DEPLOYMENT GUIDE
Version 1.2

Deploying the BIG-IP LTM for SIP Traffic Management

Table of Contents

Configuring the BIG-IP LTM for SIP traffic management

1

Configuring the BIG-IP LTM for SIP Traffic Management

Configuring the BIG-IP LTM for SIP traffic management

Welcome to the F5 deployment guide for Session Initiation Protocol (SIP). This document provides step-by-step procedures for configuring the BIG-IP Local Traffic Manager (LTM) for intelligent SIP traffic management.

SIP is a critical component of IMS architectures. F5's BIG-IP SIP traffic management solution provides high scalability, availability, and reliability to the SIP Proxy, Session Border Controller, media servers and many other SIP devices. The BIG-IP LTM can distribute and balance SIP and RTP traffic among multiple SIP devices so that service availability is guaranteed even under high call volumes. Additionally, the F5 solution can perform advanced health checks on the SIP devices, routing SIP clients away from unstable or unreliable devices and providing increased reliability to existing SIP solutions.

The BIG-IP LTM supports three transport protocols for SIP: UDP, TCP, and SCTP. This document covers the use case for UDP only. However, with minor modifications to the protocol profile and virtual server type, it could be applied to TCP and SCTP.

This guide is broken up into the following scenarios, use the one most appropriate for your configuration:

- *Configuring the BIG-IP LTM for basic inbound SIP traffic management*, on page 4
- *Configuring the BIG-IP LTM for inbound and outbound SIP traffic management*, on page 10

This guide also includes an advanced section, see *Configuring advanced SIP traffic management*, on page 15.

Note

The SIP functionality in the BIG-IP LTM implies Message-based Load Balancing. See the following white paper for more information about SIP and Message-based Load Balancing:
http://www.f5.com/pdf/white-papers/sip-mblb-wp.pdf.

For more information on the BIG-IP LTM, see
www.f5.com/products/big-ip/product-modules/local-traffic-manager.html

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 “SIP load balancing” to “SIP Traffic Management” to more accurately reflect the role of the BIG-IP LTM.
1.2	Added Traffic Flow diagrams in *Appendix A: Traffic Flow diagrams*, on page 20.

Note

This document is written with the assumption that you are familiar with the BIG-IP LTM system. For more information, see the ***Configuration Guide for BIG-IP Local Traffic Manager*** *and the* ***Implementations Guide*** *available on Ask F5 (**http://support.f5.com/kb/en-us.html**).*

Configuration example

The following logical configuration example shows a BIG-IP LTM directing traffic to multiple SIP servers as well as optional Media servers. The BIG-IP LTM provides scalability, high availability, and reliability for SIP deployments.

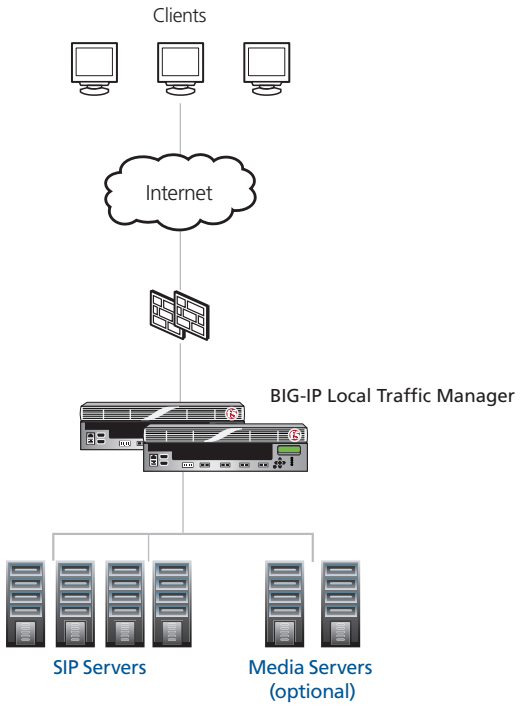

Figure 1 *Logical configuration example*

The SIP traffic flow is typically communication between two User Agents, which may or may not travel through SIP proxies. The BIG-IP LTM be used to load balance SIP proxies (or SIP servers).

For a traffic flow diagram of a typical SIP transaction, including the BIG-IP LTM, see *Appendix A: Traffic Flow diagrams*, on page 20.

Configuring the BIG-IP LTM for basic inbound SIP traffic management

The first use case we present is basic SIP traffic management for inbound SIP traffic. The servers could be SIP proxies, Session Border Controllers (SBCs) or any SIP server that can not have outbound traffic or does not have outbound traffic routed through BIG-IP.

For a traffic flow diagram, see *Inbound SIP only*, on page 20.

Creating the SIP monitor

The first task is to create a SIP health monitor on the BIG-IP system. The SIP monitor checks the status of SIP Call-ID services. By default, this monitor type issues a SIP OPTIONS request to a server device over UDP. However, you could use one of the following protocols instead: TCP, TLS, and SIPS (Secure SIP).

The request the monitor issues to a device is designed to identify the options the server device supports. If the proper request is returned, the device is considered to be up and responding to commands.

To create the SIP monitor

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 **SIP-monitor**.
4. From the **Type** list, select **SIP**. The SIP monitor options appear.
5. Configure any of the other options as applicable for your implementation. In our example, we leave the default settings.
6. Click the **Finished** button.

Creating the SIP load balancing pool

The next task is to create a load balancing pool that uses the health monitor you just created.

To create the SIP pool

1. On the Main tab, expand **Local Traffic**, and then click **Pools**.
1. Click the **Create** button. The New Pool screen opens.
2. In the **Name** box, type a name. In our example, we use **SIP-pool**.
3. In the **Health Monitors** section, select the name of the monitor you created in *Creating the SIP monitor*, on page 4, and then click the Add (**<<**) button. In our example, we select **SIP-monitor**.

4. From the **Load Balancing Method** list, select **Round Robin**.
5. For this pool, we leave the Priority Group Activation **Disabled**.
6. In the New Members section, in the **Address** box, add the first server to the pool. In our example, we type **192.0.2.123**
7. In the **Service Port** box, type the service number you want to use for this device, or specify a service by choosing a service name from the list. In our example, we type **5060**.
8. Click the **Add** button to add the member to the list.
9. Repeat steps 6-8 for each device you want to add to the pool.
10. Click the **Finished** button

Creating the profiles

The next task is to create the profiles on the BIG-IP LTM for SIP load balancing. For this configuration, we create three profiles, a SIP profile, a SIP persistence profile and a UDP profile.

Creating the SIP profile

The first profile we create is the SIP protocol profile. The SIP profile automatically configures the BIG-IP system to handle persistence for SIP sessions. In most cases, Call-ID is used as a persistent key to ensure the same call flow persists to the same server.

However, the SIP profile has the ability to insert a Via Header and a Record-Route Header. During typical SIP communication, SIP traffic may traverse multiple SIP proxies before reaching its end destination. In some cases, inserting Via and/or Record-Route headers may be required to keep the BIG-IP LTM in the signaling path.

BIG-IP can also keep track of server-initiated SIP dialog (based on Call-ID and tag in the to/from header), using the Dialog Aware and Community settings. When SIP messages come back, BIG-IP LTM can use that information to match SIP messages and direct them to the proper server.

While we use the default (Call-ID) in our example, you can configure the SIP headers in steps 5 and 6 in the following procedure if applicable for your configuration. Advanced SIP persistence can also be performed using iRules on the BIG-IP system, but that configuration is outside the scope of this document.

To create the SIP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. On the Menu bar, from the **Services** menu, click **SIP**.
3. Click the **Create** button.
4. In the **Name** box, type a name for this profile. In our example, we type **SIP-profile**.

5. *Optional*: If applicable (see explanation above), from the **Insert Via Header** row, click the **Custom** box, and then select **Enabled** from the list. The **User Via** row appears. Click the **Custom** box, and then type the appropriate Via value.
6. *Optional*: If applicable (see explanation above), from the **Insert Record-Route Header** row, click the **Custom** box, and then check the box to enable inserting the Record-Route header.
7. *Optional*: If your configuration includes server initiated SIP sessions (meaning in an existing connection originated by the client, the server sends a SIP message which belongs to a new SIP session or new Call, perform the following:
   From the **Dialog Aware** row, click the **Custom** box, and then select **Enabled** from the list. The Community row appears.
   Community specifies a string that indicates the SIP dialog group to which this profile belongs. Default community is empty
   Click the **Custom** box in the **Community** row, and then type the appropriate community string.
8. Modify any of the settings as applicable for your network. Refer to the online help for details.
   In our example, we leave the settings at their default levels.
9. Click the **Finished** button.

Creating a SIP persistence profile

The next task is to create a SIP persistence profile. This profile uses the caller-id as the persistent key.

If your implementation does not require persistence, or you have other reasons for not wanting to use persistence, see *Configuring the BIG-IP LTM without using SIP persistence*, on page 7.

In the following procedure, the persistence **Timeout** should be configured to match the needs of your application. For some applications, the persistent timeout might need to be very long, such as 3 hours.

To create the SIP persistence profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. On the Menu bar, click **Persistence**.
3. Click the **Create** button.
4. In the **Name** box, type a name. We type **SIP-persistence**.
5. From the **Persistence Type** list, select **SIP**.
6. *Optional*: We recommend clicking the **Custom** box in the **Timeout** row and setting a Timeout value appropriate for your application.
7. All other settings are optional; configure as applicable for your implementation.
8. Click the **Finished** button.

Configuring the BIG-IP LTM without using SIP persistence

If your implementation does not require persistence, or you have other reasons for not wanting to use persistence, use the following procedure.

Important

Only configure this iRule is you do not want to use persistence for your SIP implementation.

Even if you do not apply a SIP persistence profile to the virtual server, the BIG-IP LTM still uses **Call-ID** as a persistent key. To disable SIP persistence, you must create the following simple iRule which is applied to the virtual server.

Tip

*You could alternatively create custom SIP persistence profile (see the preceding procedure) and in the **SIP Info** field, select something that will never exist in the SIP message header.*

To create the no persistence 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 for this rule. In our example, we type **SIP-no-persist**.
4. In the **Definition** box, type the following iRule:

```
when SIP_REQUEST {
   persist none
}
```

5. Click the **Finished** button.

Creating the UDP profile

The final profile we create is a UDP profile. In our example, we leave the settings at the default levels. For information on the individual options, see the online help or the BIG-IP LTM documentation.

Be sure to set an Idle Timeout value appropriate for your application, otherwise returning traffic might be rejected by the BIG-IP LTM once the connection table is removed due to the timeout.

Tip

If you assign a SIP profile as recommended in this guide, the Datagram LB option has no effect on the virtual server. We recommend leaving the Datagram LB option at the default setting.

To create the UDP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. On the Menu bar, from the **Protocol** menu, click **UDP**.
3. Click the **Create** button.
4. In the **Name** box, type a name for this profile. In our example, we type **SIP-UDP-profile**.
5. *Optional*: In the **Idle Timeout** row, configure an appropriate timeout.
6. Configure any of the other options as applicable for your implementation. In our example, we leave the settings at the default levels.
7. Click the **Finished** button.

Creating a SNAT pool

The next task is to create a SNAT pool for inbound traffic. A SNAT translates the source IP address within a connection to a BIG-IP system IP address that you define. The destination node then uses that new source address as its destination address when responding to the request. For more information on SNATs or other SNAT options, see the online help or product documentation.

For more information on SNATs or SNAT pools, see the online help or the product documentation.

To create a SNAT pool

1. On the Main tab, expand **Local Traffic**, and then click **SNATs**.
2. On the Menu bar, click **SNAT Pool List**.
3. In the **Name** box, type a name for this SNAT pool. In our example, we type **SIP-snat-pool**.
4. In the **IP Address** box, type an IP address that you want to include in the SNAT pool, and then click the **Add** button.
   Repeat this step for additional SNAT addresses.
5. Click the **Finished** button.

Creating the virtual server

Next, we configure a virtual server that references the profiles 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**.
2. Click the **Create** button.
3. In the **Name** box, type a name. We type **SIP-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 type **10.133.81.22**.
6. In the **Service Port** box, type **5060**.
7. From the Configuration list, select **Advanced**.
8. From the **Protocol** list, select **UDP**.
9. From the **Protocol Profile (Client)** list, select the profile you created in *Creating the UDP profile*, on page 7. In our example, we type **SIP-UDP-profile**.
10. From the **SIP Profile** list, select the profile you created *Creating the SIP profile*, on page 5. In our example, we select **SIP-profile**.
11. From the **SNAT Pool** list, select the name of the SNAT pool you created in *Creating a SNAT pool*, on page 8. In our example, we select **SIP-snat-pool**.
    Important: *The SIP health check may fail if you use SNAT Automap. For more information, see:* ***http://support.f5.com/kb/en-us/solutions/public/9000/600/sol9675.html?sr=10086837***.
12. *Optional:* In the Resources section, ***only*** if you created the iRule for not using SIP persistence in *Configuring the BIG-IP LTM without using SIP persistence*, on page 7, from the **iRules Available** list, select the iRule you created, and then click the Add (**<<**) button.
13. from the **Default Pool** list, select the pool you created in *Creating the SIP load balancing pool*, on page 4. In our example, we select **SIP-pool**.
14. From the **Default Persistence Profile** list, select the SIP persistence profile you created in *Creating a SIP persistence profile*, on page 6. In our example, we type **SIP-persistence**.
15. Click the **Finished** button.

This completes the BIG-IP LTM configuration for load balancing inbound SIP traffic.

Configuring the BIG-IP LTM for inbound and outbound SIP traffic management

This use case is very similar to the previous one, however in this case, the SIP server also makes outbound SIP calls (creating new connections) through the BIG-IP LTM. This section includes BIG-IP LTM configuration procedures for both inbound and outbound traffic.

For a traffic flow diagram, see *Inbound and outbound SIP*, on page 21

Note

Because many of the procedures are identical for both use cases, we refer back to the procedures in the preceding use case in this section.

Creating the SIP monitor

To create the SIP monitor, use *Creating the SIP monitor*, on page 4.

There are no differences in the health monitor.

Creating the pool

To create the pool, use *Creating the SIP load balancing pool*, on page 4.

There are no differences in the pool configuration.

Creating the SNAT pool for inbound traffic

To create the SNAT pool, use *Creating a SNAT pool*, on page 8. There are no differences in the SNAT pool configuration.

Creating the profiles

In this section, we create the profiles. Because this use case has two virtual servers, we recommend creating unique profiles for each virtual server.

Creating the SIP profiles

Use the following procedure to create the SIP profiles. The SIP profile automatically configures the BIG-IP system to handle persistence for SIP sessions. In most cases, Call-ID is used as a persistent key to ensure the same call flow persists to the same server.

However, the SIP profile has capability to persist on any SIP header using the Insert Via Header and Insert Record-Route Header options. In typical SIP communication, SIP traffic may traverse multiple SIP proxies before it reaches the end destination. In some cases, Via and/or Record-Route header may be required to keep BIG-IP in the signalling path.

While we use the default (Call-ID) in our example, you can configure the SIP headers in steps 5 and 6 in the following procedure if applicable for your configuration. Advanced SIP persistence can also be performed using iRules on the BIG-IP system, but that configuration is outside the scope of this document.

To create the SIP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. On the Menu bar, from the **Services** menu, click **SIP**.
3. Click the **Create** button.
4. In the **Name** box, type a name. We type **SIP-inbound**.
5. Optional: If applicable (see explanation above), from the **Insert Via Header** row, click the **Custom** box, and then select **Enabled** from the list. The **User Via** row appears. Click the **Custom** box, and then type the appropriate Via value.
6. Optional: If applicable (see explanation above), from the **Insert Record-Route Header** row, click the **Custom** box, and then check the box to enable inserting the Record-Route header.
7. If your configuration includes server initiated SIP sessions (meaning in an existing connection originated by the client, the server sends a SIP message which belongs to a new SIP session or new Call, perform the following:
   From the **Dialog Aware** row, click the **Custom** box, and then select **Enabled** from the list. The Community row appears. Click the **Custom** box in the **Community** row, and then type the appropriate community string.

   IMPORTANT: The Dialog Aware setting and associated Community string is required for the outbound profile. It is optional for inbound.
8. Modify any of the settings as applicable for your network. Refer to the online help for details.
   In our example, we leave the settings at their default levels.
9. Click the **Repeat** button.
10. Return to step 4 and repeat this procedure for the outbound profile.
    In our example, we name this profile **SIP-outbound**.
    If you used a Community string in step 7, be sure to use the same string on this profile.

    IMPORTANT: The Dialog Aware setting and associated Community string is required for the outbound profile. It is optional for inbound.

Creating the UDP profile

Next, we create two UDP profiles. In our example, we leave the settings at the default levels. For information on the individual options, see the online help or the BIG-IP LTM documentation.

Be sure to set an Idle Timeout value appropriate for your application, otherwise returning traffic might be rejected by the BIG-IP LTM once the connection table is removed due to the timeout.

◆ Tip

If you assign a SIP profile as recommended in this guide, the Datagram LB option has no effect on the virtual server. We recommend leaving the Datagram LB option at the default setting.

To create the UDP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. On the Menu bar, from the **Protocol** menu, click **UDP**.
3. Click the **Create** button.
4. In the **Name** box, type a name for this profile. In our example, we type **SIP-UDP-inbound**.
5. *Optional*: We recommend clicking the **Custom** box in the **Idle Timeout** row and setting a Idle Timeout value appropriate for your application.
6. Configure any of the options as applicable for your implementation. In our example, we leave the settings at the default levels.
7. Click the **Repeat** button.
8. Return to step 4 and repeat this procedure for the outbound profile. In our example, we name this profile **SIP-outbound**.

Creating the SIP persistence profile

To configure the SIP persistence profile, use *Creating a SIP persistence profile*, on page 6.

There are no differences in the persistence profile configuration between the use cases. You only need to create one profile for persistence for this use case.

Creating the virtual server for inbound traffic

Use the following procedure for creating the virtual server for inbound traffic.

To create the 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 for this virtual server. In our example, we type **SIP-inbound-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 **10.133.81.25**.
6. In the **Service Port** box, type **5060**.
7. From the Configuration list, select **Advanced**.
8. From the **Protocol** list, select **UDP**.
9. From the **Protocol Profile (Client)** list, select the profile you created for inbound traffic in *Creating the UDP profile*, on page 12. In our example, we type **UDP-inbound**.
10. From the **SIP Profile** list, select the name of the profile you created for inbound traffic in *Creating the SIP profiles*, on page 10. In our example, we select **SIP-inbound**.
11. From the **SNAT Pool** list, select the name of the SNAT pool you created in *Creating the SNAT pool for inbound traffic*, on page 10. In our example, we select **SIP-snat-pool**.

    Important: *The SIP health check may fail if you use SNAT Automap. See the following link for more detail:* ***http://support.f5.com/kb/en-us/solutions/public/9000/600/sol9675.html?sr=10086837***.
12. In the Resources section, from the **Default Pool** list, select the pool you created in *Creating the pool*, on page 10. In our example, we select **SIP-pool**.
13. From the **Default Persistence Profile** list, select the SIP persistence profile you created in *Creating the SIP persistence profile*, on page 12. In our example, we type **SIP-persistence**.
14. Click the **Finished** button.

Creating a SNAT pool for outbound traffic

The next task is to create a SNAT pool for outbound traffic. For more information on SNATs or other SNAT options, see the online help or product documentation.

To create a SNAT pool

1. On the Main tab, expand **Local Traffic**, and then click **SNATs**.

2. On the Menu bar, click **SNAT Pool List**.
3. In the **Name** box, type a name for this SNAT pool. In our example, we type **SIP-snat-outbound**.
4. In the **IP Address** box, type the IP address of the Inbound virtual server you created in *Creating the virtual server for inbound traffic*, on page 12, and then click the **Add** button. In our example, we type **10.133.81.25**.
5. Click the **Finished** button.

Creating the virtual server for outbound traffic

Use the following procedure to create the virtual server for outbound traffic.

To create the 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 for this virtual server. In our example, we type **SIP-outbound-virtual**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type **0.0.0.0**.
6. In the **Service Port** box, type **5060**.
7. From the Configuration list, select **Advanced**.
   The Advanced configuration options appear.
8. From the Protocol list, select **UDP**.
9. From the **Protocol Profile (Client)** list, select the profile you created for outbound traffic in *Creating the UDP profile*, on page 12. In our example, we type **UDP-outbound**.
10. From the **SIP Profile** list, select the name of the profile you created for outbound traffic in *Creating the SIP profiles*, on page 10. In our example, we select **SIP-outbound**.
11. From the **VLAN and Tunnel Traffic** list, select **Enabled on**. The VLANs and Tunnels row appears. From the **Available** list, select the VLAN on which your servers reside and then click the Add (<<) button.
12. From the **SNAT Pool** list, select the SNAT pool you created in *Creating a SNAT pool for outbound traffic*, on page 13. In our example, we type **SIP-snat-outbound**.
13. Click the **Finished** button.

This completes the BIG-IP LTM configuration for inbound and outbound SIP traffic.

Configuring advanced SIP traffic management

The following are optional procedures for supporting implementations with high traffic rates. For some of the following procedures, you must have command line access to the BIG-IP LTM.

Important

This section assumes you have already configured the BIG-IP LTM as described in this guide.

Creating a MBLB profile

The advanced configuration option is to create a message-based load balancing profile. This profile (as configured below) can buffer 10,000 messages.

This profile must currently be created from the command line.

To create the MBLB profile

1. Log on to the BIG-IP LTM and open a command prompt.
2. Type the following command. Note you can change the values as applicable for your configuration.

```
bigpipe profile mblb mymblb { ingress high 10000 ingress low 9000 }
```

3. Use the following syntax to apply the MBLB profile to the virtual server

```
tmsh modify ltm virtual <virtual-name> profiles add { mymblb }
```

In our example, we type the following for use case 1:

```
tmsh modify ltm virtual SIP-virtual profiles add { mymblb }
```

In our example, we type the following for use case 2:

```
tmsh modify ltm virtual SIP-inbound virtual profiles add { mymblb }
```

4. Exit the command line.

Configuring the BIG-IP to offload TLS for SIP over TCP

The BIG-IP LTM supports offloading TLS from the SIP devices for SIP over TCP.

To support offloading SSL, you should have the appropriate certificate and key pair imported onto the BIG-IP LTM. For information on importing certificates and keys, see the ***Configuration Guide for BIG-IP Local Traffic Management***, available on Ask F5 (*http://support.f5.com/kb/en-us.html*).

Creating a Client SSL profile

The first task is to create a Client SSL profile that uses the certificate and key pair.

To create a new Client SSL profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then, on the Menu bar, from the **SSL** menu, select **Client**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **SIP-client-ssl**.
4. In the Configuration section, click a check in the **Certificate** and **Key** Custom boxes.
5. From the **Certificate** list, select the appropriate Certificate.
6. From the **Key** list, select the appropriate Key.
7. Click the **Finished** button.

Creating a virtual server

The next task is to create a new virtual server for inbound SIP traffic on port 5061 that uses the Client SSL profile you just created.

To create the 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 for this virtual server. In our example, we type **SIP-inbound-5061**.
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 **10.133.81.26**.
6. In the **Service Port** box, type **5061**.
7. From the Configuration list, select **Advanced**.
   The Advanced configuration options appear.
8. From the **Protocol** list, select **UDP**.
9. From the **Protocol Profile (Client)** list, select the appropriate UDP profile you created for inbound traffic.
10. From the **SSL Profile (Client)** list, select the Client SSL profile you created in *Creating a Client SSL profile*, on page 16.
11. From the **SIP Profile** list, select the appropriate SIP profile you created for inbound traffic.

12. From the **SNAT Pool** list, select the appropriate SNAT Pool you created for this configuration.
Important: *The SIP health check may fail if you use SNAT Automap. See the following link for more detail:* ***http://support.f5.com/kb/en-us/solutions/public/9000/600/sol9675.html?sr=10086837***.
13. In the Resources section, from the **Default Pool** list, select the appropriate pool you created.
14. From the **Default Persistence Profile** list, select the appropriate SIP persistence profile you created.
15. Click the **Finished** button.

Configuring the BIG-IP LTM to pass RTP/RTCP traffic

SIP communication may include RTP/RTCP traffic; for example the User Agent (UA) making a VOIP call using SIP.

In most deployments, the RTP/RTCP traffic bypasses the BIG-IP LTM, as RTP/RTCP consumes a large amount of throughput and/or CPU cycles on BIG-IP LTM.

However, in some cases, organizations may prefer to deploy the Media Gateway behind the BIG-IP LTM for security or NAT purposes. In this case, the LTM must be configured to pass RTP/RTCP traffic.

If RTP/RTCP traffic must pass through LTM, use one of the following procedures, depending on whether the media server has a routable address or not.

Creating a wildcard virtual server if the media server has a routable address

If the media server address behind the BIG-IP LTM has a routable address, create a wildcard forwarding virtual server to allow traffic to originate from both the client-side and server-side VLANs.

To create a 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 for this virtual server. In our example, we type **SIP-wildcard**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type **0.0.0.0**.
6. In the **Service Port** box, type ***** or select ***All Ports** from the list.

7. From the **Type** list, select **Forwarding (IP)**.
8. From the **VLAN and Tunnel Traffic** list, select **Enabled on**. The VLANs and Tunnels row appears.
   From the **Available** list, select the VLAN that the clients reside on, and then click the Add button.
   From the **Available** list, select the VLAN that the servers reside on and then click the Add button.
9. Click the **Finished** button.

Creating NATs if the media server does not have a routable address

If the BIG-IP LTM performs NAT for the media gateway, perform the following procedure. Note that the SIP server has to use the associated media server's NAT IP address for the SDP information that it sends to client.

To create NATs

1. On the Main tab, expand **Local Traffic**, and then click **SNATs**.
2. On the Menu bar, click **NAT List**.
3. Click the **Create** button.
4. In the **NAT Address** box, type an available public facing IP address. This is the NAT Address that the SIP server must put in the SDP information.
5. In the **Origin Address** box, type the IP address of the first Media Server.
6. Click the **Repeat** button and return to step 3 to repeat for each additional Media server in your configuration.
7. Click the **Finished** button.

Configuring the BIG-IP LTM for advanced SIP traffic manipulation using an iRule

The BIG-IP LTM can support advance SIP traffic manipulation using a SIP/SDP iRule.

With a SIP specific iRule, the BIG-IP LTM can:

- manipulate any SIP headers such as FROM, TO, METHOD, URI, and VIA
- manipulate SIP payload
- manipulate SDP data inside SIP payload

There are 4 SIP specific iRule events:

- SIP_REQUEST
- SIP_REQUEST_SEND
- SIP_RESPONSE
- SIP_RESPONSE_SEND

The SIP_REQUEST and SIP_RESPONSE events are triggered when the BIG-IP LTM fully parses a complete SIP request and SIP response. SIP_REQUEST_SEND and SIP_RESPONSE_SEND are triggered immediately before a SIP request or response is sent.

All SIP events could be triggered regardless of whether the SIP message is coming from the client or server. For example, when a SIP client sends a SIP request, a SIP_REQUEST is triggered. When the SIP server sends a SIP request in an existing connection initiated by client, a SIP_REQUEST event is also triggered.

For more information on creating SIP and SDP iRules, see the following documents on DevCentral:

http://devcentral.f5.com/wiki/default.aspx/iRules.SIP

http://devcentral.f5.com/wiki/default.aspx/iRules.SDP

In the following example, we show how to direct traffic based on SIP URI. In some situations, SIP traffic may be directed to a different destination based on phone number or SIP user name. This information usually comes in SIP URI. The following iRule picks a LTM pool based on the SIP URI.

```
when SIP_REQUEST {
    switch -glob [SIP::uri] {
        "sip:206*" {    log local0. "pool local_sip_proxy"    }
        default    {    log local0. "pool default_sip_proxy"    }
    }
}
```

After creating an iRule, associate it with the appropriate virtual server.

This completes the configuration in the Deployment guide. See Appendix A for traffic flow diagrams.

Appendix A: Traffic Flow diagrams

In this appendix, we provide diagrams that show the SIP traffic flows through the BIG-IP LTM.

Typical SIP transaction

The first traffic flow diagram shows a typical SIP transaction, with the BIG-IP LTM in front of a pool of SIP proxies (or SIP servers). The following diagram shows the typical location of the BIG-IP LTM.

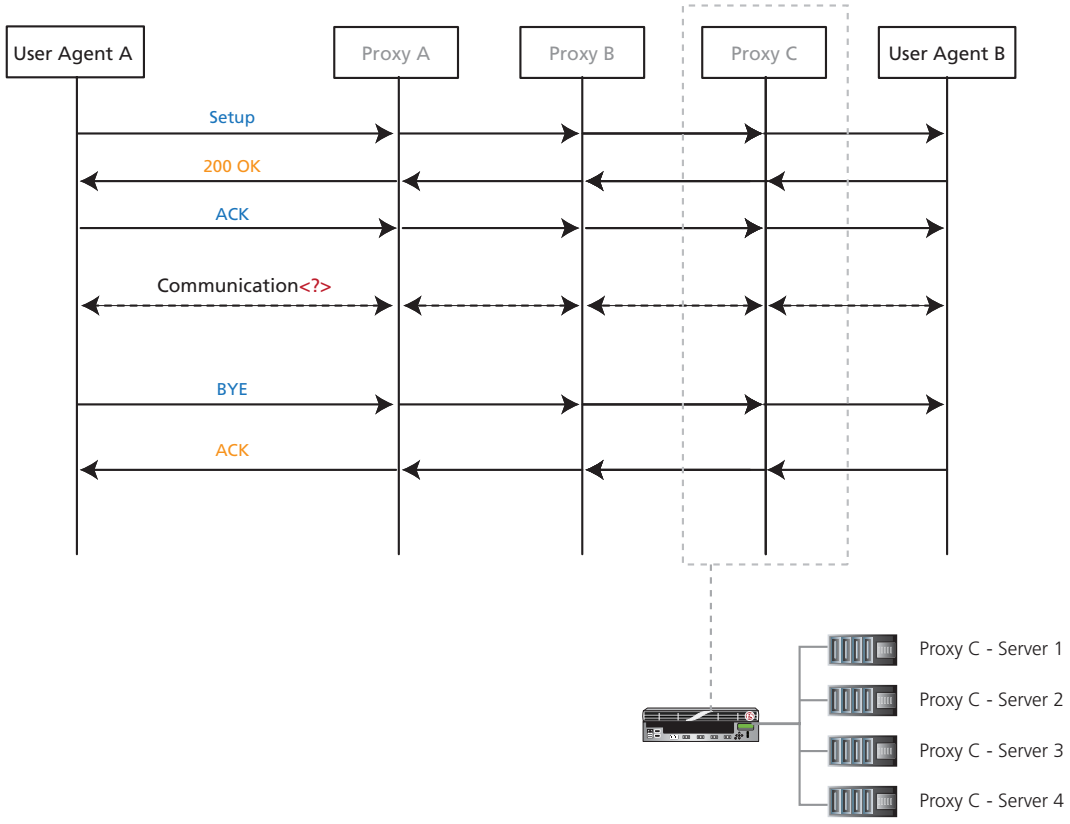

Figure 2 *Typical SIP transaction flow*

Inbound SIP only

In this next flow diagram, we show the BIG-IP LTM for inbound SIP traffic.

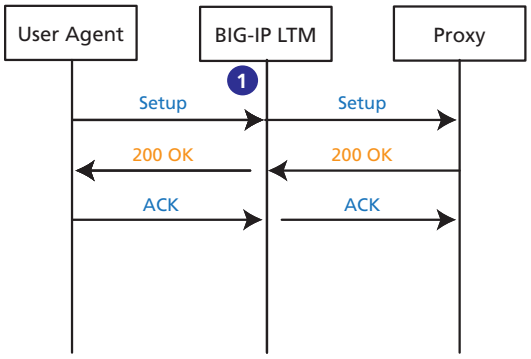

Figure 3 *SIP inbound transaction flow with BIG-IP*

Inbound and outbound SIP

In this final flow diagram, we show the BIG-IP in the middle of inbound and outbound SIP traffic.

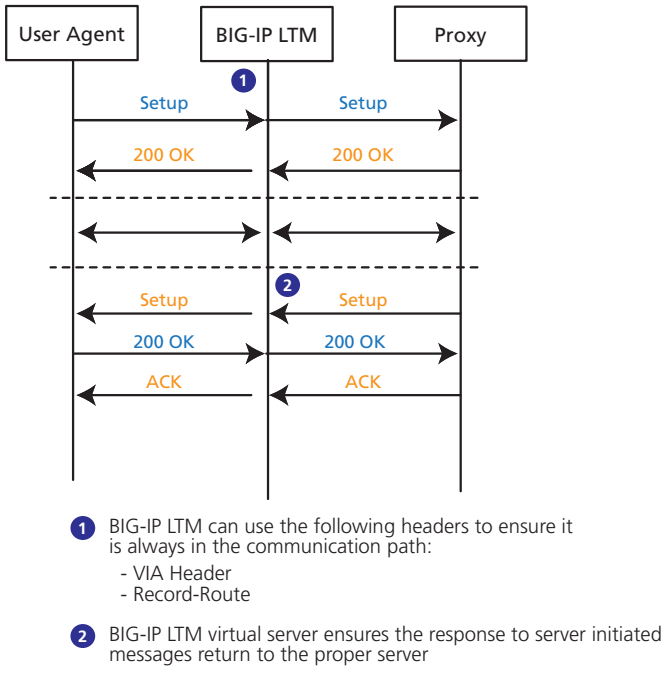

Figure 4 *SIP inbound and outbound transaction flow with BIG-IP*