Dynamic Service Delivery with Intelligent DNS

Service providers require a high-performing solution for DNS services with DDoS and security protections. At the same time, they need an available and resilient Intelligent DNS solution for their authoritative DNS requirements that leverage additional security and flexibility through technologies like GSLB and DNSSEC.

White Paper

Introduction

The Domain Name System (DNS) is arguably the technical powerhouse of the Internet. It is also one of the most important components in an operator's networking infrastructure. An operator's DNS services are the first point of contact for subscribers, and they drive the internal networks for the operator themselves. These services not only manage communication service delivery and access but also enable a redundant architecture to ensure high availability and quality user response time.

Several factors—new value-added services, long-term evolution (LTE) 4G networks, and innovations like VoLTE, NFV, and SDN—will create a flood of packet-based traffic, driving the demand for faster, more available DNS. On any given day, a single web page can consume 100-plus DNS queries from active content, advertising, and analytics. In the past five years, the volume of DNS queries has more than doubled, increasing to an average daily query load of 114 billion by the third quarter of 2014. More than four million domain names were added to the Internet in the third quarter of 2014.[1] Future growth is expected to occur at an even faster pace as more cloud implementations are deployed.

Even the web applications themselves are contributing to DNS/HTTP query growth as they become increasingly more complex. If DNS goes down, most web applications will fail to function properly, affecting subscriber experience. Meanwhile, DNS continues to be a tempting target for attackers, and a distributed denial-of-service attack can affect all external data center services.

In this environment—dealing with millions of service names and IP addresses, along with growing IPv6 deployments—it's now more critical than ever for operators to enable dynamic service-delivery infrastructure for managing and securing the impending flood of DNS traffic.

Enabling a dynamic service-delivery infrastructure

Creating a dynamic service-delivery infrastructure based on DNS will require a tremendous amount of real-time management, stability, and room to grow. The F5® Intelligent DNS reference architecture provides an optimal way to respond and scale to DNS queries. It takes into account a variety of network conditions and situations to distribute application requests and application services based on subscriber policies, data center conditions, network conditions, and application performance.

Delivering continuous availability to subscribers

The F5 Intelligent DNS for Service Providers reference architecture helps ensure that applications and services are continuously available to subscribers. 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 the efficient response of DNS queries. DNS Express simplifies the DNS query-response process and significantly improves DNS architecture performance and response times.

DNS is a critical technology to enable Internet access. Service providers need a robust DNS infrastructure that can handle the demand of their expanding subscriber pool. With DNS Express, a single F5 VIPRION® chassis can handle more than 20 million DNS responses per second—almost 100 times the capacity of a typical BIND DNS server.

To enhance the availability, BIG-IP GTM supports hardware and software failover capabilities to ensure the ability to deliver DNS responses. For global availability, BIG-IP GTM supports IP Anycast utilizing a single IP address for the DNS infrastructure that relies on ECMP routing to deliver the DNS queries to the most appropriate DNS server.

Ultimately, the DNS infrastructure is designed to provide access to the content and applications on the network. This requires a dynamic and intelligent DNS system that can provide the appropriate address response for the subscriber based on network and application health and availability. BIG-IP GTM delivers advanced global server load balancing (GSLB) technologies to dynamically identify and deliver the best application address to the DNS request based on multiple factors including availability, latency, session load, and other parameters.

Remaining secure

All BIG-IP devices are ICSA-certified network firewalls, and by intelligently evaluating the reputation of Internet hosts, BIG-IP can prevent attackers from compromising available resources or otherwise disrupting business functions and services. DNSSEC can be enabled for whenever a secure DNS infrastructure is required.

Key benefits

- Enable 4G/LTE subscriber growth through faster DNS responses
- Better manage existing traffic to DNS server infrastructure with BIG-IP
- Enhance performance through transparent caching, offloading DNS infrastructure
- Reduce DNS servers by offloading DNS infrastructure
- Gain high performance DNSSEC validation, offload DNSSEC computations, and consolidate services
- Proactively manage DNS client traffic for greater availability and stability

The F5 Intelligent DNS solution incorporates an ICSA-certified firewall and DNS services on a single platform—preventing firewall bottlenecks and scaling to over 20 million query RPS. This solution is lower in both OpEx and CapEx while delivering much higher performance and security protection. Other solutions require substantially more resources to accomplish the same results. In additional, operators can greatly reduce the constant patching of servers that many of today's DNS solutions require since the F5 Intelligent DNS solution does not rely on open source BIND.

DNS is the most frequently attacked network technology because of both its importance in matching IP addresses to names and its general openness as a technology that was created over 30 years ago. DDoS attacks are a daily occurrence, and service providers are one of the first targets when DNS infrastructure is attacked. Because DNS has a basic network footprint with the typical DNS query consisting of one packet for the request and one packet for the response, it is often more efficient to absorb the volumetric DDoS attack than to identify and differentiate the traffic. Ultimately, the service provider wants the delivery of DNS responses to continue unabated.

For those times when further validation is needed, BIG-IP GTM also supports the inspection of the DNS requests to determine whether the DNS query has properly formatted fields and appropriate content. BIG-IP GTM has advanced F5 iRules® programmability to customize the inspection and validation of any and all DNS communications.

Scaling on demand

To address DNS surges and DNS DDoS attacks (which can easily exceed typical DNS rates), operators have traditionally added more DNS servers, leaving them with unutilized equipment when spikes in demand halt. This costly solution also often requires manual intervention for changes.

In addition, traditional DNS servers require frequent maintenance and patching, primarily for new vulnerabilities. Rather than purchasing additional DNS infrastructure to combat surges, one can simply install a BIG-IP device in the network to replace the existing DNS infrastructure. The BIG-IP engine handles application requests at very high levels and responds to all DNS queries. 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 service availability or access to the critical applications.

F5 provides open APIs through F5 iCall™ and F5 iControl® to support the external management of the DNS infrastructure. The orchestration capabilities through these APIs enable the DNS infrastructure to support the cloud technologies necessary for dynamic scaling of the infrastructure. The F5 DNS infrastructure enables the agility and elasticity of the cloud infrastructure.

Agility opens the door to adding and removing services quickly and efficiently. Service providers need to become more dynamic and to deliver new applications and services in order to stay competitive in this rapidly changing environment. Dynamic DNS services are required in order to enable the availability of these solutions in an efficient and programmatic method.

Elasticity is the on-demand resourcing within the cloud infrastructure. Service providers need the flexibility to add and remove resources based on service demand. The load on these resources is distributed and directed to different server farms and data centers by DNS. The DNS infrastructure must be dynamic and deliver responses based on current demand and on an understanding of which destination is best suited to the specific subscriber request.

Conclusion

Today, DNS needs to be flexible and dynamic to adapt to the existing network and application conditions and to deliver the best experience for subscribers and their content. With Intelligent DNS services, service providers can drive greater reliability, availability, flexibility, and security within the DNS infrastructure. At the end of the day, this means greater operational consistency, better quality of experience, and the cost control necessary to meet spikes in demand while also securely pushing out new services to subscribers.

[1] http://www.verisigninc.com/assets/domain-name-report-january2015.pdf

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