Welcome to the F5 Deployment Guide for DNSSEC with Global Traffic Manager (GTM). This guide shows how to configure Authoritative DNSSEC signing for a zone in front of a pool of DNS servers, to sign responses from virtual servers in a global server load balancing configuration, or to do both in Authoritative Screening mode.

DNSSEC is a 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.

This guide explains how to configure DNSSEC in BIG-IP Global Traffic Manager. 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

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIG-IP GTM/LTM</td>
<td>10.2.1 and later</td>
</tr>
</tbody>
</table>

Important: Make sure you are using the most recent version of this deployment guide, available at http://www.f5.com/pdf/deployment-guides/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 10.2.1 or later.
- 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.
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 online help or the BIG-IP documentation.

You must have administrative control of the DNS zone being protected.

If there are firewalls, 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. Even if you are not using Infoblox, this brief provides detailed information on the concepts found in this deployment guide.

We recommend you read the NIST Secure Domain Name System Deployment guide (http://csrc.nist.gov/publications/nistpubs/800-81r1sp-800-81r1.pdf). We use the NIST recommended values in this guide.

### 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 whether 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 DNS 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.
The following describes the traffic flow for Authoritative Screening:

1. The client, via LDNS, requests the MX record for company.com.
2. The BIG-IP GTM asks the DNS server pool for the MX record
3. The DNS server responds to the MX record request with `mail.company.com`.
4. The BIG-IP GTM matches a wide IP for `mail.company.com`. The GTM responds to the client request with `mail.company.com` and adds the IP address of the mail server. GTM adds the DNSSEC signature.

**DNS Load Balancing**

You can also use only the DNS load balancing components of screening mode to sign responses from 3rd-party DNS servers. This saves time by using F5’s DNSSEC rather than signing the DNS zones manually.

**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.
The following describes the traffic flow for delegation:

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 BIG-IP for Authoritative Screening mode. Some of the procedures in this section depend on whether you are using a BIG-IP LTM in front of a pool of DNS servers.

Screening mode for Global Server Loading Balancing

Use the following procedures to configure screening mode for GSLB.

Configuring a GTM Listener

The first task is to create a Listener on the BIG-IP GTM. A listener is an object that monitors the network for DNS queries.

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.
4. Be sure to use a Self IP address and not the Management address of the BIG-IP GTM.
5. From the VLAN Traffic list, select a VLAN setting appropriate for this listener.
6. Click the Finished button.

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_Datcenter.
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.

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)**.

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

   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 5*. 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.

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 7, 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 www.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 7, 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.

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 13.

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 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-dns-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-dns-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 unique name for this Pool.
4. In the **Health Monitors** section, from the **Available** list, select the name of the monitor you created in **Creating the LTM monitors on page 8**, and then click the **Add** button after each. In our example, we select `ltm-dns-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 DNS servers to the pool.
   a. In the **Address** box, type the IP address of one of the DNS 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.

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 13.
Configuring DNS load balancing only mode

In this section, we configure the BIG-IP for DNS Load Balancing mode without the components of GSLB described in the first section. 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.

Configuring a GTM Listener

To configure the GTM Listener, follow the procedure Configuring a GTM Listener on page 5 with no modifications.

Configuring the LTM monitors

The next task is to create the LTM health monitors. To configure the monitors, follow the procedure Creating the LTM monitors on page 10 with no modifications.

Configuring the LTM pool

The next task is to create the LTM health monitors. To configure the monitors, follow the procedure Creating the LTM pool on page 10 with no modifications.

Attaching the pool to the GTM Listener

The next task is to attach the LTM pool to the GTM Listener. To attach the pool to the Listener, follow the procedure Attaching the pool to the GTM Listener on page 9.

Configuring the GTM for DNSSEC

When you have finished the preceding configuration, continue to Configuring the BIG-IP GTM for DNSSEC on page 13.
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.

Configuring a GTM Listener

To configure the GTM Listener, follow the procedure Configuring a GTM Listener on page 5 with no modifications.

Configuring 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 5 with no modifications.

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 8. 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.

Configuring the GTM for DNSSEC

When you have finished the preceding configuration, continue to Configuring the BIG-IP GTM for DNSSEC on page 13.
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.

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

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.

Protecting the Zones
Next, we protect the zones with the zone signing keys.

To 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.

Providing the DNSSEC DS Record to the parent domain
One of the steps in configuring DNSSEC on the BIG-IP GTM system involves establishing an authentication chain between the parent and child DNSSEC zones. When you create a DNSSEC zone, or renew keys for an existing DNSSEC zone, you must provide the Delegation Signer (DS) Resource Record(s) to the parent domain. Providing the DS record to the parent domain establishes the authentication chain between the parent and child DNS zones, allowing each link in the chain to vouch for the next. Without a complete authentication chain, an answer to a DNS lookup cannot be securely authenticated.

For detailed configuration instructions, see Ask F5 SOL12981: http://support.f5.com/kb/en-us/solutions/public/12000/900/sol12981.html
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.siterequest.com +dnssec +multiline www.dnssec.f5demo.com

You see a result similar to the following example:

```
; >>>> DiG 9.6.0-APPLE-P2 <<< @bigip10.siterequest.com +dnssec +multiline www.dnssec.f5demo.com
; (1 server found)
; global options: +cmd
; Got answer:
; ->>HEAEDER<<<< 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 61232 dnssec.f5demo.com. vJS+4Cf8EM6b73LG6LblxxNENxh71etC70dggCnC5lw 91D0wpwhDKzXX8ya4URBar/y+5jr/Px2EHk/hhJzat4/8 R/n+gx1Mo29a71Y8chMqXpYgEyXVYV7009+akjp83 3oYbNmVg7YbnYE1NuEnL+6UiitX089FtayQ=[I= )
www.dnssec.f5demo.com. 30 IN RRSIG A 7 4 30 20100116005323 (20100109005323 46472 dnssec.f5demo.com. fdioSeNraa1eIEM+NCqBT6W+Ku9qo2Z2vU9f2X/Q ocwcRyc01da2SlpKEeh6LRT2E4z13MrwQbyh6AuaaU/LE2 8V6U2V1K9wXwKLMFsnqPMLz0Bps3a+ANcb96Ovsj 9F4DSS9CFV3D0kaGfQqPYwJnpdMLyN/B1hLNpwy= )
www.dnssec.f5demo.com. 30 IN A 30 7 4 30 20100116005323 (20100109005323 31052 dnssec.f5demo.com. NToSnwK13bYgsCY5EhVSz2745A6NafCfAAnhki1yCN us+8TYKoRwXFGK0DNDj/M3rj+e3O98vS5xSU9cY93x K0I07ghLvclemyYTsICExW39BFxKMMJDQa93Qvq9 FKQWNHrWvNg5g7TwCvVQ9ZqzGWMcbejCEK29I= )
www.dnssec.f5demo.com. 30 IN A 65.197.145.93
www.dnssec.f5demo.com. 30 IN RRSIG A 7 4 30 20100116005323 (20100109005323 28328 dnssec.f5demo.com. K2wXVNMM4A4E8G8G57qPcdg9k10Cmg0lHw9GgL5DSK qflaqo0Nhdbal2Asf/F/57H5K5ZNVNkJ/L591vF5T A15I3E2z2W09uV08ifeztV9pY9P q6kID6eX54VKjunoZKR W3DINSAX2UCIQsn5P5Ac+c01Keen/yj+4PwxmQ= )
```

;; 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

Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>New deployment guide</td>
</tr>
<tr>
<td>1.1</td>
<td>Modified the Rollover Period for Key Signing Key from 180 to 185. While the NIST standard for rollover is 180 days, the BIG-IP requires a rollover that is at least half of the Expiration Period (365 in our example).</td>
</tr>
<tr>
<td>1.2</td>
<td>Added section on providing the DNSSEC DS record to the parent domain and referenced SOL12981 on Ask F5 for configuration instructions.</td>
</tr>
</tbody>
</table>