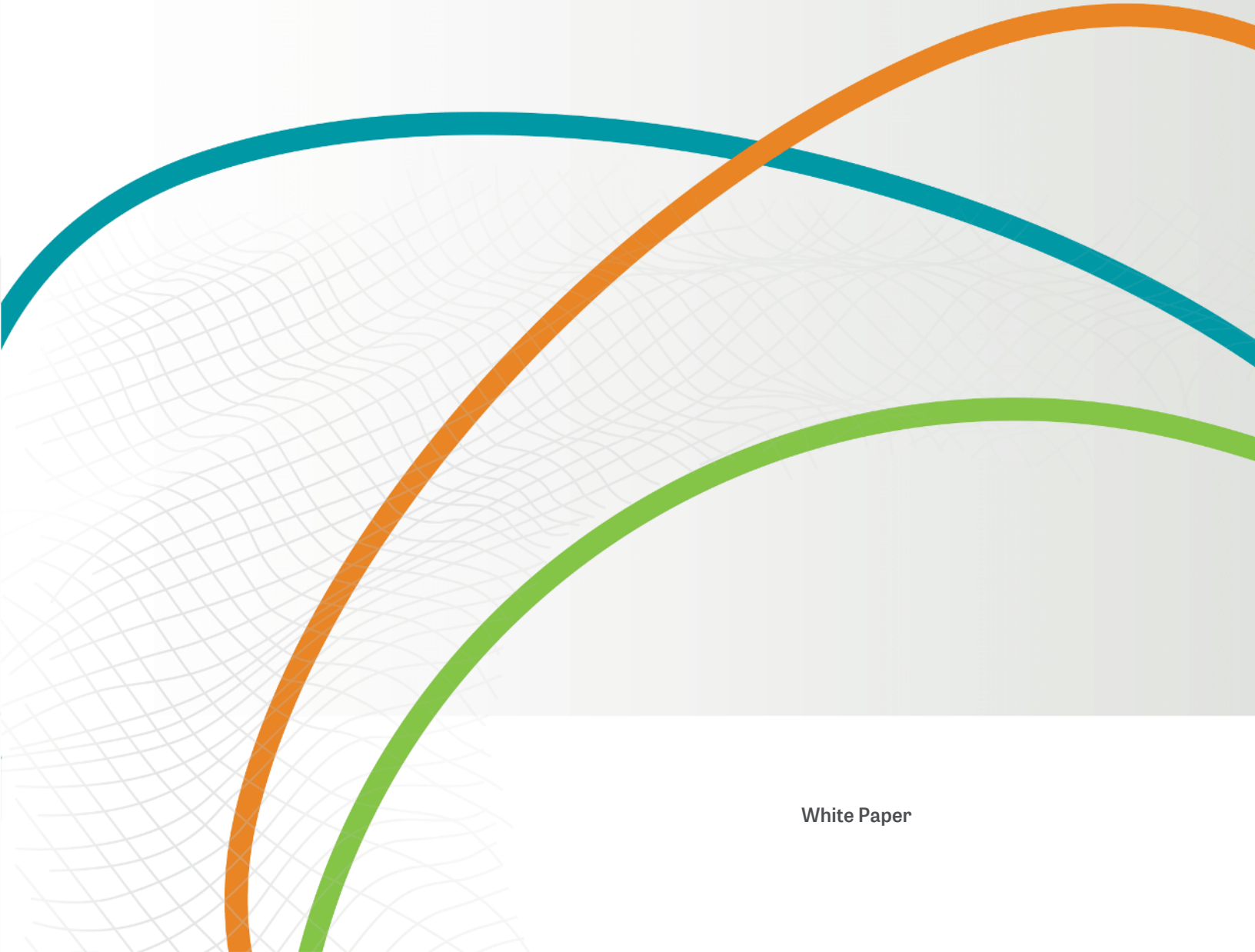
The F5 Intelligent DNS Scale Reference Architecture

End-to-end DNS delivery solutions from F5 maximize the use of organizational resources, while remaining agile and intelligent enough to scale and support existing and future network architectures, devices, and applications.



White Paper

Introduction

The Domain Name System (DNS) was created in 1983 to enable humans to easily identify all the computers, services, and resources connected to the Internet by name—instead of by Internet Protocol (IP) address, an impossible-to-memorize string of binary information.

Imagine how difficult it would be to use the Internet if you had to remember dozens of number combinations to do anything. Think of DNS as the Internet's phone book. A DNS server translates the domain names you type into a browser into an IP address, which allows your device to find the service or site you're looking for on the Internet.

As arguably the primary technology enabling the Internet, DNS is also one of the most important components in networking infrastructure. In addition to delivering content and applications, DNS also manages a distributed and redundant architecture to ensure high availability and quality user response time—so it is critical to have an available, intelligent, secure, and scalable DNS infrastructure. If DNS goes down, most web applications will fail to function properly, affecting your business—and your brand.

F5's end-to-end Intelligent DNS Scale reference architecture enables organizations to build a strong DNS foundation that maximizes the use of resources and increases service management, while remaining agile enough to support both existing and future network architectures, devices, and applications.

DNS Services Are Critical to Availability

When a user requests a web page, that request is passed to a local DNS server, which in turn communicates with the main DNS servers. Everything works well until a traffic surge or an attacker floods the server with DNS query requests. If your main DNS server gets overloaded, it will stop responding, which can make your website unavailable to visitors.

DNS failures account for 41 percent of web infrastructure downtime, so it's essential to keep your DNS available. According to a survey by the Aberdeen Group, organizations lose an average of $138,000 for every hour their data centers are down. Downtime negatively affects visiting customers, can lead to loss of revenue, and can even affect employees trying to access their corporate resources, such as email.

That's why the importance of a strong DNS foundation cannot be overstated. Without one, your customers may not be able to access your content and applications when they want to—and if they can't get what they want from you, they'll likely turn elsewhere.

According to a survey by the Aberdeen Group, organizations lose an average of $138,000 for every hour their data centers are down.[1]

Growing Pains

There are many reasons why DNS requirements are growing so quickly. Over the last five years, the number of active websites has grown by 180 percent;[2] the number of active users has doubled;[3] and the number of DNS queries has grown by 100 percent.[4]

In addition, nearly 60 percent of web users say they expect a website to load on their mobile phone in three seconds or less.[5]

Organizations are experiencing rapid growth in terms of applications as well as the volume of traffic accessing those applications. Plus, the web applications themselves are growing and continually becoming more complex. Every icon, URL, and piece of embedded content on a web page requires a DNS lookup. Loading complex sites may require hundreds of DNS queries, and even simple smartphone apps can require numerous DNS queries just to load.

In the last five years, the volume of DNS queries on for .com and .net addresses has more than doubled, increasing to an average daily query load of 77 billion in the fourth quarter of 2012.[6] More than 6 million domain names were added to the Internet in the fourth quarter of 2012.[7] Future growth is expected to occur at an even faster pace as more cloud implementations are deployed.

Security Issues

If DNS is the backbone of the Internet—answering all the queries and resolving all the numbers so you can find your favorite sites—it is also one of the most vulnerable points in your network. Due to the crucial role it plays, DNS is a high-value security target. DNS DDoS attacks can flood your DNS servers to the point of failure or hijack the request and redirect requests to a malicious server. To prevent this, a distributed high-performing, secure DNS architecture and DNS offload capabilities must be integrated into the network.

Generally, organizations have a set of DNS servers, each one capable of handling up to 150,000 DNS queries per second. High-performance DNS servers can handle around 200,000 queries per second. The bad guys can easily exceed those rates, as exemplified by DNS outages affecting The New York Times,[8] LinkedIn,[9] Network Solutions,[10] and Twitter.[11]

To address DNS surges and DNS DDoS attacks, companies add more DNS servers, which are not really needed during normal business operations. This costly solution also often requires manual intervention for changes. In addition, traditional DNS servers require frequent maintenance and patching, primarily for new vulnerabilities.

The Traditional Solution

When looking for DNS solutions, many organizations select BIND (Berkeley Internet Naming Daemon), the Internet's original DNS resolver. Installed on approximately 80 percent of the world's DNS servers, BIND is an open-source project maintained by Internet Systems Consortium (ISC). ISC is a non-profit organization with a for-profit consulting arm called DNS-CO, which offers five levels of subscription that range from $10,000 to $100,000 annually.

Despite its popularity, BIND requires significant maintenance multiple times a year primarily due to vulnerabilities, patches, and upgrades. It can be downloaded freely, but needs servers (an additional cost, including support contracts) and an operating system. In addition, BIND typically scales to only 50,000 responses per second (RPS), making it vulnerable to both legitimate and malicious DNS surges.

Solutions for a Changing Landscape

The F5 Intelligent DNS Scale reference architecture provides a more intelligent way to respond and scale to DNS queries and takes into account a variety of network conditions and situations to distribute user application requests and application services based on business policies, data center conditions, network conditions, and application performance.

Instead of worrying about DNS outages and purchasing additional DNS infrastructure to combat surges, you can simply install an F5 BIG-IP device in your network's DMZ and allow it to handle requests on behalf of your main DNS server.

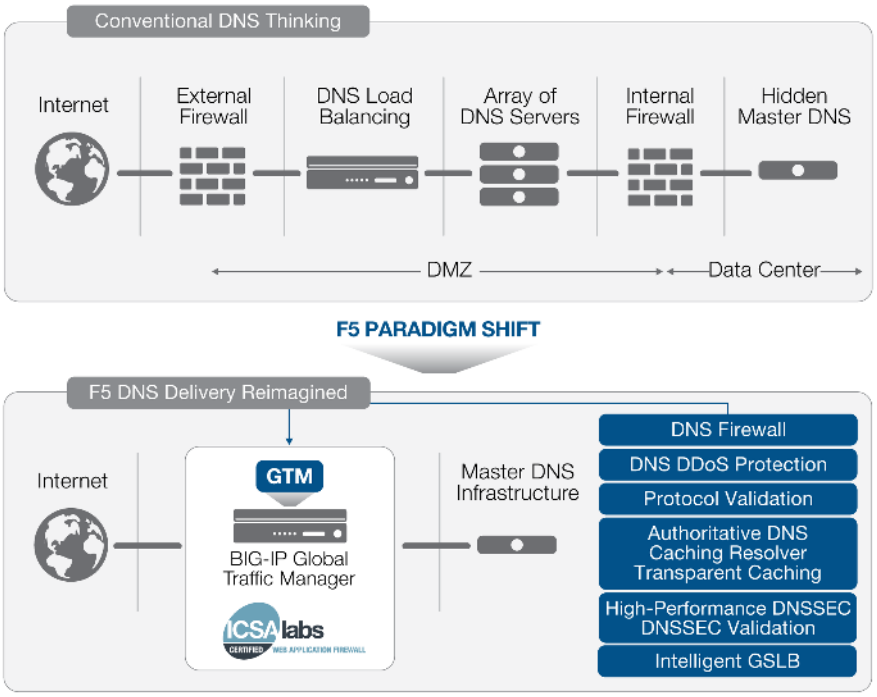


Figure 1: Simplify DNS delivery with F5 technology.

Scale On Demand

Each BIG-IP device can respond to up to 10 million RPS, which means that even large surges of DNS requests (including the malicious ones) will not disrupt your content or affect the availability of your critical applications. Your network administrators can rest easy, knowing that your site will respond to all DNS queries and remain available even during an attack. Your brand is protected and your company can avoid an embarrassing front-page story.

Enhance Availability with DNS Express

The F5 Intelligent DNS Scale reference architecture helps ensure that your applications and content are continuously available to your users. One of the most important pieces of this architecture is the specifically designed F5 DNS Express query response feature in BIG-IP Global Traffic Manager (GTM), which manages authoritative DNS queries by transferring zones from the primary DNS server to its own RAM.

BIG-IP GTM only has to open the DNS query packet once, as long as the request is for an address that is in the zone that was transferred to DNS Express—which simplifies the process and significantly improves performance and response times of your DNS architecture.

With DNS Express, the individual core of each BIG-IP device can answer approximately 125,000 to 200,000 requests per second, scaling up to more than 10 million query RPS, greater than 12 times the capacity of a typical primary DNS server.

Video: DNS Express: DNS Die Another Day

The BIG-IP Platform: Your Firewall in the DMZ

In addition, each BIG-IP device is ICSA Labs Certified as a network firewall. By intelligently evaluating the reputation of Internet hosts, the BIG-IP device can prevent attackers from knocking your DNS offline with a DNS DDoS attack, stealing data, compromising corporate resources, or otherwise disrupting your business. In addition, DNSSEC can protect your DNS infrastructure, including cloud deployments, from cache poisoning attacks and domain hijacks. With DNSSEC support, you can digitally sign and encrypt your DNS query responses. This enables the resolver to determine the authenticity of the response, preventing DNS hijacking and cache poisoning. The F5 IP Intelligence service enhances your overall security by denying access to IP addresses known to be infected with malware, in contact with malware distribution points, and with poor reputations.

DNS Services at the Edge of the Network

The F5 Intelligent DNS Scale reference architecture also helps keep your content and applications available by responding to DNS queries from the edge of the network, rather than from deep within your critical infrastructure. When you offload DNS responses to the BIG-IP platform, no request reaches the back end of your network, which greatly increases your ability to scale and respond to DNS surges along with protecting your DNS infrastructure.

By increasing the speed, availability, scalability, and security of your DNS infrastructure, the F5 Intelligent DNS Scale reference architecture ensures that your customers—and your employees—can access your critical web, application, and database services whenever they need them.

Distributed DNS

This also applies to cloud deployments or infrastructures where DNS is distributed. Organizations can replicate their high-performance DNS infrastructure in almost any environment. They may have cloud DNS for disaster recovery/business continuity, or even a cloud DNS service with signed DNSSEC zones. F5 DNS Services enhanced AXFR support offers zone transfers from a BIG-IP device to any DNS service, enabling organizations to replicate DNS in physical, virtual, and cloud environments. The DNS replication service can be sent to other BIG-IP devices or other general DNS servers in data centers or clouds that are closest to the users.

In addition, organizations can send users to a site that will give them the best experience. F5 DNS Services uses a range of load balancing methods and intelligent monitoring for each specific app and user. Traffic is routed according to your business policies, as well as current network and user conditions. F5 DNS Services includes an accurate, granular geolocation database, giving you control of traffic distribution based on user location.

Video: In 5 Minutes or Less: IP Intelligence Service

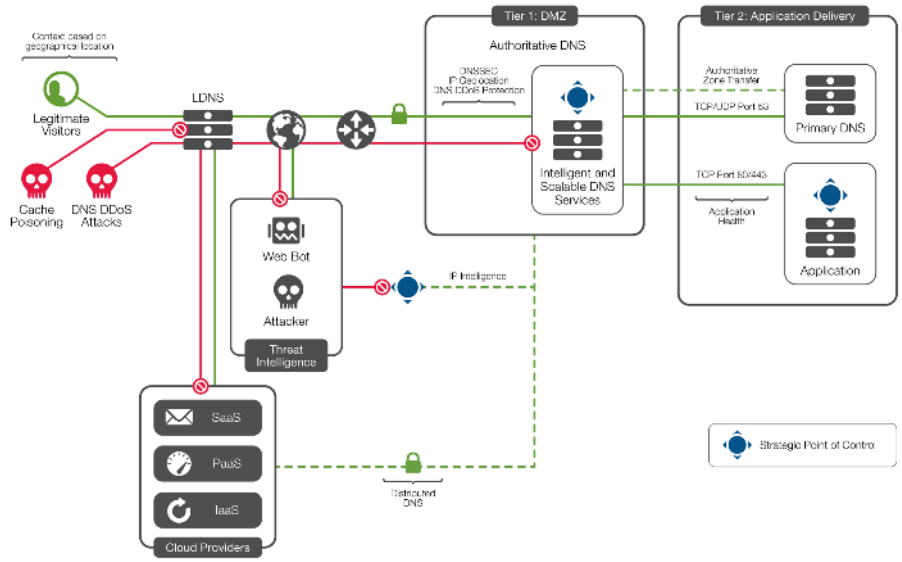


Figure 2: Increase the speed, availability, scalability, and security of your DNS infrastructure.

BIG-IP GTM and DNS Services

BIG-IP GTM is a global DNS solution, providing name services at the very edge of your service delivery and access networks. By employing geographic location services, BIG-IP GTM can direct users to the best service delivery data center based on their physical location.

BIG-IP GTM provides the following name services:

- DNS services at the edge of the network for all internal and external services.
- Geolocation services for pinpoint application or service delivery accuracy based on location of the mobile user.
- The IP Intelligence service safeguards infrastructures by detecting and stopping access from IP addresses associated with malicious activity.
- A single point of control for management of all global and local name services.
- Additional BIG-IP intelligent services solutions such as global application delivery, policy enforcement, NAT64 and DNS64 translation, health monitors, and the F5 scripting language, iRules.
- Support for global DNS services
- Integration with DNS iRules for granular DNS decisions and name service delivery.
- Support for service provider–specific protocols such as ENUM requests for SIP transactions.

BIG-IP LTM and DNS Services

Within the data center, BIG-IP Local Traffic Manager (LTM) can ensure that your applications and content remain highly available by creating a fault-tolerant architecture from the mobile edge through to the service. In addition to providing this high availability, BIG-IP LTM also supports service provider–specific applications such as load balancing ENUM requests for SIP transactions.

BIG-IP LTM solutions for naming services include:

- Integration with BIG-IP GTM to extend rich naming services into the local data center and services network.
- Load balancing support for both local DNS and recursive DNS.
- Support for service provider–specific protocols such as ENUM requests for SIP transactions.
- Transparent health monitors to evaluate service health before sending users to the service. BIG-IP LTM can relay health information back to BIG-IP GTM to bring application awareness to the edge of the SDN.
- Integration with iRules for granular DNS decisions and name service delivery.

Deploying a Complete Service Delivery Infrastructure

The F5 Intelligent DNS Scale reference architecture adjusts seamlessly for high-availability and high-volume applications while simultaneously supporting millions of user requests per second. They work together with other BIG-IP service delivery features, such as the iRules scripting language, transparent application monitoring, modules such as BIG-IP Application Acceleration Manager (AAM), and other IP-related services to create a complete service delivery infrastructure: the F5 Service Delivery Network. Seamless scale and flexibility is achieved by leveraging the intelligent service delivery platform common to all BIG-IP devices.

Conclusion

The F5 Intelligent DNS Scale reference architecture is an end-to-end DNS delivery solution that improves web performance by reducing DNS latency, protects your web properties and brand reputation by mitigating DNS DDoS attacks, reduces data center costs by consolidating DNS infrastructure, and most importantly, directs your customers to the best performing components for optimal application and service delivery.

In addition, the F5 Intelligent DNS Scale reference architecture delivers the peace of mind that comes with knowing that your web applications will respond to all DNS queries—keeping your content and applications available to your users wherever and whenever they want to access them.

By using the F5 Intelligent DNS Scale reference architecture, organizations can:

- Increase the speed, availability, scalability, and security of their DNS infrastructure.
- Reduce complexity and cost by eliminating unnecessary additional DNS servers.
- Enjoy the peace of mind that comes with knowing their site will respond to all DNS requests.

---

[1] http://www.thinkgig.com/do-you-know-the-cost-of-data-center-downtime-infographic/

[2] http://news.netcraft.com/archives/2013/10/02/october-2013-web-server-survey.html

[3] http://royal.pingdom.com/2012/04/19/world-internet-population-has-doubled-in-the-last-5-years/

[4] https://investor.verisign.com/releaseDetail.cfm?ReleaseID=591560

[5] http://www.slideshare.net/Gomez_Inc/2011-mobile-survey-what-users-want-from-mobile

[6] http://blogs.verisigninc.com/blog/entry/verisign_shares_q4_2012_domain

[7] https://investor.verisign.com/releasedetail.cfm?releaseid=754909

[8] http://www.forbes.com/sites/andygreenberg/2013/08/28/syrian-hack-of-nytimes-com-and-twitter-could-have-inflicted-much-morethan-mere-embarrassment/

[9] http://www.zdnet.com/linkedin-hit-by-outage-from-dns-issue-7000017058/

[10] http://www.crn.com/news/security/240158492/ddos-attack-behind-latest-network-solutions-outage.htm

[11] http://www.ciozone.com/index.php/Security/Twitter-Outage-Caused-by-DNS-Attack.html

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 www.f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com