Solution Overview

One DNS, Four Expressions with F5

What is F5 DNS? Versatile deployment options, robust app delivery performance, hardened attack security.

Key Benefits

Versatile deployment options
Leverage a solution that can scale with business needs and adapt to diverse deployment environments—software as a service (SaaS), hardware, software, or cloud-native network functions.

Ultra-high performance
Optimize how network resources are used, route to the best-performing server to improve user experience, and adapt to changing network conditions to maintain service levels.

Security-centric by design
We place user safety and privacy at the forefront of development and deployment.

A Complex Digital Landscape Demands Versatility

As the digital landscape continues to evolve year over year, so does the volume and complexity of traffic flowing between billions of linked applications, connected devices, and web pages worldwide. Domain name system (DNS) plays a central role, ensuring that traffic can reach its target destination safely.

Because of where it sits in the flow of traffic, and how it interacts with that traffic, DNS is often exposed to bad actors and a lot of bad traffic. Vulnerabilities within a DNS solution can make it easy for criminals to turn an otherwise high-performing application into a dead end. Without the right solutions in place, organizations can experience revenue and reputation losses, or even worse, data exfiltration.

DNS challenges are further complicated as applications are delivered through more diverse and complex digital ecosystems. As enterprises, governmental agencies, and telecom providers diversify platforms, applications run in data centers, public clouds, private clouds, "as-a-service" systems, and even cloud-native networks. For the greatest performance, security, and redundancy, some applications live in multiple locations simultaneously, spread out across two, or sometimes three different deployment environments.

To manage these increases in traffic and complexity, an effective DNS solution must have the versatility to keep apps online, secure, and performant, regardless of where those apps live or the volume of traffic they experience.

Versatility, Agility, and Consistency

Whether it's opening your favorite application, checking email, or booking a hotel, the first thing happening in the background is a DNS resolution. Without DNS, digital experiences simply can't happen.

Whether it's opening your favorite application, checking email, or booking a hotel, the first thing happening in the background is a DNS resolution. Without DNS, digital experiences simply can't happen. That's why F5® offers DNS solutions with four deployment options—SaaS, hardware, software, and cloud-native network function (CNF)—each one addressing different challenges faced across different industries, giving users the tools to cover almost every conceivable deployment environment.

At the core of each DNS expression is F5's Traffic Management Microkernel (TMM). This is the driving force that has made F5 a leader in DNS and application delivery for decades. Its ability to process traffic with intelligence, speed, and scale situates TMM as the highest-performing means of secure, reliable application delivery.

Let's dive a little deeper into the four use cases that highlight how F5 DNS solves today's most challenging application networking problems.

PROBLEM 1:

A solo data-center-based DNS solution leads to increased latency and risk to business continuity, necessitating a robust, authoritative DNS solution.

SOLUTION:

Authoritative DNS with Distributed-Cloud DNS is a cloud-based, “as-a-service" solution that provides an authoritative DNS solution that doesn’t require an on-premises DNS solution. This improves efficiency by reducing costs and management time. If leveraged as part of a dual-provider primary DNS arrangement, DNS configuration is managed in-house. API calls are sent to both DNS providers to create or update DNS zones, and client traffic from the internet can hit both DNS servers before being routed to the desired location. The two primary DNS solutions work together as a combined service, or as fallback services in case of an outage. [see Figure 1]

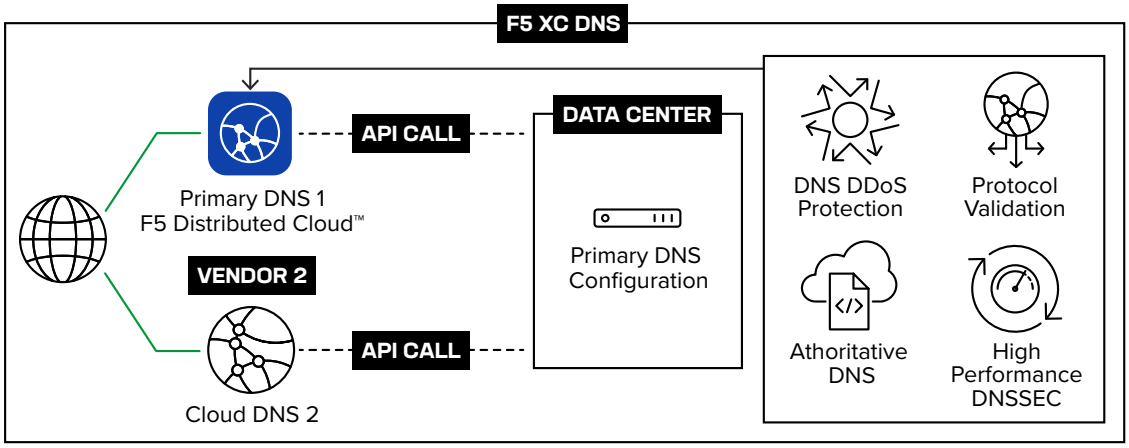

Figure 1: In this SaaS-based Authoritative DNS solution, DNS setup is managed in-house. F5 Distributed-Cloud DNS can work in tandem with a second vendor’s DNS solution to provide enhanced security, performance, and availability.

Note: *The F5 BIG-IP DNS solution will also address this use case by providing a hyperscaling, authoritative DNS solution for every data center or cloud instance, expressed in virtual or hardware form factors.*

PROBLEM 2:

Users experience excessive latency when attempting to reach an application in a data center. In response, the supporting team deploys second, third, and fourth instances of the app across four data centers.

SOLUTION:

The Global Server Load Balancing (GSLB) function in F5 BIG-IP® DNS and Distributed Cloud DNS Load Balancer is a multi-faceted tool that directs traffic across multiple data centers and app instances, along myriad traffic management rules. Far from being just a load balancer, GSLB monitors app instance health and directs traffic to the nearest, best-performing application. GSLB can also help teams meet data sovereignty regulations by sending application traffic to specific sites within a given region. That way, user data is kept secure and stored only in approved locales. Moreover, GSLB enables more robust business continuity and risk management, as services can failover safely to other application instances in the event of an outage or disaster. [see Figure 2]

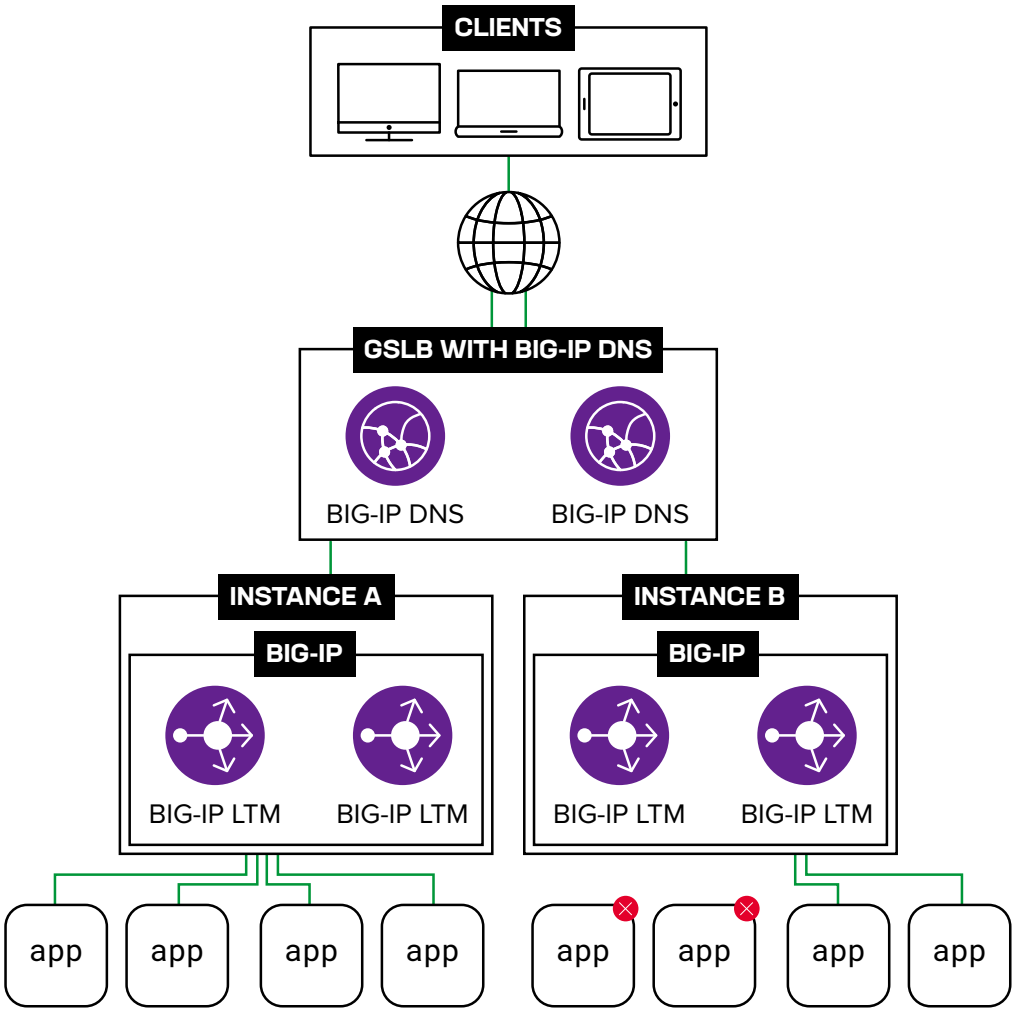

Figure 2: Most commonly used by enterprises to balance traffic across multiple data centers or cloud deployments, BIG-IP DNS will route traffic to the healthiest, highest-performing application instance.

PROBLEM 3:

Distributed denial of service (DDoS) attack traffic that causes outages and leaves apps inaccessible.

SOLUTION:

DDoS, local domain name server (LDNS) cache poisoning, and other DNS attacks can dramatically spike traffic and take down DNS servers. To mitigate DNS outages, lost productivity, and decreased revenue, BIG-IP DNS defends against malicious traffic, limits queries and response rates, filters query validation, and much more. Combining BIG-IP DNS with BIG-IP Advanced Firewall Manager™ (AFM), or combining BIG-IP Next™ DNS CNF with BIG-IP Next Edge Firewall CNF, empowers teams with a robust, whole-solution DNS firewall that defends against even the most insidious layer two through seven attack types, keeping users online and connected to the services they need. [see Figure 3]

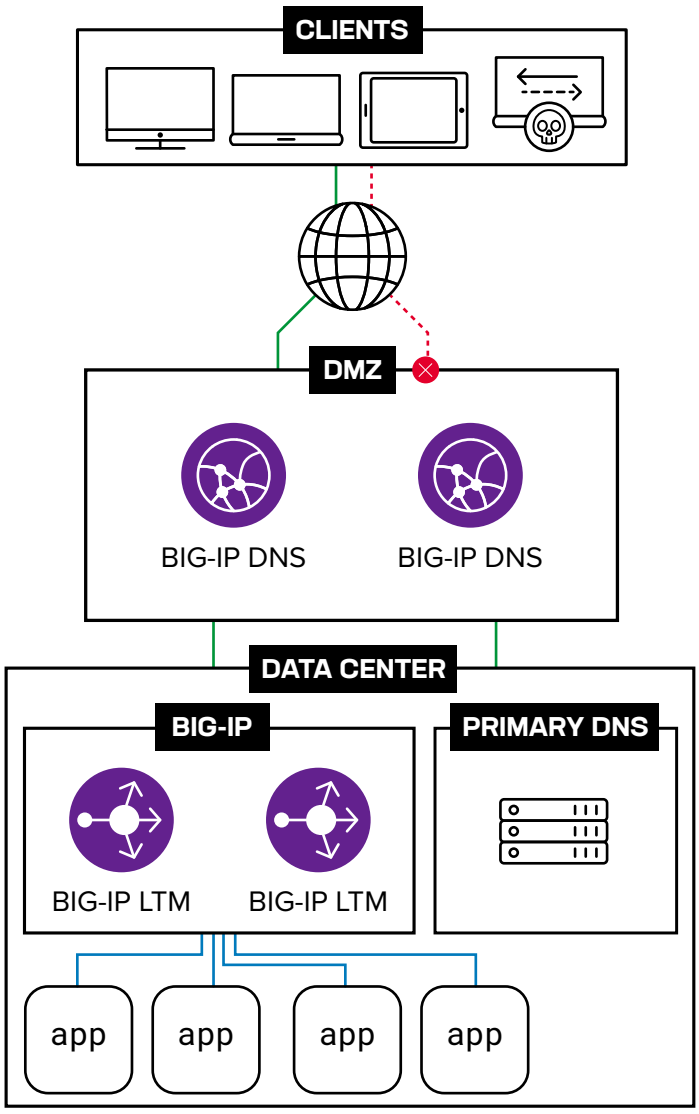

Figure 3: Shield DNS from myriad DDoS attacks, block malicious IP addresses, or integrate with third-party domain filtering services with BIG-IP DNS as your network firewall.

PROBLEM 4:

Poor user experiences caused by excessive latency from long DNS resolution times.

SOLUTION:

Enabling a DNS cache to immediately respond to client requests, as well as consolidate the cache and increase the cache hit rate, can reduce latency up to 80%. When used on the F5 VELOS® chassis platform, DNS caching can hyperscale for ultimate query response performance, delivering linear scalability across multi-bladed chassis. In addition to caching, BIG-IP DNS allows the service to do its own DNS resolving without requiring the use of an upstream DNS resolver; this reduces the time it takes to resolve subsequent queries for the same domain, leading to faster load times so that users are more likely to stay on the site or application. [see Figure 4]

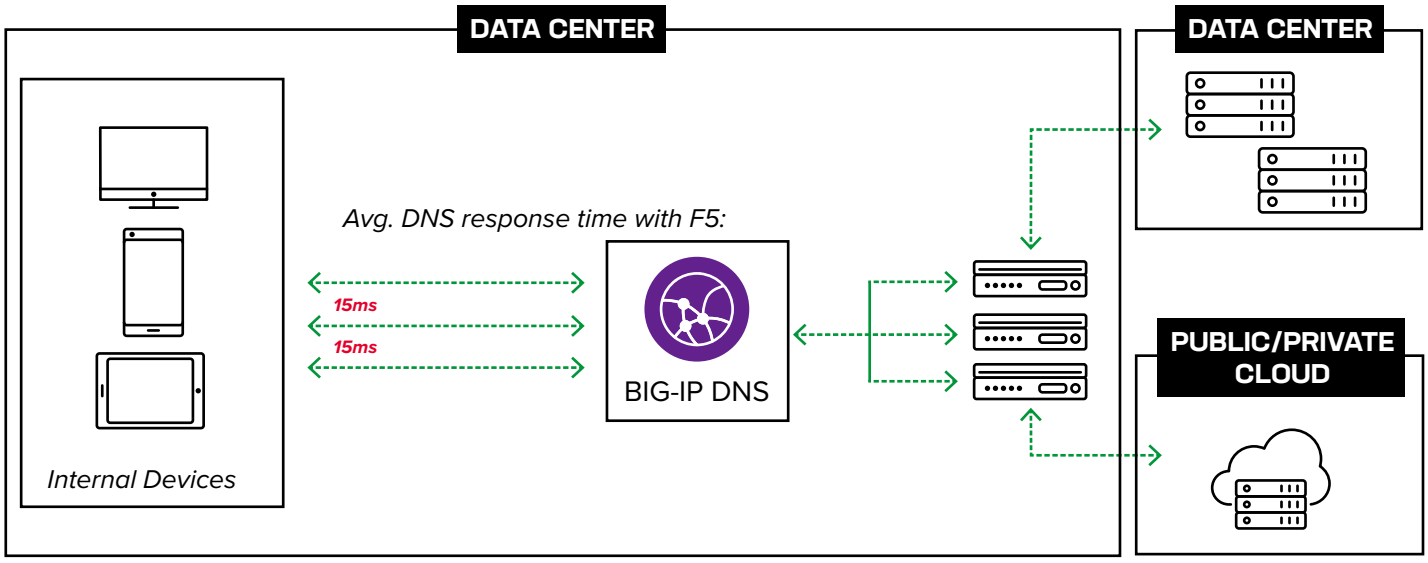

Figure 4: Experience faster web browsing, reduced latency, and decreased DNS query response times with an F5 DNS solution deployed for DNS caching and resolving.

This list represents only the most common use cases that DNS and GSLB are called upon to solve; because of their flexibility and robustness, our DNS solutions can address many more challenges.

Key Features

Global server load balancing
Ensure high availability and reliability by distributing client requests to the healthiest servers, reducing the risk of server overload and minimizing latency.*

Authoritative DNS
Hyperscale up to 100 million responses per second (RPS) with DNS Express in Rapid Response Mode (RRM) while F5 Distributed-Cloud DNS scales across 26 regional edge locations around the globe.

Caching and resolving
Enable a DNS cache and have it respond immediately and authoritatively to client requests for up to 80% less latency.

DNS firewall
Resist common teardrop, internet control message protocol (ICMP), and daemon attacks with BIG-IP AFM, and defend against attacks on layers two through seven.

DDoS attack protection
Get DNS DDoS protection capabilities, keeping apps online and available even during the heaviest traffic periods.

One Foundation, Many Solutions

F5 DNS solutions empower organizations to deliver fast, secure, and highly available applications across diverse and complex environments. As seen in these four use cases, F5 offers versatile DNS solutions that address the needs of an increasingly diverse user base—filling the roles of major firewall component, global server load balancer, resolver, authoritative DNS server, and more—built on the industry's leading traffic management technology.

Next Steps

DNS for providers

Discover a carrier-grade, DNS-resolving solution with hyperscaling and security services.
Read the solution overview

BIG-IP DNS data sheet

Learn how to hyperscale and protect your DNS while optimizing global app delivery.
Read the data sheet

DNS as-a-Service overview

Simplify your move to cloud-based DNS with a SaaS-based solution from F5. Find out how.
Read the solution overview

Get in touch

Reach out for more information on how F5 solutions can benefit your organization.
Contact F5 today

*Global Server Load Balancing is available in BIG-IP as part of the DNS solution, or through the F5 Distributed-Cloud DNS Load Balancer.

DC 10.2024 | OV-1481327637