BIG-IP® Service Provider: Message Routing Administration

Version 13.1

Table of Contents

Using the Diameter Configuration Wizard

Overview: Diameter Configuration Wizard

The Diameter Configuration Wizard provides a simple, straightforward way to configure Diameter message routing functionality for Stream Control Transmission Protocol (SCTP) support, load balancing, AVP transformation, and session management. Additionally, Diameter message routing functionality supports high availability (HA) functionality.

You can use this wizard to quickly configure the following functions.

Table 1: Diameter Configuration Wizard functions

Function	Description
Routing	Specifies the routing table configuration to support Diameter functionality, including the routing decision parameters (such as Diameter protocol, expression test, and action associated with a matched expression).
Transformations	Enables you to insert, modify, or delete Attribute Value Pairs (AVPs) in Diameter messages.
Session Management	Specifies a session timeout value, as well as session binding parameters for master-only persistence and master-slave persistence.
System Configuration	Specifies the system configuration used to support Diameter functionality, including the following: • Virtual Servers. Specifies an applicable virtual server (including virtual server name, virtual IP address, port number, client transport protocol, and description). • Nodes. Specifies local traffic node parameters (including a node name, address, and description). • Pools. Specifies local traffic pool settings (including pool name, description, pool members, and port number), protocol, and multihoming settings (including alternative source IP addresses). • Routing Destinations. Specifies routing destination parameters (including a destination, pool selection mode, and pool). • List of Values. Specifies a list of values (including a list name, description, and values) that can be referenced in transformation rules.
Dictionaries	Enables you to manage Diameter dictionaries.

Important: *You must use a Chrome browser when setting up and using the Diameter Configuration Wizard. Browsers other than Chrome are not currently supported.*

Tip: *Workflow messages appear in the yellow banner to help guide you during the configuration of Diameter message routing functionality.*

About setting up the Diameter Configuration Wizard

When you set up the Diameter Configuration Wizard, you need to complete the following actions:

- Download the Diameter Configuration Wizard RPM package from the F5 Downloads site.

- Import the downloaded file into iApps Package Management LX.

Important: *You must use a Chrome browser when setting up and using the Diameter Configuration Wizard. Browsers other than Chrome are not currently supported.*

Task summary

Downloading the Diameter Configuration Wizard RPM package

You can download the latest Diameter Configuration Wizard RPM package from F5 Networks.

1. Log in to the F5 Downloads site, `https://downloads.f5.com`, and click the **Find a Download** button.
2. Click the name of the product line.

   Note: *To download the Diameter Configuration Wizard RPM package, click the product line* ***iAppLX Templates****.*
3. Click the name of the version of the product you want to download.

   Note: *The name appears as* ***iAppLX_Templates*** *and the version appears as* ***iAppLX****.*
4. Read the End User License Agreement, and click the **I Accept** button if you agree with the terms.
   The Select a Download screen appears.
5. Click the name of the file you want to download.

   Note: *The Diameter Configuration Wizard RPM package is named* `diameterConfigurationWizard-xx.x.x-x.xx.x.xxx.noarch.rpm`*.*

The latest Diameter Configuration Wizard file is downloaded from F5 Networks.

Importing the Diameter Configuration Wizard RPM package

You can import the latest Diameter Configuration Wizard RPM package onto a BIG-IP® system.

1. Log on to the command line of the system using the root account.
2. Type the following command to enable iApps LX controls.

   ```
   touch /var/config/rest/iapps/enable
   ```
3. Type the following command to restart `restjavad`.

   ```
   bigstart restart restjavad
   ```
4. Open the BIG-IP Configuration utility.
5. On the Main tab, click **iApps** > **Package Management LX**.
   The Package Management LX screen appears.
6. Click **Import**.
7. For the **File Name** setting, click **Browse** to navigate to the Diameter Configuration Wizard RPM package, and then click **Open** to upload the package.

   Note: *The Diameter Configuration Wizard RPM package is named* `diameterConfigurationWizard-xx.x.x-x.xx.x.xxx.noarch.rpm`*.*
8. Click **Upload**.
   The Diameter Configuration Wizard RPM package uploads to the Applications Service List screen.

The latest Diameter configuration wizard file is imported and available on the Applications LX screen.

Opening the Diameter Configuration Wizard

Before you can open the Diameter Configuration Wizard, you need to set up the wizard in the iApps LX interface.

After you set up the Diameter Configuration Wizard in the iApps LX intereface, you can open the wizard to configure Diameter message routing functionality.

1. On the Main tab, click **iApps** > **Application Services** > **Applications LX**.
   The Application Service List screen opens.
2. Click the name of a Diameter application.

   Note: *The default iApps LX Diameter application is* ***Diameter Configuration Wizard****.*

The Diameter Configuration Wizard is open and available for configuration.

About the Diameter system configuration

The Diameter Configuration Wizard System Configuration tab enables you to configure virtual servers, nodes, pools, routing destinations, and a list of values for Diameter functionality.

Important: *You must use a Chrome browser when setting up and using the Diameter Configuration Wizard. Browsers other than Chrome are not currently supported.*

Task summary

Configuring a Diameter virtual server

Before you configure a Diameter virtual server, you need to configure the appropriate destination nodes and pools.

You can configure a Diameter virtual server to use a client transport protocol, and SCTP multihoming for Diameter clients.

Important: *Do not click* ***Save*** *until you have configured all Diameter functions. If you click* ***Save*** *before configuring all Diameter functions, an error might occur.*

1. In the Diameter Configuration Wizard, click the System Configuration tab, and then click the Virtual Servers tab.

   The Virtual Servers screen opens.
2. In the **Virtual Server Name** field, type the name of the virtual server.
3. In the **Virtual Ip** field, type the IP address for the virtual server.
4. In the **Port Number** field, type the port number for the virtual server.
5. From the **Client Transport Protocol** list, select one of the following protocols to use with Diameter clients.
   - **TCP**
   - **SCTP**
   - **TLS/TCP**
6. Click **More Options**.
7. In the **Description** field, type a description.
8. (Optional) Configure SCTP multihoming functionality for Diameter clients.

a) Select the **Enable Multihoming** check box.
b) In the **Alternative Destination IPs** field, type the address for an alternative BIG-IP destination that a client can use.
c) For each additional **Alternative Destination IPs** address, click the plus (+) button to add the destination IP address, as necessary.

9. (Optional) Click **Add Virtual Server** to configure an additional Diameter virtual server, as necessary.

A Diameter virtual server is configured to use a client transport protocol, and SCTP multihoming functionality for Diameter clients.

Configuring a Diameter node

You can configure the properties of Diameter destination nodes for pools. Note that a destination node can include multiple active user sessions.

Important: *Do not click* ***Save*** *until you have configured all Diameter functions. If you click* ***Save*** *before configuring all Diameter functions, an error might occur.*

1. In the Diameter Configuration Wizard, click the System Configuration tab, and then click the Nodes tab.

   The Nodes screen opens.
2. In the **Node Name** field, type the name for the node.
3. In the **Address** field, type the address for the node.
4. In the **Description** field, type a description for the node.
5. (Optional) Click **Add Node** to configure an additional node, as necessary.

The Diameter destination nodes are configured, and available to assign to a pool.

Configuring a Diameter pool

Before you configure a Diameter pool, you need to configure the appropriate destination nodes.

In a basic Diameter message routing configuration, you can define a routing pool that contains Diameter servers as its members, specify a protocol to use with Diameter servers, and configure multihoming destination IP addresses.

Important: *Do not click* ***Save*** *until you have configured all Diameter functions. If you click* ***Save*** *before configuring all Diameter functions, an error might occur.*

Note: *If a peer specifies a pool without pool members, the message is unroutable.*

1. In the Diameter Configuration Wizard, click the System Configuration tab, and then click the Pools tab.

   The Pools screen opens.
2. In the **Pool Name** field, type the name of the pool.
3. In the **Description** field, type a description for the pool.
4. Add the applicable pool member destination nodes to the pool.
   a) Click the **Show Pool Members** button.
   b) For each pool member, click the **Add Pool Member** plus (+) button.
   c) From the **Pool Members** list, select a pool member destination node.
   d) In the **Port Number** field, type the port number.
5. Click **More Options**.
6. From the **Protocol** list, select one of the following protocols to use with Diameter servers.

- **TCP**
- **SCTP**
- **TLS/TCP**

7. (Optional) Configure SCTP multihoming functionality for Diameter servers.
   a) Select the **Enable Multihoming** check box.
   b) In the **Alternative Source IPs** field, type the address for an alternative BIG-IP destination address that a server can use.
   c) For each additional **Alternative Source IPs** address, click the plus (+) button to add the source IP address, as necessary.
8. (Optional) Click **Add Pool** to configure an additional Diameter pool, as necessary.

A Diameter message routing configuration is complete, including a routing pool that contains Diameter servers as its members, a protocol to use with Diameter servers, and SCTP multihoming destination IP addresses.

Configuring Diameter routing destinations

To configure Diameter static routing destinations, you must first configure the applicable destination nodes and pools.

You can configure one or more static routing destinations for a Diameter application, specifying a destination address and a pool selection mode, comprising one or more pools.

Important: *Do not click* ***Save*** *until you have configured all Diameter functions. If you click* ***Save*** *before configuring all Diameter functions, an error might occur.*

---

1. In the Diameter Configuration Wizard, click the System Configuration tab, and then click the Routing Destinations tab.

   The Routing Destinations screen opens.
2. In the **Destination** field, type an address for the static route destination.
3. From the **Pool Selection Mode** list, select one of the following settings:

Setting	Description
By Precedence	Specifies a sequential selection of pools based on availability. If only one pool is specified, the virtual server directs all traffic to it. If two or more pools are specified, the virtual server sends traffic to the next pool in the specified sequence (top to bottom) when the nodes in the preceding pool are down.
By Percents	Specifies a percentage of traffic for each specified pool. If only one pool is specified, the virtual server directs all traffic to it. If two or more pools are specified, the virtual server manages traffic sent to each pool in accordance with the specified percentage. You can drag the slider bar to specify a percentage for a pool.

4. From the **Pools** list, select a Diameter pool.
5. (Optional) Click **Add Pool** to specify an additional pool for the routing destination, as necessary.
6. For each pool, do one of the following:

Pool Selection Mode	Steps
By Precedence	• In the Pools area, from the **Pools** list, sequentially select each pool, from top to bottom.
By Percents	• In the Pools area, do one of the following for each selected pool:

Pool Selection Mode	Steps
	• Drag the slider bar for each selected pool to specify the applicable percentage of traffic. • In the percent field, type the applicable percentage of traffic.

7. (Optional) Click **Add Destination** to add another routing destination, as necessary.

One or more Diameter static routing destinations are configured to manage traffic in accordance with a destination name and a pool selection mode, comprising one or more pools.

Configuring a Diameter list of values

You can create a list composed of unique values and apply them in a routing decision to an Attribute Value Pairs (AVP) with a string-format output.

Important: *Do not click* ***Save*** *until you have configured all Diameter functions. If you click* ***Save*** *before configuring all Diameter functions, an error might occur.*

1. In the Diameter Configuration Wizard, click the System Configuration tab, and then click the List of Values tab.
2. In the **List Name** field, type a name for the list.
3. In the **Description** field, type a unique description for the list of values.
4. Click **Show List of Values**.
5. In the **List of Values** field, type a value.
6. To specify an additional value for the list, in the **Add Values** area, click the plus (+) button, and then, in the **List of Values** field, type a value..
7. Click **Add List** to configure an additional list, as necessary.

A list of values is available.

About configuring Diameter routing

The Diameter Configuration Wizard Routing tab enables you to configure routing decisions. Routing decisions specify the protocol conditions and associated actions assigned to a virtual server.

Task summary

Configuring a Diameter routing decision

To assign a Diameter routing decision to a virtual server for SCTP server-side multihoming, you must first configure an applicable virtual server.

You can configure one or more routing decisions for a Diameter application to use SCTP server-side multihoming, specifying the protocol conditions and associated actions assigned to a virtual server.

1. In the Diameter Configuration Wizard, click the Routing tab.

   The Routing screen opens.
2. From the **All Virtual Servers** list, select the virtual server to which you want to assign the routing decision.

   The default is **All Virtual Servers**.
3. In the Default Route area, from the **Action** list, select an action.
4. From the **Destination** list, select a destination.

Note: *Depending upon the Action that you select, the Destination list and associated paramenters might not appear.*

5. Click **More Options**.
6. In the **Description** field, type a description.
7. In the **Origin Host** field, type an identifier for the originating server, for example, `siteserver.f5.com`.

   If the **Origin Host** setting is not specified, the BIG-IP system host is used.

   Note: *To display the **Origin Host** field, from the Action list, select **Reject**, **Redirect**, or **Terminate**.*
8. In the **Origin Realm** field, type the origin realm matching the Origin-Realm AVP value in the message.

   A blank value routes all origin-realms.

   Note: *To display the **Origin Realm** field, from the Action list, select **Reject**, **Redirect**, or **Terminate**.*
9. Click **Add** to configure an additional routing decision, as necessary.
   Controls to configure a protocol, its attributes, and an associated action open.
10. From the **Protocol** list, select a protocol.
11. From the **Attribute** list, select a heading.
12. From the **Expression** list, select an expression.
13. For the Value setting, do one of the following:
    - From the **Value** list, select a value for the expression.
    - In the **Value** field, type a value for the expression.
14. From the **Action** list, select an action.
15. From the **Destination** list, select a destination.

    Note: *Depending upon the Action that you select, the Destination list and associated paramenters might not appear.*
16. (Optional) Click **More Options**, and then, in the **Description** field, type a description for the configured routing decision.
17. In the **Origin Host** field, type an identifier for the originating server, for example, `siteserver.f5.com`.

    If the **Origin Host** setting is not specified, the BIG-IP system host is used.

    Note: *To display the **Origin Host** field, from the Action list, select **Reject**, **Redirect**, or **Terminate**.*
18. In the **Origin Realm** field, type the origin realm matching the Origin-Realm AVP value in the message.

    A blank value routes all origin-realms.

    Note: *To display the **Origin Realm** field, from the Action list, select **Reject**, **Redirect**, or **Terminate**.*

A routing decision is configured, specifying the protocol conditions and associated actions assigned to a virtual server.

About configuring Diameter transformations

The Diameter Configuration Wizard Transformations tab enables you to insert, modify, or delete Attribute Value Pairs (AVPs).

Important: *You must use a Chrome browser when setting up and using the Diameter Configuration Wizard. Browsers other than Chrome are not currently supported.*

Task summary

Configuring a Diameter transformation

You can configure the transformation of Attribute Value Pairs (AVPs) by using the Transformations tab, preventing exposure of server topologies.

1. In the Diameter Configuration Wizard, click the Transformations tab.

   The Transformation screen opens.
2. From the **All Virtual Servers** list, select the virtual server to which you want to assign the transformation.

   The default is **All Virtual Servers**.
3. From the **Protocol** list, select a protocol.
4. From the **Attribute** list, select an attribute.
5. From the **Expression** list, select an expression.
6. For the Value setting, do one of the following:
   - From the **Value** list, select a value for the expression.
   - In the **Value** field, type a value for the expression.
7. For each additional **Attribute**, click the plus (+) button to add the parameters, as necessary.
8. From the **Operation** list, select an operation.
9. From the **Attribute** list for the operation, select a protocol attribute.
10. For the Value setting, do one of the following:
    - From the **Value** list, select a value for the expression.
    - In the **Value** field, type a value for the expression.
11. For each additional **Operation**, click the plus (+) button to add the parameters, as necessary.
12. Click **More Options**.
13. (Optional) In the **Description** field, type a description for the transformation.
14. Select the check box for each transformation that you want to enable, and then click **Enable**.

The AVP transformations are configured, preventing exposure of server topologies

About Diameter session management

The Diameter Configuration Wizard Session Management tab enables you to configure the session management and session binding for Diameter functionality.

Important: *You must use a Chrome browser when setting up and using the Diameter Configuration Wizard. Browsers other than Chrome are not currently supported.*

Task summary

Configuring Diameter session management

A session management configuration provides a session timeout setting and session binding settings that you can apply to master-only or master-slave persistence sessions.

1. In the Diameter Configuration Wizard, click the Session Management tab.

The Session Management screen opens.

2. Select the **Session Management** check box.
3. In the **Session Timeout** field, type a timeout value for the session persistence in minutes.
4. Select the **Session Binding** check box to configure a master-only or a master-slave persistence session.
5. In the Master Session area, from the **Protocol** list, select a protocol.
6. From the **AVP** list, select an AVP attribute to apply to the master session.
7. In the Slave Sessions area, from the **Protocol** list, select a protocol.
8. From the **AVP to use for resolving** list, select an AVP attribute.

   Important: *For Master-Slave persistence, the specified AVP value for a Slave session must match the specified AVP value for a Master session, in order for the Slave messages to be routed according to a different protocol interface for a Master session.*

9. From the **AVP to use in Master Session for persistence** list, select an AVP attribute.

   Note: *The default setting is* ***Same as Slave session AVP****.*

10. Click **Add Row** to add another slave session protocol configuration, as necessary.
11. Click **Save** to save the session management configuration.

A session management configuration is available to provide a session timeout and session binding for master-only or master-slave persistence sessions.

About Diameter dictionaries

The Diameter Configuration Wizard Dictionaries tab enables you to easily manage each 3GPP protocol interface Diameter dictionary. You can modify, download, upload, rename, and delete dictionary files, as necessary.

Important: *You must use a Chrome browser when setting up and using the Diameter Configuration Wizard. Browsers other than Chrome are not currently supported.*

Task summary

Modifying a Diameter dictionary file

You can modify a Diameter dictionary file to add proprietary AVPs, as necessary.

1. In the Diameter Configuration Wizard, click the Dictionaries tab.

   The Dictionaries screen opens.

2. Click the name of a dictionary XML file to download the file.

   The XML file downloads to the workstation.

3. Open the dictionary XML file in an editor application, modify the content, as necessary, and save the file.
4. Click **Upload**, click **Browse** to navigate to the modified dictionary XML file, and then click **Open** to upload the modified dictionary XML file.

The Diameter dictionary file is modified and available for use.

Downloading a Diameter dictionary file

You can download a Diameter dictionary file to modify it, to copy and customize it, or to examine its contents.

1. In the Diameter Configuration Wizard, click the Dictionaries tab.
   The Dictionaries screen opens.
2. Click the name of a dictionary XML file to download the file.
   The XML file downloads to the workstation.

The Diameter dictionary file is downloaded.

Uploading a Diameter dictionary file

Before you can upload a Diameter dictionary XML file to the BIG-IP® device, you need to download the Diameter dictionary file to a preferred location, for example, the workstation.

You can upload a Diameter dictionary file to the BIG-IP device, as necessary.

1. In the Diameter Configuration Wizard, click the Dictionaries tab.
   The Dictionaries screen opens.
2. Click **Upload**, click **Browse** to navigate to the modified dictionary XML file, and then click **Open** to upload the modified dictionary XML file.

A Diameter dictionary XML file is uploaded to the BIG-IP device.

Renaming a Diameter dictionary file

You can rename a Diameter dictionary XML file, as necessary.

1. In the Diameter Configuration Wizard, click the Dictionaries tab.
   The Dictionaries screen opens.
2. Click **Rename** to rename the applicable Diameter dictionary XML file.
3. In the **New Dictionary Name** field, type a new name for the Diameter dictionary.
4. Click **Rename** to rename the applicable Diameter dictionary XML file.

The Diameter dictionary is renamed.

Deleting a Diameter dictionary file

You can delete a Diameter dictionary file, as necessary.

1. In the Diameter Configuration Wizard, click the Dictionaries tab.
   The Dictionaries screen opens.
2. Select the check box for the applicable dictionary.
3. Click **Delete Dictionary** to remove the applicable dictionary.

The dictionary XML file is deleted from the BIG-IP® device.

Saving a Diameter Configuration Wizard configuration

All Diameter Configuration Wizard functions need to be configured before saving the configuration.

You can save the Diameter Configuration Wizard configuration after you complete configuring all of the functions.

1. In the Diameter Configuration Wizard, click one of the following tabs:
   - **Routing**
   - **Transformations**
   - **Session Management**
   - **System Configuration**
2. Click **Save**.

The Diameter Configuration Wizard configuration is saved.

Configuring Diameter Load Balancing and Message Routing

Overview: Diameter message routing

The Diameter protocol provides message-routing functionality that the BIG-IP® system supports in a load-balancing configuration.

Diameter message routing configuration

In a message routing configuration, the BIG-IP system manages requests and responses among peers. The following illustration shows a Diameter routing configuration with requests from Client 1 and Client 2 to servers located in different destination realms, Realm-A and Realm-B.

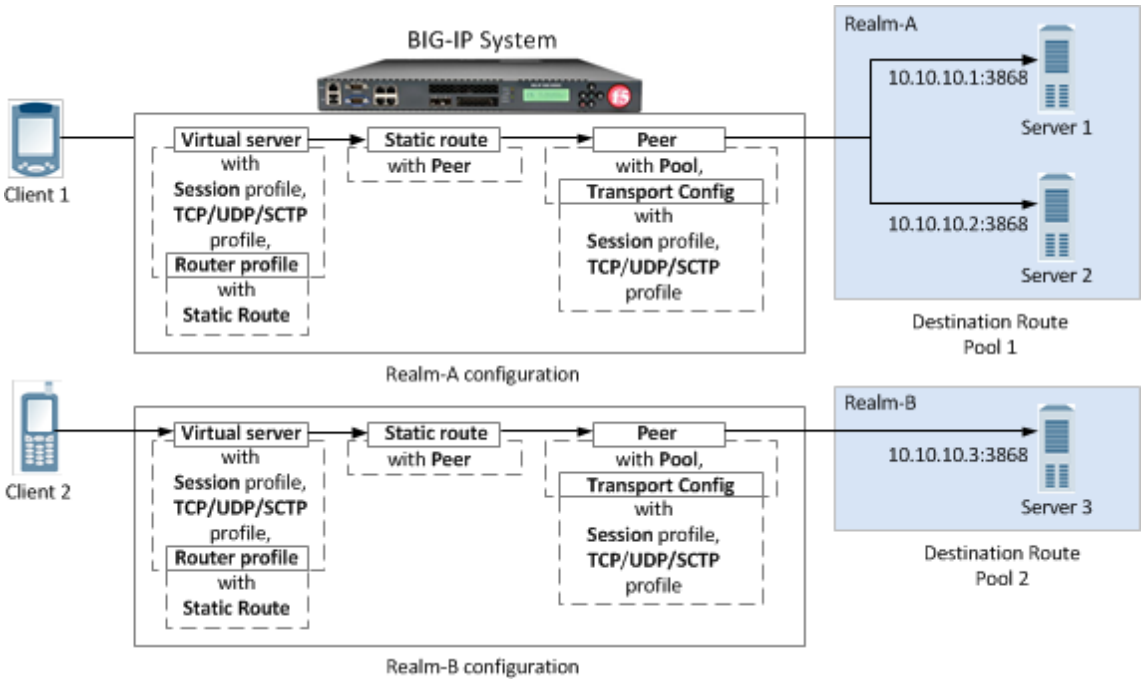

Figure 1: A Diameter message routing configuration

A typical Diameter message routing configuration with two realms involves configuring the following items.

Functionality	Description
Pool	A pool for each realm directs Diameter traffic to servers.
Session profile	A session profile for each realm configures a session as a set of messages between two Diameter nodes on behalf of a user.
Transport configuration	An optional transport configuration for each realm defines how the BIG-IP system connects with the servers on your network when routing messages. You can assign a transport configuration to a virtual server or peer, as needed.

Functionality	Description
Peer	Each BIG-IP message-routing peer routes messages to a destination host. In this example, BIG-IP message-routing peers route messages to `10.10.10.1:3868`, `10.10.10.2:3868`, and `10.10.10.3:3868`.
Static Route	Each static route specifies a set of peers in a destination realm to use in forwarding messages. In this example, `Realm-A` includes `Peer 1` , and `Realm-B` includes `Peer 2`.
Router profile	A router profile configures Diameter message routing parameters and static routes to be used by a virtual server in routing Diameter messages.
Virtual server	Manages Diameter traffic to and from each realm and pool members.

About the Diameter session profile

The Diameter *session profile* includes Diameter protocol parameters that can be used by a virtual server or transport configuration in managing Diameter traffic. The profile enables you to configure the properties of a Diameter session as a set of messages between two diameter nodes on behalf of a user. Note that those same two diameter nodes can also include multiple active user sessions. The session profile provides you with parameters to configure settings for timeout, watchdog failures, and message-size, as well as persistence, rewrite, and capabilities-handshake functionality.

Functionality	Description
Settings	Configure timeout functionality, watchdog failures, and message size.
Persistence	Configure persistence functionality, including a type, AVP, and timeout.
Rewrite	Provide AVP rewriting to conceal clients from servers, as well as to conceal servers from clients.
Capabilities Handshake	When the Diameter session profile is configured as a proxy, the BIG-IP system generates capabilities-exchange messages, sending a Capabilities-Exchange-Request (CER) and responding with a Capabilities-Exchange-Answer (CEA), to establish a diameter session with connected nodes.

You can apply different session profiles to different transport configurations, and then apply the different transport configurations to different message routing peers, which point to different physical pools. You can also apply different session profiles by applying one session profile to the transport configuration, and a different session profile to the virtual server.

About message routing peers

A *message routing peer* defines how the BIG-IP® system routes messages to destination hosts. When you configure a message routing peer, you define a pool of destination hosts, and a connection method for them, an optional transport configuration configured with a Diameter session profile, as needed, the number of connections to a destination host, and a ratio value for selection of a peer. After defining the peers, you can use those peers in configuring static routes.

When an inband monitor is assigned to a Diameter message routing pool, the inband monitor marks a pool member down when the total failures from the pool member exceeds or equals the maximum number of failures configured. When a pool member is marked down, the connection remains alive, but load balancing functions only among the remaining pool members within the same pool. The active Diameter monitor marks the pool member up when service is restored.

If a peer does not specify a pool, the BIG-IP system uses the destination IP address and port of the ingress message's connection. If a peer specifies a pool without pool members, the message is unroutable.

When you configure a message routing peer to use a transport configuration, you can enable that peer to use *auto-initialization* functionality, which automatically creates outbound connections to active pool members in the peer's specified pool. In order for the auto-initialization functionality to work, you need to specify the peer in a static route, and then specify that static route in a router profile that is assigned to a message routing virtual server, The BIG-IP system automatically initiates a connection for each router profile that contains the peer. You enable auto-initialization functionality for a peer by selecting the **Auto-Initialization Enabled** check box. Additionally, you can specify an **Auto-Initialization Interval** value, which compensates for latency, to verify the connection between the BIG-IP system and pool members (ranging from 500ms through 65535ms, with a default value of 5000ms). If a connection does not exist, auto-initialization functionality attempts to reestablish a connection.

If a peer does not specify a transport configuration, the BIG-IP system uses the transport type of the message's originating connection.

About Diameter peer selection

When you configure a Diameter static route, the BIG-IP® system provides two modes for peer selection: sequential and ratio.

In *sequential mode*, the BIG-IP system uses peers in the order specified by the Peers Selected list. If a message is retried, the next peer in the Peers Selected list is used.

In *ratio mode*, the BIG-IP system uses peers in accordance with the peer's ratio value, which you specify when configuring each peer. The relative ratio value for each peer determines whether a peer is selected from the list. For example, a peer with a ratio value of 1 is typically selected over a peer with a ratio value of 2. The lower the ratio value, the greater the probability for selection.

Before configuring a mode for peer selection, you must first configure each peer, using the Peer tab, to include peers in the Available list.

About the election process for peer connections

In the rare instance when a Diameter peer connects to the BIG-IP® system, and the BIG-IP system simultaneously initiates a connection to that peer, the BIG-IP system resolves the connection conflict by means of an election process. The BIG-IP system uses an algorithm that evaluates and resolves which connection to use (whereupon the election winner drops the unused connection), based on the Origin-Host Attribute-Value Pair (AVP).

This election process is enabled only when the Diameter peer **Connection Mode** is set to **Per Peer** and the **Number of Connections** value equals `1`.

In an active-standby configuration, the election process runs only on the active device. If mirroring is enabled, the used connection is mirrored on the standby device.

You can examine the election process results in the Diameter log files. The following examples show typical log messages for the election process.

Table 2: Example Diameter election process log messages

Condition	Message
Election process results	DIAMETER: Election process `won` | `lost` between peer `peer-host-name` and `big-ip-host-name`.
Closing outgoing connection due to winning election	DIAMETER: Closing outgoing connection to `ip:port-id` closed by election process.

About static routes

The message routing functionality *Static Routes* enables you to configure a route that specifies a set of peers to use in forwarding messages. When you configure a static route, you can specify an application ID, destination realm, origin realm, virtual server, peer selection mode, and peers.

The required static route attributes (each of which must match the respective request parameter) are prioritized in this order:

1. Destination Realm
2. Application Id
3. Origin Realm
4. Virtual Server

A static route is a *default route* when each of these attributes is set to the default (wildcard) value.

About the Diameter router profile

With the Diameter router profile, you can configure Diameter routing parameters to be used by a virtual server in routing Diameter messages. When you configure a Diameter router profile, you can specify persistence, rewrite, and capabilities-handshake functionality.

About mirroring Diameter message routing

A Diameter proxy and router implementation can mirror client and server connections.

In a high-availability configuration, the active device mirrors connections (including auto-initialization connections) on the standby device, creating and maintaining the same state on each device. The standby device, however, does not route the messages. Instead the standby device stores the messages until the active device notifies the standby device that the message has been routed. This enables the standby device to deliver the message to the equivalent connection for egress processing. A sweeper drops the messages if the standby device stores them longer than the specified value. Enabling this setting ensures a higher level of connection reliability, but it can also affect system performance. As the mirrored messages flow though the client-side connection, normal ingress iRule events and routing occur.

Diameter AVP names

This list specifies supported Diameter Attribute-Value Pair (AVP) names.

AVP Names

- ACCOUNTING-REALTIME-REQUIRED
- ACCOUNTING-RECORD-NUMBER
- ACCOUNTING-RECORD-TYPE
- ACCOUNTING-SUB-SESSION-ID
- ACCT-APPLICATION-ID
- ACCT-INTERIM-INTERVAL
- ACCT-MULTI-SESSION-ID
- ACCT-SESSION-ID
- AUTH-APPLICATION-ID

- AUTH-GRACE-PERIOD
- AUTH-REQUEST-TYPE
- AUTH-SESSION-STATE
- AUTHORIZATION-LIFETIME
- CALLING-STATION-ID
- CLASS
- DESTINATION-HOST
- DESTINATION-REALM
- DISCONNECT-CAUSE
- E2E-SEQUENCE
- ERROR-MESSAGE
- ERROR-REPORTING-HOST
- EVENT-TIMESTAMP
- EXPERIMENTAL-RESULT
- EXPERIMENTAL-RESULT-CODE
- FAILED-AVP
- FIRMWARE-REVISION
- FRAMED-IP-ADDRESS
- HOST-IP-ADDRESS
- INBAND-SECURITY-ID
- MULTI-ROUND-TIME-OUT
- ORIGIN-HOST
- ORIGIN-REALM
- ORIGIN-STATE-ID
- PRODUCT-NAME
- PROXY-HOST
- PROXY-INFO
- PROXY-STATE
- RE-AUTH-REQUEST-TYPE
- REDIRECT-HOST
- REDIRECT-HOST-USAGE
- REDIRECT-MAX-CACHE-TIME
- RESULT-CODE
- ROUTE-RECORD
- SESSION-BINDING
- SESSION-ID
- SESSION-SERVER-FAILOVER
- SESSION-TIMEOUT
- SUBSCRIPTION-ID
- SUBSCRIPTION-ID-DATA
- SUBSCRIPTION-ID-TYPE
- SUPPORTED-VENDOR-ID
- TERMINATION-CAUSE
- USER-EQUIPMENT-INFO
- USER-EQUIPMENT-TYPE
- USER-EQUIPMENT-VALUE
- USER-NAME
- VENDOR-ID

- VENDOR-SPECIFIC-APPLICATION-ID

Task summary

Complete these tasks to configure Diameter message routing on a BIG-IP® system.

Task list

Creating a pool to manage Diameter traffic

In a basic Diameter message routing configuration, you can define a routing pool that contains Diameter servers as its members.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add each resource that you want to include in the pool:
   a) (Optional) In the **Node Name** field, type a name for the node portion of the pool member.
   b) In the **Address** field, type an IP address.
   c) In the **Service Port** field, type a port number, or select a service name from the list.
   d) (Optional) In the **Priority** field, type a priority number.
   e) Click **Add**.
5. Click **Finished**.

The pool is configured to manage Diameter servers as pool members.

Creating a Diameter Session profile

You can create a Diameter Session profile to specify protocol parameters, as necessary.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Message Routing** > **Diameter**.
   The Diameter session profiles list screen opens.
2. Click **Create**.
   The New Diameter Session Profile screen opens.
3. In the **Name** field, type a unique name for the diameter session profile.
4. From the **Parent Profile** list, select a profile from which the new profile inherits properties.
5. Add a description.
   a) In the General Properties area, for the **Description** field, select the check box.
   b) In the **Description** field, type a description.
6. For the Settings area, select the **Custom** check box to enable editing, and specify the following parameters.
   a) In the **Handshake Timeout** field, type the number of seconds before the handshake to a peer times out.
   b) In the **Maximum Watchdog Failures** field, type the maximum number of device watchdog failures that the traffic management system can receive before it tears down the connection.

*Note: If the number of device watchdog failures exceeds the specified value, and the **Reset on Timeout** check box is selected, then the connection will be reset. If the number of device watchdog failures is greater than 3 times the specified value, the connection will be reset, even if the **Reset on Timeout** check box is cleared.*

c) Select the **Reset on Timeout** check box to reset the connection when watchdog failures exceed the specified number of maximum watchdog failures.

d) In the **Watchdog Timeout** field, type the number of seconds that a client-side or server-side connection can be idle before a device watchdog request (DWR) is sent.

Note: The default value of `0` prevents sending a DWR.

e) In the **Maximum Message Size** field, type the maximum number of bytes allowed for a message.

7. For the Persistence area, select the **Custom** check box and specify the following parameters.

a) From the **Persist Type** list, select a type of persistence.

Setting	Description
None	Disables persistence.
AVP	Enables persistence as determined by the AVP within the message.
Custom	Enables persistence as determined by a custom key specified within an iRule.

b) In the **Persist AVP** field, type an expression for the session-key that identifies the Diameter AVP.

c) In the **Persist Timeout** field, type a timeout value for persistence entries in seconds.

8. For the Rewrite area, select the **Custom** check box and specify the following parameters.

a) In the **Origin Host Rewrite** field, type a value to use in rewriting the Origin-Host AVP on egress.

Note: This value applies to all Diameter messages and can override specified Capabilities Handshake AVP values.

b) In the **Origin Realm Rewrite** field, type a value to use in rewriting the Origin-Realm AVP on egress.

Note: This value applies to all Diameter messages and can override specified Capabilities Handshake AVP values.

c) In the **Destination Host Rewrite** field, type a value to use in rewriting the Destination-Host AVP on egress.

d) In the **Destination Realm Rewrite** field, type a value to use in rewriting the Destination-Realm AVP on egress.

9. For the Capabilities Handshake area, select the **Custom** check box and specify the following parameters.

Note: You must configure these settings to initiate Capabilities-Exchange-Request (CER) handshake requests to downstream peers, as well as to provide Capabilities-Exchange-Answer (CEA) responses to upstream peers within Device-Watchdog-Request (DWR), Device-Watchdog-Answer (DWA), Disconnect-Peer-Request (DPR), and Disconnect-Peer-Answer (DPA) messages.

a) In the **Origin Host** field, type an identifier for the originating server, for example, `siteserver.f5.com`.

If the **Origin Host** setting is not specified, the BIG-IP system host is used.

b) In the **Origin Realm** field, type an identifier for the originating realm, for example, `f5`.

If the **Origin Realm** setting is not specified, the BIG-IP system realm is used.

c) In the **Vendor ID** field, type the vendor identification number assigned to the diameter server by the Internet Assigned Numbers Authority (IANA).

Note: *You can use a vendor-specific* `vendor-id`, `auth-application-id`, *or* `acct-application-id`.

d) In the **Product Name** field, type a vendor-assigned name for the product.
e) In the **Authentication Application ID** field, type the AAA identifier for a specific application.
f) In the **Accounting Application ID** field, type the accounting identifier for a specific application.

10. Click **Finished**.

The Diameter Session profile is configured to apply protocol parameters, as necessary

Creating a transport config

Before you can create a transport config, you must ensure that at least one Diameter session profile exists in the BIG-IP® system configuration.

Create a transport config to define how the BIG-IP system connects with the servers on your network when routing and load balancing Diameter messages.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Message Routing** > **Diameter**.
The Diameter session profiles list screen opens.
2. On the menu bar, click **Transport Config**.
The Diameter screen opens.
3. Click **Create**.
The New Transport Config screen opens.
4. In the **Name** field, type a unique name for the transport configuration.
5. For the **Profiles** setting, move both a transport protocol profile (TCP, UDP, or SCTP) and a Diameter session profile from the **Available** list to the **Selected** list.
You can only associate one protocol profile and one session profile with each transport configuration.
6. For the **iRules** setting, select an iRule from the **Available** list, and move it to the **Selected** list.
7. In the **Source Port** field, type the number of the port this transport configuration uses to connect to the servers on your network.
8. From the **Source Address Translation** list, select an option to define how this transport configuration implements selective and intelligent source address translation. The default is **Auto Map**.

Option	Description
SNAT	The system uses the specified SNAT pool for source address translation.
Auto Map	The system uses the self IP addresses of BIG-IP as the translation addresses.
None	The system does not translate source addresses.

9. Click **Finished**.

Creating a peer

In order to create a peer, you must first ensure that at least one transport configuration and one pool exist in the BIG-IP® system configuration.

You create a peer to define how the BIG-IP system connects with the servers on your network, and to which servers the system routes and load balances messages.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Message Routing** > **Diameter**.
The Diameter session profiles list screen opens.

2. On the menu bar, click **Peers**.
   The Peers list screen opens.
3. Click **Create**.
   The New Peer screen opens.
4. In the **Name** field, type a unique name for the peer.
5. In the **Description** field, type a description of the peer.
6. From the **Connection Mode** list, select an option to specify how connections are distributed to a remote host.

Option	Description
Per Blade	The number of connections are distributed and controlled per blade on a VIPRION® system.
Per Peer	(Default) The number of connections to a remote host is per peer.
Per TMM	The number of connections to a remote host is per TMM on the BIG-IP system.
Per Client	The number of connections to a remote host is per client connection. Responses are delivered to the connection initiating the request. This option is typically used when implementing a firewall, because of its restrictive functionality.

Note: *The configured* ***Connection Mode****,* ***Number of Connections****, and* ***Ratio*** *settings determine how the BIG-IP system uses connections to pool members in delivering messages.*

---

7. From the **Pool** list, select the pool of servers to which the system load balances Diameter messages.
   If you configure only one peer on this BIG-IP system, ensure that you select a pool with only one member.

Note: *If a peer does not specify a pool, the BIG-IP system uses the destination IP address and port of the ingress message's connection. If a peer specifies a pool without pool members, the message is unroutable.*

---

8. From the **Transport Config** list, select the transport configuration that defines the egress message routing peer connection.
9. In the **Number of Connections** field, type the number of allowed connections between the BIG-IP system and the servers in the selected pool.
10. In the **Ratio** field, type the ratio assigned to this peer for use within a static route.
11. Click **Finished**.

A peer determines how the BIG-IP system connects with the servers on your network, and to which servers the system routes and load balances messages.

Creating a static route

Before you can create a static route, you must ensure that at least one peer and one virtual server exist in the BIG-IP® system configuration.

You create a static route when you want to route proxiable messages from specific clients to specific domains, and load balance those messages across a group of peers. If the configured attributes of a static route match the attributes in a message, the system forwards the message to a member of the pool associated with one of the peers.

Note: *The BIG-IP system can use multiple session profiles in a single routing instance, because a different profile can be associated with each member of a pool.*

---

1. On the Main tab, click **Local Traffic** > **Profiles** > **Message Routing** > **Diameter**.

The Diameter session profiles list screen opens.

2. On the menu bar, click **Static Routes**.
   The static routes list screen opens.
3. Click **Create**.
   The New Route screen opens.
4. In the **Name** field, type a unique name for the static route.
5. In the **Description** field, type a description.
6. In the **Application ID** field, type the identifier matching the application-id in the Diameter message. A value of `0` matches every application-id.
7. In the **Destination Realm** field, type the destination realm matching the Destination-Realm AVP value in the message.

   Note: *A blank value routes all destination-realms.*

8. In the **Origin Realm** field, type the origin realm matching the Origin-Realm AVP value in the message.

   Note: *A blank value routes all origin-realms.*

9. From the **Virtual Server** list, select the virtual server from which the system receives client requests for this static route.

   If you do not select a virtual server, the system uses this static route to route messages originating from any client.
10. From the **Peer Selection Mode** list, select an option to specify how the system selects the Peer to route a message to:

Option	Description
Ratio	Peer selection is based on the ratio that is set for each peer in the **Selected** list.
Sequential	Peer selection is based on the order of the peers in the **Selected** list.

11. For the **Peers** setting, move, from the **Available** list to the **Selected** list, the peers that define the servers to which the system load balances or routes messages.

    Note: *Entries in the **Selected** list are not prioritized; consequently, the order of items appearing in the list is not enforced.*

12. Click **Finished**.

A static route is configured to route messages from specific clients to specific domains.

Creating a Diameter Router profile

You can create a Diameter Router profile to route traffic as specified.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Message Routing** > **Diameter**.
   The Diameter session profiles list screen opens.
2. On the menu bar, click **Router Profiles**.
   The Router Profiles list screen opens.
3. Click **Create**.
   The New Diameter Router Profile screen opens.
4. In the **Name** field, type a unique name for the diameter session profile.
5. From the **Parent Profile** list, select a profile from which the new profile inherits properties.
6. For the **Description** setting, select the check box at the right, and type a description in the field.
7. At the top of the Settings area, select the **Custom** check box.

8. Select the **Use Local Connection** check box to specify that connections established by the ingress TMM are preferred to connections that are established by another TMM when selecting an egress connection to a destination peer.
9. In the **Maximum Pending Messages** field, type the maximum number of pending messages held while waiting for a connection to a peer to be created.

   Note: *If the specified value is reached, any additional messages to the peer will be undeliverable, and held messages are delivered to the peer.*
10. In the **Maximum Pending Bytes** field, type the maximum number of bytes contained within pending messages that will be held while waiting for a connection to a peer to be created.

    Note: *If the specified value is reached, any additional messages to the peer will be undeliverable, and held messages are delivered to the peer.*
11. (Optional) For use with connection mirroring, configure the **Traffic Group** setting:
    a) Clear the **Inherit traffic group from current partition / path** check box.
    b) From the list, select a traffic group, such as, **traffic-group-1**

    Important: *Changing traffic groups with Connection Mirroring enabled drops all mirrored connections and loses all persistence data. If you change traffic groups, mirroring must restart.*
12. (Optional) Select the **Connection Mirroring** check box.

    Note: *For connection mirroring to properly function, this device must be a member of a device group.*
13. In the **HA Message Sweeper Interval** field, type a value (in milliseconds) for the frequency of the mirrored message sweeper.
14. In the **Transaction Timeout** field, type the maximum number of seconds the system allows for a transaction, that is, the time between a request and response.

    Note: *When the system receives a provisional response, the timer restarts.*
15. For the **Static Routes** setting, select a static route from the **Available** list, and move it to the **Selected** list.
16. Click **Finished**.

The Diameter Router profile is configured to route traffic, as you have specified.

Creating a virtual server to manage Diameter traffic

The final task in configuring Diameter message routing for load balancing is to define a virtual server that references the custom Diameter profile and Router profile that you created in previous tasks.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. From the **Type** list, select **Message Routing**.
5. In the **Destination Address** field, type the IP address in CIDR format.

   The supported format is address/prefix, where the prefix length is in bits. For example, an IPv4 address/prefix is `10.0.0.1` or `10.0.0.0/24`, and an IPv6 address/prefix is `ffe1::0020/64` or `2001:ed8:77b5:2:10:10:100:42/64`. When you use an IPv4 address without specifying a prefix, the BIG-IP® system automatically uses a `/32` prefix.

Note: *The IP address you type must be available and not in the loopback network.*

6. In the **Service Port** field, type `3868`.
7. From the **Configuration** list, select **Advanced**.
8. From the **Application Protocol** list, select **Diameter**.
9. From the **Session Profile** list, select a Diameter session profile.

Note: *You can specify a different session profile, as needed, when configuring the transport configuration that is assigned to a peer.*

10. From the **Router Profile** list, select a Diameter router profile.
11. Click **Finished**.

The virtual server that references the Diameter session profile and Router profile appears in the Virtual Server list.

About checking Diameter pool member health

You can configure the BIG-IP® system to monitor pool member health using a Diameter monitor. Use a Diameter monitor to check the health of a host with an active Diameter session. The Diameter monitor also monitors a Diameter connection independently of a specific Diameter session and marks a host that had been marked down, but is online again, as available.

Task summary

Perform these tasks to configure health monitors and apply the monitors to a pool:

Creating a custom Diameter monitor

After you create a Diameter profile, you can create a custom Diameter monitor. The purpose of the Diameter monitor is to monitor the health of all servers running the Diameter service.

1. On the Main tab, click **Local Traffic** > **Monitors**.
   The Monitors List screen opens.
2. Click **Create**.
   The New Monitor screen opens.
3. In the **Name** field, type a name for the monitor.
4. From the **Type** list, select **Diameter**.
   The screen refreshes, and displays the configuration options for the **Diameter** monitor type.
5. Configure additional settings based on your network requirements.
6. Click **Finished**.

Adding a health monitor to a pool

Add health monitors to a pool when you want the BIG-IP system to monitor the health of the pool members. Repeat this procedure for each desired pool.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click the name of the pool you want to modify.
3. For the **Health Monitors** setting, in the **Available** list, select a monitor type, and click **<<** to move the monitor to the **Active** list.

Tip: *Hold the Shift or Ctrl key to select more than one monitor at a time.*

4. Click **Finished**.

The new pool appears in the Pools list.

About viewing Diameter session and router statistics

You can view statistics for Diameter sessions and routes.

Task summary

Viewing Diameter session statistics

Ensure that a Diameter session profile is assigned to at least one virtual server.

When you want to see how the BIG-IP® system is handling Diameter communications, you can view statistics per Diameter session profile.

1. On the Main tab, click **Statistics** > **Module Statistics** > **Local Traffic**.
   The Local Traffic statistics screen opens.
2. From the **Statistics Type** list, select **Profiles Summary**.
3. In the Details column for the Diameter Session profile, click **View** to display detailed statistics about Diameter sessions.

Viewing Diameter router statistics

Ensure that at Diameter router profile is assigned to at least one virtual server.

When you want to see how the BIG-IP® system is handling Diameter message routing, you can view statistics per Diameter router profile.

1. On the Main tab, click **Statistics** > **Module Statistics** > **Local Traffic**.
   The Local Traffic statistics screen opens.
2. From the **Statistics Type** list, select **Profiles Summary**.
3. In the Details column for the Diameter Router profile, click **View** to display detailed statistics about the routing of Diameter messages.

Using the SIP Configuration Wizard

Overview: SIP Configuration Wizard

The Session Initiation Protocol (SIP) Configuration Wizard provides an easy way to configure SIP message routing functionality for forwarding, load balancing, routing, and transforming SIP messages. You can use this wizard to quickly configure the following functions.

Table 3: SIP Configuration Wizard functions

Function	Description
General Configuration	Enables you to create one or more SIP applications, specifying the parameters for inbound, outbound, and wildcard virtual servers to manage SIP and RTP message traffic. Additionally, based on your configuration, you can enable session persistence, and manage Via headers and route headers. Finally, you can specify the SNAT functionality for each virtual server.
Transformation	Enables you to configure a template that specifies transformation parameters for conditions and actions, and apply them to a virtual server in a SIP application. ***Tip:*** *You can apply one or more templates to a virtual server. Also, you can apply one template to multiple virtual servers, as necessary.*
Logging	Enables you to log request and response messages, as well as specific headers, and specify a logging destination.
Headers	Enables you to specify which SIP headers to make available for transformation.

Important: *You must use a Chrome browser when setting up and using the SIP Configuration Wizard. Only the Chrome browser is currently supported.*

Tip: *Workflow messages appear in the yellow banner to help guide you during the configuration of SIP message routing functionality.*

About setting up the SIP Configuration Wizard

When you set up the SIP Configuration Wizard, you need to complete the following actions:

- Download the SIP Configuration Wizard RPM package from the F5 Downloads site.
- Import the downloaded file into iApps® Package Management LX.

Task summary

Downloading the SIP Configuration Wizard RPM package

You can download the latest SIP Configuration Wizard RPM package from F5 Networks.

1. Log in to the F5 Downloads site, `downloads.f5.com`, and click the **Find a Download** button.
2. Click the name of the product line.

Note: *To download the SIP Configuration Wizard RPM package, click the product line* ***iAppLX Templates****.*

3. Click the name of the version of the product you want to download.

Note: *The name appears as* ***iAppLX_Templates*** *and the version appears as* ***iAppLX****.*

4. Read the End User License Agreement, and click the **I Accept** button if you agree with the terms.
   The Select a Download screen opens.
5. Click the name of the file you want to download.

Note: *The SIP Configuration Wizard RPM package is named* `SIPConfigurationWizard-xx.x.x-x.xx.x.xxx.noarch.rpm`*.*

The latest SIP Configuration Wizard file downloads from F5 Networks.

Importing the SIP Configuration Wizard RPM package

You can import the latest SIP Configuration Wizard RPM package onto a BIG-IP® system.

1. Log on to the command line of the system using the root account.
2. Type the following command to enable iApps® LX controls.

```
touch /var/config/rest/iapps/enable
```

3. Open the BIG-IP Configuration utility.
4. On the Main tab, click **iApps** > **Package Management LX**.
   The Package Management LX screen opens.
5. Click **Import**.
6. For the **File Name** setting, click **Browse** to navigate to the SIP Configuration Wizard RPM package, and then click **Open** to upload the package.

Note: *The SIP Configuration Wizard RPM package is named* `sipConfigurationWizard-xx.x.x-x.xx.x.xxx.noarch.rpm`*.*

7. Click **Upload**.
   The SIP Configuration Wizard RPM package uploads to the Applications Service List screen.

The latest SIP Configuration wizard file is imported and available on the Applications LX screen.

Opening the SIP Configuration Wizard

Before you can open the SIP Configuration Wizard, you need to import the wizard into the iApps® LX interface.

After you import the SIP Configuration Wizard into the iApps LX interface, you can open the wizard to configure SIP message routing functionality.

1. On the Main tab, click **iApps** > **Application Services** > **Applications LX**.
   The Application Service List screen opens.
2. Click the name of a SIP application.

Note: *The default iApps LX SIP application is* ***SIP Configuration****.*

The SIP Configuration Wizard opens and is available for configuration.

About the SIP general configuration

Using the SIP Configuration Wizard General Configuration tab, you can configure an application to specify SIP virtual server functionality.

Task summary

Creating a SIP application

You create a SIP application to define how the SIP virtual servers process SIP messages.

1. In the SIP Configuration Wizard, click the General Configuration tab.
   The General Configuration screen opens.
2. Click **Add Application**.
3. In the **Application Name** field, type a unique name for the SIP application.
4. For the inbound, outbound, and wildcard virtual servers, complete the following steps.
   a) In the **Virtual Server Name** field, type a unique name for the virtual server.

   Note: *A virtual server name cannot include special characters.*

   a) In the **Virtual Server IP** field, type the IP address for the virtual server.
   b) In the **Netmask** field, type a value for the netmask.
   c) In the **Port** field, type a value for the ingress port for the virtual server.
   d) From the **Type** list, select a type of virtual server: **SIP** or **RTP (forward)**.

   Note: RTP (forward) *uses fastL4 functionality and requires no pool.*

   e) From the **Client Protocol** list, select a client-side protocol: **UDP** or **TCP**.
   f) In the **Egress Port** field, type the egress port for the virtual server.
   g) From the **Destination** list, select a destination:

Destination	Description
Pool	Load balances traffic across pool members. ***Important:*** *When configuring a SIP ALG, do not configure a Port Block Allocation (PBA) translation LSN pool with a zombie timeout. Configuring a SIP ALG with an LSN pool that uses PBA mode with a zombie timeout can stop media translations.*
Route by URI	Routes messages based on the URI (forwards messages to the IP address of the domain SIP proxy server associated with the Request-URI) in the SIP header. Resolves Name Authority Pointer (NAPTR) resource records.
Forward	For a wildcard virtual server using RTP, routes messages using the Transport Destination IP Address of the message. No pool is required.

   h) Click **More Options**.
   i) In the **Vlan List** list, select a VLAN for the virtual server, for example, internal, external, or HA.
   j) For a Route by URI destination, in the DNS Pool Members area, type an IP address and port number.

   Note: *You cannot configure a wildcard DNS pool member.*

   k) (Optional) Click the plus (+) button to add another DNS pool member.

Note: *You must configure a DNS pool member IP address and port number before you can add another DNS pool member.*

l) Select the **Session Persistence** check box to enable session persistence.

m) Select the **Insert Via Header** check box to insert a top Via Header at the egress side of the flow, after the SIP_REQUEST_SEND event.

n) Select the **Honor Via Header** check box to honor a Via header that was inserted by a system other than the BIG-IP system.

o) Select the **Insert Record-Route Header** check box to insert a record-route header, that is, the local-IP address and port of the flow the system uses to forward the message.

p) Select the **Honor Route Header** check box to honor a Route header that was inserted by a system other than the BIG-IP system.

q) From the **SNAT** list, select the one of the options:

- **none**.
- **automap**.
- **snatpool**.

    1. In the IP address field, type an IP address.
    2. Click the plus (+) button to add an IP address, as necessary.

r) For a Pool destination, in the Destination Pool Members area, type an IP address and port number.

Note: *You cannot configure a wildcard destination pool member.*

s) (Optional) Click the plus (+) button to add another destination pool member.

Note: *You must configure a destination pool member IP address and port number before you can add another destination pool member.*

5. Click **Add Application** to configure an additional SIP application, as necessary.

About configuring SIP transformations

With the SIP Configuration Wizard Transformations tab, you can configure templates to insert, modify, or delete SIP headers, and assign those templates to virtual servers.

Task summary

About logical operators for conditions, headers, and actions

SIP Transformation template conditions and actions provide you with different types of logical operators for matching and transforming headers, which are determined by the order and configuration of the headers within and between the conditions and actions. The different types of logical operators that you can configure are AND logical operators for multiple headers and actions within a condition, and OR logical operators for headers between conditions. When AND logical operators apply, then all logical operators must match. When OR logical operators apply, then any logical operator must match.

AND logical operators for multiple headers and actions within a condition

When you create a condition, you can configure two or more headers and actions that use AND logic within that condition. For example, you can create a condition with two headers, `a` and `b`, which uses AND logic when that condition is used by the transformation. This means that all headers within a condition must succeed in order to be used by a transformation.

Similarly, when you configure multiple actions for a header, AND logic determines if all matching actions for the header succeed. For example, you can create a condition with a header configured with two or more actions. The matching strategy uses AND logic to determine if all configured actions match.

OR logical operators for headers between conditions

When you create two or more conditions, you can configure each condition with multiple headers that use OR logic between the conditions. For example, you can create a first condition with a set of headers, and a second condition with another set of headers. The matching strategy uses OR logic to determine whether any condition matches.

Examples

These examples show the logical operation of three headers (`a`, `b`, and `c`) and two conditions (`condition1` and `condition2`).

In this first example, consider the following scenario, where you want to match header `a` or `b`, and `c` ((a | b) & c). You can configure this logic by creating `condition1` to use headers `a` and `c` (a & c), and `condition2` to use headers `b` and `c` (b & c). The result is when `condition1` matches the strategy, headers `a` and `c` (a & c) are used for transformation, or when `condition2` matches, headers `b` and `c` (b & c) are used for transformation.

In this second example, consider the scenario where you want to match headers `a` and `b`, or `c` ((a & b) | c). You can configure this logic by creating `condition1` to use headers `a` and `b`, and `condition2` to use header `c`. The result is when `condition1` matches the strategy, both headers `a` and `b` are used for transformation, or when `condition2` matches the strategy, header `c` is used for transformation.

Creating a SIP transformation template

You can create a SIP transformation template to specify transformation parameters for conditions and actions, and apply the template to a virtual server.

1. On the Transformation tab, click the Templates tab.
   The Templates screen opens.
2. Click **Add Template**.
3. In the **templatex** field, type a name for the template.
4. Click **Add** to open Conditions and Actions fields and controls.
   The Conditions and Actions fields and controls open.
5. In the Conditions areas, from the **Header** list, select a header.
6. From the **Expression** list, select an expression.
7. In the **Value** field, type a value.
8. To configure an additional header, click the plus (+) button.
9. In the Actions area, from the **Operation** list, select an operation.
10. From the **Header** list, select a header.
11. In the **Value** field, type a value.
12. To configure an additional operation, click the plus (+) button.
13. (Optional) Click **More Options**.
14. In the **Description** field, type a description for the template.
15. Click **Add** to configure additional Conditions and Actions, as necessary.
16. Click **Add Template** to configure an additional SIP template, as necessary.

Creating a SIP transformation

You need to create a SIP application on the General Configuration tab before you can create a SIP transformation.

You can create a SIP transformation to apply transformation parameters, configured in the transformation template, to a virtual server.

1. In the SIP Configuration Wizard, click the Transformation tab.
   The Transformation screen opens.
2. Click **Add Application**.
3. If multiple applications are configured, select an application name from the application list.
4. Click **Add**.
5. From the **Virtual Server** list, select a virtual server.
6. In the **Select Template(s)** field, select one or more templates to assign to the virtual server.
7. Select the check box for each configured virtual server that you want to enable.
8. Click **Enable**.

About configuring SIP logging

Using the SIP Configuration Wizard Logging tab, you can configure logging parameters and a logging destination, and assign them to a virtual server.

Task summary

Configuring SIP logging

To use external logging or high-speed logging for SIP logging, you first need to configure the external logging or high-speed logging before configuring SIP logging.

You can configure SIP logging for local, external, or high-speed logging of SIP request and response messages and headers, as necessary.

1. In the SIP Configuration Wizard, click the Logging tab.
   The Logging screen opens.
2. In the Messages to Log area, select the check box for each request to log.

   Tip: *Select the* ***All Requests*** *check box to log all of the requests in the requests list.*
3. In the Messages to Log area, select the check box for each response to log.

   Tip: *Select the* ***All Responses*** *check box to log all of the responses in the responses list.*
4. In the **Apply logging to following Virtual Servers** setting, click the arrow to select the virtual servers to which you want to apply logging.
5. In the Headers to log area, select the headers to log.

   Tip: *Select the* ***Log all Headers*** *check box to log all headers in the headers list.*
6. To log additional headers excluded from the Headers to log area, in the Custom Headers area, click the arrow in the **Select Headers** field, and then click each header that you want to log.
7. In the Log Destination area, click the arrow to select a log destination.

About configuring SIP headers

With the SIP Configuration Wizard Headers tab, you can create, modify, and delete SIP headers.

Task summary

Creating a SIP header

You can create a SIP header, as necessary.

1. In the SIP Configuration Wizard, click the Headers tab.
   The Headers screen opens.
2. To create a header, either:
   - Click **Add**, and type the header value in the field.
   - Select the check box for a header, click **Duplicate**, and modify the copied header value.

Modifying a SIP header

You can modify a SIP header, as necessary.

1. In the SIP Configuration Wizard, click the Headers tab.
   The Headers screen opens.
2. To modify a header, type a modified header value in the applicable header field.

Deleting a SIP header

You can delete a SIP header, as necessary.

1. In the SIP Configuration Wizard, click the Headers tab.
   The Headers screen opens.
2. To delete a header, select the check box for the header, and click **Delete**.

Saving a SIP Configuration Wizard configuration

You must configure all SIP Configuration Wizard functionsbefore you save the configuration.

You can save the SIP Configuration Wizard configuration after you complete configuring all of the functions.

1. In the SIP Configuration Wizard, click one of the tabs:
   - General Configuration
   - Transformations
   - Logging
   - Headers
2. Click **Save**.

The system saves the SIP Configuration Wizard configuration.

Configuring SIP Load Balancing

Overview: Configuring a SIP proxy

You can use the BIG-IP® system as a Session Initiation Protocol (SIP) proxy. When the BIG-IP system is placed between your SIP routers, session border controllers, and soft switches, you can configure the system to route and load balance SIP messages across the servers on your SIP network.

This graphic illustrates the relationships of the configuration objects that you must configure on the BIG-IP system.

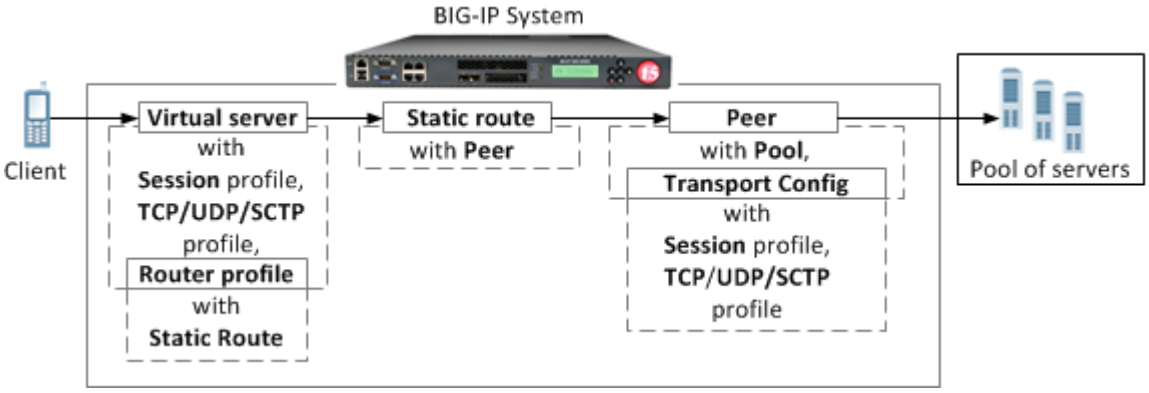

Figure 2: SIP proxy configuration objects

Task summary

About managing MRF SIP session traffic

Through the SIP Session Profile, you can use Message Routing Framework (MRF) to manage SIP traffic across pool members by means of configuring and using Via headers. When you configure Via headers to manage SIP traffic, dependencies between settings apply, enabling you to steer traffic and control requests and responses, as necessary.

Note: *When a client Via header only specifies an address, without specifying a port, the BIG-IP® system uses default port* `5060`*. For example, if a client sends a request with Via header* `SIP/2.0/TCP 192.168.20.1`*, in SIP session traffic scenario 1 (default), the BIG-IP system sends a response to the client with Via header* `SIP/2.0/TCP 192.168.20.1/5060`*.*

Example: SIP session traffic scenario 1 (default)

In SIP session traffic scenario 1 (default), the BIG-IP system receives a request with a Via1 header from a client, and inserts a Via2 header into the request before forwarding the request to the server. When the server provides a response, the BIG-IP system removes the Via2 header from the response, before forwarding the response to the client. If the originating connection no longer exists, the Via2 header that BIG-IP system inserted is no longer available; consequently, the BIG-IP system uses the Via1 header, forwarding the message to the client IP address and port specified by that Via header.

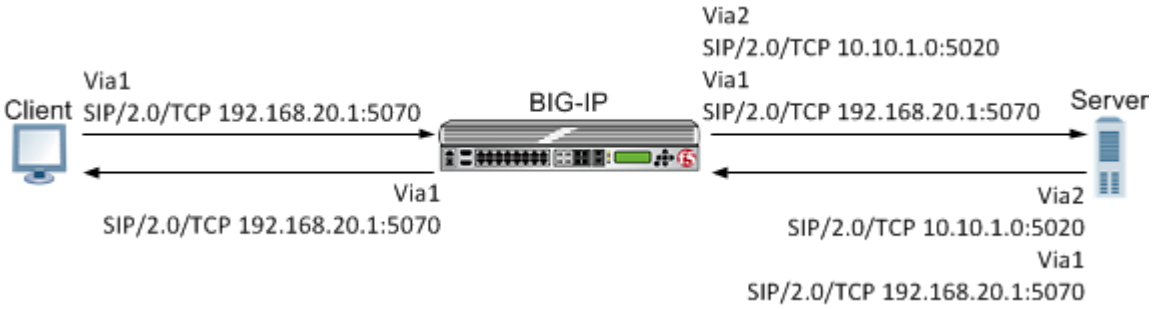

Figure 3: An example of SIP session traffic scenario 1 (default)

When configuring this scenario, the following SIP Session Profile settings apply.

SIP Session Profile control	Setting or value
Honor Via	**Enabled**
Do Not Connect Back	**Disabled**
Insert Via Header	**Enabled**
Custom Via	Not applicable

Example: SIP session traffic scenario 2

In SIP session traffic scenario 2, the BIG-IP system receives a request with a Via1 header from a client, and inserts a Via2 header into the request before forwarding the request to the server. When the server provides a response, the BIG-IP system removes the Via2 header from the response, before forwarding the response to the client. When the originating connection no longer exists, then the BIG-IP system drops the response message and increments the statistic for **Messages failed due to connection dropped**.

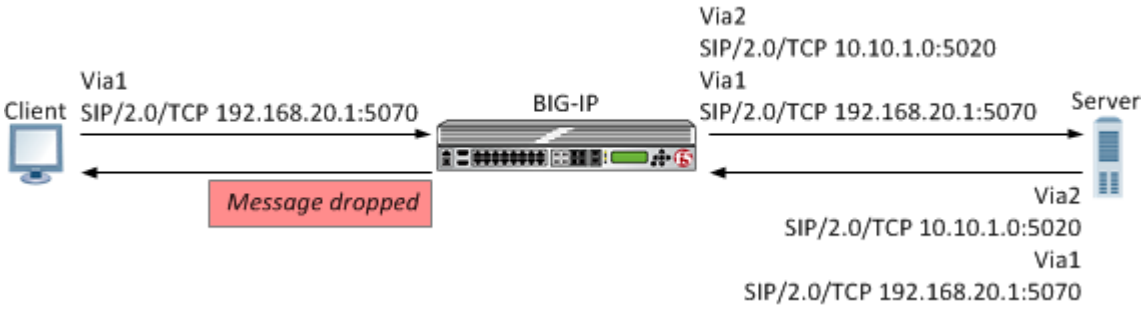

Figure 4: An example of SIP session traffic scenario 2

When configuring this scenario, the following SIP Session Profile settings apply.

SIP Session Profile control	Setting or value
Honor Via	**Enabled**
Do Not Connect Back	**Enabled**
Insert Via Header	**Enabled**
Custom Via	Not applicable

Example: SIP session traffic scenario 3

In SIP session traffic scenario 3, the BIG-IP system receives a request with a Via1 header from a client, and inserts a Via2 header into the request before forwarding the request to the server. When the server

provides a response, the BIG-IP system removes the Via2 header from the response, before forwarding the response to the client. If the originating connection no longer exists, then the Via header that BIG-IP system inserted is no longer available; consequently, the BIG-IP system uses the next available Via header, but, because the **Honor Via** setting is **Disabled**, the BIG-IP system does not forward the message to the client IP address and port specified by that Via header.

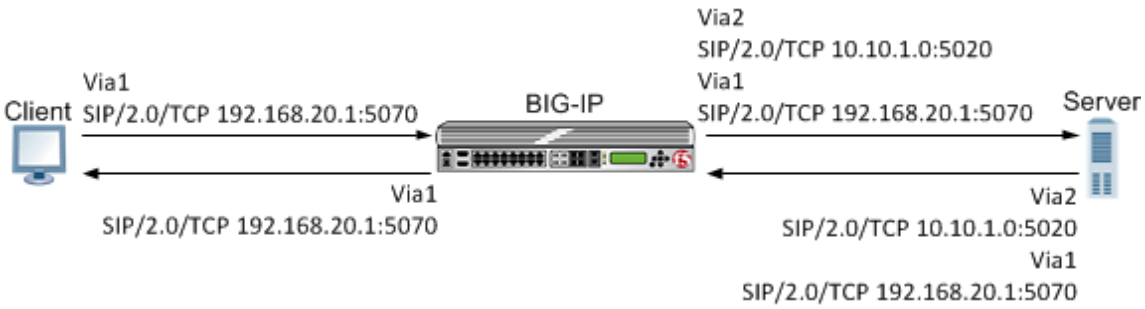

Figure 5: An example of SIP session traffic scenario 3

When configuring this scenario, the following SIP Session Profile settings apply.

SIP Session Profile control	Setting or value
Honor Via	**Disabled**
Do Not Connect Back	**Disabled**
Insert Via Header	**Enabled**
Custom Via	Not applicable

Example: SIP session traffic scenario 4

In SIP session traffic scenario 4, the BIG-IP system receives a request with a Via1 header from a client, and inserts a Via2 header into the request before forwarding the request to the server. When the server provides a response, the response from the BIG-IP to the client must be managed by means of an iRule, for example, `MR::message nexthop TMM:flow_id` or `MR::message route virtual vs_name host ip:port`.

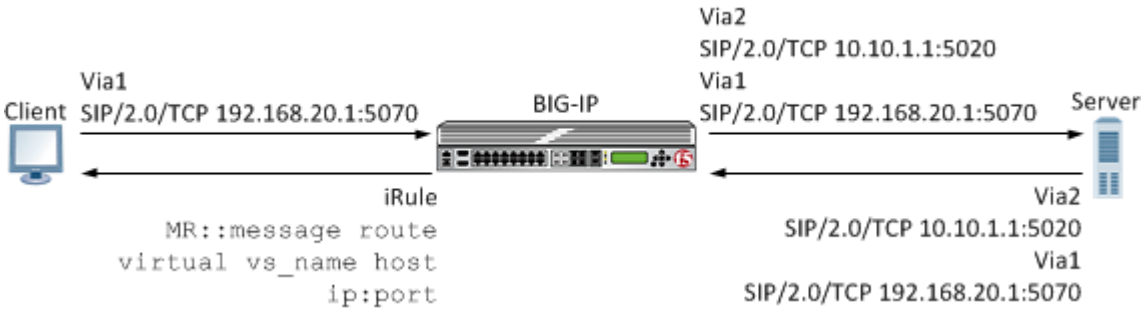

Figure 6: An example of SIP session traffic scenario 4

When configuring this scenario, the following SIP Session Profile settings apply.

SIP Session Profile control	Setting or value
Honor Via	Not applicable
Do Not Connect Back	Not applicable
Insert Via Header	**Enabled**

SIP Session Profile control	Setting or value
Custom Via	Custom Via header value, for example: `SIP/2.0/TCP www.siterequest.com:4343` or `SIP/2.0/SCTP 10.10.4.32`

Example: SIP session traffic scenario 5

In SIP session traffic scenario 5, the BIG-IP system receives a request with a Via1 header from a client, but does not insert a Via header into the request before forwarding the request to the server. When the server provides a response, the BIG-IP system uses the client Via1 header in the response to forward the message to the client IP address and port specified by that Via header.

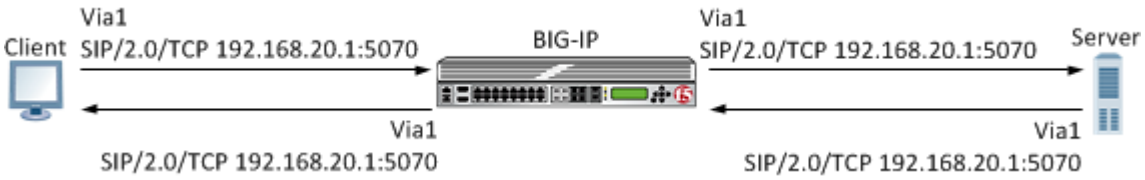

Figure 7: An example of SIP session traffic scenario 5

When configuring this scenario, the following SIP Session Profile settings apply.

SIP Session Profile control	Setting or value
Honor Via	**Enabled**
Do Not Connect Back	Not applicable
Insert Via Header	**Disabled**
Custom Via	Not applicable

Example: SIP session traffic scenario 6

In SIP session traffic scenario 6, the BIG-IP system receives a request with a Via1 header from a client, but does not insert a Via header into the request before forwarding the request to the server. Instead, the BIG-IP system uses the Via1 header specified in the request. When the server provides a response, the BIG-IP system uses the Via1 header in the response, but does not forward the message to the client IP address and port specified by that Via header.

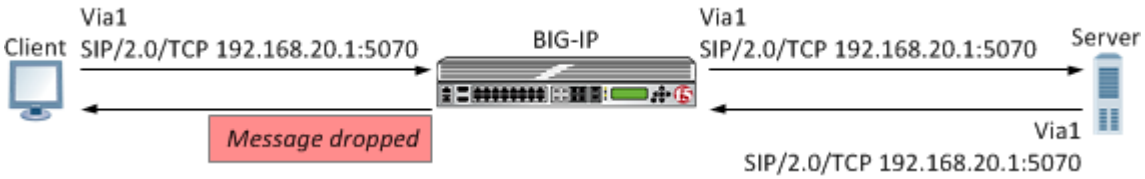

Figure 8: An example of SIP session traffic scenario 6

When configuring this scenario, the following SIP Session Profile settings apply.

SIP Session Profile control	Setting or value
Honor Via	**Disabled**
Do Not Connect Back	Not applicable
Insert Via Header	**Disabled**
Custom Via	Not applicable

Configuration objects required for a SIP proxy

This table names and describes the objects necessary to configure the BIG-IP system as a SIP proxy.

Configuration Objects	Description
Session Profile	Defines how BIG-IP processes SIP messages, including the data used to persist SIP connections.
Transport config	Defines how BIG-IP connects with the servers on your SIP network.
Pool	Defines how BIG-IP load balances connections across a group of servers.
Peer	Defines how BIG-IP connects with the servers on your network and to which servers the system routes and load balances SIP messages.
Static route	Defines how BIG-IP routes SIP messages.
Router profile	Defines an instance of a SIP router.
Virtual Server	Defines the destinations in your network, including the servers that process incoming SIP requests and the pool members that process connections between BIG-IP and your SIP network.

Task summary

Complete these tasks to configure SIP message routing on a BIG-IP® system.

Task list

Creating a SIP session profile

Create a SIP session profile to define how the BIG-IP® system processes SIP messages, including the data the system uses to persist SIP connections.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Message Routing** > **SIP**.
   The SIP transport config list screen opens.
2. On the menu bar, click **Session Profiles**.
   The Session Profiles list screen opens.
3. Click **Create**.
   The New SIP Session Profile screen opens.
4. In the **Name** field, type a unique name for the SIP session profile.
5. From the **Persist Key** list, select the value the system uses for persistence of a SIP session. The options are:

Option	Description
Call-ID	The system uses the value in the Call-ID header field in the SIP message.
Custom	The system uses the value of a custom key specified in an iRule.
Src-Addr	The system uses the originating IP address in the SIP message.

6. From the **Persist Type** list, select one of these options:

Option	Description
Session	Persistence is enabled.
None	Persistence is disabled.

7. In the **Persist Timeout (seconds)** field, type the number of seconds before a SIP session persistence record expires.
8. Click **Finished**.

Creating a transport config

Ensure that at least one SIP session profile exists in the BIG-IP® system configuration.

Create a transport config to define how the BIG-IP system connects with the servers on your network when routing and load balancing SIP messages.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Message Routing** > **SIP**.
   The SIP session profiles list screen opens.
2. On the menu bar, click **Transport Config**.
   The New Transport Config screen opens.
3. Click **Create**.
4. In the **Name** field, type a unique name for the transport config.
5. For the **Profiles** setting, move both a transport protocol profile (TCP, UDP, or SCTP) and a SIP session profile from the **Available** list to the **Selected** list.

   You can associate only one protocol profile and one SIP session profile with each transport config.
6. Click **Finished**.

Creating a pool

You can create a pool of servers that you can group together to receive and process traffic.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add each resource that you want to include in the pool:
   a) (Optional) In the **Node Name** field, type a name for the node portion of the pool member.
   b) In the **Address** field, type an IP address.
   c) In the **Service Port** field, type a port number, or select a service name from the list.
   d) (Optional) In the **Priority** field, type a priority number.
   e) Click **Add**.
5. Click **Finished**.
6. Repeat these steps for each pool you want to create.

The new pool appears in the Pools list.

Creating a peer

Ensure that at least one transport config and one pool exist in the BIG-IP® system configuration.

Create a peer to define how the BIG-IP system connects with the servers on your network and to which servers the system routes and load balances SIP messages.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Message Routing** > **SIP**.
   The SIP session profiles list screen opens.
2. On the menu bar, click **Peers**.
   The Peers list screen opens.
3. Click **Create**.
   The New Peers screen opens.
4. In the **Name** field, type a unique name for the peer.
5. In the **Description** field, type a description of the peer.
6. From the **Connection Mode** list, specify how connections are limited for this peer. The options are:

Option	Description
Per Blade	The number of connections to this peer is per blade on a VIPRION system.
Per Peer	The number of connections to this peer is per peer.
Per TMM	The number of connections to this peer is per TMM on the BIG-IP system.
Per Client	The number of connections to a remote host is per client connection.

7. From the **Pool** list, select the pool of servers to which the system load balances SIP messages.
   In the case where the calls should be always sent to a single SIP Server, you will still need to create a pool with a single member (the SIP Server), and add the same to the peer.
8. From the **Transport Config** list, select the transport config that defines how the BIG-IP system communicates with the servers on your network.
9. Click **Finished**.

Creating a static route

Ensure that at least one peer and one virtual server exist in the BIG-IP® system configuration.

Create a static route when you want to route SIP messages from specific clients to specific domains, and load balance those SIP messages across a group of peers. If the configured attributes of a static route match the attributes in a SIP message, the system forwards the message to a member of the pool associated with one of the peers.

Note: *The BIG-IP system can use multiple SIP session profiles in a single routing instance, because a different profile can be associated with each member of a pool.*

---

1. On the Main tab, click **Local Traffic** > **Profiles** > **Message Routing** > **SIP**.
   The SIP session profiles list screen opens.
2. On the menu bar, click **Static Routes**.
   The Static Routes list screen opens.
3. Click **Create**.
   The New Route screen opens.
4. In the **Name** field, type a unique name for the static route.
5. In the **Request URI** field, type the value found in the request-uri of a SIP message that the system matches when routing a message.
6. In the **From URI** field, type the value found in the **From** field of a SIP message that the system matches when routing a message.
7. In the **To URI** field, type the value found in the **To** field of a SIP message that the system matches when routing a message.
8. From the **Virtual Server** list, select the virtual server from which the system receives client requests for this static route.

If you do not select a virtual server, the system uses this static route to route SIP messages originating from any client.

9. From the **Peer Selection Mode** field, select how the system selects the Peer to route a SIP message to:

Option	Description
Ratio	Peer selection is based on the ratio that is set for each peer in the **Selected** list.
Sequential	Peer selection is based on the order of the peers in the **Selected** list.

10. For the **Peers** setting, move the peers that define the servers to which the system load balances SIP messages from the **Available** list to the **Selected** list.
11. Click **Finished**.

Creating a SIP router profile

Before you start this task, ensure that at least one static route exists on the BIG-IP® system.

Create a SIP router profile to define how a router handles SIP traffic.

Note: *A SIP routing profiles binds the virtual server that processes SIP requests from clients with the peers that connect with the servers on your SIP network.*

---

1. On the Main tab, click **Local Traffic** > **Profiles** > **Message Routing** > **SIP**.
   The SIP transport config list screen opens.
2. On the menu bar, click **Router Profiles**.
   The Router Profiles list screen opens.
3. Click **Create**.
   The New SIP Router Profile screen opens.
4. In the **Name** field, type a unique name for the SIP router profile.
5. In the Settings area, select the **Custom** check box.
6. From the **Operation Mode** list, select **Load Balancing**.
7. (Optional) To use connection mirroring, configure the **Traffic Group** setting.
   a) Clear the **Inherit traffic group from current partition / path** check box.
   b) From the list, select a traffic group, such as, **traffic-group-1**.

   Important: *Changing traffic groups, with Connection Mirroring enabled, drops all mirrored connections and loses all persistence data. If you change traffic groups, mirroring must restart.*

   Note: *The traffic group for the virtual address and mirrored attribute are overwritten by the attached router profile.*

   ---
8. (Optional) Select the **Connection Mirroring** check box.

   Note: *For connection mirroring to properly function, this device must be a member of a device group.*

   ---
9. In the **Mirrored Message Sweeper Interval** field, type the milliseconds for the frequency of the mirrored message sweeper.
10. For the **Static Routes** setting, move routes that define how the BIG-IP system load balances SIP traffic from the **Available** list to the **Selected** list.
11. Click **Finished**.

Creating a virtual server to handle SIP client requests

Ensure that both a SIP session profile and a SIP router profile exist in the BIG-IP® system configuration.

Create a virtual server to handle SIP client requests.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. In the **Name** field, type a unique name for the virtual server.
3. From the **Type** list, select **Message Routing**.
4. In the **Destination Address/Mask** field, type an address, as appropriate for your network.
   The supported format is address/prefix, where the prefix length is in bits. For example, an IPv4 address/prefix is `10.0.0.1` or `10.0.0.0/24`, and an IPv6 address/prefix is `ffe1::0020/64` or `2001:ed8:77b5:2:10:10:100:42/64`. When you use an IPv4 address without specifying a prefix, the BIG-IP® system automatically uses a `/32` prefix.
5. In the **Service Port** field, type `5060` to route SIP traffic or `5061` to route TLS traffic.
6. From the **Configuration** list, select **Advanced**.
7. From the **Application Protocol** list, select **SIP**.
8. From the **Session Profile** list, select a SIP session profile.
9. From the **Router Profile** list, select a SIP router profile.
10. Click **Update**.

Configuration objects required for a SIP proxy

This table names and describes the objects necessary to configure the BIG-IP system as a SIP proxy.

Configuration Objects	Description
Session Profile	Defines how BIG-IP processes SIP messages, including the data used to persist SIP connections.
Transport config	Defines how BIG-IP connects with the servers on your SIP network.
Pool	Defines how BIG-IP load balances connections across a group of servers.
Peer	Defines how BIG-IP connects with the servers on your network and to which servers the system routes and load balances SIP messages.
Static route	Defines how BIG-IP routes SIP messages.
Router profile	Defines an instance of a SIP router.
Virtual Server	Defines the destinations in your network, including the servers that process incoming SIP requests and the pool members that process connections between BIG-IP and your SIP network.

About checking pool member health

You can configure the BIG-IP® system to monitor pool member health using a SIP monitor. Use a SIP monitor to check the health of a host with an active SIP session. The SIP monitor also monitors a SIP

connection independent of a specific SIP session and marks a host that had been marked down, but is online again, as available.

Task summary

Perform these tasks to configure health monitors and apply the monitors to a pool:

Creating a SIP monitor

Create a SIP monitor to mark a pool member as down when that server stops responding and then to mark the pool member as available when service is restored.

1. On the Main tab, click **Local Traffic** > **Monitors**.
   The Monitors List screen opens.
2. Click **Create**.
   The New Monitor screen opens.
3. In the **Name** field, type a name for the monitor.
4. From the **Type** list, select **SIP**.
   The screen refreshes, and displays the configuration options for the **SIP** monitor type.
5. Configure additional settings based on your network requirements.
6. Click **Finished**.

Adding a health monitor to a pool

Add health monitors to a pool when you want the BIG-IP system to monitor the health of the pool members. Repeat this procedure for each desired pool.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click the name of the pool you want to modify.
3. For the **Health Monitors** setting, in the **Available** list, select a monitor type, and click **<<** to move the monitor to the **Active** list.

   Tip: *Hold the Shift or Ctrl key to select more than one monitor at a time.*
4. Click **Finished**.

The new pool appears in the Pools list.

About viewing SIP session and router statistics

You can view statistics for SIP sessions and routes.

Task summary

Viewing SIP session statistics

Ensure that at SIP session router profile are assigned to at least one virtual server.

When you want to see how the BIG-IP® system is handling SIP communications, you can view statistics per SIP session profile.

1. On the Main tab, click **Statistics** > **Module Statistics** > **Local Traffic**.
   The Local Traffic statistics screen opens.

2. From the **Statistics Type** list, select **Profiles Summary**.
3. In the Details column for the SIP Session profile, click **View** to display detailed statistics about SIP sessions.

Viewing SIP router statistics

Ensure that at SIP session and SIP router profile are assigned to at least one virtual server.

When you want to see how the BIG-IP® system is handling SIP message routing, you can view statistics per SIP router profile.

1. On the Main tab, click **Statistics** > **Module Statistics** > **Local Traffic**.
   The Local Traffic statistics screen opens.
2. From the **Statistics Type** list, select **Profiles Summary**.
3. In the Details column for the SIP Router profile, click **View** to display detailed statistics about the routing of SIP messages.

Configuring a SIP Message Routing Firewall

Overview: Configuring a SIP message routing firewall

You can use the BIG-IP® system Session Initiation Protocol (SIP) message routing functionality in a firewall configuration to provide stateful handling of SIP communication and media flows. A virtual server handles the SIP communications and related media flows, allowing them to pass through otherwise restrictive firewall rules. You configure a Local Traffic message routing SIP profile, router profile, and virtual server, and then use that configuration with an Advanced Firewall Manager™ (AFM™) DoS profile. In this firewall configuration, the SIP session profile, SIP router profile, and virtual server use Application Level Gateway (ALG) functionality, where the BIG-IP system does not perform address translation or subscriber registration tracking.

Note: *When using ALG functionality, you cannot use a SIP router profile with an operation mode that is configured to use load balancing settings. Instead, you need to use a SIP router profile with the operation mode configured to use Application Level Gateway settings.*

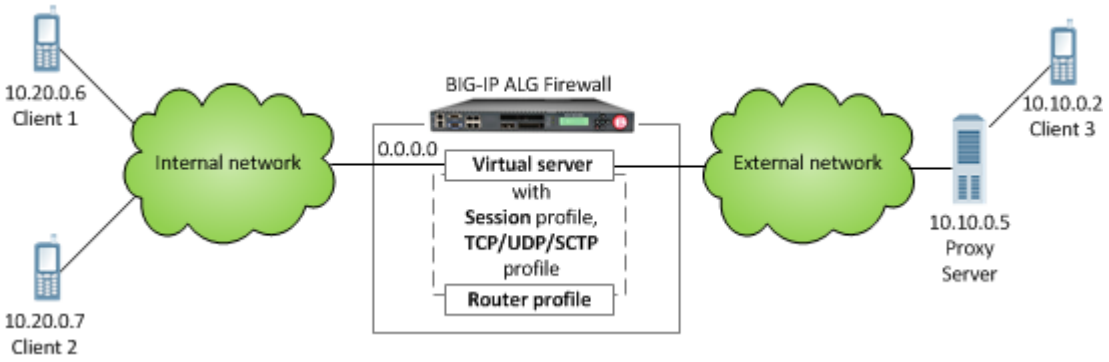

Figure 9: A SIP firewall configuration

Task summary

Creating a SIP ALG router profile

You can create a SIP router profile with mirroring functionality for a SIP ALG firewall configuration.

Note: *If you do not want to configure mirroring functionality, you can configure a virtual server to use the default settings provided in the preconfigured* ***siprouter-alg*** *profile.*

1. On the Main tab, click **Local Traffic** > **Profiles** > **Message Routing** > **SIP**.
   The SIP session profiles list screen opens.
2. On the menu bar, click **Router Profiles**.
   The Router Profiles list screen opens.
3. Click **Create**.
   The New Router Profiles screen opens.
4. In the **Name** field, type a unique name for the router profile.
5. In the Settings area, select the **Custom** check box.
6. From the **Operation Mode** list, select **Application Level Gateway**.
7. To use connection mirroring, configure the **Traffic Group** setting.

a) Clear the **Inherit traffic group from current partition / path** check box.
b) From the list, select a traffic group, such as, **traffic-group-1**.

Important: *Changing traffic groups, with Connection Mirroring enabled, drops all mirrored connections and loses all persistence data. If you change traffic groups, mirroring must restart.*

Note: *The traffic group for the virtual address and mirrored attribute are overwritten by the attached router profile.*

8. Select the **Connection Mirroring** check box.

Note: *For connection mirroring to properly function, this device must be a member of a device group.*

9. In the **Mirrored Message Sweeper Interval** field, type the milliseconds for the frequency of the mirrored message sweeper.
10. Click **Finished**.

A SIP router profile appears in the Router Profiles list.

Creating a virtual server for SIP firewall

Before you start this task, ensure that a SIP Session Profile, configured for a firewall, and a SIP Router Profile, configured for Application Level Gateway, exist in the BIG-IP® system configuration.

You can create a virtual server to handle SIP communications and related media flows, allowing them to pass through otherwise restrictive firewall rules.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, type a unique name for the virtual server.
4. From the **Type** list, select **Message Routing**.
5. In the **Source Address** field, type `0.0.0.0/0` for the source address and prefix length.
6. In the **Destination Address** field, type the IP address in CIDR format.

   The supported format is address/prefix, where the prefix length is in bits. For example, an IPv4 address/prefix is `10.0.0.1` or `10.0.0.0/24`, and an IPv6 address/prefix is `ffe1::0020/64` or `2001:ed8:77b5:2:10:10:100:42/64`. When you use an IPv4 address without specifying a prefix, the BIG-IP® system automatically uses a `/32` prefix.

   Note: *The IP address for this field needs to be on the same subnet as the external self-IP.*

7. In the **Service Port** field, type `5060`.
8. From the **Configuration** list, select **Advanced**.
9. From the **Application Protocol** list, select **SIP**.
10. From the **Session Profile** list, select a SIP session profile.

    Note: *For a SIP firewall configuration, you can use the* ***sipsession-alg*** *profile.*

11. From the **Router Profile** list, select a SIP router profile.

    Note: *For a SIP firewall configuration without mirroring, you can use the* ***siprouter-alg*** *profile. For a SIP firewall configuration with mirroring, you must use a router profile configured for mirroring.*

12. Complete the following steps to disable all translation functionality on the virtual server.

a) From the **Source Address Translation** list, select **None**.
b) Clear the **Address Translation** check box.
c) Clear the **Port Translation** check box.

13. Click **Finished**.

A message routing virtual server is configured to handle SIP firewall communication as defined by the SIP Session Profile and Router Profile.

You can configure a DoS Profile in Advanced Firewall Manager™ (AFM™) to use this virtual server.

Legal Notices

Legal notices

Publication Date

This document was published on June 15, 2018.

Publication Number

MAN-0653-01

Copyright

Trademarks

For a current list of F5 trademarks and service marks, see *http://www.f5.com/about/guidelines-policies/trademarks*.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by one or more patents indicated at: *https://f5.com/about-us/policies/patents*.

Link Controller Availability

This product is not currently available in the U.S.

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a

residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Index

T

V