Deployment Guide

Document Version 1.0

What's inside:

Deploying the BIG-IP GTM v11 with Infoblox Grid Servers for DNSSEC

Welcome to the F5 Deployment Guide for Global Traffic Manager (GTM) version 11 and Infoblox® Grid™ servers for DNSSEC. This guide shows how to configure the BIG-IP GTM v11 and Infoblox for Authoritative DNSSEC signing for a zone in front of a pool of DNS servers, to sign responses for GTM Wide IP names in a global server load balancing configuration, or to do both in Authoritative Screening mode. Additionally, this guide provides information on optional ways to further secure your DNS implementation with the BIG-IP System.

DNSSEC is an extension to the Domain Name Service (DNS) that ensures the integrity of data returned by domain name lookups by incorporating a chain of trust in the DNS hierarchy. The basis of DNSSEC is public key cryptography (PKI). A chain of trust is built with public-private keys at each layer of the DNS architecture.

DNSSEC provides origin authenticity, data integrity and secure denial of existence. Specifically, Origin Authenticity ensures that resolvers can verify that data has originated from the correct authoritative source. Data Integrity verifies that responses are not modified in-flight and Secure Denial of Existence ensures that when there is no data for a query, that the authoritative server can provide a response that proves no data exists.

The Infoblox Grid provides resilient network services, failover, recovery, and seamless maintenance for an Infoblox deployment inside a single building, across a networked campus, or between remote locations.

For more information on Infoblox Grid, see *http://www.infoblox.com/en/products/infoblox-grid.html*

This guide explains how to configure DNSSEC in BIG-IP GTM version 11. For more information on the F5 BIG-IP GTM, see *http://www.f5.com/products/big-ip/global-traffic-manager.html*

To provide feedback on this deployment guide or other F5 solution documents, contact us at *solutionsfeedback@f5.com.*

Products and versions tested

Product	Version
BIG-IP GTM/LTM	11.0, 11.0.1, 11.1
Infoblox Grid	6.1.0

Important: *Make sure you are using the most recent version of this deployment guide, available at http://www.f5.com/pdf/deployment-guides/infoblox-gtm-dnssec-dg*

Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

- You must be running BIG-IP version 11.0 or a later version in the 11.x series. If you are running BIG-IP version 10.2.x, see *http://www.f5.com/pdf/deployment-guides/gtm-infoblox-dnssec-dg.pdf*.
- You must have the BIG-IP GTM licensed, either as a standalone device, or a module on the BIG-IP system. For DNSSEC, you must also have the DNSSEC add-on license.
- Your Infoblox appliances must already be licensed and configured as a Grid.
- The Infoblox Grid member servers running the DNS service should be on version 6.1.0 or later.
- While not required for this configuration, we also strongly recommend using the BIG-IP Local Traffic Manager (LTM) as described in this document.
- You must have administrative access to both the Web management and SSH command line interfaces on the BIG-IP system.
- The BIG-IP system must be initially configured with the proper VLANs and Self IP addresses. For more information on VLANs and Self IPs, see the BIG-IP documentation.
- You must have administrative control of the DNS zone being protected.
- If there are firewalls in your infrastructure, you must have TCP port 443 open in both directions. TCP port 22 for SSH access to the command line interface is also needed for configuration verification.
- For more configuration options on the BIG-IP GTM, see the Configuration Guide for BIG-IP GTM Module, available on Ask F5.
- We recommend you read the Technical Brief F5 and Infoblox DNS Integrated Architecture (*http://www.f5.com/pdf/white-papers/infoblox-wp.pdf*) for a configuration overview.
- We recommend you read the NIST Secure Domain Name System Deployment guide (*http://csrc.nist.gov/publications/nistpubs/800-81r1/sp-800-81r1.pdf*). We use the NIST recommended values in this guide.
- For information on additional, optional ways to secure your DNS implementation, see *Using the BIG-IP system to protect against DNS attacks on page 18.*

Configuration options

There are three main ways to configure the BIG-IP GTM system for DNSSEC shown in this guide. The method you choose depends on your configuration and if you are also using the BIG-IP LTM.

Authoritative Screening mode

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 Grid servers. Additionally, the Authoritative Screening architecture seamlessly provides all of the benefits of intelligent GSLB services.

When a DNS query is received, the BIG-IP checks the record type. If the type is an A, AAAA, A6, or CNAME request, it is sent to BIG-IP GTM module. The BIG-IP GTM checks each request and response, looking for a match against the Wide IP (WIP) list of FQDN names. If there is a match, the BIG-IP GTM performs the appropriate GSLB functions and return the best IP address appropriate for the requesting client.

If the DNS request does not match the Wide IP list, BIG-IP GTM passes the request to a pool of DNS servers, which provides an additional layer of scalability and availability, increasing the query performance and ensuring optimal uptime of DNS services. Screening mode simplifies management when used with Infoblox DNS servers (see the Technical Brief mentioned above).

GTM inspects all DNS responses from the DNS servers. If the response contains a DNS name that matches a Wide IP, GTM intercepts the response, applies the GTM operations for that item, and re-writes the response before sending it on to the client.

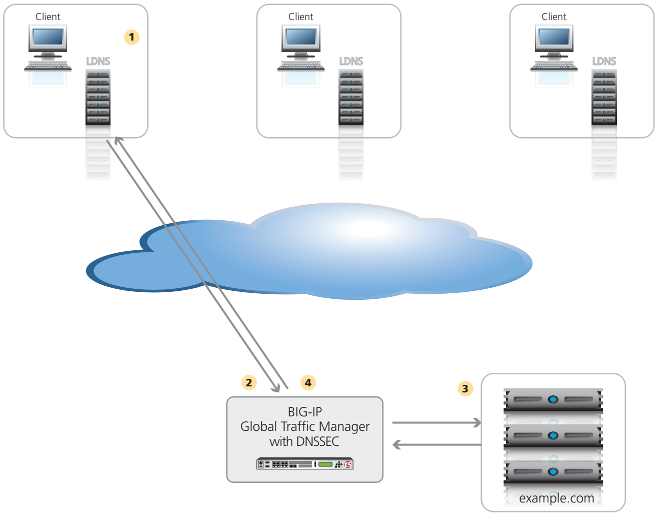

Figure 1: *Authoritative screening mode with DNS load balancing*

The following describes the traffic flow for Authoritative Screening:

1. The client, via LDNS, requests the MX record for example.com.
2. The BIG-IP GTM asks the Infoblox Grid server pool for the MX record
3. The Infoblox server responds to the MX record request with the CNAME *mail.example.com* and an A record with an IP address.
4. The BIG-IP GTM matches a wide IP for mail.example.com. The GTM responds to the client request with mail.example.com and rewrites the IP address of the mail server. GTM adds the DNSSEC signature.

DNS Load Balancing

You can use F5's DNSSEC to sign screened responses from 3rd party DNS servers as well as responses from the BIG-IP GTM, saving time and effort by automating DNSSEC configuration.

Delegation

Delegation has been the traditional deployment method. This solution involves delegating a specific subzone 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 subzone. One drawback with delegation mode is that the administrator is required to create a CNAME for all related DNS records.

In this example, the DNS servers completely manage the top-level zone (such as example.com). The NS records point to the names and, indirectly, the IP address of the DNS servers. 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.

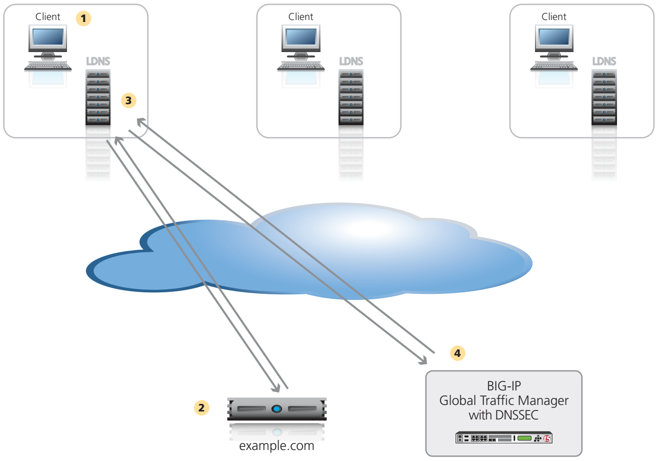

Figure 2: *Delegation mode*

The following describes the traffic flow for delegation:

1. Client requests *www.example.com*.
2. The DNS server that owns www.example.com returns a CNAME for *www.example.com* to *www.gtm.example.com*.
3. The local DNS requests *www.gtm.example.com*.
4. The BIG-IP GTM has the wide IP and owns the **gtm** subzone. The GTM handles DNSSEC for the subzone only. The GTM responds with the best IP address based on the load balancing configuration for the pool.

Configuring Authoritative Screening mode

In this section, we configure the Infoblox appliances and the BIG-IP GTM for Authoritative Screening mode. Some of the procedures in this section depend on whether you are using a BIG-IP LTM in front the pool of servers.

Configuring the Infoblox appliances for Authoritative Screening mode

The following list provides guidance on configuring the Infoblox appliances for use with the BIG-IP GTM in Authoritative Screening mode. On the Infoblox appliances, you enable DNSSEC and create a zone, as well as creating MX and A records to be matched by the GTM Wide IP.

Important

Although all responses are signed only by the BIG-IP, you must configure the Infoblox appliances to allow DNSSEC information to be added to them. Do NOT configure Infoblox to sign any zones.

For specific instructions on configuring Infoblox devices, see the Infoblox documentation.

- **Start DNS services on Grid**
  Grid-->Services-->DNS-->select Grid members-->Start
- **Enable DNSSEC**
  Grid-->Members-->Grid Properties-->DNSSEC-->Enable (do **NOT** sign any zones)
- **Create a zone**
  Data Management-->DNS-->Zones-->Add-->Authoritative Forward Mapping Zone-->Zone Name (match DNSSEC zone name in GTM)-->Use This Set of Name Servers-->Add-->Add Grid Primary and Secondary servers to Zone-->Save and Close
- **Create a MX record**
  Data Management-->DNS-->Zone-->Add-->Record-->MX-->Fill out Mail Destination and Mail Exchanger (record to be matched by GTM Wide IP, e.g. mail.iblox.example.com)
  - Create an additional A record for the mail exchanger name (to be rewritten by GTM, e.g. mail.iblox.example.com) and uncheck the Minimal Response setting (Data Management-->DNS>Members-->Select check box (one at a time)-->click the Edit icon-->uncheck “Return minimal responses”).)

This completes the Infoblox configuration.

Configuring the BIG-IP GTM in Screening mode for GSLB

Use the following procedures to configuring Screening mode for Global Server Load Balancing.

Creating the DNS profile

The first task is to create a DNS profile. The DNS profile has a number of options that you can set depending on how you are configuring the BIG-IP GTM. Use the table in the following procedure to configure the DNS profile according to your implementation.

To create the DNS profile

1. On the Main tab of the navigation pane, expand **Local Traffic** and then click **Profiles**.
2. On the Menu bar, from the **Services** menu, click **DNS**.
3. Click the **Create** button. The new DNS Profile screen opens.

4. Use the following table to configure the DNS profile options. The Setting column contains the required settings for this configuration. If there are two options, use the one applicable for your implementation.

Option	Description	Setting
Global Traffic Management	Enables Global Server Load Balancing (GTM) functions. Needed for Wide IPs to match DNS traffic	**Enabled**
DNS IPv6 to IPv4	Enables translation of IPv6 addresses to IPv4.	**Disabled**
DNS Express	Enables the BIG-IP to function as a DNS slave server for accelerating responses and securing DNS servers.	**Disabled**
DNSSEC	Enables DNSSEC signing of responses.	**Enabled**
Unhandled Query Actions	Determines how the BIG-IP system should process queries not matching a record in GTM or DNS Express.	If not using DNS Load Balancing: **Drop** If using DNS Load Balancing: **Allow**
Use BIND Server on BIG-IP	Enables BIND server on the BIG-IP system. Should always be Disabled.	**Disabled**
Recursion Desired	Enables the BIG-IP system to query other DNS servers to resolve a name. When using the BIG-IP as an authoritative DNS server, this should be disabled; all queries with the recursion bit set are dropped immediately.	If configuring BIG-IP as an authoritative DNS Server: **Disabled** Otherwise[1]: **Enabled**

[1] For example, if configuring the BIG-IP as a DNS server resolving internal client queries for external records

5. Click the **Finished** button.

Creating GTM Listeners

The next task is to create a Listener on the BIG-IP GTM. A listener is an object that monitors the network for DNS queries. For a complete GTM configuration, you need four DNS listeners: IPv4 TCP, IPv4 UDP, IPv6 TCP, and IPv6 UDP.

To create a Listener

1. On the Main tab of the navigation pane, expand **Global Traffic** and then click **Listeners**. The main Listeners screen opens.
2. Click the **Create** button. The new Listener screen opens.
3. In the **Destination** box, type the IP address on which the Global Traffic Manager listens for network traffic. In our example, this is the Self IP address of the GTM on the internal VLAN.

Important →

Be sure to use a Self IP address and not the Management address of the BIG-IP GTM.

4. From the **VLAN Traffic** list, select a VLAN setting appropriate for this listener.
5. From the **DNS Profile** list, select the DNS profile you created.
6. Click the **Finished** button.
7. Repeat to create additional listeners. If creating an IPv6 listener, be sure to use an IPv6 address as the destination.

Creating the GTM Data Center

The next task is to create a new GTM Data Center that corresponds to your physical data center.

To create the data center

1. On the Main tab, expand **Global Traffic** and then click **Data Centers**.
2. Click the **Create** button. The New Data Center screen opens.
3. In the **Name** box, type a name for this data center. In our example, we type **Local_Datacenter**.
4. Complete the rest of the configuration as applicable for your deployment.
5. Click the **Finished** button.

Creating the GTM Server objects

Next, we create the GTM Servers. A server defines a specific system on the network.

The steps in this procedure are slightly different if you are using a standalone GTM device or the GTM module in combination with a BIG-IP LTM. These differences are clearly marked in the following procedures.

Important →

You must add a Server object for the BIG-IP GTM you are currently configuring and every GTM that is a part of the sync group. For more information on GTM sync groups, see the online help or GTM documentation.

To create the GTM servers

1. On the Main tab, expand **Global Traffic** and then click **Servers**.
2. Click the **Create** button. The New Server screen opens.
3. In the **Name** box, type a name that identifies this GTM. In our example, we type **GTM-1**.
4. From the **Product** list, select the either **BIG-IP System (Single)** or **BIG-IP System (Redundant)**.

   Note →

   Redundant is only used when the GTM is also an LTM/GTM combo and specifically configured for LTM failover of the listener. Otherwise use BIG-IP System (Single).

5. In the **Address List** section, type the self IP of this GTM, and then click the **Add** button.

   Important →

   Be sure to use a Self IP address and not the Management address of the BIG-IP GTM.

   If you selected *BIG-IP System (Redundant)* in step 4, type the appropriate IP address in the Peer Address List section.

6. From the **Data Center** list, select the Data Center you created in *Creating the GTM Data Center on page 7.* In our example, we select **Local_Datacenter**.

7. *Optional*: In the **Health Monitors** section, from the **Available** list, select the monitor type **bigip** and then click the Add (**<<**) button.
8. From the **Virtual Server Discovery** list, perform the following depending on whether you are using a third party load balancer, or a remote BIG-IP LTM:
   - Third Party Load Balancer: Leave Discovery set to **Disabled**.
   - GTM Module: From the Discovery list, select **Enabled**. (We strongly recommend Enabling Discovery, however you can leave this set to Disabled and manually configure the virtual server information).
9. Click **Finished**.

10. The next step depends on your configuration:
    - If you have additional BIG-IP GTMs in your implementation, repeat this procedure to add them.
    - If you are using the GTM and LTM on the same box, continue with the next section. However, if there are external BIG-IP LTM devices that are a part of the configuration, you must add a GTM Server object for those as well. Repeat this procedure for each external LTM.
    - If you are using a GTM standalone, repeat this procedure to create the GTM Server objects for each of the load balancers (a BIG-LTM in our example) and continue with step 10.

Enabling connectivity with remote BIG-IP systems

If you are adding a remote BIG-IP LTM server, you must make sure ***big3d*** agent on the same version on the BIG-IP LTM and GTM.

Important

This is only necessary if you are using remote LTM devices.

From the GTM device command line, type

```
big3d_install <IP address of target system>
```

where the target system is the LTM that you want to add as a server on the GTM. This pushes out the newest version of big3d.

Next, type

```
bigip_add
```

to exchange SSL keys with the LTM. Type the password at the prompt, and then type

```
iqdump <ip address of remote box>.
```

If the boxes are communicating over iQuery, you see a list of configuration information from the remote BIG-IP.

The **bigip_add** command must be run for every BIG-IP in the configuration.

Adding GTM servers to a Sync Group

You must run **gtm_add** on each additional GTM in the sync group as well to ensure the iQuery configuration is working. If not already part of a sync group, this command adds the GTM to the sync group. For more information on sync groups, see the GTM documentation.

Creating the GTM health monitors

The next task is to create the GTM health monitors. If you are using the BIG-IP LTM, status from the LTM monitors will be available in the GTM. The following GTM monitors add an additional layer of monitoring that is initiated by the GTM. While health monitors are not technically required, they are strongly recommended. The monitors shown in the following sections are examples, you can use other monitor types appropriate to your deployment.

To create the TCP and HTTP monitors

1. On the Main tab, expand Global Traffic and then click Monitors.
2. Click the Create button. The New Monitor screen opens.
3. In the **Name** box, type a name for the monitor. In our example, we type **gtm-monitor-tcp**.
4. From the **Type** list, select **TCP**.
5. From the **Configuration** list, select **Advanced**.

6. Configure any of the other options as applicable for your implementation.
7. Click the **Repeat** button to create another monitor for HTTP.
8. In the **Name** box, type a name for this monitor. In our example we named it **gtm-monitor-http**.
9. From the **Type** list, select **HTTP**.
10. Configure the other options as applicable for your implementation.
11. Click the **Finished** button.

Creating the GTM Pool

First, we create a pool on the BIG-IP GTM system that includes the virtual servers of load balancing device (BIG-IP LTM in our example).

To create a GTM pool

1. On the Main tab, expand **Global Traffic** and then click **Pools** (located under Wide IPs).
2. Click the **Create** button. The New Pool screen opens.
3. In the **Name** box, type a name for the pool. In our example, we type **Local_pool**.
4. In the *Health Monitors* section, from the **Available** list, select the name of the monitors you created in *Creating the GTM health monitors on page 8*, and then click the Add (**<<**) button after each. In our example, we select **gtm-monitor-tcp** and **gtm-monitor-http**.
5. In the *Load Balancing Method* section, choose the load balancing methods from the lists appropriate for your configuration.
6. In the *Member List* section, from the **Virtual Server** list, select the appropriate virtual server on the load balancer for the application, and then click the **Add** button.

   Note that you must select the virtual server by IP Address and port number combination. In our example, we select **10.10.11.3:80**.

   Repeat this step for additional virtual servers.
7. Configure the other settings as applicable for your deployment
8. Click the **Finished** button.

Creating the GTM Wide IP

In this procedure, we create a wide IP that includes the GTM pool you created, and the <hostname>. In our example, we use **www.example.com**. GTM attempts to match DNS requests and responses to the resource indicated by the Wide IP.

To create a wide IP

1. On the Main tab, expand **Global Traffic** and then click **Wide IPs**.
2. Click the **Create** button. The New Wide IP screen opens.
3. In the **Name** box, type a name for the Wide IP. In screening mode, this is the FQDN of the host. In our example, we type **mail.example.com**.
4. From the **State** list, ensure that **Enabled** is selected.
5. From the *Pools* section, from the **Load Balancing Method** list, select a load balancing method appropriate for your configuration.

6. In the *Pool List* section, from the **Pool** list, select the name of the pool you created in *Creating the GTM Pool on page 9*, and then click the **Add** button. In our example, we select **Local_pool**.
7. All other settings are optional, configure as appropriate for your deployment.
8. Click the **Finished** button.

Important

Configuring the GTM for DNSSEC
If you are not planning to use DNS load balancing in your configuration as described in the following section, continue to *Configuring the BIG-IP GTM for DNSSEC on page 15.*

Adding DNS load balancing to Screening mode for GSLB

Use the following procedures to add DNS Load Balancing to Screening mode for GSLB.

Creating the LTM monitors

If you are using the BIG-IP LTM, configure the following monitors. These monitors test the servers to ensure the Infoblox Grid server DNS services are operational. DNS is available over UDP and TCP protocols, so we create a health monitor for each protocol over port 53. If you only choose to implement one monitor, we recommend the UDP monitor.

To create the LTM monitors

1. On the Main tab, expand **Local Traffic** and then click **Monitors**.
2. Click the **Create** button. The New Monitor screen opens.
3. In the **Name** box, type a name for the monitor. In our example, we type **ltm-infoblox-monitor-tcp**.
4. From the **Type** list, select **TCP**.
5. From the **Configuration** list, select **Advanced**.
6. In the **Alias Service Port** box, type **53**.
7. Configure any of the other options as applicable for your implementation.
8. Click the **Repeat** button to create another monitor for UDP.
9. In the **Name** box, type a name for this UDP monitor. In our example we named it **ltm-infoblox-monitor-udp**.
10. From the Type list, select UDP.
11. Make sure the **Alias Service Port** box is set to **53**.
12. Configure the other options as applicable for your implementation.
13. Click the **Finished** button.

Creating the LTM pool

The next task is to create a pool on the Local Traffic Manager for the DNS servers.

To create a LTM pool

1. On the Main tab, expand **Local Traffic**, and then click **Pools**.
2. Click the **Create** button.

3. In the **Name** box, type a name for this Pool. In our example, we type **infoblox-ltm-pool**.
4. In the *Health Monitors* section, from the **Available** list, select the name of the monitor you just created, and then click the Add (**<<**) button after each. In our example, we select **ltm-infoblox-monitor-tcp** and **ltm-dns-monitor-tcp**.
5. In the Resources section, from the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).
6. In the New Members section, you add the Infoblox Grid servers to the pool.
   a. In the **Address** box, type the IP address of one of the Infoblox Grid servers.
   b. In the **Service Port** box, type **53**.
   c. Click the **Add** button to add the member to the list.
   d. Repeat steps a-c for each device you want to add to the pool.
7. Click the **Finished** button.

Attaching the pool to the GTM Listener

The next task is to attach the LTM pool to the GTM Listener. This procedure can be performed from the TMSH command line or the Configuration utility. If you choose to use the Configuration utility, you must have LTM provisioned (even if you are using a GTM standalone, you can use Resource Provisioning to set the LTM to minimal without a full LTM license).

An addition command in step 4 configures the GTM Listener for SNAT and IP translation.

To attach the pool to the Listener using the command line

1. Log on to the GTM and open a command prompt.
2. At the prompt, type **tmsh**.
3. Type the following command, replacing **<listener name>** and **<ltm pool name>** with the name of your Listener and Pool:

```
modify /ltm virtual <listener name> pool <ltm pool name>
```

4. Type the following command:

```
modify /ltm virtual <listener name> snat automap translate-address enabled
```

To attach the pool to the Listener using the Configuration utility

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. As mentioned in the introduction to this section, you must have LTM provisioned to see the virtual server.

Note → *Even if you have only licensed GTM, you can provision LTM and view the virtual servers.*

2. Click the virtual server name that was automatically created for the Listener. This virtual server name includes the IP address you used for the Listener, starting with **vs_** and ending with **_gtm**. For example, **vs_10_1_102_5_53_gtm**.
3. From the **Configuration** list, select **Advanced**.
4. From the **SNAT Pool** list, select **Automap**.
5. From the **Address Translation** row, click a check in the **Enabled** box to enable Address Translation.
6. Click **Update**.

7. On the Menu bar, click **Resources**.
8. From the **Default Pool** list, select the name of your LTM pool.
9. Click **Update**.

Important →

Configuring the GTM for DNSSEC
When you have finished the preceding configuration, continue to *Configuring the BIG-IP GTM for DNSSEC on page 15.*

Configuring Delegation mode

In this section, we configure the BIG-IP for Delegation mode. After the BIG-IP has been initially configured, we configure the DNSSEC components.

Because this mode uses some of the same objects as in screening mode, we refer back to the procedures in the previous section instead of repeating the information.

Creating a CNAME record on the Infoblox appliances for Delegation mode

This section provides guidance on configuring the Infoblox appliances for use with the BIG-IP GTM in Delegation mode. For specific instructions on configuring Infoblox devices, see the Infoblox documentation.

- CNAME record (Alias will be the record they request, e.g. www.iblox.example.com and Canonical Name will be the Wide IP name on the GTM, e.g. www.gtm.iblox.example.com)

Creating the DNS Profile

To configure the GTM Listener, follow the procedure *Creating the DNS profile on page 5* with no modifications.

Creating a GTM Listener

To configure the GTM Listener, follow the procedure *Creating GTM Listeners on page 6* with no modifications.

Creating the Data Center

The next task is to create the GTM Data Center. To configure the Data Center, follow the procedure *Creating the GTM Data Center on page 7* with no modifications.

Creating a Zone

The next task is to create a Zone on the GTM. This zone will be a subzone of CNAME record you created on the Infoblox appliances.

To create a Zone

1. On the Main tab, expand **Global Traffic** and then click **ZoneRunner**.
2. On the menu bar, click **Zone List**.
3. Click the **Create** button.
4. If applicable, from the View Name list, select a view. We select **external**, the default.
5. In the **Name** box, type the subzone of the CNAME you created above (for example, gtm.iblox.example.com).
6. From the **Zone Type** list, select **Master**.
7. From the Records Creation, SOA Record section, in the **TTL** box, type a Time to Live. In our example, we type **30**.
8. In the **Master Server** box, type the host name of the GTM device.
9. In the **Email Contact** box, type the email address of the contact.
10. All other settings can be configured as applicable. We leave the defaults.
11. From the NS Record section, in the **TTL** box, type a Time to Live. In our example, we type **30**.

12. In the **Master Server** box, type the host name of the GTM device.
13. Click **Finished**.

Configuring the Wide IP

The next task is to create the Wide IP. To configure the Wide IP, follow the procedure *Creating the GTM Wide IP on page 9*. This Wide IP must be the new CNAME the DNS server refers to in the subzone assigned to the GTM. For example *gtm.example.com*. For example, if the GTM owns gtm.example.com, the CNAME for www.example.com may redirect the query to www.gtm.example.com

Because the GTM will be entirely responsible for managing the subzone, all of the other records for the subzone (NS, SOA, and so on) need to be added to the local BIND configuration on the GTM using ZoneRunner. Note that the NS record needs to point to the address of the GTM Listener. For information on configuring ZoneRunner, see the online help or GTM documentation.

Important →

Configuring the GTM for DNSSEC

When you have finished the preceding configuration, continue to *Configuring the BIG-IP GTM for DNSSEC on page 15.*

Configuring the BIG-IP GTM for DNSSEC

Deploying DNSSEC involves signing DNS zones with public/private key encryption and returning DNS signed responses. A client trust for the signatures is based on a chain of trust established across administrative boundaries.

In this section, we configure the global traffic settings on the BIG-IP GTM.

Before beginning the configuration in this section, you should have configured the BIG-IP GTM as described in one of the scenarios in this guide.

Important

Any zone that contains a Wide IP name in the GTM configuration must be signed by F5.

Warnings

If GTM is not properly configured with data centers and GTM devices defined, and the DNSSEC license, key generation will fail.

If you are using DNS load balancing or BIND, you should ***never*** *sign the responses with the back end DNS servers* ***if*** *you are going to sign them using GTM.*

Creating the Key Signing Key

The first task in this section is to create the Key Signing Key on the GTM.

To create the Key Signing Key

1. On the Main tab, expand **Global Traffic** and then click **DNSSEC Key List**.
2. Click the **Create** button.
3. In the **Name** box, type the domain name. In our example, we type **example.com_ksk**.
4. In the **BIT Width** box, we recommend you type a larger value for the Key Signing Key because it is the master key. In our example, we change the default value of 1024 to **2048**.
5. *Optional*: If you have a BIG-IP FIPS hardware security module installed in your BIG-IP device, you have the option of storing this key on the hardware device. If so, from the **Use FIPS** list, select **Enabled**. If you are unsure if you have this module, consult with your F5 Sales Representative.
6. From the **Type** list, select **Key Signing Key**.
7. In the **Rollover Period** row, we recommend a rollover set to 185 days. While the NiST standard for rollover is 180 days, the BIG-IP requires a rollover that is at least half of the Expiration (365 in our example). In the **Days** box, we type **185**.
8. In the **Expiration Period** row, we recommend 1 year, the NiST standard for expiration. In the **Days** box, we type **365**.
9. Click the **Finished** button (see Figure 3).

Creating the Zone Signing Key

The next task is to create the Zone Signing Key.

To create the Zone Signing Key

1. On the Main tab, expand **Global Traffic** and then click **DNSSEC Key List**.
2. Click the **Create** button.

3. In the **Name** box, type the domain name. In our example, we type **example.com_zsk**.
4. *Optional*: If you have a BIG-IP FIPS hardware security module installed in your BIG-IP device, you have the option of storing this key on the hardware device. If so, from the **Use FIPS** list, select **Enabled**. If you are unsure if you have this module, consult with your F5 Sales Representative.
5. From the **Type** list, select **Zone Signing Key**.
6. In the **Rollover Period** row, we recommend a rollover set to 15 days, the NiST standard for rollover. In the **Days** box, we type **15**.
7. In the **Expiration Period** row, we recommend 30 days, the NiST standard for expiration. In the **Days** box, we type **30**.
8. We recommend you leave the other settings at the defaults.
9. Click the **Finished** button.

Creating and protecting the Zone

Next, we create and protect the zone with the zone and key signing keys.

To create and protect the zones

1. On the Main tab, expand **Global Traffic**, click **DNSSEC Zone List**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this zone. In our example, we use **example.com**.
4. In the *Zone Signing Key* section, from the **Available** box, click the **Zone Signing Key** you created, and then click the Add (**<<**) button. In our example, we select **example.com_zsk**.
5. In the *Key Signing Key* section, from the **Available** box, click the Key Signing Key you created, and then click the Add (**<<**) button. In our example, we select **example.com_ksk**.
6. Click **Finished**.

You have now protected your Zone with DNSSEC.

DNSSEC Integration Verification

The final task is to verify the configuration is operating properly. We use a test client to access the GTM Wide IP to perform DNS lookup requests. A DNS client application called Dig can be used to query the DNS Server.

Launch a terminal application and issue a request that includes DNSSEC, such as:

```
dig @bigip10.example.com +dnssec +multiline www.dnssec.f5demo.com
```

You see a result similar to the example on the following page.

```
; <<>> DiG 9.6.0-APPLE-P2 <<>> @bigip10.example.com +dnssec +multiline www.dnssec.f5demo.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60496
;; flags: qr aa rd ad; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;www.dnssec.f5demo.com.     IN A

;; ANSWER SECTION:

www.dnssec.f5demo.com.                         30 IN A   65.197.145.93

www.dnssec.f5demo.com.                         30 IN RRSIG A 7 4 30 20100116005323 (
                                               20100109005323 31052 dnssec.f5demo.com.
                                               NtOnSwWK1JhbYgsCY5EhVSzZ7475A6NAfcAAnhxkiYCN
                                               us+0TYKoRwXfGKOdNJd/WjrcD+J08Vz8SxSuQ19cY9Jx
                                               KtO1o7ghLgvcIemyYTsICEWXJ98FrX9MdJCQvaeg3Qvj
                                               FKQMVHvrNxVgzTkTdcVvK8Q/zgVMCbejcEK29iI= )

www.dnssec.f5demo.com.                         30 IN RRSIG A 7 4 30 20100116005323 (
                                               20100109005323 61232 dnssec.f5demo.com.
                                               vJS+4Cf8EM6b73LG6LblxxNxENWx7ylct7QdggCnCSlu
                                               9iD0pW0dDKaZIH8ya4UD8Ar/V+yJjrPxA2ShK/nhlW4t
                                               81/R+njx1MJoZ9a71Y8cHMqXLpYgEpYXVHY7OJ+akp83
                                               3oYbFbMVg7YbnYEItNUEM+6LuitXo89FUTaY2QI= )

www.dnssec.f5demo.com.                         30 IN RRSIG A 7 4 30 20100116005323 (
                                               20100109005323 46472 dnssec.f5demo.com.
                                               fdio5eNraa1eBM+/NCbVT6rKWukoq1Z2VICpY2wa2X/Q
                                               ocWRcyOlda2slpKEh6LRTEZ4z13MrwQbyh6AuaaU/LEZ
                                               8VEU2ViK90wwKBLMFsnWqPMyLZ0PSd3a+ANcbr869vsJ
                                               9F4DSs9CfbVJdOkaGFqPYwjWpqMLxN/B1aHlNpw= )

www.dnssec.f5demo.com.                         30 IN RRSIG A 7 4 30 20100116005323 (
                                               20100109005323 64235 dnssec.f5demo.com.
                                               7cpHDxhdqAips+rLTpprDnjSJc+J6qDZ6x9JNYR4PelJ
                                               MplpmVq72tYUVIcJPZ3fpdpCW83cLSj6Ij83/zPORP3p
                                               MubfIe4mtk3ysGQGzA/Aatx8+J3T8AHHiO0y7qo4XEUy
                                               N1sItDAi9nCXlXD4QwBXmQtur+QYESQCy937uRM= )

www.dnssec.f5demo.com.                         30 IN RRSIG A 7 4 30 20100116005323 (
                                               20100109005323 28328 dnssec.f5demo.com.
                                               K2WXvNNMa4AEGE8q5e7qPcdg9ki0LcMgOgiHhwG8fD5K
                                               qfLaqo89BNdhbal2AKs+F/8T+H0K5ZNRnW/L591vTFxT
                                               Al5iVEzZwO9Uv0O8UeztvWafYbfq41D6e/S0KjnXo2kR
                                               W3DiNSA2UFC1QSNp5Aic+cf0IKEem/yJ/+PwxmQ= )

;; Query time: 70 msec
;; SERVER: 65.197.145.83#53(65.197.145.83)
;; WHEN: Fri Jan  8 16:53:23 2010
;; MSG SIZE  rcvd: 1077
```

This completes the configuration. For more information on configuring the BIG-IP GTM for DNSSEC, see the product documentation, available on Ask F5: *http://support.f5.com/kb/en-us.html*.

Using the BIG-IP system to protect against DNS attacks

You can use iRules, the BIG-IP system's powerful and flexible scripting language to help protect your implementation from a wide variety of DNS (and other) attacks. F5's DevCentral (*http://devcentral.f5.com/*) contains a number of examples and iRule specific commands you can use to help protect your deployment. DevCentral requires a free registration.

For example, the iRules feature includes several commands and events that are specifically designed to work with DNS queries on the BIG-IP GTM and LTM using version 11 and later. The following table contains a command and event list, and a description of each. Each command or event links to the specific DevCentral page for complete syntax and examples.

Command	Description
DNS::additional	Returns, inserts, removes, or clears RRs from the additional section.
DNS::answer	Returns, inserts, removes, or clears all RRs from the answer section.
DNS::authority	Returns, inserts, removes, or clears RRs from the authority section
DNS::class	Gets or sets the resource record class field
DNS::disable	Sets the service state to disabled for the current dns packet
DNS::drop	Drops the current DNS packet after the execution of the event.
DNS::edns0	Gets (v11.0+) and sets (v11.1+) the values of the edns0 pseudo-RR
DNS::enable	Sets the service state to enabled for the current dns packet
DNS::header	Gets (v11.0+) or sets (v11.1+) simple bits or byte fields.
DNS::last_act	Sets the action to perform if no DNS service handles this packet
DNS::len	Returns the dns packet message length
DNS::name	Gets or sets the resource record name field
DNS::origin	Returns the originator of the DNS message
DNS::ptype	Returns the type of the DNS packet
DNS::query	Returns or constructs and sends a query to the DNS-Express database for a name and type
DNS::question	Gets (v11.0+) or sets (v11.1+) the question field value
DNS::rdata	Gets or sets the resource record rdata field
DNS::return	Skips all further processing after TCL execution and sends the dns packet in the opposite direction
DNS::rr	Creates a new resource record object with specified attributes or as a complete string
DNS::rrname	Returns the name requested by the client
DNS::rrtype	Returns the resource record type requested by the client
DNS::ttl	Gets or sets the resource record ttl field
DNS::type	Gets or sets the resource record type field
whereis	Returns geographical information on an IP address
DNS_REQUEST	Triggered when the system receives a DNS request.
DNS_RESPONSE	Triggered when the system responds to a DNS request

Example: DNS Blackhole

DevCentral contains detailed configuration instructions for creating a "DNS Blackhole." In this scenario, the BIG-IP intercepts DNS requests for prohibited FQDNs, does not send those to BIND for recursive look-up, returns a DNS response with an A record to an LTM virtual server, and has a LTM virtual server with a second iRule that logs the request and serve a static page. The solution uses an iRule to the listener virtual server. This virtual server processes all GTM/BIND traffic. Incoming requests are matched against an external data group that contains a list of prohibited FQDNs.

The blackhole iRule logs all requests for prohibited FQDNs and returns a DNS response that matches an LTM virtual server. The blackhole iRule only provides valid responses for A records, however all blackhole DNS requests are logged.

For specific instructions, see *https://devcentral.f5.com/wiki/iRules.DNS_Blackhole.ashx*.

Document Revision History

Version	Description
1.0	New deployment guide

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