SOLUTION OVERVIEW

Maintaining application availability with a cloud-based DNS service

Combine on-premises and cloud-based DNS solutions to ensure high availability, infrastructure redundancy, and business continuity.

Key benefits

Maintain high availability
Establish redundancy to keep applications available in the event of primary or secondary DNS failures.

Add resilience to the primary DNS infrastructure
Ensure high availability of DNS environments with seamless failover to F5® Distributed Cloud DNS.

Experience the best of both worlds
Combine an on-premises DNS deployment with a cloud-based DNS service to double up your environment's capacity to deliver applications.

The critical role of DNS in application availability

DNS sits at the front of our networks, enabling users to connect with the applications and services they need, but it typically resides at the back of our minds—unnoticed until something goes wrong. If that happens, mission-critical applications and services become invisible to the world. This is why relying on a single DNS provider introduces risks: infrastructure outages, distributed denial-of-service (DDoS) attacks, latency issues, or configuration errors can lead to service disruptions and disconnected users, harming revenue and brand reputation, and potentially derailing business goals.

To mitigate these risks, many organizations implement a primary/secondary DNS strategy, running two DNS solutions in conjunction for added performance, redundancy, resilience, and enhanced global coverage. Without this layered approach, a DNS failure could compromise app availability, tarnishing the end-user experience.

But spinning up and deploying a separate on-premises DNS solution for the sake of redundancy is not feasible for most organizations. The additional cost to buy, deploy, and maintain two separate on-premises DNS solutions means organizations have fewer resources to focus on delivering value or innovation in other areas.

Fortunately, there's an option for resource-conscious teams who still want the insurance that a secondary DNS solution provides.

Relying on a single DNS provider introduces risks: infrastructure outages, DDoS attacks, latency issues, or configuration errors can lead to service disruptions and disconnected users, harming revenue and brand reputation, and potentially derailing business goals.

Key features

Increase attack protection with DNS security
Strengthen defenses by adding redundancy between on-premises and cloud-based DNS environments, minimizing vulnerabilities and maximizing protection.

Maximize performance and scalability with a global private backbone
Handle millions of DNS queries per second to support the most demanding environments, even during local outages.

Minimize downtime by combining DNS services
Deploy dual DNS solutions to keep users connected even if the primary DNS service goes offline.

More than just cheap insurance

F5® BIG-IP® DNS is one of F5's most widely adopted solutions, second only to BIG-IP® Local Traffic Manager™ (LTM). Thanks to its Traffic Management Microkernel (TMM) core, BIG-IP DNS is adept at intelligently routing application traffic, managing load balancing duties at a global scale, and resolving DNS queries at a rapid rate. But what if it breaks? Or, as is increasingly common, what if an extreme weather event impacts the data center that deploys BIG-IP DNS and knocks it offline? Building an application environment that leaves a DNS service as the single point of failure invites undue risks that can unnecessarily expose this vital infrastructure component to attacks, traffic floods, and critical outages.

Distributed Cloud DNS and BIG-IP DNS can work together to deliver a robust, flexible DNS environment that maintains application availability in the face of modern challenges. By deploying F5's highly available, cloud-based DNS as a secondary DNS service in front of an on-premises, primary DNS solution, organizations can embrace best practices for application availability while minimizing undue operational complexity.

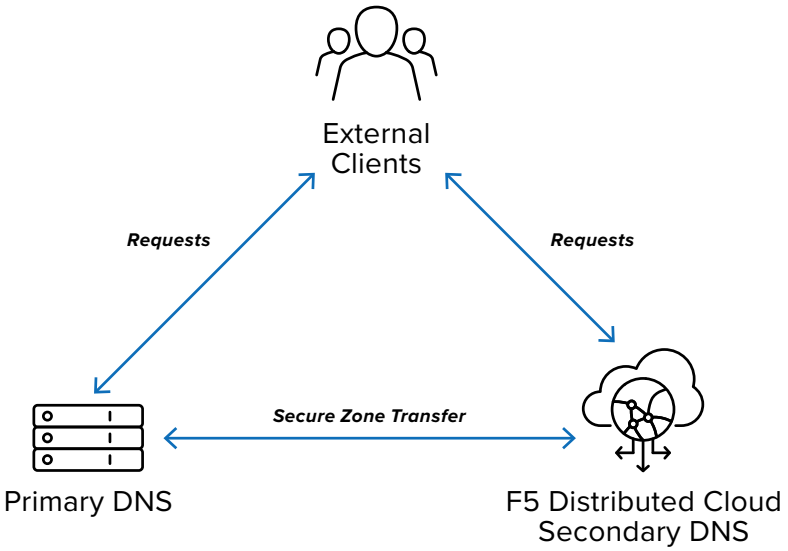
In this primary/secondary DNS scenario, BIG-IP DNS serves as the authoritative, primary resolver for a network, ensuring rapid query resolution and full control over DNS operations. To mitigate risks that come with a single point of failure and facilitate a safe failover, Distributed Cloud DNS deploys alongside BIG-IP DNS as a secondary DNS service. This allows for better protection against disruptions in business continuity, application availability, and network resilience across the entire environment.

But how does the pairing between these two DNS solutions work? Zone transfers, a standard mechanism for DNS synchronization based in the control plane, ensure that Distributed Cloud DNS maintains an accurate, real-time copy of DNS records. Updates are securely transferred to Distributed Cloud DNS at regular intervals, ensuring consistency without manual intervention.

In the event of failure or reduced availability of the primary DNS service, Distributed Cloud DNS automatically takes over query resolution, ensuring uninterrupted service.

In the event of a failure or reduced availability of the primary DNS service, Distributed Cloud DNS automatically takes over query resolution, ensuring uninterrupted service. If there is a lack of response at one server, the DNS query is routed to the backup server. This hybrid architecture combines the performance and control of on-premises services with the scalability, high availability, and resilience of the cloud, delivering enterprise-grade redundancy for your DNS infrastructure.

Figure 1: The dual DNS solution is simpler to deploy, improves availability with automatic failover, leverages existing automation or workflows for zone record updates, pushes DNS zone records closer to users to improve performance, and reduces load on the primary DNS service.



Conclusion

Whether it's for operational efficiency, customer trust, or overall agility, the advantages of a multi-DNS setup far outweigh the risks of doing nothing.

Nobody hopes for a data center outage, but bad actors, severe weather, and human error make such scenarios a matter of "when," not "if." The easiest way to prevent a DNS outage from taking an entire online presence offline is to use multiple DNS providers.

By standing up a cloud-based secondary DNS service to complement an on-premises primary DNS, teams can create effective redundancy and enhance resiliency. This approach minimizes the fallout from unforeseen events, ensuring applications and users remain online and connected. A secondary DNS reduces the load on the primary DNS service, provides failover in the event of a service outage, and improves response times when the primary service is degraded or unavailable.

Planning for resiliency is a necessity in today's digitally driven economy. Organizations that invest in a robust DNS strategy today are better prepared to deal with the increasing frequency and severity of outages tomorrow. Whether it's for operational efficiency, customer trust, or overall agility, the advantages of a multi-DNS setup far outweigh the risks of doing nothing.

Contact F5 to get started or learn more about BIG-IP DNS and Distributed Cloud DNS.