



DNS Traffic Management using the BIG-IP Local Traffic Manager

Important: This guide has been archived. While the content in this guide is still valid for the products and versions listed in the document, it is no longer being updated and may refer to F5 or third party products or versions that have reached end-of-life or end-of-support. For a list of current guides, see <https://f5.com/solutions/deployment-guides>.

Table of Contents

Introducing DNS server traffic management with the BIG-IP LTM	
Prerequisites and configuration notes	1-1
Product versions and revision history	1-2
Configuring the BIG-IP for DNS traffic management using the application template	1-3
Advanced DNS traffic management using the BIG-IP LTM	
Using the Application Template to create a DNS health monitor	2-1
Stateless UDP with nPath Routing	2-2
Creating a DNS health monitor	2-3
Creating the pool	2-5
Creating a Fast L4 profile	2-5
Creating the virtual server	2-6
Modifying the DNS server configuration	2-7
Stateless UDP traffic management	2-8
Creating the health monitor	2-8
Creating the pool	2-8
Creating the Fast L4 profile	2-9
Creating the virtual servers	2-9
Basic Stateful UDP traffic management	2-11
Creating the health monitor	2-12
Creating the pool	2-12
Creating the Fast L4 profile	2-12
Creating the virtual server	2-12
Stateful UDP Datagram traffic management	2-13
Creating the health monitor	2-13
Creating the pool	2-13
Creating a UDP profile	2-13
Creating the virtual server	2-14
Layer 7 UDP traffic management	2-15
Creating the health monitor	2-15
Creating the pool	2-15
Creating a UDP profile	2-15
Creating the iRule	2-15
Creating the virtual server	2-16
Appendix A: Configuring the BIG-IP LTM for DNS TCP traffic	2-17
Creating the TCP profiles	2-17
Creating the virtual server	2-18



I

DNS Traffic Management using the BIG-IP LTM

- Introducing DNS server traffic management with the BIG-IP LTM
- Configuring the BIG-IP for DNS traffic management using the application template

Introducing DNS server traffic management with the BIG-IP LTM

Welcome to the DNS server load balancing deployment guide. This guide gives you step-by-step configuration procedures for intelligent traffic management for DNS servers with the BIG-IP Local Traffic Manager (LTM).

This guide is broken into two major sections:

- ◆ *Configuring the BIG-IP for DNS traffic management using the application template*, on page 1-3
- ◆ *Advanced DNS traffic management using the BIG-IP LTM*, on page 2-1

We recommend you read the entire deployment guide, especially the *Advanced DNS Load Balancing* chapter, before choosing the deployment scenario, to ensure you find the implementation that best fits your needs.

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

Prerequisites and configuration notes

The following are general prerequisites for this deployment.

- ◆ In order to use the Application Template on the BIG-IP LTM, you must be using BIG-IP 10.2.
- ◆ For advanced DNS load balancing techniques, see *Advanced DNS traffic management using the BIG-IP LTM*, on page 2-1.

Overview of DNS

At the most basic level, Domain Name System, or DNS as it is commonly known, is an Internet service that maps domain names into IP addresses and is an essential component of any network. There are two types of DNS servers: authoritative and non-authoritative.

- ◆ **Authoritative DNS**
Authoritative DNS is the authoritative source for all DNS requests made for a designated domain.
- ◆ **Non-Authoritative DNS**
Also referred to as a Local DNS (LDNS) or a caching DNS server -- is often located near the DNS client, caching DNS answers received from Authoritative DNS servers, speeding future resolution requests. Local DNS servers are usually provided by ISPs or an enterprise's IT department.

The following is a brief explanation of how DNS queries are handled.

A client sends a DNS query to the local DNS server. If the local DNS server does not have either an authoritative or cached response for the target of the query, it then forwards the query to other DNS servers. The query follows the DNS hierarchical system until the query reaches either the authoritative or non-authoritative DNS server for the target. When the domain is found, the LDNS receives the query response and caches it (for a period of time specified by the Time To Live (TTL)), replying to the requesting client.

Typically there is more than one authoritative DNS server for each domain. To make configuration management easier, primary and secondary roles are defined. The configuration file (zone file) may be updated only on the primary DNS server, while the secondary DNS server downloads updated information from the primary via the process called zone transfer. DNS queries and responses use UDP port 53, while zone transfers use TCP port 53.

Load balancing both authoritative and non-authoritative DNS servers requires handling DNS queries coming from a variety of sources. The minor difference between the two is that the non-authoritative DNS servers need to make outbound connections to other authoritative DNS servers, while authoritative DNS servers require zone transfers. In theory, DNS clients of non-authoritative DNS servers are local subscribers or internal enterprise users— a reasonably finite number which could be approximated. DNS clients of authoritative DNS servers could be any local DNS server around the world; so the number of clients for authoritative DNS servers depends on how popular their domain names are. In a small to medium-size load environment, DNS servers may be both authoritative and non-authoritative. In a large environment, DNS servers may be dedicated to serve as either authoritative or non-authoritative.

Product versions and revision history

Product and versions tested for this deployment guide:

Product Tested	Version Tested
BIG-IP system	v10.2

Document Version	Description
1.0	New deployment guide
1.1	Changed title and some headings from “DNS load balancing” to “DNS Traffic Management” to more accurately reflect the role of the BIG-IP LTM.

Configuring the BIG-IP for DNS traffic management using the application template

In this section, we describe how to configure the BIG-IP for DNS load balancing using the Application Template. For more information on specific settings, see the online help.

The sections following the Application Template configuration show other ways to configure the BIG-IP for load balancing DNS.

◆ Note

Even if you want to configure the BIG-IP manually without using the template, you must use the template to create the health monitor.

To run the Generic DNS application template

1. Verify that your current administrative partition is set to **Common**. The Partition list is in the upper right corner.
2. On the Main tab, expand **Templates and Wizards**, and then click **Templates**. The Templates screen opens, displaying a list of templates.
3. In the Application column, click **Generic DNS**. The Generic DNS application template opens.
4. In the **Virtual Server Questions** section, complete the following:
 - a) You can type a unique prefix for the DNS objects this template creates. In our example, we leave this setting at the default, **my_DNS_**.
 - b) If you are using the template for the entire configuration, leave the Monitor Only list at **No**.

If you want to use this Template only to create the health monitor and configuring the rest of the settings manually, select **Yes** from the list.

- c) Enter the IP address for this DNS virtual server. The system creates a virtual server named **my_DNS_virtual_server**. In our example, we type **192.0.2.150**.
- d) If the servers can communicate with the clients using a route through the BIG-IP system to deliver response data to the client, select **Yes** from the list. In this case, the BIG-IP does **not** translate the client's source address.

If the BIG-IP system should translate the client's source address to an address configured on the BIG-IP system, leave the list at the default setting, **No**. Selecting **No** means the BIG-IP system uses SNAT automap. See the Online Help for more information. In our example, we leave this at the default setting: **No**.

Templates and Wizards » Templates » Generic DNS	
Virtual Server Questions	
What unique prefix do you want the BIG-IP system to use when naming objects that this template creates?	<input type="text" value="my_DNS_"/>
Do you want to use this template to create a health monitor only?	<input type="button" value="No"/>
What IP address do you want to use for this virtual server?	<input type="text" value="192.0.2.150"/>
Do the Generic DNS servers have a route back to application clients via this BIG-IP system?	<input type="button" value="No"/>

Figure 1.1 DNS template virtual server questions

5. In the **Server Pool and Load Balancing Questions** section, complete the following:
 - a) From the Load Balancing Method list, select an appropriate load balancing method. In our example, we leave this setting at the default, **Least Connections (member)**.
 - b) Next, add each of the DNS servers that are a part of this deployment.
 In the **Address** box, type the IP address of the first DNS device. In our example, we type **192.0.2.10**.
 In the **Service Port** box, leave the port at **53**.
 Click the **Add** button. Repeat this step for each of the DNS servers.

Server Pool and Load Balancing Questions	
Do you want to create a new pool or use an existing one?	<input type="button" value="Create New Pool"/>
Which load balancing method do you want to use?	<input type="button" value="Least Connections (member)"/>
Which servers do you want this virtual server to reference? (the virtual server will not be available until at least one server is added)	Address: <input type="text" value="192.0.2.12"/>
	Service Port: <input type="text" value="53"/> <input type="button" value="53"/>
	<input type="button" value="Add"/>
	<input type="text" value="R:1 P:1 C:0 192.0.2.10 :53"/> <input type="text" value="R:1 P:1 C:0 192.0.2.11 :53"/> <input type="text" value="R:1 P:1 C:0 192.0.2.12 :53"/>
	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Figure 1.2 DNS template server pool and load balancing questions

6. In the **Protocol Optimization Questions** section, if most clients will be connecting to the virtual server from a WAN, select **WAN** from the list. If most clients will be connecting from a LAN, select **LAN** from the list.
This option determines the profile settings that control the behavior of a particular type of network traffic.
7. In the **Monitor Questions** section, complete the following:
 - a) From the Record type list, select the record type to test the DNS servers. In our example, we leave this at the default **A**.
 - b) Type the host name you want to send the DNS server for this monitor. In our example, we type **www.example.com**.
 - c) Type IP address you expect to receive from the DNS server from from the host name in step b. In our example, we type **192.0.2.50**.
8. Click the **Finished** button.

The screenshot shows a configuration window with two main sections: "Protocol Optimization Questions" and "Monitor Questions".

Protocol Optimization Questions

Will clients be connecting to this virtual server primarily over a LAN or a WAN?	WAN
--	-----

Monitor Questions

What record type do you want to use to test these DNS servers?	A
What hostname do you want to send to the DNS server for this health monitor?	www.example.com
What IP address do you expect to receive from the DNS server if the server is healthy?	192.0.2.50

At the bottom of the window are two buttons: "Cancel" and "Finished".

After clicking Finished, the BIG-IP system creates the relevant objects. You see a summary screen that contains a list of all the objects that were created. In this example, the BIG-IP LTM creates the following objects:

- TCP Virtual Server
- UDP Virtual Server
- LAN-optimized TCP profile
- WAN-optimized TCP profile
- UDP profile
- Load Balancing Pool
- Custom UDP health monitor

To learn about advanced DNS load balancing techniques, see *Advanced DNS traffic management using the BIG-IP LTM*, on page 2-1.



2

Advanced DNS Traffic Management using the BIG-IP LTM

- Stateless UDP with nPath Routing
- Stateless UDP traffic management
- Basic Stateful UDP traffic management
- Stateful UDP Datagram traffic management
- Layer 7 UDP traffic management
- Appendix A: Configuring the BIG-IP LTM for DNS TCP traffic

Advanced DNS traffic management using the BIG-IP LTM

In this chapter, we provide options for advanced DNS traffic management techniques. This chapter is divided into the following sections:

- *Stateless UDP with nPath Routing*, on page 2-2
- *Stateless UDP traffic management*, on page 2-8
- *Basic Stateful UDP traffic management*, on page 2-11
- *Stateful UDP Datagram traffic management*, on page 2-13
- *Layer 7 UDP traffic management*, on page 2-15

An important consideration to keep in mind when choosing the appropriate DNS load balancing option is that there is a trade-off between performance and how deep into the DNS packets the BIG-IP LTM system inspects. The load balancing options are presented in order of performance; from the highest performing (thus the least inspection) to the deepest inspection.

◆ **Note**

*DNS queries and responses use UDP port 53, while zone transfers use TCP port 53. In an advanced configuration, you may only want to load balance the UDP traffic. In the following scenarios, we detail the specific UDP configuration. Because the TCP configuration is the same across all scenarios, we include those procedures in **Appendix A: Configuring the BIG-IP LTM for DNS TCP traffic**, on page 2-17.*

Using the Application Template to create a DNS health monitor

In this chapter, we use the Application Template to create the health monitor. In order to use the DNS Application Template on the BIG-IP LTM, you must be using BIG-IP 10.2 or later.

The template creates a new monitor based on the UDP monitor. The monitor creates a hex string for Send String in the monitor, which represents the DNS query. It also creates a Receive String as a hex string representing the IP address part of DNS response. These Send and Receive strings are derived from the answers you provide while running the template wizard.

Using the template to create a monitor is not a requirement for the following configuration options. You can create your own health monitor on the BIG-IP system; however the template makes the process much easier.

In our examples below, we only show how to create a monitor using the template. For more information on creating your own UDP monitor, see the *Configuring Monitors* chapter in the **Configuration Guide for BIG-IP Local Traffic Manager**, available on <https://support.f5.com>.

Stateless UDP with nPath Routing

With nPath routing, the BIG-IP LTM forwards DNS queries to DNS servers without modifying the destination IP address. The IP address on the loopback interface of the DNS servers must be the IP address of the BIG-IP LTM virtual server, and the default gateway of DNS servers is a router and not the BIG-IP LTM.

In a high-load environment (for example, more than 500,000 DNS queries per second), nPath is the best option. The advantage of nPath routing is that the BIG-IP LTM does not need to process returning traffic, resulting in a lighter load. Even though the DNS servers connect directly to the BIG-IP LTM, the LTM acts as a line-rate, non-blocking layer-2 switch for the returning traffic. This mode requires minor configuration changes on the DNS servers (see steps 4 and 5 in the Configuration section).

By using nPath with a timeout value of immediate in the BIG-IP LTM Fast L4 profile, the LTM does not create an entry in the connection table for DNS query sessions. This prevents the connection table from filling up. For example, if there are one million DNS queries per second, and each DNS query comes from a unique source IP/port with an idle timeout of 300 seconds, the connection table could fill in 16 seconds on a BIG-IP LTM 8900 (the BIG-IP LTM 8900 supports a maximum of 16 million concurrent connections).

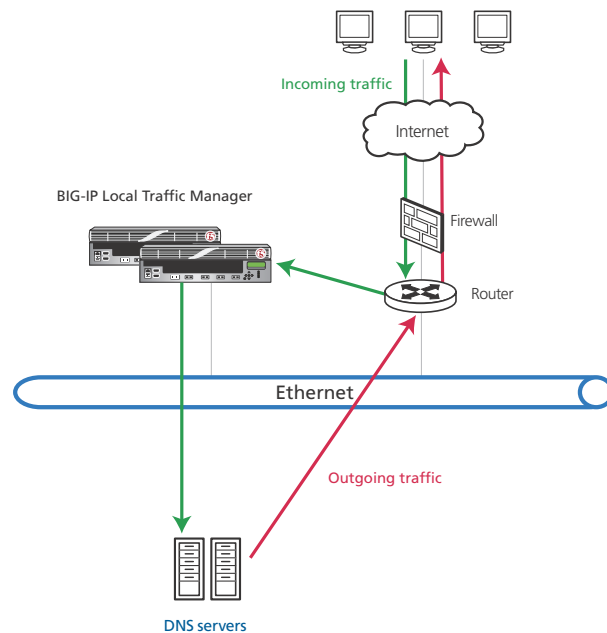


Figure 2.1 Logical nPath configuration example

For more information on nPath routing, see the *Configuring nPath Routing* chapter in the **BIG-IP Local Traffic Manager: Implementations** guide, available on <https://support.f5.com>.

Creating a DNS health monitor

In the following procedure, we use the DNS Application Template only to create the DNS health monitor.

To run the Generic DNS application template

1. Verify that your current administrative partition is set to **Common**. The Partition list is in the upper right corner.
2. On the Main tab, expand **Templates and Wizards**, and then click **Templates**. The Templates screen opens.
3. In the Application column, click **Generic DNS**.
4. In the **Virtual Server Questions** section, complete the following:
 - a) You can type a unique prefix for the DNS objects this template creates. In our example, we leave this setting at the default, **my_DNS_**.
 - b) Select **Yes** from the list asking if you only want the template to configure the monitor.
5. In the **Monitor Questions** section, complete the following:
 - a) From the Record type list, select the record type you want to use to test the DNS servers. In our example, we leave this at the default **A**.
 - b) Type the host name you want to send the DNS server for this monitor. In our example, we type **siterequest**.
 - c) Type IP address you expect to receive from the DNS server from from the host name in step b. In our example, we type **192.0.2.50**.
6. Click the **Finished** button.

Creating a monitor to support transparent mode

If you need to use transparent mode for any reason (such as in an nPath configuration), create the following health monitor.

Important

*This monitor imports the settings from the custom monitor created by the template. You must have already created a monitor using the Application Template as describe in **Creating a DNS health monitor**, on page 3.*

To create the new monitor to support transparent mode

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 **my_DNS_transparent_monitor**.

4. From the **Type** list, select **UDP**.
5. **Important:** From the **Import Settings** list, select the name of the monitor that was created by the template. In our example, we select **my_DNS_transparent_monitor**.
6. From the Configuration list, select **Advanced**.
7. In the **Transparent** row, click the **Yes** button.
8. In the **Alias Address** box, type the IP address the DNS service starts on (this should match the virtual server IP address you will create in *Creating the virtual server*, on page 2-6). We type **192.0.2.125**.
9. In the **Alias Port** box, type **53**.
10. Click the **Finished** button.

General Properties	
Name	my_DNS_transparent_monitor
Type	UDP
Import Settings	my_DNS_monitor
Configuration: Advanced	
Interval	30 seconds
Up Interval	Disabled
Time Until Up	0 seconds
Timeout	91 seconds
Manual Resume	<input type="radio"/> Yes <input checked="" type="radio"/> No
Send String	\xc3\x9f\x01\x00\x01\x00\x00\x00\x00\x00
Receive String	\x00\x01.*\x04\xc0\x00\x02\x32
Receive Disable String	
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Transparent	<input checked="" type="radio"/> Yes <input type="radio"/> No
Send Packets	2
Timeout Packets	2
Alias Address	192.0.2.125
Alias Service Port	53 Domain
Debug	No
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>	

Figure 2.2 Transparent DNS monitor (truncated)

Creating the pool

Next, we create the load balancing pool that contains the DNS servers.

To create the pool

1. On the Main tab, expand **Local Traffic**, and then click **Pools**.
2. Click the **Create** button. The New Pool screen opens.
3. In the **Name** box, type a name for your pool. We type **DNS-pool**.
4. In the **Health Monitors** section, select the name of the monitor that was created by the template in *Creating a DNS health monitor* (or the transparent monitor if you created one), and click the Add (<<) button. In our example, we select **my_DNS_monitor**.
5. From the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).
In our example, we select **Least Connections (member)**.
6. In this pool, we leave the Priority Group Activation **Disabled**.
7. In the New Members section, select the **New Address** option.
8. In the **Address** box, add the first DNS server to the pool. In our example, we type **10.132.81.100**.
9. In the **Service Port** box, type **53**.
10. Click the **Add** button to add the member to the list.
11. Repeat steps 8-10 for each server you want to add to the pool.
In our example, we repeat these steps four times for the remaining servers, **10.132.81.101 - .104**.
12. Click the **Finished** button.

Creating a Fast L4 profile

The next task is to create a Fast L4 profile. When using a Fast L4 profile with a timeout value of immediate, the LTM does not create an entry in the connection table for DNS query sessions. This prevents the connection table from filling up.

To create a new Fast L4 profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
The HTTP Profiles screen opens.
2. On the Menu bar, click **Protocol**, and then click **Fast L4**.
3. Click the **Create** button.
4. In the **Name** box, type a name for this profile. In our example, we type **DNS-fastL4**.

5. In the **Idle Timeout** row, check the **Custom** box, and then select **Immediate** from the list.
6. Click the **Finished** button.

Creating the virtual server

Next, we configure a virtual server that references the profile and pool you created in the preceding procedures.

To create the virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. Click the **Create** button. The New Virtual Server screen opens.
3. In the **Name** box, type a name for this virtual server. In our example, we type **DNS_virtual**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address of this virtual server. In our example, we use **192.0.2.125**.
6. In the **Service Port** box, type **53**.
7. From the **Configuration** list, select **Advanced**.
8. From the **Type** list, select **Performance (Layer 4)**.
9. From the **Protocol** list, select **UDP**.
10. From the **Protocol Profile (Client)** list, select the profile you created in *Creating a Fast L4 profile*. In our example, we select **DNS-fastL4**.
11. From the **Source Port** list, select **Preserve Strict**. (Note: This is only necessary for nPath configurations).
12. In the Resources section, from the **Default Pool** list, select the pool you created in the *Creating the pool* section. We select **DNS-pool**.
13. Click the **Finished** button.

◆ Note

*For instructions on configuring the BIG-IP LTM for TCP DNS traffic, see **Appendix A: Configuring the BIG-IP LTM for DNS TCP traffic**, on page 2-17.*

Modifying the DNS server configuration

The final task in this section is to modify the DNS server configuration.

◆ Note

It is outside the scope of this document to provide step-by-step instructions for configuring DNS servers, refer to your DNS server documentation for specific instructions.

Perform the following tasks to complete the configuration

- ◆ Configure the address of the virtual server you just created (step 5 of *To create the virtual server*) on each DNS server loopback interface.
- ◆ The default route on the DNS servers does not need to change. Do NOT set the default route of the DNS servers to the BIG-IP LTM.

Stateless UDP traffic management

With Stateless UDP traffic management, the BIG-IP LTM acts as a Layer 4 proxy, but does not track connection state, which would bind incoming UDP requests and outgoing UDP responses together. In medium to high load environments, this configuration option may provide a good balance between performance and flexibility.

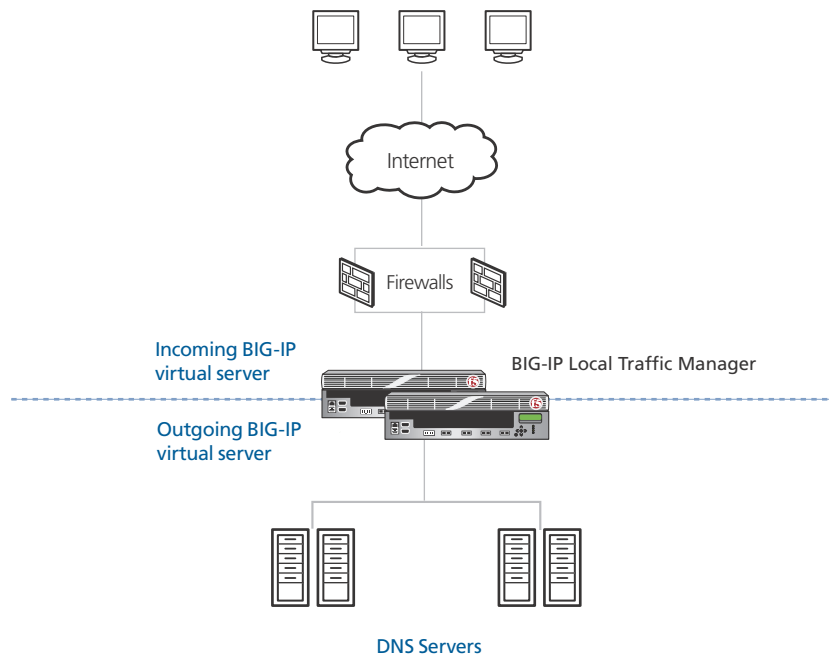


Figure 2.3 Logical Stateless UDP configuration example

In this section, where applicable, we refer back to the procedures in the previous section.

Creating the health monitor

To create the health monitor, follow the procedure *Creating a DNS health monitor*, on page 2-3 without modification.

Creating the pool

To create the pool, follow the procedure *Creating the pool*, on page 2-5 without modification.

Creating the Fast L4 profile

To create the Fast L4 profile, follow the procedure *Creating a Fast L4 profile*, on page 2-5 without modification.

Creating the virtual servers

In this scenario, we create multiple virtual servers, one on the incoming VLAN, another on the Outgoing VLAN, and others to allow other outgoing traffic from the DNS servers.

Creating the virtual server on the incoming VLAN

To create this virtual server, follow the procedure *Creating the virtual server*, on page 2-6, with the following modifications:

- ◆ This virtual server should be on the incoming VLAN.
- ◆ Clear the check box to disable **Port Translation**. Leave **Address translation** enabled.
- ◆ Do not modify the **Source Port** list in Step 11.
- ◆ Associate the Fast L4 profile and pool you created in this section with the virtual server.

Creating the SNAT Pool

The next task is to configure a SNAT pool that includes the virtual server address you just created. This SNAT pool is used in the following virtual server.

To create the SNAT pool

1. On the Main tab, expand **Local Traffic**, and then click **SNATs**.
2. On the Menu Bar, click **SNAT Pool List**.
3. Click the **Create** button.
4. In the **Name** box, type a name for this SNAT pool. In our example, we type **DNS-SNAT-pool**.
5. In the **IP Address** box, type the IP address you used for virtual server you just created in *Creating the virtual server on the incoming VLAN*, on page 2-9, and then click the **Add** button.
6. Click **Finished**.

Creating the virtual server on the outgoing VLAN

For the virtual server on the outgoing VLAN, we create a wildcard virtual server. Use the following procedure.

To create the wildcard virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**.
2. Click the **Create** button.
3. In the **Name** box, type a name. We type **DNS_wildcard**.
4. In the **Address** box, type *****.
5. In the **Service Port** box, type ***** or select ***All Ports** from the list.
6. From the **Configuration** list, select **Advanced**.
7. From the **Type** list, select **Forwarding (IP)**.
8. From the **Protocol** list, select **UDP**.
9. From the **Protocol Profile (Client)** list, select the profile you created in *Creating a Fast L4 profile*. In our example, we select **DNS-fastL4**.
10. From the **SNAT Pool** list, select the SNAT Pool you created in *Creating the SNAT Pool*. In our example, we select **DNS-SNAT-pool**.
11. In the Resources section, from the **Default Pool** list, select the pool you created in the *Creating the pool* section. In our example, we select **DNS-pool**.
12. Click **Finished**

◆ **Note**

Because this is a forwarding virtual server, the BIG-IP system forwards traffic based on routing. You may need to configure a default gateway on the BIG-IP LTM. See the online help or BIG-IP documentation for more information.

To create additional virtual servers to allow outgoing traffic

Because the wildcard virtual server on the outgoing VLAN can match any UDP traffic from the DNS servers to any IP/port, it may affect other traffic because of the timeout value is set to immediate. To allow other types of outgoing UDP traffic from the DNS servers to be handled properly, you must create the appropriate BIG-IP LTM virtual servers.

For example, in order to allow outgoing DNS queries, you would create wildcard virtual server on port 53 with a Type of Forwarding (IP). You may need to assign a custom SNAT address to the virtual server, depending on your topology. See the BIG-IP documentation or the online help for more information on SNATs.

◆ **Note**

*For instructions on configuring the BIG-IP LTM for TCP DNS traffic, see **Appendix A: Configuring the BIG-IP LTM for DNS TCP traffic**, on page 2-17.*

Basic Stateful UDP traffic management

With basic stateful UDP traffic management, the BIG-IP LTM acts as a Layer 4 proxy. All DNS queries and answers pass through LTM, and the LTM tracks the state of UDP sessions in the connection table.

The BIG-IP LTM creates an entry in the connection table for each unique UDP session as defined by 4-tuple: a unique combination of source and destination IP addresses and ports. Because the LTM performs destination address translation for DNS queries, entries in the connection table are required so the BIG-IP LTM can match returning DNS answers and perform necessary address translation.

By treating UDP as a stateful session, subsequent DNS queries which match an entry in connection table requires no load balancing decision and are forwarded to the DNS server stored in that entry. This means the BIG-IP LTM uses less CPU processing. The idle timeout should be adjusted to ensure that connection table consumes a reasonable amount of memory (a longer idle timeout causes the connection table to consume more memory).

This configuration option applies to local DNS server load balancing or enterprise environments more than authoritative DNS server load balancing or ISP deployments. Local DNS servers usually support a specific number of clients which normally re-use their original source ports when they send subsequent queries to local DNS servers. Authoritative DNS servers may receive DNS queries from variety of source IPs and ports. Tracking these sessions may overwhelm the BIG-IP LTM's connection table, depending on popularity of the domain name.

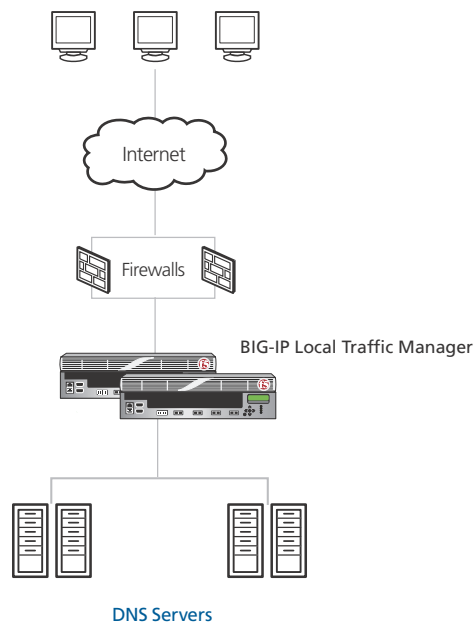


Figure 2.4 Logical Stateful configuration example

Creating the health monitor

To create the health monitor, follow the procedure *Creating a DNS health monitor*, on page 2-3 without modification.

Creating the pool

To create the pool, follow the procedure *Creating the pool*, on page 2-5 without modification.

Creating the Fast L4 profile

To create the Fast L4 profile, follow the procedure *Creating a Fast L4 profile*, on page 2-5 with the following modification:

- ◆ Step 5, in the **Idle Timeout** box, type an appropriate timeout. Do NOT select an Idle Timeout of Immediate.

Creating the virtual server

To create this virtual server, follow the procedure *Creating the virtual server*, on page 2-6, with the following modifications:

- ◆ Do not modify the **Source Port** list in Step 11.
- ◆ If your topology requires a SNAT, you will need to configure a SNAT pool. See *Creating the SNAT Pool*, on page 2-9.

◆ Note

*For instructions on configuring the BIG-IP LTM for TCP DNS traffic, see **Appendix A: Configuring the BIG-IP LTM for DNS TCP traffic**, on page 2-17.*

Stateful UDP Datagram traffic management

With stateful UDP datagram traffic management, the BIG-IP LTM treats each new DNS query as a new session. The BIG-IP LTM also creates session entries in the connection table. Configuring a UDP profile with Datagram load balancing enabled allows the BIG-IP LTM to load balance DNS queries coming from same source IP/port to multiple DNS servers on a granular level.

The BIG-IP LTM adds a new entry in the connection table for each new DNS query and removes that entry once the DNS response has been sent back to the requester, or if the idle timeout is reached. The Idle timeout should be adjusted to ensure the connection table consumes a reasonable amount of memory.

Creating the health monitor

To create the health monitor, follow the procedure *Creating a DNS health monitor*, on page 2-3 without modification.

Creating the pool

To create the pool, follow the procedure *Creating the pool*, on page 2-5 without modification.

Creating a UDP profile

The next task is to create a custom UDP profile.

To create a new UDP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. On the Menu bar, click **Protocol**, and then click **UDP**.
3. Click the **Create** button.
4. In the **Name** box, type a name for this profile. In our example, we type **DNS-UDP**.
5. In the **Idle Timeout** row, check the **Custom** box, and then type an appropriate timeout value. In our example, we type **3** seconds.
6. In the **Datagram LB** row, check the **Custom** box, and then check the box to enable Datagram load balancing.
7. Click the **Finished** button.

Creating the virtual server

To create this virtual server, follow the procedure *Creating the virtual server*, on page 2-6, with the following modifications:

- ◆ In Step 8, the **Type** list should remain set at **Standard**.
- ◆ In Step 10, instead of a Fast L4 profile, select the UDP profile you created in *Creating a UDP profile*, on page 2-13. In our example, we select **DNS-UDP**.
- ◆ Do not modify the **Source Port** list in Step 11.

◆ **Note**

For instructions on configuring the BIG-IP LTM for TCP DNS traffic, see Appendix A: Configuring the BIG-IP LTM for DNS TCP traffic, on page 2-17.

Layer 7 UDP traffic management

With Layer 7 UDP load balancing, the BIG-IP LTM acts as a Layer 7 proxy, and is able to inspect and modify the DNS protocol information using an iRule. The BIG-IP LTM can extract UDP payload, decode DNS protocol, direct traffic based on DNS protocol information, or even manipulate the DNS answer.

F5's DevCentral (requires a free registration) contains a number of customized iRule examples, such as:

<http://devcentral.f5.com/wiki/default.aspx/iRules/DnsFloodProtection.html>

http://devcentral.f5.com/wiki/default.aspx/iRules/DNS_Flood_Protection_v2.html

http://devcentral.f5.com/Wiki/default.aspx/iRules/DNS_non_english_domain_name_detection.html

http://devcentral.f5.com/Wiki/default.aspx/iRules/DNS_no_more_non_existent_domain.html

http://devcentral.f5.com/Wiki/default.aspx/iRules/DNS_query_id_zero_blocking.html

Creating the health monitor

To create the health monitor, follow the procedure *Creating a DNS health monitor*, on page 2-3 without modification.

Creating the pool

To create the pool, follow the procedure *Creating the pool*, on page 5 without modification.

Creating a UDP profile

To create the UDP profile, follow the procedure *Creating a UDP profile*, on page 2-13 with the following modification:

- ◆ Step 6, enabling Datagram Load Balancing is optional. This scenario does not require Datagram Load Balancing.

Creating the iRule

The next task is to create an iRule. Choose an iRule from the list above, or one of your own.

To create the iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**.
2. Click the **Create** button.
3. In the **Name** box, type a name. We type **DNS-irule**.

4. In the **Definition** box, copy and paste the iRule code from one of the DevCentral links (or create your own).
5. Click **Finished**.

Creating the virtual server

To create this virtual server, follow the procedure *Creating the virtual server*, on page 2-6, with the following modifications:

- ◆ In Step 8, the **Type** list should remain set at **Standard**.
- ◆ In Step 10, instead of a Fast L4 profile, select the UDP profile you created in *Creating a UDP profile*, on page 2-13. In our example, we select **DNS-UDP**.
- ◆ Do not modify the **Source Port** list in Step 11.
- ◆ In the Resources section, from the iRule **Available** list, select the iRule you created in the preceding procedure and click the Add (<<) button.
- ◆ From the **Default Pool** list, select the Pool you created in this section.

◆ Note

*For instructions on configuring the BIG-IP LTM for TCP DNS traffic, see **Appendix A: Configuring the BIG-IP LTM for DNS TCP traffic**, on page 2-17.*

Appendix A: Configuring the BIG-IP LTM for DNS TCP traffic

DNS traffic management consists of both TCP and UDP traffic. DNS queries and responses use UDP port 53, while zone transfers use TCP port 53. You may only want to load balance UDP traffic, or you may want to load balance both TCP and UDP (the Application Template creates both the UDP and TCP virtual servers by default).

If you want to configure the BIG-IP LTM to load balance the DNS TCP traffic, complete the procedures in this section. The TCP virtual server uses the existing pool containing the DNS servers you already created.

◆ Note

If your topology requires a SNAT, you may need to configure a SNAT pool. See [Creating the SNAT Pool](#), on page 2-9.

Creating the TCP profiles

For the TCP configuration, we create TCP profiles. In this example, we use a WAN-optimized parent profile for the client traffic and a LAN optimized profile for the server traffic.

Creating the LAN optimized TCP profile

First we configure the LAN optimized profile.

To create a TCP LAN optimized profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Protocol** menu, click **tcp**.
3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **DNS-tcp-lan**.
5. From the **Parent Profile** list, select **tcp-lan-optimized**.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating the WAN optimized TCP profile

Now we configure the WAN optimized profile. If most of the users are accessing the system over the LAN or other low latency links, you do not need to create this profile.

To create a new TCP WAN optimized profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Protocol** menu, click **tcp**.
3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **DNS-tcp-wan**.
5. From the **Parent Profile** list, select **tcp-wan-optimized**.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating the virtual server

Next, we configure a virtual server that references the profiles you created in the preceding procedures and the existing DNS server pool.

To create the virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. Click the **Create** button. The New Virtual Server screen opens.
3. In the **Name** box, type a name for this virtual server. In our example, we type **DNS-tcp-virtual**.
4. In the **Address** box, type the IP address of this virtual server. In our example, we use **192.168.10.127**.
5. In the **Service Port** box, type **53**.
6. From the Configuration list, select **Advanced**.
7. Leave the **Type** list at the default setting: **Standard**.
8. From the **Protocol Profile (Client)** list select the name of the profile you created in the *Creating the WAN optimized TCP profile* section. In our example, we select **DNS-tcp-wan**.
9. From the **Protocol Profile (Server)** list, select the name of the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **DNS-tcp-lan**.
10. If you created a SNAT pool, select it from the **SNAT Pool** list.
11. In the Resources section, from the **Default Pool** list, select the pool you created in the *Creating the pool* section. In our example, we select **DNS-pool**.
12. Click the **Finished** button.