White Paper

The Dynamic DNS Infrastructure

Between the proliferation of mobile devices and the ever-increasing amount of content on the web, DNS usage has seen a huge increase in recent years. Meanwhile, DNS continues to be a tempting target for attackers, and when they succeed in disrupting DNS, all external data center services are affected. For organizations confronting these growth and security challenges, F5's new full-proxy architecture for DNS provides a complete solution for global, local, and cloud load balancing.

by David Holmes
Senior Technical Marketing Manager

Contents

Introduction **3**

The Problem of Growth 3

The Problem of Security 4

F5's Complete Solution for Global, Local, and Cloud Load Balancing **5**

Solutions for the Global Data Center Infrastructure **6**

Global Server Load Balancing 6

DNS Express for the Global Data Center Infrastructure 7

Complete DNS Control and Agility 9

Securing Customer Connectivity with DNSSEC Signing 10

Performance and Security for the Enterprise Local DNS **11**

High-Performance DNSSEC Validation for the Local DNS 12

Cloud Balancing with DNS and GSLB Services **13**

Simple and Robust Cloud DNS Management 13

Conclusion **16**

Introduction

The Domain Name System (DNS) is a technical cornerstone of the Internet, but it faces significant challenges in growth and security. The Internet depends on DNS; when it doesn't work, neither does the Internet. Today's organizations depend not only on the Internet DNS, but their own DNS as well, and when their DNS systems break, their applications break.

The Problem of Growth

As smartphones became ubiquitous over the last decade, the number of Internet users increased over 500 percent to more than 2.6 billion. Forrester[1] predicts that by 2016, there will be over 1 billion smartphones in use worldwide, and the resulting explosion of smartphone applications on Long Term Evolution (LTE) 4G networks will drive an exponential increase in DNS traffic.

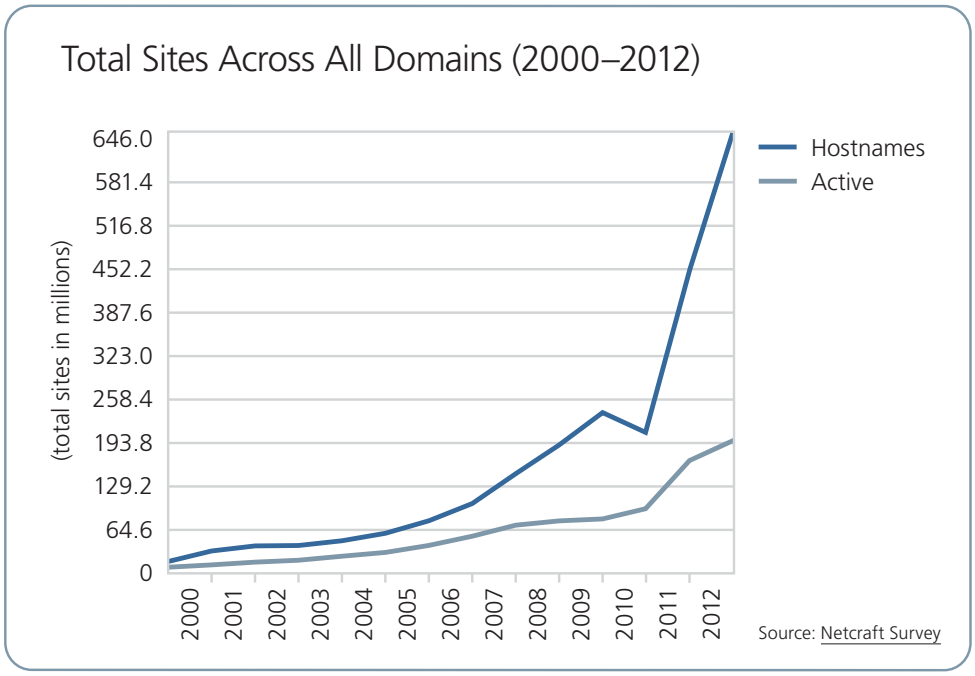

Figure 1: DNS growth is increasing exponentially.

1 Campinas, Wilian. Number of smartphones in the world is expected to reach 1 billion by 2016, consultancy projects. February 13, 2012.

Growth in entertainment sites, social media, search, and online purchases is also putting pressure on DNS. In the last five years, the volume of DNS queries has climbed over 200 percent—the average daily query load in the first quarter of 2011 was a staggering 57 billion.

As sites and applications become richer and more sophisticated, the burden on DNS increases. For example, on a modern web page, every image, add button, widget, link, icon, and other embedded content has a potential IP address that must be looked up. It is not uncommon for a single page to require over two dozen different DNS lookups by a browser. A top-level page such as cnn.com requires over *one hundred* DNS lookups. A larger, more complex web means ever-increasing DNS requests.

The Problem of Security

Nearly all clients rely on DNS to reach their intended services, making DNS the most critical—and public—of all services. DNS disruptions affect all external data center services, not just a single application. This single point of total failure, along with the historically under-provisioned DNS infrastructure, especially within Internet and enterprise data centers, makes DNS a very tempting target for attackers. It has become the second most frequently used attack vector for distributed denial-of-service (DDoS) attacks (after HTTP), leaving organizations scrambling for effective defenses.

Equally significant is the fact that the most financially damaging attacks, such as phishing and man-in-the-middle (MITM) attacks, start with DNS response manipulation. The Domain Name System Security Extensions (DNSSEC) technology aims to address these issues, but its added overhead and complexity are proving to be an additional burden on organizations that are already racing to address problems introduced by rapid growth and DDoS defense.

Even traditional security measures such as browser toolbar blockers rely on DNS services, so when those services are disrupted, security measures can fail. The same issue exists to some degree with SSL site certificates.

Organizations need to take a new look at DNS solutions to ensure that they are meeting the performance and security requirements of today's Internet—and tomorrow's.

F5's Complete Solution for Global, Local, and Cloud Load Balancing

Organizations that meet the challenges of growth and security have been turning to F5 Networks for over 10 years for DNS and global application delivery. F5 BIG-IP® Global Traffic Manager™ (GTM) has historically been the highest-performing, most flexible multi-site application delivery technology. Now F5 is pushing the technological envelope with a full-proxy architecture for dynamic DNS that provides a complete solution for global, local, and cloud load balancing.

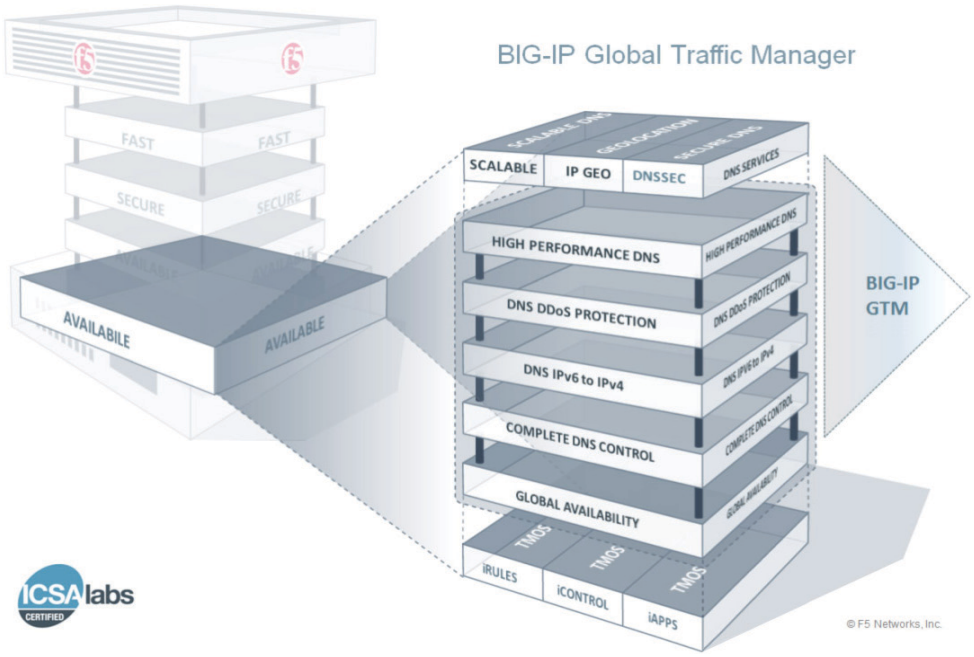

Figure 2: F5 DNS Services and global traffic management ensure application availability.

A complete DNS solution from F5 offers:

- High efficiency and productivity and reduced downtime
- Faster web browsing from reduced DNS latency
- Improved multi-site application performance
- Protection against DNS DDoS attacks
- Network migration supporting IPv6 to IPv4 communication
- Complete DNS security with DNSSEC services

Global inbound DNS solutions

For global organizations with multiple data centers and an existing DNS infrastructure, BIG-IP GTM provides a range of services, from global server load balancing (GSLB) to full zone service with F5's unique DNS Express™ technology. DNSSEC signing ensures that clients aren't getting maliciously redirected.

Local DNS: control and agility for the enterprise

For the enterprise, BIG-IP GTM can act as a central clearing house for outbound DNS name resolution, caching and resolving, and DNSSEC validation. DNS Express scales, secures, and accelerates the local zone resolution.

Cloud balancing: virtual data center load balancing

For organizations with any combination of physical and virtual data centers, BIG-IP GTM provides the agility to control how names move between them and inside them. With BIG-IP GTM Virtual Edition (VE) in public and private cloud environments, organizations can spin up new deployments at will and provide flexible global application availability.

Solutions for the Global Data Center Infrastructure

Global Server Load Balancing

GSLB via DNS has been a method for distributing load since DNS first incorporated multiple IP addresses per response. Even today, many sites still use the round-robin DNS response technique to attempt to spread traffic across servers and applications.

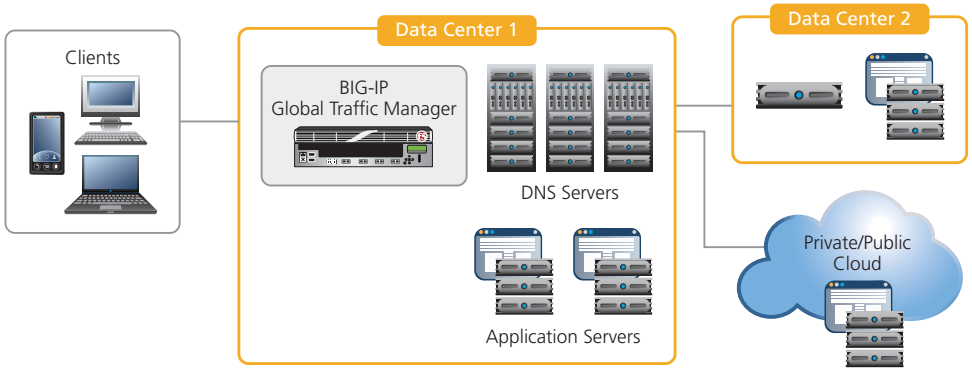

Figure 3: Global server load balancing between data centers and cloud.

While simple and useful, primitive round-robin DNS load balancing has two significant weaknesses. First, conventional DNS servers have no knowledge of the health of application servers. If a name maps to four application server addresses, and the third server is down, 25 percent of the served connections will be refused. Second, the conventional round-robin technique does not take into account the profile of the user querying the name itself. That is, it has no ability to match users to nearby data centers.

BIG-IP Global Traffic Manager has provided a GSLB solution that addresses these weaknesses and more since 2002. Internet sites and enterprise data centers have relied on BIG-IP GTM for the advanced global server load balancing that provides high application availability and a positive user experience. For the enterprise, BIG-IP GTM considers the health of the underlying application and delivers only addresses for healthy servers. For global Internet sites with multiple data centers, BIG-IP GTM can employ sophisticated load balancing methods that implement the business logic for each application. The method can be as simple as a priority-based preference list that spreads the load using static or dynamic ratios; client proximity–based; or as complex as using multiple factors and inputs to choose the optimal resource for the clients. Many organizations now use geolocation data to connect users to the data center closest to them. Users get fewer bad connections and a richer experience, and the data centers get better global server load balancing.

DNS Express for the Global Data Center Infrastructure

Historically, BIG-IP GTM provided GSLB by offering intelligent but non-authoritative DNS resolution. The new DNS Express feature improves on this by offering world-class high-performance authoritative DNS resolution. It does this by transferring the zone information from existing DNS servers into its own RAM, and then responding to all queries itself. DNS Express makes BIG-IP GTM an authoritative server without requiring a new management infrastructure.

When used behind DNS Express, the DNS servers become merely the storage and administrative control points for DNS management. This means fewer servers are required. Like other F5 products, BIG-IP GTM is an ICSA Labs Certified Network Firewall, so it can be placed in a DMZ or even outside the firewall perimeter.

F5 Technologies Enable DNS Protection

Benefit	Enabling Technology
High-performance GSLB	Multi-core BIG-IP GTM
Scalable DNS offload	DNS Express
Spread the load across devices	IP Anycast
Secure DNS queries	DNSSEC
Route based on nearest data center	Geolocation
Complete DNS control	F5's iRules® scripting language
DDoS protection	DNS Express
Protocol validation	Full L7 DNS proxy

DNS DDoS protection

BIG-IP GTM offers a set of security services that provides protection against DDoS attacks at the DNS security perimeter. For example, BIG-IP GTM easily mitigates typical distributed UDP floods by scaling performance far beyond that of a normal DNS server. Similarly, for more advanced query attacks, the DNS Express feature can outperform a typical DNS server because it retains all its valid zone entries even during an NXDOMAIN DDoS attack.

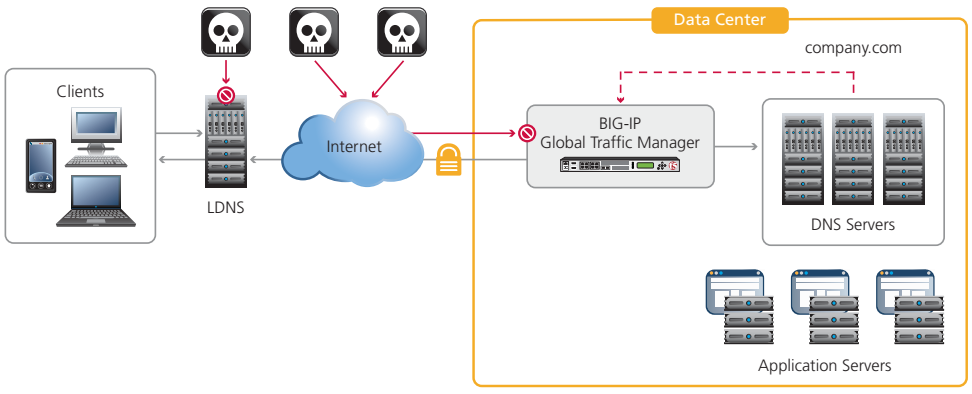

Figure 4: F5 technologies enable DNS protection.

Since 2002, when the first major attacks against the global DNS infrastructure occurred, the IP Anycast technology has become a crucial defense against many kinds of DDoS attacks. IP Anycast dilutes DDoS attacks by spreading the load (be it legitimate traffic or a network attack) across multiple devices, usually in different

data centers in different parts of the globe. This foils global botnets because they are never able to concentrate their firepower against a single target.

All of F5's TMOS-based products, including BIG-IP GTM, include ICSA Labs Certified Network Firewall functionality that mitigates network attacks. The new, full-proxy architecture of BIG-IP version 11 enables BIG-IP GTM to perform native protocol validation for all DNS queries. By terminating both sides of the DNS dialogue, BIG-IP GTM can quickly eliminate any invalid DNS requests.

Complete DNS Control and Agility

DNS Express is revolutionizing the way that DNS responses are served; however F5 is continuing to evolve its conventional DNS server load balancing solution. BIG-IP GTM version 11.1 introduced true full-proxy inline functionality, where BIG-IP GTM proxies requests from the DNS client and responses from the DNS server to provide maximum control.

This new full-proxy architecture gives organizations the control to provide a complete set of DNS performance- and security-related services including caching, resolving, and DNSSEC signing and validation.

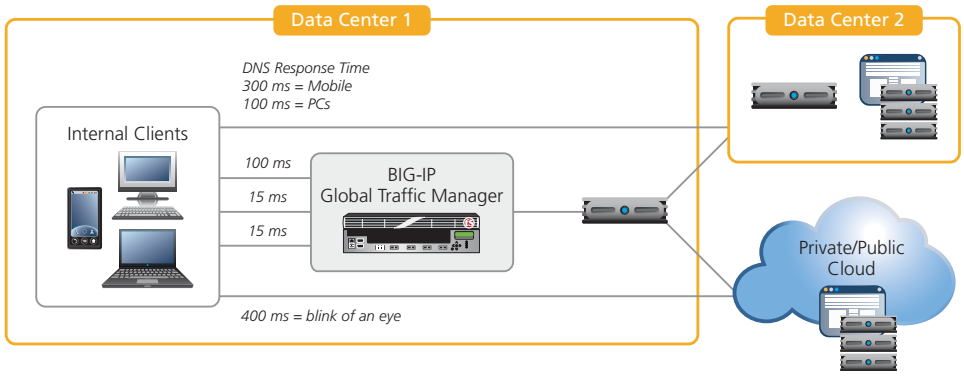

Figure 5: BIG-IP GTM enhances user experience through scalable, high-performance DNS caching and resolving.

Better performance by caching multiple servers

Its full-proxy architecture means that with DNS caching and resolving, BIG-IP GTM can act as a transparent cache not just for a single DNS server, but for an entire pool of DNS servers. Transparent caching at a single point of control provides faster response, because the single BIG-IP GTM cache can populate faster than the

individual caches on each DNS resolver. This leads to higher overall performance and, ultimately, a better user experience.

Securing Customer Connectivity with DNSSEC Signing

Because DNS is usually the first step that a customer takes when connecting to an organization's data center, attacks that hijack DNS responses (such as phishing and MITM attacks) are the easiest way to compromise assets. DNS response spoofing has always been a popular method with attackers, and cache poisoning against recursive name servers is significantly easier than the IT community first thought. In 2008, security researcher Dan Kaminsky revealed a flaw in the design of DNS message identifiers, and as a result, high-security organizations like the U.S. Department of Defense made securing DNS a high priority and mandatory for regulatory compliance.

F5's DNSSEC solution defends against the entire class of cache poisoning attacks, mitigating phishing and MITM threats. It assures organizations' customers that they are indeed connecting to their data center and not to a phishing proxy. F5's DNSSEC signing keys can be stored in tamper-protected FIPS 140-2 Level 3 hardware security modules (HSMs) for maximum security.

F5 combines security with agility

The adoption of DNSSEC has been difficult and slow for many in the name resolution industry. In particular, some global server load balancing solutions are incompatible with DNSSEC. Most follow the initial reference implementation and statically sign the entire zone once a month, and then serve the pre-signed responses. However, there are problems with a statically signed solution (see sidebar).

F5's dynamic DNS infrastructure provides a superior approach.[2] With BIG-IP GTM, DNSSEC and GSLB coexist because BIG-IP GTM signs responses in real time so that all the benefits of GSLB can be realized while still protecting the responses with strong asymmetric cryptography.

When used with DNS Express, BIG-IP GTM signs responses for any query that it serves, including those that it serves from its own zone information, from other local DNS servers (which may not be using DNSSEC), and from BIG-IP GTM's own caching resolver. BIG-IP GTM is also smart enough not to sign any response that has already been signed by another server.

Problems with Statically Signed Zones

- Administrators can't make small zone changes until the entire zone is re-signed
- Statically signed zones cannot utilize application health monitoring to ensure high availability
- Advanced client qualification techniques such as geolocation cannot be supported in a statically signed environment
- GSLB implementations break static DNSSEC to make routing decisions

2 See the F5 DNSSEC Solution video: http://vimeo.com/37677275.

F5 offers the only complete GSLB and DNSSEC solution, and can protect signing keys with tamper-proof FIPS 140-2 level 3 hardware key protection.

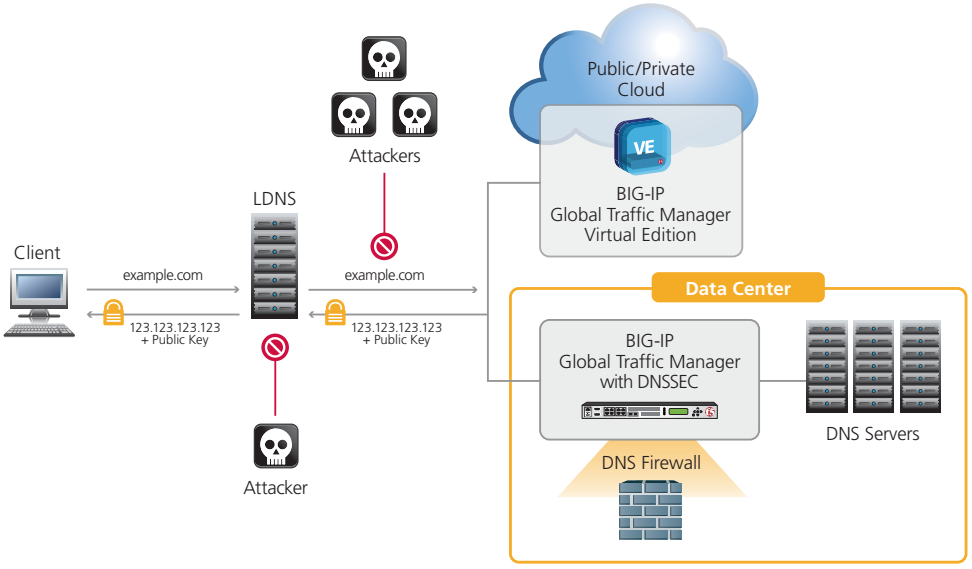

Figure 6: BIG-IP GTM with DNSSEC delivers real-time signed DNS query responses to clients.

Performance and Security for the Enterprise Local DNS

Local DNS (LDNS) services resolve outbound name queries on behalf of enterprise clients. By providing this basic service, LDNS can become a central point of control for enterprise administrators to manage performance, scalability, and security.

- **Performance.** When populated, the BIG-IP GTM cache and resolver can reduce outbound DNS queries by 80 percent, resulting in higher performance and better user experience.
- **Scalability.** The BIG-IP GTM multi-core architecture can scale along with DNS Express to meet the needs of even the largest enterprise data centers.
- **Security.** BIG-IP GTM provides a high-performance, drop-in DNSSEC validation solution, which offloads cryptographically intensive services from other internal clients and DNS services.

High-Performance DNSSEC Validation for the Local DNS

The full-proxy functionality of BIG-IP GTM can help an organization validate DNSSEC responses by performing the validation for any combination of resolving, caching, and DNS response functionality. Not only can BIG-IP GTM accept and resolve each query, it can validate the DNSSEC responses as well.

Validation by BIG-IP GTM secures the communication and frees the client from having to perform computationally costly cryptographic operations, and caching improves the performance of subsequent queries. As multiple clients request the same DNS resolution, all subsequent clients will receive the already cached and validated response.

DNSSEC solutions have the potential to finally secure the Internet. Now that the .com name root has been signed, there is finally a global infrastructure in place that allows customers to verify, for example, that an email from their bank really is from their bank. As the Internet overcomes its DNSSEC growing pains, adoption of this key technology will become a reality for more than just the federal organizations for whom it's mandatory.

Because DNSSEC validation can be so computationally expensive, large enterprises will require the right combination of caching and performance to keep internal clients functioning smoothly.

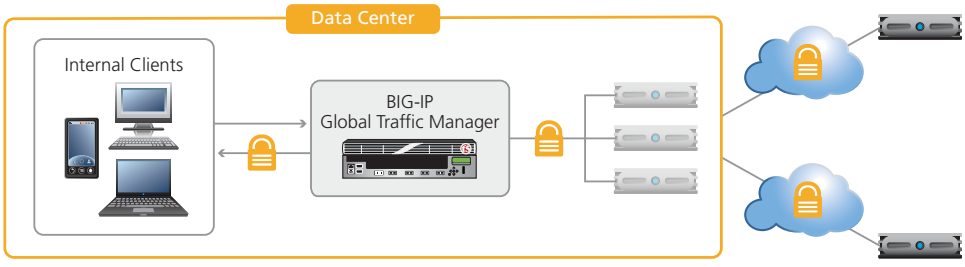

Figure 7: BIG-IP GTM is the DNS resolver responsible for requesting the additional DNSSEC records and doing the crypto calculations to validate that the DNS response is correctly signed.

BIG-IP GTM's high-performance, on-board cryptographic hardware offloads DNSSEC validation computation. BIG-IP GTM can perform DNSSEC validation even for legacy clients that do not request DNSSEC, making it a transparent, drop-in security solution for the entire enterprise.

"A high-performance DNSSEC validation solution is going to be extremely important as more and more sites deploy DNSSEC."

Cricket Liu, Vice President, Architecture at Infoblox

Dynamic DNS health monitoring

BIG-IP GTM includes a new application health monitor that queries the health of DNS services every five seconds. The monitor verifies that active, available servers are responding properly to queries. It can then evaluate any aspect of the response, or simply watch for any response.

The DNS health monitor's flexibility means that it can effectively become a path monitor. For example, an administrator can monitor whether an external name is not resolving. By signaling this failure, the monitor alerts an organization that a name break exists somewhere between the enterprise server and the Internet.

Cloud Balancing with DNS and GSLB Services

Simple and Robust Cloud DNS Management

Data centers are in a state of flux today. Some organizations are consolidating data centers, while others are using new virtual data centers and cloud deployments to manage growth. Still others are using a combination of managed service hosting and Internet software-as-a-service (SaaS) to provide virtual applications. BIG-IP GTM provides solutions that accommodate all of these architectures.

Simple and robust cloud DNS management:

- Extends query management and caching to cloud deployments.
- Ensures DNS queries are efficiently routed to the best cloud.
- Increases productivity with DNS caching with fast application responses.

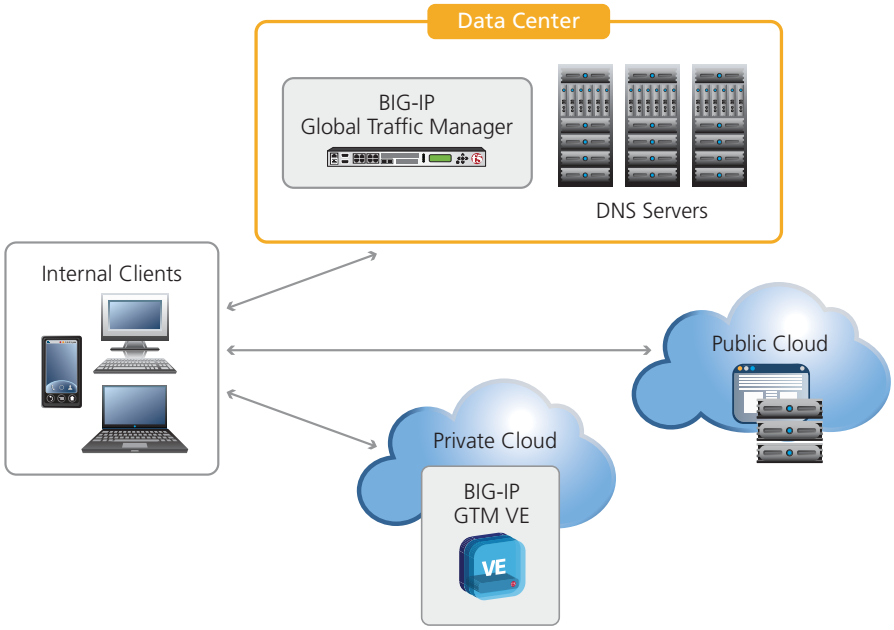

Figure 8: BIG-IP GTM provides agility for any combination of physical or virtual data centers.

BIG-IP GTM VE in virtual environments

With BIG-IP GTM, organizations can gain a single point of control for their inbound DNS and global server load balancing in cloud deployments. The virtual edition (VE) of BIG-IP GTM can be deployed in VMware vSphere, Microsoft Hyper-V, and Citrix XenServer environments[3] to provide the same services that the physical version provides. BIG-IP GTM VE inside the virtual environment can provide LDNS for virtual applications, and a physical BIG-IP GTM standalone device can ensure availability externally.

Virtual data center global server load balancing

The same principles that make GSLB such a compelling solution still apply to virtual environments. BIG-IP GTM enables organizations to easily implement flexible global application availability by routing users to applications in virtual data centers. The DNS health monitor ensures virtual application availability. The native DNS intelligence of BIG-IP GTM directs users to the most available cloud applications and between various clouds for virtual deployments.

3 BIG-IP GTM VE is compatible with Microsoft Hyper-V for Windows Server 2008 R2 (lab only), Citrix XenServer 5.6, and VMware vSphere Hypervisor 4.0, 4.1, and 5.0.

Easing the evolution to IPv6 services

As organizations migrate to IPv6, legacy systems, customer requirements, and compatibility all play a part in how quickly the migration takes place. Further complicating matters, some networks are IPv6-only, yet also need access to IPv4 resources such as hosts on the Internet and legacy servers that don't support IPv6. Many organizations have subnets that simply cannot support a dual stack, and need a solution to bridge the gap.

F5's full-proxy architecture offers a unique, compelling solution that takes advantage of strategic points of control in the network to bridge the gap between IPv6 clients and IPv4 servers.

Network address translation with the NAT64 gateway in BIG-IP® Local Traffic Manager™ (LTM) provides an IPv6 to IPv4 proxy for application delivery. BIG-IP GTM'S DNS64 gateway automatically simulates the IPv6 address and invokes the NAT64 proxy.

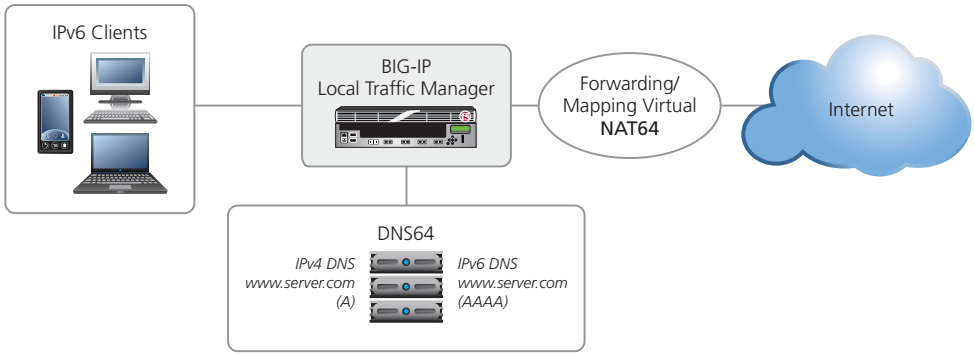

Figure 9: Bridging IPv6 clients and IPv4 services.

Organizations are using DNS64 and NAT64 to build out new IPv6-only networks that still have access to IPv4 infrastructure—without having to implement dual stacks in their networks. F5's strategic points of control in the network are the critical components that enable these solutions.

BIG-IP GTM bridges the gap between IPv6 and IPv4 by:

- Offering critical support for LTE mobile devices
- Supporting pure IPv6 clients that access both IPv6 and IPv4
- Combining NAT64 and DNS64 to provide automatic translation

Conclusion

F5 has offered high-performance DNS solutions since 2002. With its most recent suite of DNS technologies, F5 remains at the cutting edge of global application delivery. DNS Express, for authoritative and local zones, provides the best performance for DNS delivery and adds DNS DDoS protection. The new full-proxy architecture of BIG-IP GTM enables organizations to maximize agility through DNS resolution, performance through caching, and complete DNS security through signing and validation. For organizations moving to cloud services, BIG-IP GTM VE enables flexibility within the private cloud and virtual environments. And for organizations moving to IPv6, DNS64 in BIG-IP GTM successfully bridges the worlds of IPv6 and IPv4 during transition.

Whether organizations have global data center infrastructure, enterprise data centers, or a mix of both plus private or hybrid cloud services, solutions based on BIG-IP GTM help them protect, scale, and deliver their applications to the world.

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

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com