Networking

Intelligent Domain Name System resolution for application delivery

By Andrew Walker and Fred Johnson

Dell™ platforms leveraging F5® BIG-IP® Global Traffic Manager™ systems and DNS Security Extensions create agile application infrastructures that are designed to reliably direct clients to the most-available and best-performing data centers.

The Domain Name System (DNS) is a fundamental building block for the Internet. Much like a phone book, it provides a translation service from human-readable names to computer network addresses for global systems, applications, and services across the Internet and within organizations. To use a simple example, the domain name example.com resolves to the IP address 192.0.32.10. Domain names are user friendly because people tend to remember names and forget long strings of numbers like IP version 4 addresses, not to mention even longer IP version 6 addresses. DNS resolution has been around for a long time—approximately 27 years—and its benefits are well known and understood by IT managers.

Understanding the foundation for DNS resolution

Today, DNS is one of the most critical and widely used Internet services. When it was originally developed, the goals for DNS were fairly straightforward: to define an open-standard protocol describing a distributed name-resolution system that, among other things, allows for sharing of zone data between name servers, delegation of authority for zone data, local caching of successfully resolved queries,

DNS Security Extensions in five easy steps

Walk through the basics of DNSSEC and the ability of F5 BIG-IP Global Traffic Manager (GTM) to sign DNS requests on the fly by watching this video Webinar presentation on configuring BIG-IP GTM to support DNSSEC.

bit.ly/eLW1gs
round-robin load balancing, and the ability to delegate administrative responsibility to sub-domain owners.

Security was not part of the original design for DNS. However, to be fair, back in the 1980s the creators of DNS could not predict that the future would bring an explosion of Internet use and computer security vulnerabilities. High-profile DNS vulnerabilities have involved cache poisoning, in which malicious persons modify cached zone data to hijack a domain or host name, sending users to the wrong site. Landing on the wrong site could simply result in a denial of service or have more severe consequences—for example, if the site owner were trying to collect personal data such as user name, password, or credit card information.

Fortunately, the DNS protocol standard has been modified over time to include the DNS Security Extensions (DNSSEC). The common standard DNS implementation, Berkeley Internet Name Domain (BIND), has incorporated these extensions. Through Public Key Infrastructure (PKI), DNSSEC enables a chain of trust within the DNS protocol that ensures the integrity of the zone-data source.

Today, applications are truly global in scope, and the workforce can be primarily—if not exclusively—mobile. Users may connect from almost any location or network type to access application resources located around the world. End-user expectations for application performance might be characterized by needing a consistent, secure, and responsive application experience regardless of location, time of day, or device type. To reliably deliver globally distributed applications and services in this way, the network infrastructure must be able to determine the health and availability of the applications and the data centers, with the assurances that the underlying name-resolution system is accurate. The combination of DNSSEC and global server load balancing (GSLB) helps enable this infrastructure.

Preparing the Internet for DNS Security Extensions

The digital signing of the DNS root domain and many of the top-level domains, such as .com, .gov, .edu, .org, and .net, marks a significant turning point. With these domains now signed—a prerequisite for enabling DNSSEC across the Internet—the public DNS infrastructure is ready to support widespread adoption of DNSSEC. In many cases, the drivers to adoption will be governmental, regulatory, and industry security mandates. However, the protections offered by DNSSEC should also convince organizations to adopt it as a way to protect their customers and valuable online assets, information, and reputation. For organizations with two or more data centers, a next logical step might be to combine the benefits of DNSSEC with global traffic management to achieve enhanced application availability and disaster recovery.

Delivering applications intelligently across multiple data centers

To help ensure high levels of application performance, security, and availability, Dell has incorporated the F5 BIG-IP Global Traffic Manager (GTM) system in its portfolio of enterprise solutions that include technology from Microsoft, VMware, Oracle, SAP, and others. GTM is a wide-area load balancer that offers support for DNSSEC through a license-key–enabled software module. Both the load balancing...
Implementing flexible configurations and best practices for wide-area load balancing

F5 BIG-IP Global Traffic Manager (GTM) can be deployed in three modes: authoritative screening (see Figure A), authoritative slave, and delegation (see Figure B). Authoritative screening is designed to deliver a comprehensive feature set and easy management and deployments of Domain Name Service (DNS) Security Extensions (DNSSEC) for the entire DNS infrastructure. It also provides DNS optimizations such as DNS load balancing and F5 iRules® event-driven scripting language. However, authoritative screening requires more changes to existing DNS systems during installation than does delegation mode.

Authoritative slave mode is similar to authoritative screening but incorporates zone transfers and a local configuration of Berkeley Internet Name Domain (BIND) on the GTM devices. Authoritative slave mode allows GTM to answer all incoming requests and administrators to manage DNS resource records on a separate device. In authoritative screening mode, the F5 device receives all DNS requests and checks for a wide IP match. If it finds a match, GTM handles the request by checking for a persistence record. If it finds one, GTM hands out that record; if it does not find one, GTM selects the pool and virtual server within the pool.

If it does not find a match, GTM passes the request to the standard DNS subsystem. By checking and rewriting responses, GTM can provide global server load balancing (GSLB) to almost all DNS record types, including service (SRV), mail exchanger (MX), and text (TXT).

Delegation mode offers a simplified way to deploy GTM into existing DNS environments, but it has a reduced feature set and requires additional administration. Standard DNS receives the requests and uses canonical name (CNAME) records to redirect the requests to GTM. Therefore, the client DNS request incurs the additional overhead of two DNS requests to resolve a query.

To maximize using available features, organizations should deploy GTM version 10.2 or later, using authoritative screening mode when possible. Other best practices include the following:

- Enable DNSSEC for both GTM and standard DNS systems to protect zone data against cache poisoning, man-in-the-middle attacks, and other DNS vulnerabilities. Enable Network Time Protocol (NTP) on the DNS infrastructure as part of DNSSEC deployment.
- Select dynamic load-balancing methods to take advantage of metrics such as round-trip time, hop count, and packet loss.
- Help to ensure a complete set of path metrics by deploying BIG-IP systems, such as BIG-IP Local Traffic Manager (LTM), GTM, and other F5 add-on software modules—in each data center worldwide.
- Streamline deployment using F5 deployment guides, which provide detailed procedures for configuring F5 devices with a wide variety of applications.*
- Leverage the Quova IP geolocation database for making intelligent, load-balancing decisions based on local DNS (LDNS) source address.

Authoritative screening mode is also recommended for larger environments.

* For a comprehensive list of F5 deployment guides, visit bit.ly/55NqGq.
and DNSSEC features run on the same BIG-IP system. GTM implements the DNS protocol, including DNSSEC, and extends DNS functionality to provide high-availability capabilities necessary in multi-data-center environments. Consequently, these DNSSEC protections and GSLB features enable organizations to reliably direct users to the closest or best-performing data center, provide seamless disaster recovery, and route client traffic based on quality of service or business criteria.

**Configuring Global Traffic Manager**

GTM supports three deployment configurations: two authoritative screening modes and a delegation mode (for more information, see the sidebar, “Implementing flexible configurations and best practices for wide-area load balancing”). While the authoritative modes provide more features than the delegation mode, the latter mode is a less disruptive way to introduce F5 to existing DNS environments.

GTM configuration comprises the different components that make up the physical and logical elements of the network. Physical objects include data centers, servers, virtual servers—combinations of an IP address and a port number—and links—physical connection to the Internet. Logical objects include wide IPs and pools—groups of virtual servers to be load balanced. Wide IP, the key configuration object in GTM, maps a fully qualified domain name (FQDN) to one or more pools.

The devices operate within a single managed cluster, or sync group, that uses the F5 iQuery™ encrypted communications protocol (see Figure 1). Changes that are made on one unit are replicated to other units in the sync group. Each unit receives name resolution requests from the local DNS (LDNS) server and directs client traffic to the best-available resource by responding to the DNS request with the associated IP address. If DNSSEC is requested, GTM signs the response before sending it to the LDNS.

**Determining the appropriate efficient resource**

GTM can use topology-based load balancing to inspect a client’s IP address and determine the best-available resource. Static load balancing methods include round-robin and global availability, which provides active-standby data center traffic distribution. Dynamic load balancing methods can incorporate the IP geolocation database based on Quova, proximity-based routing, and metrics. Persistence, or stickiness, enables clients to maintain connections to the same data center.

Monitors check the health, availability, and performance of global resources such as data centers and virtual servers. The monitors query the local BIG-IP systems to assess and report the status back to GTM, providing a detailed view of the conditions between the data center resource and the LDNS.

Probes monitor any path that is not already reported through the iQuery protocol. The metrics collected include round-trip time, packet loss, and hop count. These metrics help GTM decide on the best path available and avoid high-latency links. Metrics are then broadcasted to the cluster so that all members have consistent data.

Distribution of the probing tasks to other BIG-IP devices is one of the strengths of the GTM integrated approach. Assigning these monitors to a pool that contains BIG-IP devices results in additional external verification of resources and the network paths used.

**Enabling the full potential of multiple data centers**

The year 2011 brings key milestones for Internet security, including the successful deployment of DNSSEC on many DNS top-level domains, such as .com. Related advances in the F5 BIG-IP GTM enable GSLB to be deployed in combination with DNSSEC, creating an extremely reliable and flexible global traffic-management system. Solutions built on a foundation of Dell hardware, software, and services and F5 BIG-IP GTM with DNSSEC can keep end users connected to the most-available and best-performing application resources in a multi-data-center environment.

**Authors**

Andrew Walker is a solutions design engineer at F5 Networks focused on Dell Global Infrastructure Consulting Services.

Fred Johnson is a partner engineer at F5 Networks dedicated to Dell Labs.