Integration Reference Manual

Configuring TLS

4/2/2025

Configuring TLS

Contents

Secure data transfer using TLS is now supported between SIP Server and Active-Active Resource Managers in a deployment where SIP Server high-availability is configured using the F5 Networks BIG-IP LTM. TLS is also supported between SIP Server and all SIP devices in this deployment, including SBCs, Media Gateways, and SIP phones. BIG-IP LTM is not a TLS peer as are other elements in the environment; there is no TLS negotiation between BIG-IP LTM and other components.

Integration Solution Assumptions

The integration solution described in this section makes the following assumptions:

- BIG-IP LTM is deployed as a single instance
- TLS transport is used for SIP signaling
- SIP Server performs load balancing between an Active-Active Resource Manager pair

See Deployment Architecture Example.

Deploying the TLS Solution

To support TLS data transfer in a SIP Server deployment with an Active-Active RM pair and a BIG-IP LTM used for the SIP Server HA, complete the following procedures:

1. Configure BIG-IP LTM for TLS.
2. Provision SSL certificates for workstations hosting SIP Servers, RM, and MCP applications. Refer to the ''Genesys 8.1 Security Deployment Guide''.
3. Configure SIP Server to use TLS data transfer. Refer to the *Transport Layer Security for SIP Traffic* section in the *Framework 8.1 SIP Server Deployment Guide*.
4. Configure Resource Managers in an Active-Active high-availability cluster. Refer to the *Genesys Voice Platform Integration* section in the ''Framework 8.1 SIP Server Deployment Guide''.

To configure TLS data transfer between Genesys Media Server components, refer to the ''Genesys Media Server 8.1 Deployment Guide''.

Configuring BIG-IP LTM for TLS

1. Complete general configuration procedures.

Before starting the TLS-specific configuration of BIG-IP LTM, complete the configuration procedures.

2. Configure a health monitor.

To configure a health monitor:

1. Go to `Local Traffic > Monitors`.
2. Click `Create`.
3. In the dialog box that appears, specify the following properties:
   - `Name:` Enter the name for this health monitor—for example, `monSipTls`.
   - `Type:` Select `TCP`.
   - `Parent Monitor:` Select `TCP`.
   - `Configuration:` Select `Basic`.
   - `Interval:` Enter 1 (seconds).
4. Click `Finished`.

3. Configure a server pool.

To configure a server pool:

1. Go to `Local Traffic > Pools`.
2. Click `Create`.
3. In the dialog box that appears, specify the following properties:
   - `Name:` Enter the name for this server pool—for example, the `poolHa01tls`.
   - `Configuration:` Select `Advanced`.
   - `Health Monitors > Active:` Select `monSipTls`.
   - `Action On Service Down:` Select `Reselect`.
   - `Slow Ramp Time:` Enter`0` (seconds).
4. Click `Finished`.

4. Add server pool members.

To add server pool members:

1. Go to `Local Traffic > Pools > poolHa01tls > Members`.
2. Click `Add`.

3. In the dialog box that appears, specify the following properties:
    - Node Name: Select the primary server node. In our example, it would be nodeHa01Primary.
    - Address: Specify the IP address of the primary server node. In our example, it would be 192.168.167.125.
    - Service Port: Enter 5061.
4. Click Finished.
5. Click Add.
6. In the dialog box that appears, specify the following properties:
    - Node Name: Select the backup server node. In our example, it would be nodeHa01Backup.
    - Address: Specify the IP address of the backup server node. In our example, it would be 192.168.167.126.
    - Service Port: Enter 5061.
7. Click Finished.
8. Set the Load Balancing Method to Round Robin.

5. Configure a Virtual Server.

To configure a Virtual Server:

1. Go to Local Traffic > Virtual Servers.
2. Click Create.
3. In the dialog box that appears, specify the following properties:
    - Name: Enter the name for this Virtual Server—for example, vsVipTlsHa01.
    - Destination > Type: Select Host.
    - Destination > Address: Enter the IP address for this Virtual Server—for example, 192.168.166.238.
    - Service Port: Enter 5061 (Other).
    - State: Select Enabled.
    - Configuration: Select Basic.
    - Type: Select Standard.
    - Protocol: Select TCP.
    - VLAN and Tunnel Traffic: Select Enabled on...
    - VLANs and Tunnels Selected: Select dc1ext.
4. Click Finished.

5. Select `Local Traffic > Virtual Server List > vsVipTlsHa01 > Resources`.
6. Add `Default Pool`: `poolHa01tls`
7. Click `Update`.

6. Disable Virtual Servers for UDP and TCP.

At this point, the BIG-IP LTM is configured for handling communications over different protocols: UDP, TCP, and TLS. If TLS is mandatory for security reasons, Genesys strongly recommends disabling virtual servers for insecure protocols, such as UDP and TCP.

To disable Virtual Servers for UDP and TCP:

1. Go to `Local Traffic > Virtual Servers`.
2. Select check boxes of the following virtual servers: `vsVipUdpHa01` and `vsVipTcpHa01`.
3. Click `Disable`.

This completes configuring BIG-IP LTM.