



F5 White Paper

# High-Performance DNS Services in BIG-IP Version 11

To provide high-quality user experiences on the Internet, networks must be designed with optimized, secure, highly available, and high-performance IP services. Domain Name System (DNS) is one of the most difficult, but important, IP services to optimize and secure. DNS Services in F5 BIG-IP version 11 provides an intelligent DNS architecture that delivers high performance and scalability while negating the effects of network attacks.

**by Ray Vinson**

Sr. Technical Marketing Manager, Service Provider Market



# Contents

<b>Introduction</b>	<b>3</b>
<hr/>	
<b>High-Performance DNS</b>	<b>3</b>
<hr/>	
<b>DNS Security</b>	<b>4</b>
<hr/>	
<b>IP Anycast</b>	<b>5</b>
<hr/>	
<b>Conclusion</b>	<b>7</b>



## Introduction

With an increasing number of devices, applications, and services on the Internet, it's becoming more difficult to achieve network and application response times that deliver a quality user experience. This problem is not only a bandwidth issue—it's also closely tied to network and infrastructure architecture. Properly managing IP resources such as IP allocations, optimized security architecture, IPv4 to IPv6, and Domain Name System (DNS) is essential to optimizing the user experience of all multimedia IP applications. This challenge is a core issue for both enterprise and service provider networks. Wireless service providers are especially challenged by increased demands for services and applications, which they must meet while also deploying new 4G networks such as WiMAX and Long Term Evolution (LTE).

DNS is one of the key elements in the network that delivers content and applications to the user. However, DNS also manages a distributed and redundant architecture to ensure high availability and quality user response time. Due to the crucial role it plays in a network, DNS is also a high-value security target. Security attacks can flood DNS servers to the point of failure. To prevent this, a high-performing, secure DNS architecture and DNS offload capabilities must be integrated into the network. F5 DNS Services, offered in version 11 of F5® BIG-IP® Global Traffic Manager™ (GTM), provides DNS scale and high performance under DNS volume attacks and IP Anycast support in a high-performance DNS architecture. IP Anycast allows a single IP address to be advertised by multiple systems.

## High-Performance DNS

To achieve high-performance and secure DNS, the DNS architecture must be able to prevent attacks from having a significant effect, and it must be highly available and able to efficiently handle DNS requests. F5 DNS Services is designed to efficiently handle DNS requests and securely manage security services.

The architecture of F5 DNS Services is optimized by the F5 DNS Express module. DNS Express manages authoritative DNS queries by transferring zones to its own RAM. In this architecture, F5 DNS Services 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. DNS Express simplifies a single processing instance of the DNS query to significantly improve the performance of F5 DNS Services. With DNS Express, each individual core of each BIG-IP device can answer approximately 125,000 to 200,000 requests per second.

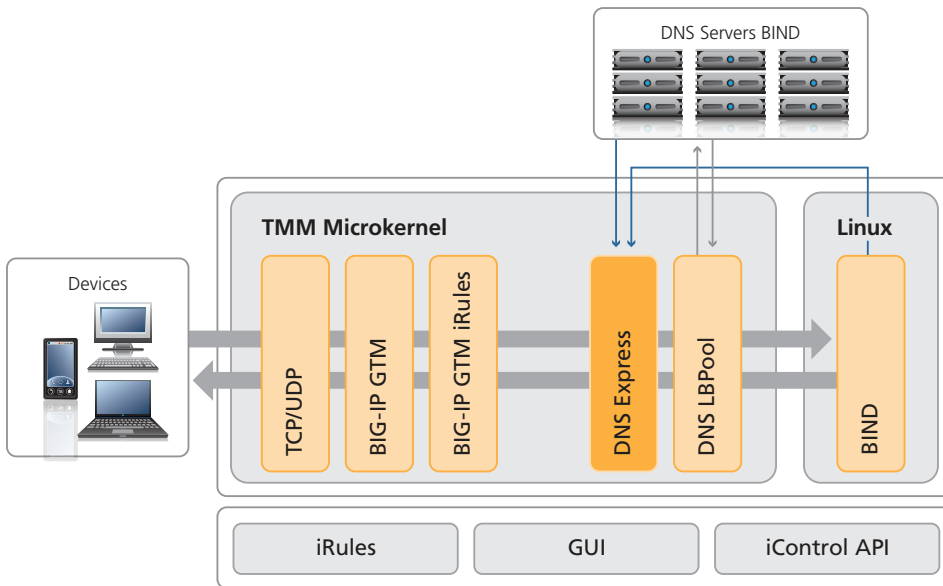


Figure 1: DNS Services is a high-speed and highly scalable architecture

## DNS Security

DNS is a key part of initial requests for Internet transactions, so organizations are at particular risk for hijacked DNS sessions or denial of service (DoS) to DNS.

The cost of denial of service attacks	
Estimated losses due to attacks in 2009 (U.S.)	\$5.6 billion
Estimated lost business from DoS attacks per hour	\$636,000
Estimated cost of a 24-hour outage for:	
Brokerage Firm	\$156 million
Cisco	\$30 million
eBay	\$4.5 million
Airline	\$2.1 million
Estimated cost of lost user access, per user, from one medium-grade attack	\$23,000

Table 1: Financial effects of DoS and DDoS attacks

These attacks have led to the development of DNS Security Extensions (DNSSEC) standards, which secure DNS requests and ensure that they are being answered by the proper DNS server. DNSSEC adds the authentication and signed responses that identify the DNS servers, which ensures that DNS responses come from a known



and authorized DNS server. Uptake of the DNSSEC standards was initially slow, but has significantly increased since January 2010.

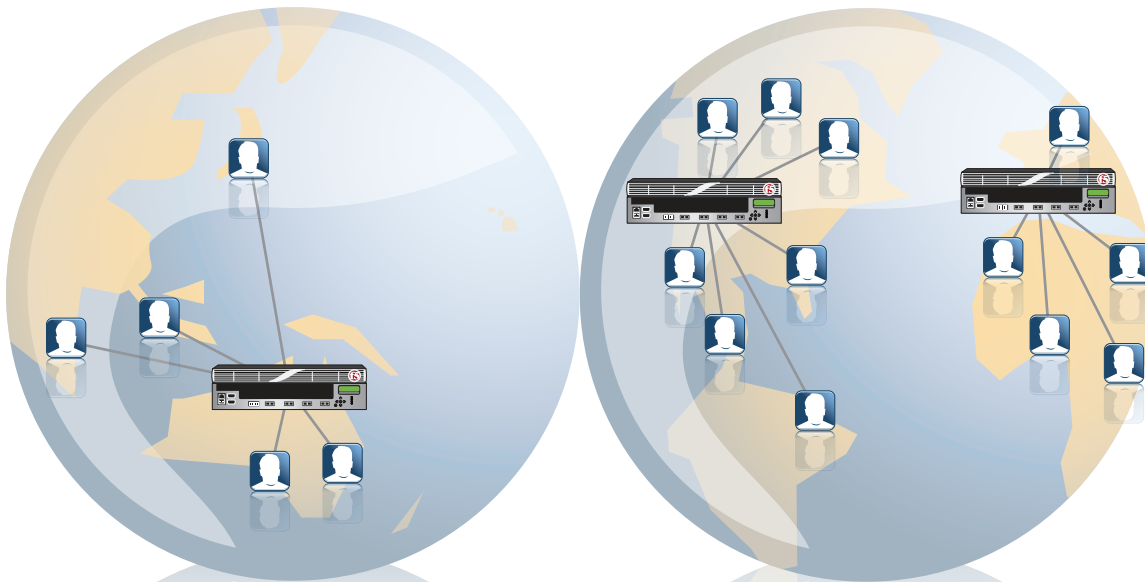
The challenge with DNSSEC, along with delayed Internet uptake of the standards, is providing these security layers without creating latency and/or a network bottleneck. One characteristic that adds to this difficulty is that DNSSEC increases the size of DNS queries by approximately 10 times. F5 DNS Services provides DNSSEC as an integrated DNS solution along with DNS load balancing and IP Anycast to prevent latency and performance bottlenecks.

Another major issue with DNSSEC is that it complicates the ability to perform global server load balancing (GSLB). DNSSEC requires that a content hash and a signature be returned with every DNSSEC request. If there is only one IP address for each name or name type, this hash and signature combination is fairly simple. However, if there are multiple uses for IP addresses, (for example, one IP address for multiple types of entries, or a GSLB configuration that uses multiple IP addresses for each name entry) then the hash and signature combinations become extremely complicated. One way to solve this problem is to pre-create a signature for every possible IP, name, and name type combination; however this is not only extremely complicated, it is unmanageable as the network grows and changes. F5 DNS Services solves this problem by creating the hash and signature in real time, after the DNS query is processed and when the DNS response is being generated—providing a highly scalable and manageable DNSSEC solution.

## IP Anycast

Scaling Internet servers and making them redundant usually results in multiple servers for single URLs. When administrators create DNS entries for these fully qualified domain names (FQDNs), they enter multiple IP addresses as either A records for IPv4 or multiple AAAA records for multiple IPv6 records. DNS responses typically include either the list of appropriate IP addresses or just the first address listed for the FQDNs.

F5 DNS Services use IP Anycast, also called Route Health Injection (RHI), to determine the closest and most available Internet server address to return for each DNS request. This methodology increases reliability, performance, and security.



**Figure 2: Replicate DNS across multiple devices with single name server IP**

IP Anycast geographically distributes DNS responses based on the least number of hops to the nearest Internet server. This supports geographic redundancy of Internet services. DNS Services uses the geographic distribution and determines the availability of the server to provide the best address to use as the DNS response. The result is a more efficient response for each DNS request.

The DNS Services method of using IP Anycast to return the nearest geographic address can also be used to support global load distribution across servers. By globally distributing responses, F5 DNS Services makes the responses from Internet servers more efficient, which improves response times to users.

Security attacks on DNS include both denial of service (DoS) and distributed denial of service (DDoS) attacks. One significant characteristic of DDoS attacks is that even though these attacks use millions of IP addresses, they still tend to be from identifiable geographic regions. The key to surviving any DoS or DDoS attack is to keep the network available to serve as many users as possible. An alternative method is to use a DNS cache to mitigate the attacks by having the target domain in the DNS cache; however this method is still susceptible to a multi-query and multi-target DoS attack. The IP Anycast module in F5 DNS Services enables organizations to isolate these geographic regions, and it helps avoid DDoS attacks.

IP Anycast, as implemented by DNS Services, provides scaling, redundancy (both local and geographic), and additional security. Scaling networks with IP Anycast simplifies IP address management, speeds deployments, and lowers the cost of IP network expansion.

## Conclusion

As IP traffic grows, and the number of IP devices increases, both enterprises and service providers must create secure, efficient, and high-performing DNS architectures. They are looking for solutions to manage traffic, increase response times, prevent latency, and provide an optimized quality of experience for their users.

For service providers, the challenge in deploying an all-IP, 4G network such as LTE or WiMAX, is to maintain the quality of experience of the 3G network while deploying 4G technology. This means that from the subscriber's point of view, the network is at least as reliable as previous technology, while offering a better experience, new technology, and new services. This maintained reliability includes voice and data reliability, security, and network response.

Enterprise and e-commerce networks require high-performance response from their networks. This quality response is threatened by the security attacks on DNS. To prevent this, networks must be able to mitigate the effects of these attacks by efficiently scaling the DNS and incorporating security measures that help prevent attacks, but don't affect performance. F5 DNS Services utilizes DNS Express, IP Anycast, and DNSSEC to implement high-performance, easy-to-scale, and secure DNS services.

For all networks, increases in both traffic and data size will increase the use and required scale of DNS. The only effective method of addressing the scale and complexity of this problem is to deploy a smart, secure, and high-performing DNS solution. F5 DNS Services provides this through a comprehensive, scalable solution with smart integration of IP Anycast and DNSSEC in a high-performance architecture.

