeted cyber attacks. Regardless of the reason, however, the cost is usually severe: a recent study found that the per-minute cost of a data center outage averages $8,851.[11]

To protect against these service disruptions — and achieve 100% uptime — businesses need a redundant DNS infrastructure, one in which traffic is load balanced across multiple servers. Using multiple DNS servers helps ensure that your site remains online, even when faced with attacks or server failure.

Optimizing DNS for reliability

When developing strategies to improve DNS redundancy and uptime, there are several key components to keep in mind:

Opt for a managed DNS

In a managed DNS setup, a third-party cloud or CDN provider manages DNS servers on behalf of multiple organizations. This is an appealing alternative for many organizations, as it takes considerable resources, time, and expertise to maintain on-premise DNS servers.

Choose a multi-DNS approach

In a single-provider DNS setup, all users are answered by that provider's nameserver set, leaving sites vulnerable to provider outages. Alternatives include:

Primary/secondary DNS (dual DNS): 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

Hidden primary DNS: The authoritative server is not visible to the public Internet, and is often hidden behind a firewall. Its DNS records are replicated to the secondary DNS server, which responds to requests

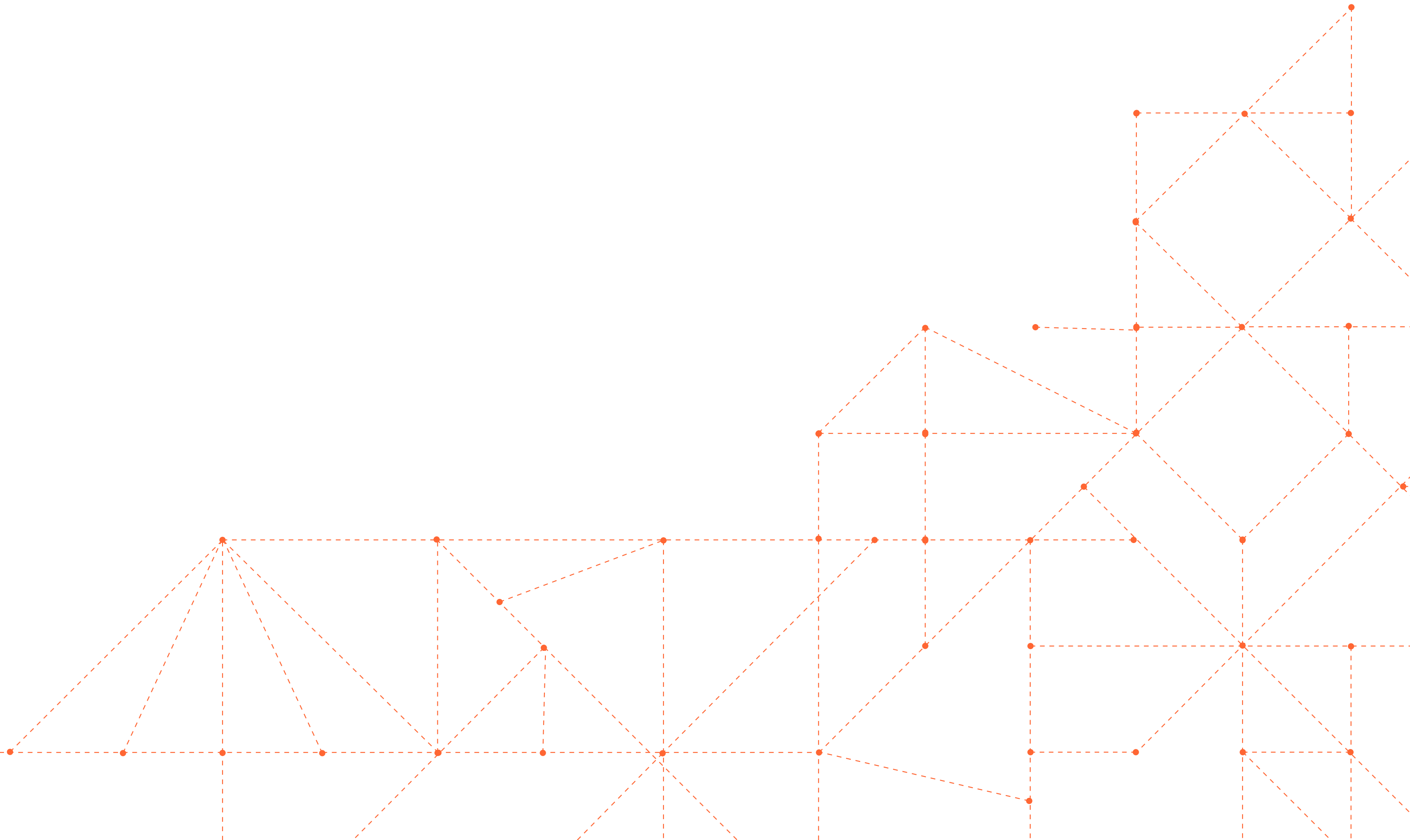
Primary-primary DNS: Both servers are visible to the public Internet and work in tandem with each other

Implement nameserver segmentation

With nameserver segmentation, one DNS server turns into multiple servers, so different subnets and IP address ranges are responsible for handling different traffic loads. However, some DNS providers cluster many (or all) of their customers into the same nameserver record — so when one customer suffers a DDoS attack, all adjacent customers are severely impacted. Select a DNS provider that segments their network, ensuring that only a small number of customers share nameserver records.

Use global load balancing

Your provider's DNS network should include a large number of globally-distributed DNS servers, so if one server fails, its traffic can be routed to any of the remaining servers. A global network also allows for geo-steering, which improves DNS performance.



Conclusion

Fast DNS performance is crucial to quality user experiences and conversion rates, but without proper security measures, your infrastructure can be severely compromised by common cyber attacks.

Bolstering your DNS infrastructure requires an integrated approach to security, performance, and reliability, one that factors in multi-layered DNS attack mitigation, Anycast routing, global load balancing, and DNS redundancy, among other key strategies and tools.

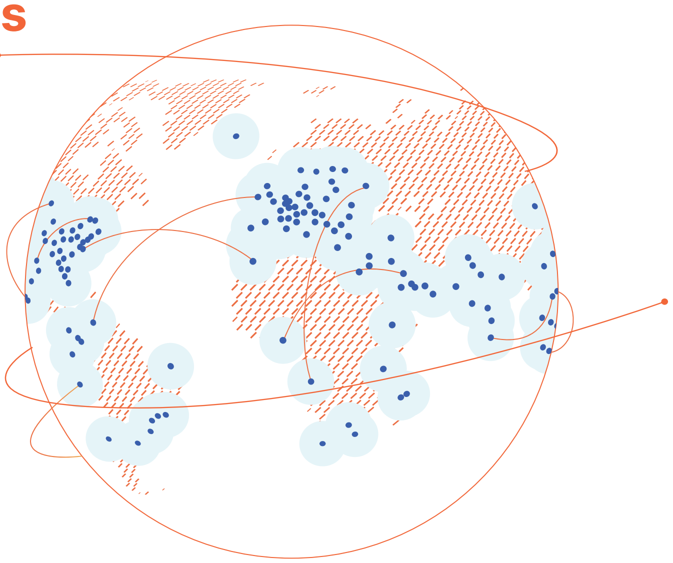
With the right DNS provider, you can ensure that your DNS infrastructure remains resilient and guarantee 100% uptime for your customers — no matter what attacks come your way.

How Cloudflare can help

Cloudflare's enterprise-grade managed DNS solution offers built-in DDoS mitigation and DNSSEC for all customers, even those who use alternative DNS providers. Our authoritative DNS is the fastest in the world, offering average DNS lookup speeds of 9ms and worldwide DNS propagation in less than 5 seconds. As of Q1 2023, Cloudflare also processes approximately 24.6 million DNS queries per second (both authoritative and resolution requests).

For DNS service providers and organizations that host their own DNS infrastructure, the Cloudflare DNS Firewall not only helps protect infrastructure and users from large scale DDoS attacks, but also improves performance by caching DNS records and responding on their behalf.

The Cloudflare global Anycast network allows DNS resolution in each data center across 285+ cities, resulting in unparalleled redundancy and 100% uptime. As Cloudflare's network capacity is equipped to absorb massive amounts of malicious traffic, the result is a DNS service that is both more attack-proof and resilient.



<5 seconds

For worldwide DNS propagation

9ms

Average DNS lookup speed

To learn more about how Cloudflare can help improve your DNS security and performance, visit:

Cloudflare DNS

Cloudflare DNS Firewall

Cloudflare DDoS Mitigation

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