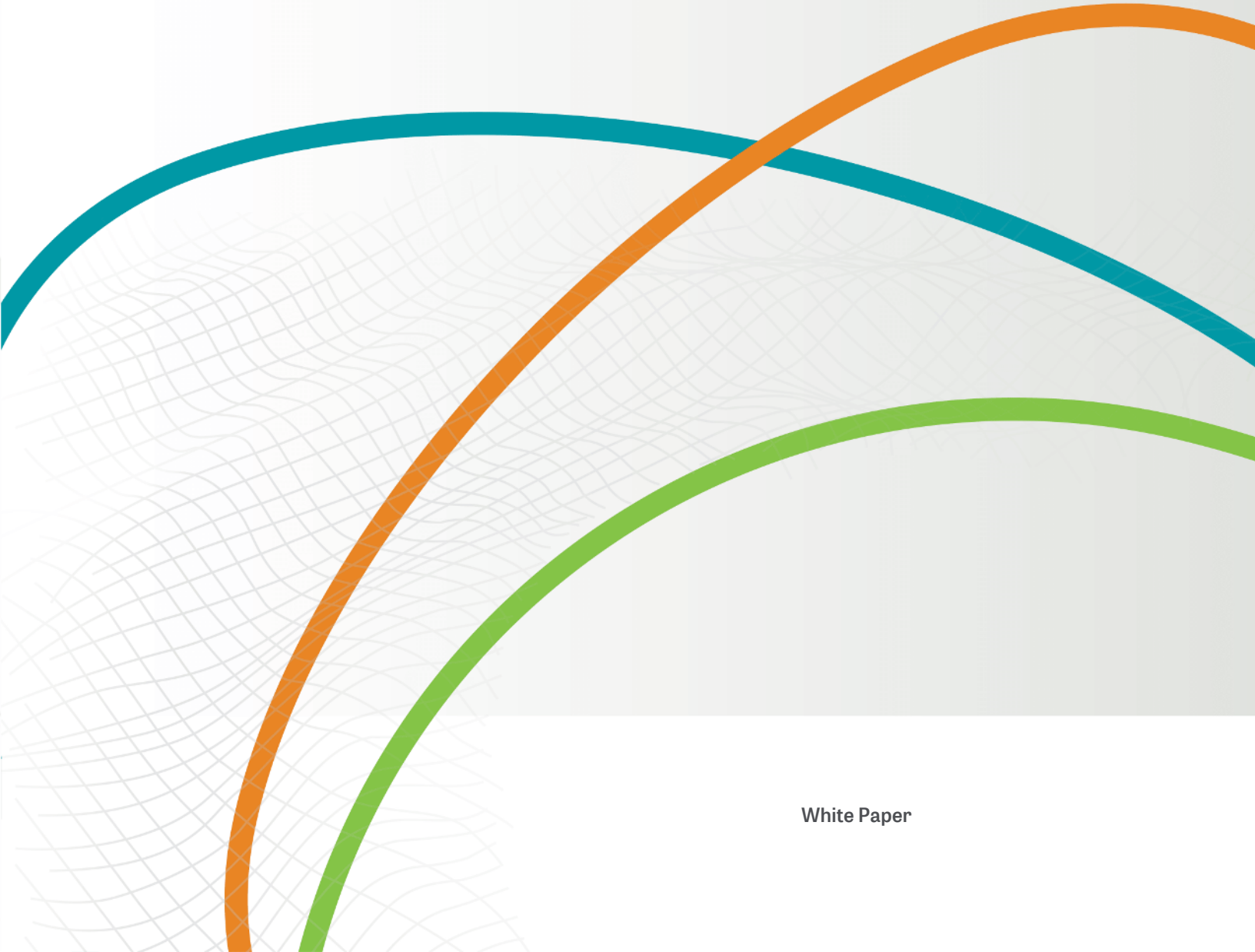
F5 and Infoblox DNS Integrated Architecture

F5 and Infoblox DNS Integrated Architecture



White Paper

Prerequisite Knowledge

This document assumes the reader already has general familiarity with standard DNS architectures as well as a basic understanding of the workings of DNSSEC and how DNSSEC is normally deployed. Additionally, this document assumes a general understanding of global server load balancing techniques, functions, and features. There are many resources available to learn about DNS and DNSSEC. The Infoblox and F5 websites respectively contain more information regarding the features, implementation, and detailed configuration of the products.

This tech guide provides high-level architecture covering three possible architectures for integrating F5 and Infoblox appliances. Additionally, this document provides functional information regarding real-time DNSSEC to give a better grasp of the various architecture implementations. There are many ways to architect an organization's DNS system and many configuration tricks. This document is not meant to be an exhaustive study of all the possible ways to architect an integrated DNS solution, but rather to illustrate the most useful and common architectures. Readers of this document will be able to gain insight into what comprises an F5 and Infoblox integrated architecture, and begin planning for a BIG-IP GTM and Infoblox DNS deployment. Please refer to the respective manuals for the F5 BIG-IP GTM and Infoblox appliances on each organization's website for detailed configuration information.

Terminology

Several abbreviations, general DNS, and product specific terms are used throughout this document.

Local domain name server (LDNS) - A client recursive DNS server. Most DNS queries originate from an LDNS server rather than a client.

Fully qualified domain name (FQDN) - This refers to a complete DNS name that includes both the host and domain (for example, www.example.com).

Global server load balancing (GSLB) - A generic term referring to a collection of intelligent DNS techniques and methods used to provide the best possible IP address answer for a given record query.

BIG-IP Global Traffic ManagerTM (GTM) - An F5 product used to provide GSLB services. BIG-IP GTM manages traffic between application clients and data centers.

F5 BIG-IP Local Traffic Manager™ (LTM) - An F5 product used to provide load balancing and application delivery services for a particular web service or other application. BIG-IP LTM manages traffic in a data center or a group of servers.

Wide IP address (WIP) - An F5 product term for a fully qualified domain name representing a resource managed by BIG-IP GTM (for example, www.example.com or www.gtm.example.com).

Key signing key (KSK) - This is used to sign other keys including ZSKs.

Zone signing key (ZSK) - This is used to sign the zone's signature records.

Start of authority (SOA) - This specifies authoritative information about a DNS zone, including the primary name server, the email address of the zone's administrator, the zone's serial number, and several timers relating to refreshing the zone.

Canonical name record (CNAME) - A type of resource record in the Domain Name System (DNS) that specifies that the domain name is an alias of another, canonical domain name.

Address record (A-record) - Returns a 32-bit IPv4 address, most commonly used to map host names to a host IP address.

Mail exchanger record (MX record) - Maps a domain name to a list of message transfer agents for that domain; usually returns an A-record (for example, mail.example.com).

Introduction

Many organizations are looking for a complete DNS solution that will enable the best-of-breed features in DNS management, intelligent global server load balancing, performance, and security. Traditionally, there has been a gap between the easy management features offered by DNS appliance vendors and application delivery vendors focused on global server load balancing. This gap is evident in the new requirements needed to provide DNSSEC features that guarantee the authenticity of DNS responses, enabling a much more secure Internet environment. No single vendor is able to offer a complete solution. As market leaders in the application delivery market and DNS, DHCP, and IP Address Management (DDI) market respectively, F5 and Infoblox have teamed up to provide customers with a complete solution. This solution provides superior DNS management capabilities, flexible intelligent global server load balancing, high performance scalable DNS, and complete DNSSEC signing for all zones.

Overview of DNS Security Extensions

Many security experts, including Dan Kaminsky, Director of Penetration Testing at IOActive, consider DNS Security Extensions (DNSSEC) to be an essential tool in "sealing" DNS vulnerabilities and mitigating DNS cache poisoning attacks that undermine the integrity of the DNS system. DNS attackers are able to direct users to alternate sites enabling collection of credit cards and passwords, redirect e-mail, and compromise any other Internet application that is dependent on DNS. DNSSEC implements an automated trust infrastructure enabling systems to verify the authenticity of DNS information.

Unfortunately, DNSSEC adoption has been hampered by concerns over the operational complexity of provisioning encryption keys and the processing overhead required to sign DNS information. Prior to F5's innovative real-time signing capability, there were no options to secure the DNS responses from a global server load balancing system (GSLB). Organizations had to choose between deploying highly available intelligent DNS systems or securing their DNS infrastructure with DNSSEC.

The combined F5 and Infoblox solution addresses these issues with complementary solutions, bringing to market a fully integrated and complete DNSSEC solution including high performance DNS and GSLB functions, all supporting, signed DNSSEC data. This provides customers a scalable, manageable, and secure DNS infrastructure that is equipped to withstand DNS attacks.

> The lack of DNS security not only makes the Internet vulnerable, but is also crippling the scalability of important security technologies. DNSSEC offers the most feasible solution to a serious threat.
>
> —Dan Kaminsky, Director of Penetration Testing, IOActive

The solution is a combination of Infoblox purpose-built appliances that deliver highly reliable, manageable, and secure DNS services, with built-in, automated DNSSEC features, and F5 BIG-IP Global Traffic Manager™ (GTM) appliances optimized to facilitate real-time signing of DNS responses. Infoblox's DNSSEC features replace manual key generation and zone signing with a "one-click" process that automatically generates encryption keys, signs zone data, and distributes signed data to all Infoblox appliances that serve DNS data. F5 provides a Federal Information Processing Standard - (FIPS) compliant option to satisfy FIPS 140-2 requirements. Both F5 and Infoblox systems handle the National Institute of Standards and Technology (NIST) recommended key polices that are outlined in NIST Special Publication 800-81 Secure DNS Deployment Guide.

Real-time DNSSEC

F5's implementation of DNSSEC through patent-pending, real-time signing is a crucial architectural element in the F5 and Infoblox joint three architecture solutions. Standard implementations of DNSSEC assume a fairly static zone configuration that provides the same responses to a specific DNS query, whether an SOA, MX, or A-record. Changes to a zone's records are generally minimal. The zones are usually pre-signed with all the appropriate keys and hashing and stored in the same static zone files. Signing a large zone can take longer than thirty minutes depending on the size of the zone. Infoblox supports incremental signing that reduces the overhead associated with record information changes. Infoblox also provides market-leading, single-step DNSSEC signing and automated key management, making it easier to provide DNSSEC responses for a standard DNS zone.

The basic premise of global server load balancing (GSLB) is to provide the best answer for a particular resource based on information obtained from the requesting LDNS's IP address. There are many options and modes for deploying GSLB, including round trip time calculations, IP geolocation, dynamic server load, ratios, and resource monitoring. Since each LDNS server can receive a different answer for a given A-record request it is possible for the same LDNS server to receive different answers at different times. In general, GSLB services are incompatible with traditional DNSSEC implementations. DNSSEC specs were not designed with consideration of GSLB.

The F5 BIG-IP system of products operates on a universal, shared product platform called TMOS. TMOS intercepts the DNS request as it enters the system and remembers if the request was a normal DNS request or a DNSSEC request. TMOS then sends the request to the BIG-IP Global Traffic Manager (GTM) module for resolution. Assuming the request is the appropriate type, BIG-IP GTM processes the request, taking into account all the business rules, monitoring, and global load balancing features. BIG-IP GTM then passes the request back to TMOS. If the original request is for DNSSEC, TMOS signs the resource record set in real-time using high-speed cryptographic hardware and sends the response back to the LDNS server. This method also works well with standard DNS queries that are passed through to an Infoblox appliance. The cryptographic hardware and a special signature RAM cache of signatures enable TMOS to sign most queries in real-time, at high speed. However, for extremely large static zones containing no GSLB elements, using the traditional DNSSEC pre-signed method offers performance and resource utilization advantages. TMOS's intelligent architecture enables a DNS response that has already been signed to pass through, allowing for hybrid DNSSEC deployments specific to each zone. Normally, private keys are stored in a triple-encrypted key storage called the secure vault. Customers that require military-grade security can use hardware FIPS cards found on different F5 devices for private key generation and storage. These FIPS cards share the same configuration and can synchronize FIPS keys, maintaining full FIPS compliance even while being geographically separated.

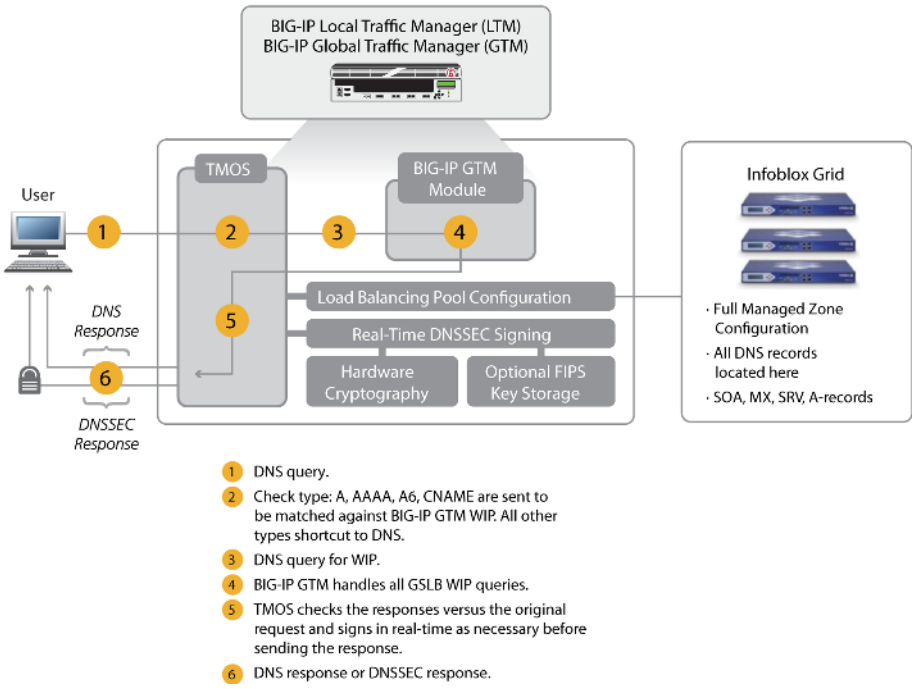


Figure 1: DNSSEC in real time with the F5 BIG-IP system and Infoblox Grid.

Configuring Real-time DNSSEC

It is a simple, three-step process to configure real-time DNSSEC signing:

1. Create a key signing key
2. Create a zone signing key
3. Assign those keys to the appropriate BIG-IP GTM-controlled subzones

The final, manual step is to export the public KSK and register it with the next-, higher-level zone authority

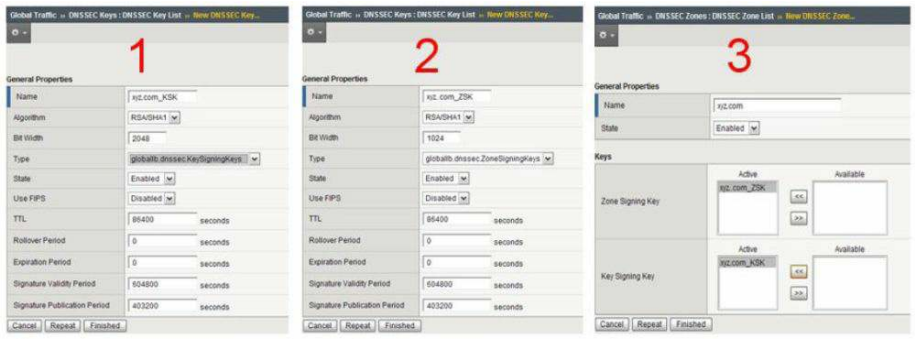


Figure 2: BIG-IP GTM configuration steps in the user interface.

Configuring Infoblox DNSSEC

Infoblox appliances support full, standard DNSSEC features. Infoblox has developed very intuitive tools. Default settings can be configured at the global grid level. The Infoblox management tools enable an easy, one-click DNSSEC upgrade of any zone to start providing DNSSEC responses. The final, manual step is to export the public KSK and register it with the next, higher-level zone authority or independent trust anchor.

Overview of F5 and Infoblox Architectures

There are several important points to consider when deploying a combined architecture:

- Authoritative systems
- Configuration hosting
- Zone updates
- Load balancing Infoblox appliances
- Service divisions between GSLB records and static zone records
- System aliasing using CNAME records
- Zone size and records types

The three architectures discussed in this document include:

1. Delegation
2. Authoritative Screening
3. Authoritative Slave

Delegation is the most common, simplest, and involves delegating a specific sub-zone that contains all the GSLB elements of the DNS architecture. In this scenario, a CNAME is used to redirect other names to one located in the delegated sub-zone. Authoritative Screening is more sophisticated and offers a highly integrated solution. It also offers greater scalability and protection of the Infoblox architecture. Using an Authoritative Slave architecture, DNS requests are processed on the BIG-IP GTM system, while the Infoblox appliance serves as the hidden primary for the zone. In addition to describing the general DNS architecture in this paper, there is a section for each architecture that discusses DNSSEC-specific options and deployment.

Delegation

The Delegation solution is recommended for organizations seeking a simple configuration with clear assignments of zones for standard DNS and GSLB services. In this example, the Infoblox appliance completely manages the top-level zone, example.com. The NS records point to the names and, indirectly, the IP address of the Infoblox appliances. BIG-IP GTM is authoritative for a subzone and handles all queries to that zone (for instance, gtm.example.com). All GSLB resources are represented by A-records in the GTM zone. A BIND name server running on BIG-IP GTM contains the subzone records. Host names in the top-level zone are referred to the GTM-controlled subzone using CNAME alias records. CNAME references can be from almost any other zone, including the subzone. More than one subzone can be delegated to and managed by GTM zone.

```
www.example.com  CNAME  www.gtm.example.com
mail.example.com CNAME  mail.gtm.example.com
```

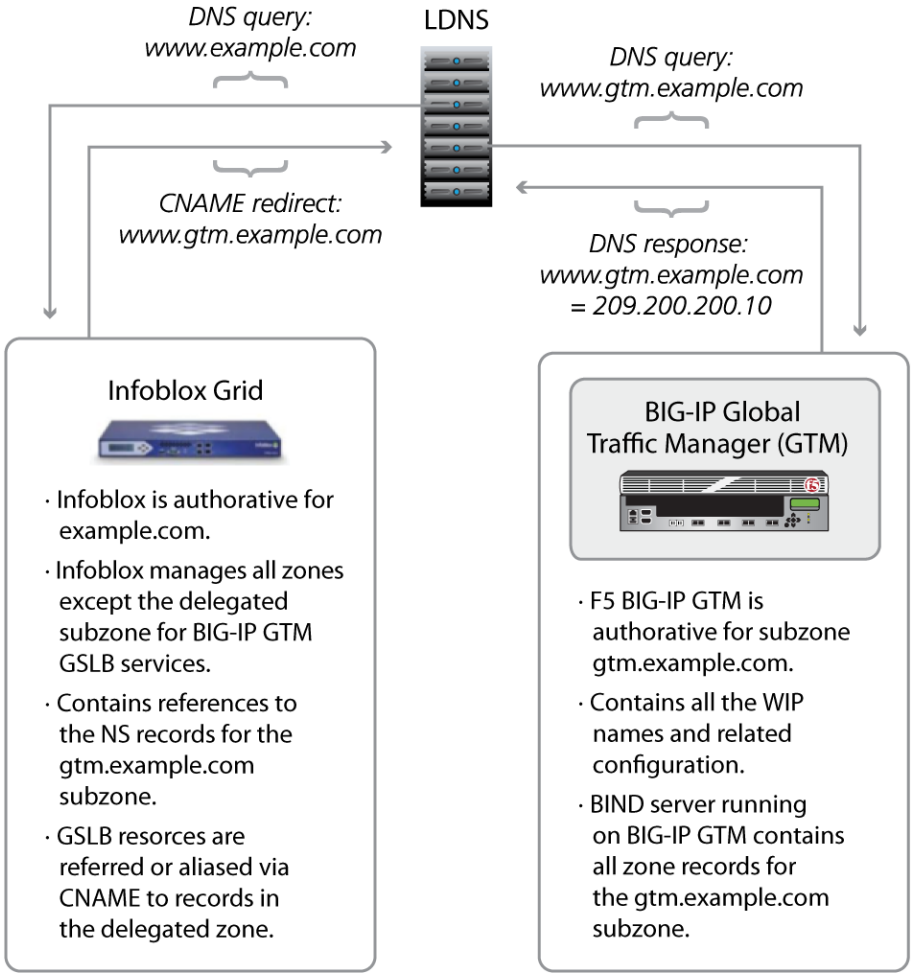


Figure 3: F5 BIG-IP GTM and Infoblox Grid manage their respective DNS zones in the Delegation architecture.

Shortcut Around Using CNAME Aliases

For high-profile, high-volume names (such as www.example.com), the use of a CNAME could cause an extra redirect and lookup, providing undesirable latency. A shortcut can be employed by creating and delegating a subzone to the BIG-IP GTM device. This shortcut only works for a single name in each subzone; however, any number of zones can be delegated in the same manner. The subzone shortcut removes the need for a CNAME redirect while still using a Delegation architecture. In this example, a subzone called www.example.com is created and delegated to the BIG-IP GTM device. The zone configuration on BIG-IP GTM includes the normal NS records, as will the higher-level example.com zone, but the zone will only contain one host record. The BIG-IP GTM WIP is configured to match that of www.example.com and always provides GSLB services for www.example.com.

DNSSEC Configuration in Delegation Architecture

The DNSSEC configuration is very simple when using a delegated zone architecture. Top-level, standard DNS zones (such as example.com) are managed and signed by the Infoblox appliance. All other standard DNS zones or subzones managed by Infoblox are signed similarly. All standard DNS queries in zones managed by Infoblox can respond with DNSSEC responses. All GSLB queries which are sent to the GTM subzone are signed in real-time by TMOS after BIG-IP GTM decides which answer is the best for each specific client.

Delegation Summary

The Delegation architecture is easy to implement for DNS and DNSSEC responses. The downside is that the Delegation architecture also requires maintaining the subzone configuration on the BIG-IP GTM device itself. Some organizations find that using CNAME records is difficult to manage on a larger scale. Other organizations are sensitive to latency and, therefore, would prefer not to use CNAME records at all. The subzone shortcut provides a solution to avoid CNAME records but does not scale as a general purpose solution. The Delegation architecture is a better fit for organizations with a smaller number of zones and resources using the GSLB features, and with lower overall DNS performance requirements.

> The combination of F5's and Infoblox's appliances provide enterprise customers an opportunity to build authoritative DNS infrastructure without giving up either global server load balancing or DNSSEC—that's a clear value-add to performance and security.
>
> —Cricket Liu, Vice President of Architecture, Infoblox

Authoritative Screening

Authoritative Screening is the most powerful, flexible, and integrated of the three solutions. Deploying the Authoritative Screening architecture running version 10.1 of BIG-IP GTM requires licensing both a BIG-IP Local Traffic Manager™ and BIG-IP GTM. BIG-IP GTM running version 10.2.0 will enable this configuration to work correctly with only BIG-IP GTM licensed. With version 10.2 the standalone BIG-IP GTM will also be able to use this architecture.

The Authoritative Screening architecture enables BIG-IP GTM to receive all DNS queries, managing very high-volume DNS by load balancing requests to a pool of Infoblox appliances. In addition, the Authoritative Screening architecture seamlessly provides all of the benefits of intelligent GSLB services. The BIG-IP GTM listener IP address should be configured in an NS record authoritative for the zone, not as a delegated subzone. When a DNS query is received, TMOS will check the record type. If the type is an A, AAAA, A6, or CNAME request, it will be sent to BIG-IP GTM. BIG-IP GTM will check each request and response, looking for a match against the wide IP (WIP) list of FQDN names. If there is a match, BIG-IP GTM will perform the appropriate GSLB functions and return the best IP address appropriate for the requesting client.

If the DNS request does not match the WIP list, BIG-IP GTM will pass the request to a pool of Infoblox appliances. Load balancing requests to a pool of Infoblox appliances provides an additional layer of scalability and availability, increasing the query performance and ensuring optimal uptime of DNS services.

The BIG-IP GTM unit is configured with a standard DNS listener on port 53 for both TCP and UDP, and uses the external IP address referenced in the SOA-record for ns1.example.com. In the virtual server configuration, create a pool that contains several Infoblox appliances, each with their own separate IP address. The Infoblox appliance can be fully authoritative for the zones for internal clients. However, all external NS records for the top-level zone (such as example.com) should point only to the external IP address allocated to the F5 BIG-IP device.

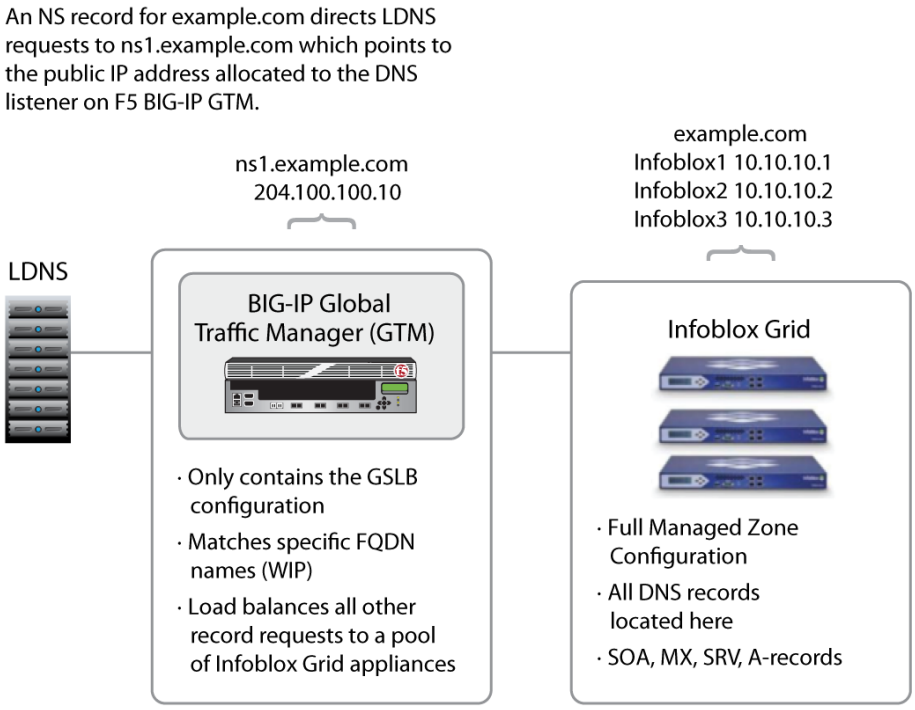


Figure 4: In the DNSSEC Authoritative Screening architecture, BIG-IP GTM load balances DNS requests to a pool of Infoblox appliances.

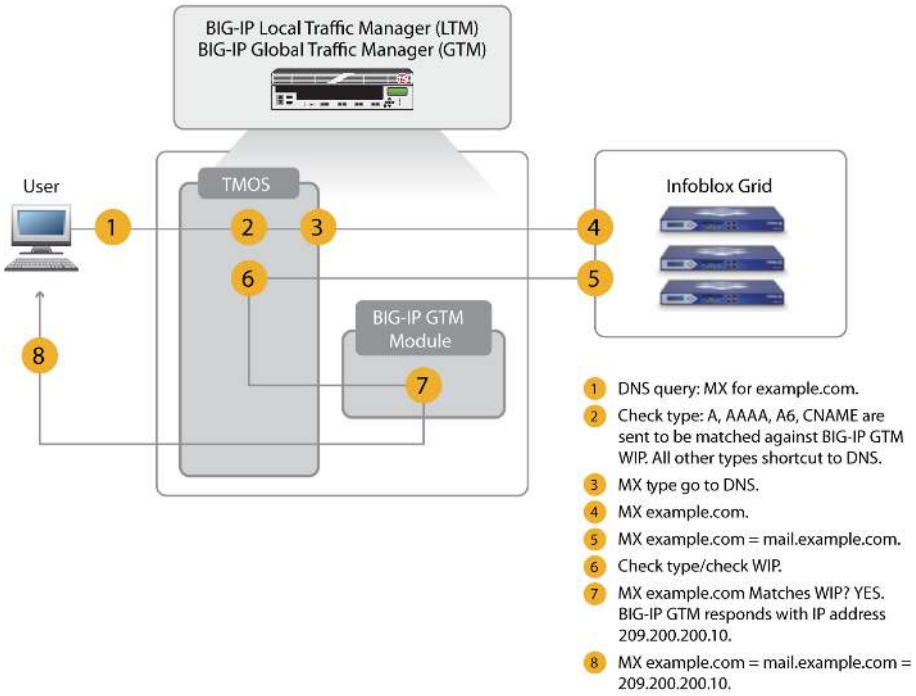


Figure 5: Authoritative Screening request flow for a mail server record.

A good illustration of the integrated capability of a BIG-IP GTM screening architectures is when an MX record is requested. BIG-IP GTM only has the WIP list and configuration for processing the WIP queries. All zone records are maintained on the Infoblox appliances. The requests flow through the system in the following steps:

1. TMOS receives the MX query for example.com. TMOS first checks the record type. Only A, AAAA, A6, or CNAME requests are sent to BIG-IP GTM. All other record types are immediately sent to DNS. Because the request in this example is for an MX record, TMOS sends the query directly to the Infoblox appliances using the configured ratio load balancing method.
2. The Infoblox appliance responds, indicating that the MX record for example.com resolves to A-record mail.example.com.
3. TMOS sends the request to BIG-IP GTM to check if there is a match for a WIP.
4. BIG-IP GTM detects a match in the WIP list for mail.example.com and processes the query according to the configuration for mail.example.com. In this case, BIG-IP GTM uses IP geolocation to find the closest mail server for the client and responds with the best IP address.
5. TMOS responds to the original MX record request—mail.example.com—and rewrites the A-record answer with the IP address that has been globally load balanced by BIG-IP GTM.

6. If DNSSEC was originally requested, the response will be signed in TMOS before it's sent to the requesting LDNS.

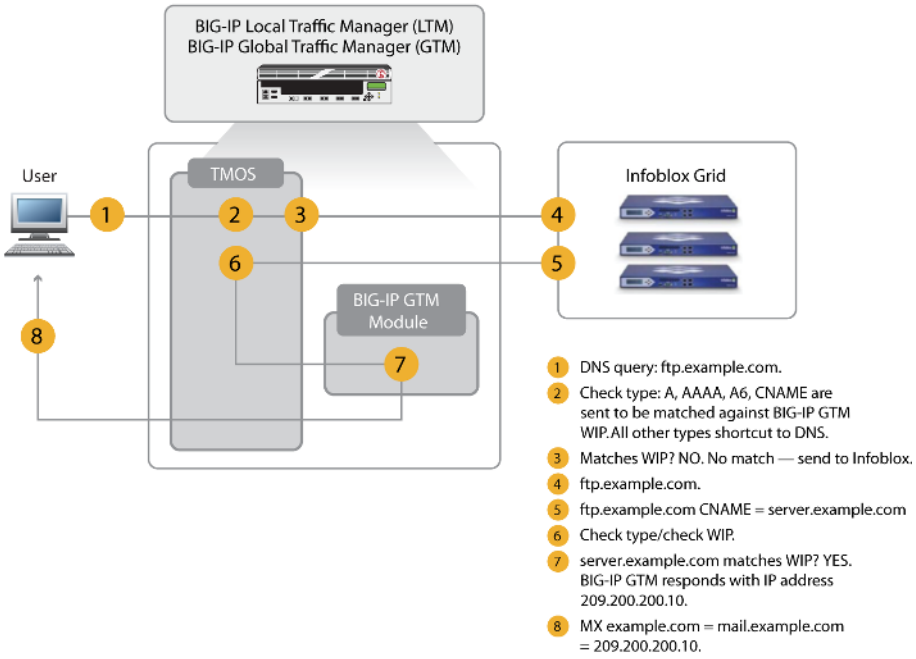


Figure 6: Authoritative Screening request flow for a CNAME record when the initial record type is an A-record.

An illustration of the request flow when the initial record type is an A-record.

1. The initial query is for ftp.example.com. TMOS first checks the record type and since it is an A-record, passes the request to BIG-IP GTM to see if it is a match against the WIP list.
2. If ftp.example.com is a match for a WIP, BIG-IP GTM handles the processing and sends the response back to TMOS. In this case, ftp.example.com is not a match, so the request is sent to DNS.
3. The request is load balanced and processed by the Infoblox appliance in exactly the same way as the MX record illustration.
4. When the CNAME response is returned from Infoblox containing an A-record, server.example.com, TMOS sends the response to BIG-IP GTM to check if server.example.com is a match for a WIP.
5. BIG-IP GTM then matches server.example.com as a WIP, processes the request, and sends the response back to TMOS.

DNSSEC Options for Authoritative Screening

It is possible for TMOS to do the DNSSEC signing in real-time and on demand, for all zones. Any zone containing dynamic GSLB names in the BIG-IP GTM configuration must be signed by TMOS, in real time.

If there are standard DNS zones that do not contain any BIG-IP GTM-configured WIP names, it is possible to use the native Infoblox DNSSEC capabilities to sign those zones. In this hybrid configuration, BIG-IP GTM will detect a DNSSEC signed response and pass it through to the requesting LDNS server without modification or re-signing. This hybrid configuration requires different KSKs and ZSKs for Infoblox-signed zones.

Advanced IP Anycast Configuration

With this architecture several F5 devices can be deployed at different locations around the world using the same external IP address. The technique is often referred to as IP Anycast. F5 calls this feature route health injection (RHI). Each F5 device advertises the same IP address(es) to the next hop routers. The routing system routes requests from LDNS servers to the closest BIG-IP GTM system. Using IP Anycast and the routing system to geographically distribute DNS queries can decrease DNS latency and provide some level of DNS denial of service (DoS) protection.

Authoritative Screening Summary

The screening architecture enables intelligent DNS and global server load balancing techniques for any record type that resolves to an A-record. This architecture offers the best of all worlds, with the ability to support and manage all DNS records on the Infoblox appliance while simultaneously providing load balancing and intelligent DNS functions for any particular service or site. This architecture avoids a designated zone for load balanced names and eliminates the use of CNAME redirects. BIG-IP GTM screens the DNS traffic sent to the Infoblox appliances and only intercepts the requests and responses when they match a name designated in the BIG-IP GTM configuration. BIG-IP GTM only manages the GSLB-specific WIP configuration information. The Infoblox appliance maintains and manages all zone records. There are several ways to implement DNSSEC. One easy method would be to use real-time DNSSEC signing for all zones. Alternatively, an organization could choose to deploy a hybrid configuration with some zones being signed and managed by the Infoblox appliance. IP Anycast techniques can be implemented for advanced architectures providing better performance and DNS DoS protection. Other than being more complex to setup, the authoritative screening architecture provides many advantages with very few caveats.

Authoritative Slave

The Authoritative Slave architecture is very similar to the Authoritative Screening architecture. Both architectures deploy BIG-IP GTM as the external authoritative name server. The major difference is that all DNS requests are handled by BIG-IP GTM and not load balanced or passed to any Infoblox appliances. There is a standard BIND name server running on the BIG-IP GTM that attempts to answer any query not handled by BIG-IP GTM module or load balanced to an external name server. In this architecture, the local BIND name server answers all standard DNS queries and acts as a slave to the Infoblox primary master server. The zone configuration is copied to the BIG-IP GTM BIND name server via standard zone transfers. The same WIP-matching occurs like in the Authoritative Screening architecture; however, any non-matching names are simply handled by the local BIND name server instead of being passed to an Infoblox appliance.

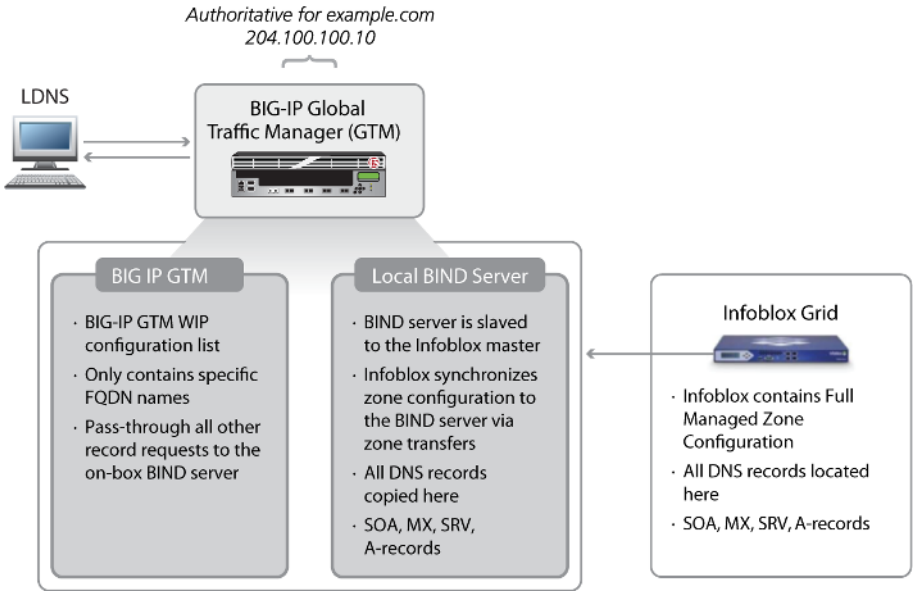


Figure 7: Authoritative Slave architecture with BIG-IP GTM as the front end but with Infoblox holding most DNS records.

DNSSEC Options for Authoritative Slave

TMOS can handle all DNSSEC signing in real-time, on demand as clients request DNSSEC authenticated responses. The setup process is exactly the same as described in the real-time DNSSEC Configuration section. Any zone that includes GSLB WIP names requires TMOS to perform the DNSSEC signing in real time. If there are standard DNS zones that contain no WIP names configured in BIG-IP GTM, then it is possible to use the native Infoblox DNSSEC capabilities to sign those zones. In this hybrid configuration, the Infoblox pre-signed DNSSEC zones will be zone-transferred to the BIG-IP GTM and used like a normal zone file. TMOS will detect a DNSSEC signed response and pass it through to the requesting LDNS server without modification and without re-signing. This hybrid configuration requires having different key signing keys and zone signing keys for the zones signed by Infoblox.

Authoritative Slave Summary

The Authoritative Slave architecture is very similar to the Authoritative Screening architecture. In addition, it uses intelligent DNS and GSLB techniques for any record type that resolves to an A-record. This solution offers some of the benefits of the screening solution. The same DNSSEC techniques apply, including a pure, real-time DNSSEC configuration or a hybrid configuration with some zones being signed and managed by the Infoblox appliance. Since the slave configuration does not spread the DNS queries across several high performance Infoblox appliances, it does not provide high performance responses for standard BIND records. This solution is ideal when the majority of DNS queries are for GSLB resources and BIND is only needed to handle the other records types and a small percentage of standard DNS queries.

Choosing an Architecture

Ultimately, each organization's unique requirements, existing infrastructure, traffic patterns, applications, growth plans, and politics will determine which architecture offers the best starting point. There are many variations possible based on these architectures:

- Organizations that are new to GSLB and have a complex Infoblox DNS architecture with the capacity to handle the DNS request volume should start with a Delegation architecture. This is a minimally disruptive way to start using intelligent GSLB services.
- Delegation is often the only option when internal politics or policies preclude the ability to change any part of the existing Authoritative architecture.
- Larger organizations with higher volumes of DNS requests, concerns about DNS DoS attacks, a need to deploy DNSSEC, and a desire to avoid using CNAMEs and subzones will likely find the Authoritative Screening architecture

a better fit for their requirements.

- Smaller organizations with fewer zones and records, relatively low performance requirements, and GSLB requirements should consider the Authoritative Slave architecture, using an Infoblox appliance to consolidate and provide superior management.

Conclusion

Each joint F5 and Infoblox solution provides unique advantages and functions that enable any organization to meet their requirements. Published DNS vulnerabilities and news of high profile DNS attacks indicate the traditional DNS system needs to adapt, becoming more scalable, available, secure, and trusted. While DNSSEC can solve at least some of the problems, it can be difficult to deploy. New capabilities provided by F5 and Infoblox remove implementation barriers and make it easy for any organization to secure their infrastructure. The combined functionality enables organizations to deploy a complete DNS solution with superior management capabilities, flexible intelligent global server load balancing, high performance scalable DNS, and complete DNSSEC signing for all zones.

Learn More

For more information on DNS and DNSSEC, please visit the links below.

DNS and BIND, 5th Edition, By Cricket Liu, Paul Albitz

Free DNS Tools at MX Toolbox

DNSSEC Deployment Initiative

DNSSEC News and Announcements

National Institute of Standards and Technology

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