Oracle SBC with Google Voice Sip Link

Technical Application Note
Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.
Contents

1 REVISION HISTORY .............................................................................................................. 6
2 INTENDED AUDIENCE ......................................................................................................... 6
3 VALIDATED ORACLE SOFTWARE VERSIONS ......................................................................... 6
4 RELATED DOCUMENTATION ................................................................................................. 6
  4.1 ORACLE SBC .................................................................................................................. 6
  4.2 GOOGLE VOICE SIP LINK ............................................................................................ 7
5 ABOUT GOOGLE VOICE SIP LINK ...................................................................................... 7
  5.1 INFRASTRUCTURE REQUIREMENTS ............................................................................ 7
  5.2 SBC DOMAIN NAME ................................................................................................. 7
6 CONFIGURING GOOGLE VOICE SIP LINK ........................................................................... 7
7 ORACLE SBC CONFIGURATION .......................................................................................... 8
  7.1 SYSTEM-CONFIG ......................................................................................................... 9
  7.1.1 NTP-Sync ............................................................................................................... 10
  7.2 NETWORK CONFIGURATION ...................................................................................... 10
  7.2.1 Physical Interfaces .................................................................................................. 11
  7.2.2 Network Interfaces ................................................................................................. 11
  7.3 SECURITY CONFIGURATION ....................................................................................... 12
  7.3.1 Hardware Requirements ......................................................................................... 12
  7.3.2 Encryption for Virtual SBC .................................................................................... 12
  7.3.3 Certificate Records ................................................................................................. 13
  7.3.4 TLS Profile ............................................................................................................. 17
  7.3.5 Media Security ....................................................................................................... 18
  7.4 TRANSCODING CONFIGURATION .............................................................................. 21
  7.4.1 Codec Policies ....................................................................................................... 21
  7.5 MEDIA CONFIGURATION ............................................................................................. 22
  7.5.1 Media Manager ....................................................................................................... 22
  7.5.2 Realm Config ......................................................................................................... 23
  7.5.3 Steering Pools ........................................................................................................ 24
  7.6 SIP CONFIGURATION .................................................................................................... 25
  7.6.1 Sip-Config .............................................................................................................. 25
  7.6.2 Sip Manipulation ..................................................................................................... 26
  7.6.3 Session Timer Profile ............................................................................................. 28
  7.6.4 Sip Interface ........................................................................................................... 29
  7.6.5 Session Agents ....................................................................................................... 29
  7.7 ROUTING CONFIGURATION ....................................................................................... 30

8 VERIFY CONNECTIVITY ....................................................................................................... 33
  8.1 ORACLE SBC OPTIONS PINGS ................................................................................... 33

9 SYNTAX REQUIREMENTS FOR SIP INVITE AND SIP OPTIONS: .................................... 33
  9.1 TERMINOLOGY ........................................................................................................... 33
  9.2 REQUIREMENTS FOR INVITE MESSAGES .................................................................. 33
  9.2.1 Contact Header-Invite ........................................................................................... 34
  9.3 REQUIREMENTS FOR OPTIONS MESSAGES ............................................................... 34
9.3.1 Contact Header-OPTIONS: ................................................................. 34
10 APPENDIX A .................................................................................................. 35
   10.1 ORACLE SBC TDM WITH SIP LINK ...................................................... 35
   10.1.1 Interface Requirements ................................................................. 35
11 APPENDIX B .................................................................................................. 36
   11.1 ORACLE SBC DEPLOYED BEHIND NAT ............................................ 36
12 ACLI RUNNING CONFIGURATION ............................................................. 38
1 Revision History

<table>
<thead>
<tr>
<th>Document Version</th>
<th>Description</th>
<th>Revision Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>• Initial Release</td>
<td>06/22/2022</td>
</tr>
<tr>
<td>1.1</td>
<td>• Added hardware and licensing requirements for TLS/SRTP</td>
<td>02/14/2023</td>
</tr>
<tr>
<td>1.2</td>
<td>• Added direct links for GTSR1 and GlobaSign Root CA</td>
<td>03/07/2023</td>
</tr>
</tbody>
</table>

2 Intended Audience
This document describes how to connect the Oracle SBC to Google Voice Sip Link. This paper is intended for IT or telephony professionals.

*Note: To zoom in on screenshots of Web GUI configuration examples, press Ctrl and +.*

3 Validated Oracle Software Versions
All testing was successfully conducted with the Oracle Communications SBC versions:
SCZ840, SCZ900

These software releases with the configuration listed below can run on any of the following products:

- AP 1100
- AP 3900
- AP 3950 (Release SCZ9.x.x Only)
- AP 4600
- AP 4900 (Release SCZ9.x.x Only)
- AP 6350
- AP 6300
- VME
- Public Clouds (OCI, AWS, Azure)

Please visit [https://support.google.com](https://support.google.com) for further information

4 Related Documentation

4.1 Oracle SBC

- [Oracle® Enterprise Session Border Controller Web GUI User Guide](#)
- [Oracle® Enterprise Session Border Controller ACLI Reference Guide](#)
- [Oracle® Enterprise Session Border Controller Release Notes](#)
- [Oracle® Enterprise Session Border Controller Configuration Guide](#)
- [Oracle® Enterprise Session Border Controller Security Guide](#)
4.2 Google Voice Sip Link

- Google Voice SIP Link

5 About Google Voice SIP Link

With Google Voice SIP Link, you can connect your existing carrier to Google through a set of certified Session Border Controllers (SBC). This flexibility allows you to use your existing telecommunication infrastructure and maintain uninterrupted service with your current carrier.

5.1 Infrastructure Requirements

<table>
<thead>
<tr>
<th>Session Border Controller (SBC)</th>
<th>See Check Voice SIP Link Requirements for More Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Trunks connected to the SBC</td>
<td></td>
</tr>
<tr>
<td>Google Voice SIP Link</td>
<td></td>
</tr>
<tr>
<td>Public IP address for the SBC</td>
<td></td>
</tr>
<tr>
<td>Public trusted certificate for the SBC</td>
<td></td>
</tr>
<tr>
<td>Firewall ports for SIP Link signaling</td>
<td></td>
</tr>
<tr>
<td>Firewall IP addresses and ports for SIP Link media</td>
<td></td>
</tr>
<tr>
<td>Media Transport Profile</td>
<td></td>
</tr>
<tr>
<td>Firewall ports for client media</td>
<td></td>
</tr>
</tbody>
</table>

5.2 SBC Domain Name

In this application note, we are using the following FQDN that is registered in our Google Admin account to pair the Oracle SBC to Google Voice SIP Link. Since our SBC is deployed behind NAT, we will only be displaying the private IP addresses configured on the SBC.

<table>
<thead>
<tr>
<th>Public IP Address</th>
<th>FQDN Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Public IP of SBC or NAT&gt;</td>
<td>solutionslab.cgbuburlington.com</td>
</tr>
</tbody>
</table>

6 Configuring Google Voice SIP Link

For detailed step-by-step guidance on setting up Google Voice SIP Link, go to:

support.google.com/a?p=siplink.

Before you begin configuring SIP Link you will need to do the following:

- Verify Google Voice has been enabled on your Corporate Google account.
- Make sure you log in using Google Workspace admin credentials.

For more information, please reach out to your local Google representative.
7 Oracle SBC Configuration

This chapter provides step-by-step guidance on how to configure Oracle SBC for interworking with Google Voice SIP Link.

Please follow the steps in this chapter to successfully configure the Oracle SBC.

There are multiple connections shown:

- Google SIP Link is on the WAN
- Service provider Sip trunk terminating on the SBC
- Google Voice Web Client both on prem and remote
- Poly OBI302 ATA on prem registering to Google Cloud

There are two methods for configuring the OCSBC, ACLI, or GUI.
For the purposes of this note, we'll be using the OCSBC GUI for all configuration examples. We will however provide the ACLI path to each element.

This guide assumes the OCSBC has been installed, management interface has been configured, product selected and entitlements have been assigned. Also, http-server has been enabled for GUI access. If you require more information on how to install your SBC platform, please refer to the ACLI configuration guide.

To access the OCSBC GUI, enter the management IP address into a web browser. When the login screen appears, enter the username and password to access the OCSBC.

Once you have access to the OCSBC GUI, at the top, click the Configuration Tab. This will bring up the OCSBC Configuration Objects List on the left hand side of the screen.

Any configuration parameter not specifically listed below can remain at the OCSBC default value and does not require a change for the connection to Google Voice SIP Link to function properly.

Note: The configuration examples below were captured from a system running the latest GA software, 9.0.0

7.1 System-Config

To enable system level functionality for the OCSBC, you must first enable the system-config.

GUI Path: system/system-config

ACLI Path: config t→system→system-config

Note: The following parameters are optional but recommended for system config

- Hostname
- Description
- Location
- Default Gateway (recommended to be the same as management interface gateway)
- Transcoding Core (This field is only required if you have deployed a VME SBC and plan to transcode media)
Click OK at the bottom

### 7.1.1 NTP-Sync

You can use the following example to connect the Oracle SBC to any network time servers you have in your network. This is an optional configuration but recommended.

GUI Path: system/ntp-config

ACLI Path: config t → system → ntp-sync

Select OK at the bottom

Now we’ll move on configuring network connection on the SBC.

### 7.2 Network Configuration

To connect the SBC to network elements, we must configure both physical and network interfaces. For the purposes of this example, we will configure two physical interfaces, and two network interfaces. One to communicate with Google Voice SIP Link, the other to connect to PSTN Network. The slots and ports used in this example may be different from your network setup.
7.2.1 Physical Interfaces

GUI Path: system/phy-interface

ACLI Path: config t → system → phy-interface

- Click Add, use the following table as a configuration example:

<table>
<thead>
<tr>
<th>Config Parameter</th>
<th>PSTN</th>
<th>Google</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>s0p0</td>
<td>S1p0</td>
</tr>
<tr>
<td>Operation Type</td>
<td>Media</td>
<td>Media</td>
</tr>
<tr>
<td>Slot</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Port</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Note: Physical interface names, slot and port may vary depending on environment

7.2.2 Network Interfaces

GUI Path: system/network-interface

ACLI Path: config t → system → network-interface

- Click Add, use the following table as a configuration example:

<table>
<thead>
<tr>
<th>Configuration Parameter</th>
<th>GoogleVoice</th>
<th>PSTN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>s1p0</td>
<td>s0p0</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.1.3.4</td>
<td>10.1.2.4</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Gateway</td>
<td>10.1.3.1</td>
<td>10.1.2.1</td>
</tr>
<tr>
<td>DNS Primary IP</td>
<td>8.8.8.8</td>
<td></td>
</tr>
<tr>
<td>DNS Domain</td>
<td>Solutionslab.cgbuburlington.com</td>
<td></td>
</tr>
</tbody>
</table>
Click OK at the bottom of each after entering config information

Next, we'll configure the necessary elements to secure signaling and media traffic between the Oracle SBC and Google Voice SIP Link.

7.3 Security Configuration

7.3.1 Hardware Requirements

The Acme Packet platforms and VNF all support SRTP.

SSM is required for TLS on Acme Packet 4600, 6100, 6300, and 6350. SSM is not required for TLS on Acme Packet 1100, 3900, 3950, 4900, and VME/VNF. TLS is used for encrypting signaling, and SRTP is used for encrypting media. In this case, then the SSM module is also required to run TLS.

```
# show security ssm
```

SSM (Security Service Module) v3 present.

7.3.2 Encryption for Virtual SBC

You must enable encryption for virtualized deployments with a license key. The following table lists which licenses are required for various encryption use cases.

<table>
<thead>
<tr>
<th>Feature</th>
<th>License Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec Trunking</td>
<td>IPSEC</td>
</tr>
<tr>
<td>SRTP Sessions</td>
<td>SRTP</td>
</tr>
<tr>
<td>Transport Layer Security Sessions</td>
<td>TLS</td>
</tr>
<tr>
<td>MSRP</td>
<td>TLS</td>
</tr>
</tbody>
</table>

*Note: The TLS license is only required for media and signaling. TLS for secure access, such as SSH, HTTPS, and SFTP is available without installing the TLS license key.*

To enable the preceding features, you install a license key at the system, license configuration element. Request license keys at the License Codes website at


After you install the license keys, you must reboot the system to see them.
This section describes how to configure the SBC for both TLS and SRTP communication with Google Voice SIP Link.

Google Voice SIP Link only allows TLS connections from SBC’s for SIP traffic, and SRTP for media traffic. It requires a certificate signed by a supported Certificate Authority (CA).

Voice SIP Link accepts TLS certificates from the following Certificate Authorities (CAs):

- DigiCert
- Entrust DataCard
- GlobalSign
- GoDaddy
- Sectigo

7.3.3 Certificate Records

“Certificate-records” are configuration elements on Oracle SBC which capture information for a TLS certificate such as common-name, key-size, key-usage etc.

This section walks you through how to configure certificate records, create a certificate signing request, and import the necessary certificates into the SBC’s configuration.

GUI Path: security/certificate-record

ACLI Path: config t→ security→ certificate-record

For the purposes of this application note, we’ll create three certificate records. They are as follows:

- SBC Certificate (end-entity certificate)
- DigiCert RootCA Cert (Root CA used to sign the SBC’s end entity certificate)
- Google GTS Root R1 (GTSR1) (Google Presents the SBC a certificate signed by this authority)

Note: The DigiCert RootCA is only part of this example, and is the Authority we used to sign our SBC certificate. You would replace this with the root and/or intermediate certificates used to sign the CSR generated from your SBC.

7.3.3.1 SBC End Entity Certificate

The SBC’s end entity certificate is the certificate the SBC presents to Google to secure the connection. The only requirements when configuring this certificate is the common name must contain the SBC’s FQDN. In this example our common name will be solutionslab.cgbuburlington.com. You must also give it a name. All other fields are optional, and can remain at default values.

To Configure the certificate record:

Click Add, and use the following example to configure the SBC certificate
Click OK at the bottom

Next, using this same procedure, configure certificate records for the Root CA certificates

**7.3.3.2 Root CA and Intermediate Certificates**

**7.3.3.2.1 DigiCert Root CA**

The following, DigitCertRoot, is the root CA certificate used to sign the SBC’s end entity certificate. As mentioned above, your root CA and/or intermediate certificate may differ. This is for example purposes only.

**7.3.3.2.2 Google GTS Root 1 (GTSR1)**

Google presents a certificate to the SBC which is signed by Google GTS Root 1. The TLS certificate and the trust chain from either of the public CAs must be added to the TLS profile of the SBC along with the Google Root certificate.

You can download the GTSR1 trusted root certificate here: https://pki.goog/repo/certs/gtsr1.pem

You can access the GlobalSign trusted root certificate here: GlobalSignRootCA

Please use the following table as a configuration reference: Modify the table according to the certificates in your environment.
At this point, before generating a certificate signing request, or importing any of the Root CA certs, we must **save and activate** the configuration of the SBC.

### 7.3.3.3 Generate Certificate Signing Request

Now that the SBC’s certificate has been configured, create a certificate signing request for the SBC’s end entity only. **This is not required for any of the Root CA or intermidiate certificates that have been created.**
On the certificate record page in the Oracle SBC GUI, select the SBC’s end entity certificate that was created above, and click the “generate” tab at the top:

Copy/paste the text that gets printed on the screen as shown above and upload to your CA server for signature. Also note, at this point, another save and activate is required before you can import the certificates to each certificate record created above.

Once you have received the signed certificate back from your signing authority, we can now import all certificates to the SBC configuration.

7.3.3.4 Import Certificates to SBC

Now that the certificate signing request has been completed – import the signed certificate to the SBC.

Please note – all certificates including root and intermediate certificates are required to be imported to the SBC. Once all certificates have been imported, issue a third save/activate from the WebGUI to complete the configuration of certificates on the Oracle SBC.
• After pasting in the text box, select Import at the bottom, then save and activate your configuration.

Repeat these steps to import all the root and intermediate CA certificates into the SBC:

7.3.4 TLS Profile

TLS profile configuration on the SBC allows for specific certificates to be assigned.

GUI Path: security/tls-profile

ACLI Path: config t → security → tls-profile

• Click Add, use the example below to configure
Next, we'll move to securing media between the SBC and SIP Link.

7.3.5 Media Security

This section outlines how to configure support for media security between the OCSBC and Google Voice SIP Link.

7.3.5.1 SDES-Profile

This is the first element to be configured for media security, where the algorithm and the crypto's to be used are configured.

The Oracle SBC and Google Voice supports the following crypto's to secure media:

- AEAD_AES_256_GCM
- AES_256_CM_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32

In the SBC’s GUI, on the bottom left, you will need to enable the switch “Show All” to access the media security configuration elements.
GUI Path: security/media-security/sdes-profile

ACLI Path: config t→security→media-security→sdes-profile

- Click Add, and use the example below to configure

![Configuration Interface](image)

The screenshot above contains all supported crypto’s for the Oracle SBC and Google Voice. This is only an example. It is not a requirement for all four to be added to the crypto list. You can choose all or any to best support your environment.

- Select OK at the bottom

### 7.3.5.2 Media Security Policy

Media-sec-policy instructs the SBC how to handle the SDP received/sent under a realm (RTP, SRTP or any) and, if SRTP needs to be used, the sdes-profile that needs to be used

In this example, we are configuring two media security policies. One to secure and decrypt media toward Sip Link, the other for non-secure media facing PSTN.

GUI Path: security/media-security/media-sec-policy

ACLI Path: config t→security→media-security→media-sec-policy

- Click Add, use the examples below to configure
• Select OK at the bottom of each when finished

This finishes the security configuration portion of the application note. We’ll now move on to configuring media and transcoding.
7.4 Transcoding Configuration

Transcoding is the ability to convert between media streams that are based upon disparate codecs. The OCSBC supports IP-to-IP transcoding for SIP sessions and can connect two voice streams that use different coding algorithms with one another.

7.4.1 Codec Policies

Codec policies are sets of rules that specify the manipulations to be performed on SDP offers allowing the Oracle SBC the ability to add, strip, and reorder codecs for SIP sessions.

While transcoding media codecs is optional, as Google supports both commonly used codecs PCMU and PCMA, it may be required in some environments if the supported codecs on each side differ. In the example below, we will configure codec policies to use the OPUS codec for Google Voice, and PCMU for PSTN.

GUI Path: media-manager/codec-policy

ACLI Path: config t → media-manager → codec-policy

Here is an example config of a codec policy for the SBC to use the OPUS codec toward Google Voice SIP Link.

Since some SIP Trunks may have issues with the codecs being offered by Google Voice, you can create another codec policy to remove unwanted or unsupported codecs from the request/responses to your Sip Trunk provider.
7.5 Media Configuration

This section will guide you through the configuration of media manager, realms, and steering pools, all of which are required for the SBC to handle signaling and media flows toward Google and PSTN.

7.5.1 Media Manager

To configure media functionality on the SBC, you must first enabled the global media manager

GUI Path: media-manager/media-manager

ACLI Path: config t→media-manager→media-manager-config

- Select OK at the bottom

This concludes the section of the application note on how to configure the Oracle SBC to trancode media. Next, we’ll move on to the media configuration.
Click OK at the bottom

### 7.5.2 Realm Config

Realms are a logical distinction representing routes (or groups of routes) reachable by the Oracle® Session Border Controller and what kinds of resources and special functions apply to those routes. Realms are used as a basis for determining ingress and egress associations to network interfaces.

GUI Path: media-manager/realm-config

ACLI Path: config t→media-manager→realm-config

- Click Add and use the following table as a configuration example for the realms. The following parameters are all required unless mentioned as optional below.

<table>
<thead>
<tr>
<th>Config Parameter</th>
<th>GoogleVoice Realm</th>
<th>PSTN Realm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>GoogleVoice</td>
<td>SipTrunk</td>
</tr>
<tr>
<td>Network Interface</td>
<td>S1p0:0</td>
<td>S0p0:0</td>
</tr>
<tr>
<td>Mm in realm</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Media Sec policy</td>
<td>GoogleMediaSecurity</td>
<td>PSTNNonSecure</td>
</tr>
<tr>
<td>Teams-FQDN</td>
<td>solutionslab.cgbuburlington.com</td>
<td></td>
</tr>
<tr>
<td>Teams-fqdn-in-uri</td>
<td>☑</td>
<td></td>
</tr>
<tr>
<td>Codec policy</td>
<td>GoogleVoiceCodecPolicy</td>
<td>SipTrunkCodecs</td>
</tr>
<tr>
<td>Access-control-trust-level</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
</tbody>
</table>

Also notice the realm configuration is where we assign some of the elements configured earlier in this document. IE…
- Network Interface
- Media Security Policy
- Codec Policy (optional on the PSTN Realm)

Steering pools define sets of ports that are used for steering media flows through the OCSBC. These selected ports are used to modify the SDP to cause receiving session agents to direct their media toward this system.

We configure one steering pool for PSTN. The other facing Google Voice SIP Link.

GUI Path: media-manager/steering-pool

ACL! Path: config t→media-manager→steering-pool

- Click Add, and use the below examples to configure
Select OK at the bottom

We will now work through configuring what is needed for the SBC to handle SIP signaling.

7.6 **Sip Configuration**

This section outlines the configuration parameters required for processing, modifying, and securing sip signaling traffic.

7.6.1 **Sip-Config**

To enable sip related objects on the Oracle SBC, you must first configure the global Sip Config element:

GUI Path: session-router/sip-config

ACL Path: config t→session-router→sip-config

There are only two recommended changes/additions to the global Sip Config.

- Set the home realm ID parameter to GoogleVoice Realm, and add the following hidden option:
  - **Max-udp-length=0**: Setting this option to zero (0) forces sipd to send fragmented UDP packets. Using this option, you override the default value of the maximum UDP datagram size (1500 bytes; sipd requires the use of SIP/TCP at 1300 bytes).
Select OK at the bottom

### 7.6.2 Sip Manipulation

Variances among SIP networks, like incompatible vendor deployments or disparate SIP services, can degrade SIP services or disrupt SIP operations. To resolve these variances, Oracle deploys Header Manipulation Rules (HMR), giving network administrators the ability to control SIP traffic by manipulating SIP messages.

We utilize this feature to present calls to Google Voice SIP Link from the SBC. The SBC would require alterations to the SIP signaling it natively created. The following are manipulations required on the SBC for to present signaling to SIP Link.

This sip manipulation changes the following for both Sip Invites and SIP Options.

- the host and port of the Request URI and TO header to the value specified by Google
- Adds a new SIP header that contains the secret key obtained when creating a SIP trunk in the Google Voice admin portal
The sip manipulation below is easily added to the Oracle SBC configuration via the GUI, but for ease of viewing, we have provided the output from ACLI.
7.6.3 Session Timer Profile

The use of session timers is a requirement when integrating the Oracle SBC with Google Voice Sip Link. Google requires the SBC to be the refresher on calls to and from SIP Link and only UPDATE messages are supported. The below session-timer-config satisfies these requirements.

GUI Path: session-router/session-timer-profile

ACLI Path: config t→session-router→session-timer-profile

Note: to see the session-timer-profile in SBC GUI, you must toggle Show All at the bottom

Click add, and use the example below to configure a session timer profile:

- Select OK at the bottom
7.6.4 Sip Interface

The SIP interface defines the transport addresses (IP address and port) upon which the Oracle SBC receives and sends SIP messages.

Configure two sip interfaces, one associated with PSTN Realm, and the other for Google Voice SIP Link.

GUI Path: session-router/sip-interface

ACLI Path: config t→session-router→sip-interface

Click Add, and use the table below as an example to configure:

<table>
<thead>
<tr>
<th>Config Parameter</th>
<th>SipTrunk</th>
<th>GoogleVoice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Realm ID</td>
<td>SIPTrunk</td>
<td>GoogleVoice</td>
</tr>
<tr>
<td>OutmanipulationID</td>
<td>SIPTrunk</td>
<td>GoogleOutManip</td>
</tr>
<tr>
<td>Session-timer-profile</td>
<td>googletimer</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sip Port Config Parameter</th>
<th>SipTrunk</th>
<th>GoogleVoice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>10.1.2.4</td>
<td>10.1.3.4</td>
</tr>
<tr>
<td>Port</td>
<td>5060</td>
<td>5061</td>
</tr>
<tr>
<td>Transport protocol</td>
<td>UDP</td>
<td>TLS</td>
</tr>
<tr>
<td>TLS profile</td>
<td>GoogleVoiceTLSProfile</td>
<td></td>
</tr>
<tr>
<td>Allow anonymous</td>
<td>agents-only</td>
<td>agents-only</td>
</tr>
</tbody>
</table>

Notice this is where we assign the TLS profile configured under the Security section of this guide, and the sip manipulation used to authenticate the call through GoogleVoice, and the session timer profile.

- Select OK at the bottom of each when applicable

7.6.5 Session Agents

Session Agents are configuration elements which are trusted agents that can both send and receive traffic from the Oracle SBC with direct access to the trusted data path.

GUI Path: session-router/session-agent

ACLI Path: config t→session-router→session-agent

For this example, we'll configure one session agent for Google Voice SIP Link, and another for PSTN.
Click Add, and use the table below to configure:

<table>
<thead>
<tr>
<th>Config parameter</th>
<th>Google Voice SIP Link</th>
<th>PSTN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>siplink.telephony.goog</td>
<td>10.1.2.10</td>
</tr>
<tr>
<td>Ip-address</td>
<td></td>
<td>10.1.2.10</td>
</tr>
<tr>
<td>Port</td>
<td>5672</td>
<td>5060</td>
</tr>
<tr>
<td>Transport method</td>
<td>StaticTLS</td>
<td>UDP</td>
</tr>
<tr>
<td>Realm ID</td>
<td>GoogleVoice</td>
<td>SIPTrunk</td>
</tr>
<tr>
<td>Ping Method</td>
<td>OPTIONS</td>
<td>OPTIONS</td>
</tr>
<tr>
<td>Ping Interval</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>Ping Response</td>
<td>☑</td>
<td>☑</td>
</tr>
</tbody>
</table>

Select OK at the bottom

**7.7 Routing Configuration**

Now that a majority of the signaling, security and media configuration is in place, we can configure the SBC to route calls from one end of the network to the other. The SBC has multiple routing features that can be utilized, but for the purposes of this example configuration, we'll configure local policies to route calls from Google Voice SIP Link to our Sip trunk, and vice versa...

GUI Path: session-router/local-policy

ACLI Path: config t→session-router→local-policy
After entering values for to and from address and source realm, click Add under policy attribute to configure the next hop destination.

Next, we'll setup routing from our SIP Trunk to SIP Link:
Select OK when applicable on each screen

This concludes the configuration portion of this application note. We'll now move on to verifying the connection between the Oracle SBC and Google Voice SIP Link.
8 Verify Connectivity

8.1 Oracle SBC Options Pings

After you've paired the OCSBC with SIPLink, validate that the SBC can successfully exchange SIP Options with Google Voice SipLink.

While in the Oracle SBC GUI, Utilize the “Widgets” to check for OPTIONS to and from the SBC.

- At the top, click “Wigits”

This brings up the Wigits menu on the left hand side of the screen

GUI Path: Signaling/SIP/Method Options

- Looking at both the Server Recent and Client Recent, verify the counters are showing OPTIONS Requests and 200OK responses.

9 Syntax Requirements for SIP Invite and SIP Options:

Google Voice Sip Link has requirements for the syntax of SIP messages. This section covers high-level requirements to SIP syntax of Invite and Options messages. The information can be used as a first step during troubleshooting when calls don’t go through. From our experience most of the issues are related to the wrong syntax of SIP messages.

9.1 Terminology

- Recommended – not required, but to simplify the troubleshooting, it is recommended to configure as in examples as follow
- Must – strict requirement, the system does not work without the configuration of these parameters

9.2 Requirements for Invite Messages

Picture 1 Example of INVITE and 200 OK
INVITE sip:+17814437243@trunk.sip.voice.google.com:5672;user=phone;transport=tls SIP/2.0
Via: SIP/2.0/TLS 141.146.36.70:5061;branch=z9hG4bKnkabte0040j1680u6ut0.1
Max-Forwards: 22
From: <sip:+19783559868@solutionslab.cgbuburlington.com:5060;user=phone>;tag=11c1edca0a020200
To: <sip:+1781437243@trunk.sip.voice.google.com:5672;user=phone>
Call-ID: 1-11c1edca0a020200.6ff26788@68.68.117.67
CSeq: 2 INVITE
Contact: <sip:+19783559868@solutionslab.cgbuburlington.com:5061;user=phone;transport=tls>
Allow: ACK, BYE, CANCEL, INVITE, OPTIONS, PRACK, REFER
User-Agent: T7100/3.0
Supported: 100rel,timer
Content-Type: application/sdp
Content-Length: 293
Session-Expires: 1800; refresher=uac
Min-SE: 90
X-MS-SBC: Oracle/AP3950/9.0.0p3
X-Google-Pbx-Trunk-Secret-Key: a7e6efa4-60a7-45f7-bdbb-fb428897c0ce

9.2.1 Contact Header-Invite

- Must have the Google Voice Sip Link FQDN in RURI and TO Host
- Must contain the X-Google-Pbx-Trunk-Secret-Key header obtained when creating a SIP trunk in the Google Voice admin portal
- Must contain the SBC’s FQDN in Contact host

9.3 Requirements for OPTIONS Messages

Example of OPTIONS message

OPTIONS sip:trunk.sip.voice.google.com:5672;transport=tls SIP/2.0
Via: SIP/2.0/TLS 141.146.36.70:5061;branch=z9hG4bKvikjce10boa65ukfe2b0
Call-ID: 3caeb5f07a4adbc1f4b1a033059bd860000g201000000g20100@141.146.36.70
To: sip:ping@solutionslab.cgbuburlington.com
Max-Forwards: 70
CSeq: 5 OPTIONS
Contact: <sip:ping@solutionslab.cgbuburlington.com:5061;transport=tls>
Expires: 30
Route: <sip:216.239.36.157:5672;lr>
X-MS-SBC: Oracle/AP3950/9.0.0p3
Content-Length: 0
X-Googled-Pbx-Trunk-Secret-Key: a7e6efa4-60a7-45f7-bdbb-fb428897c0ce

9.3.1 Contact Header-OPTIONS:

- When sending OPTIONS to Sip Link, “Contact” header should have SBC FQDN in URI
- OPTIONS must contain the X-Google-Pbx-Trunk-Secret-Key header obtained when creating a SIP trunk in the Google Voice admin portal
10 Appendix A

10.1 Oracle SBC TDM with Sip Link

Oracle® designed the Time Division Multiplexing (TDM) functionality for companies planning to migrate from TDM to SIP trunks by using a hybrid TDM-SIP infrastructure, rather than adopting VoIP-SIP as their sole means of voice communications. The TDM interface on the Oracle® Enterprise Session Border Controller (E-SBC) provides switchover for egress audio calls, when the primary SIP trunk becomes unavailable. You can use TDM with legacy PBXs and other TDM devices.

- Only the Acme Packet 1100, Acme Packet 3900 and Acme Packet 3950 platforms support TDM, which requires the optional TDM card.
- TDM supports bidirectional calls as well as unidirectional calls.
- TDM operations require you to configure TDM Config and TDM Profile, as well as local policies for inbound and outbound traffic.
- The software upgrade procedure supports the TDM configuration.
- Options for the Acme Packet 1100, Acme Packet 3900 and Acme Packet 3950 platforms include CallingLine Identification Presentation (CLIP) and Connected-Line Identification Presentation (COLP).
- Options for the Acme Packet 1100 platform include the four-port Primary Rate Interface (PRI), the Euro ISDN Basic Rate Interface (BRI), and the Foreign Exchange Office-Foreign Exchange Subscriber (FXO-FXS) card.

10.1.1 Interface Requirements

- PRI—Digium1TE133F single-port or Digium 1TE435BF four-port card.
- BRI—Digium 1B433LF four-port card
- FXS—Digium 1A8B04F eight-port card, green module (ports 1-4)
- FXO—Digium 1A8B04F eight-port card, red module (ports 5-8)

For further information on the setup and configuration of TDM on the Oracle SBC, please refer to the TDM Configuration Guide
11 Appendix B

11.1 Oracle SBC deployed behind NAT

The Support for SBC Behind NAT SPL plug-in changes information in SIP messages to hide the end point located inside the private network.

The specific information that the Support for SBC Behind NAT SPL plug-in changes depends on the direction of the call, for example, from the NAT device to the SBC or from the SBC to the NAT device.

Configure the Support for SBC Behind NAT SPL plug-in for each SIP interface that is connected to a NAT device. One public-private address pair is required for each SIP interface that uses the SPL plug-in, as follows.

- The private IP address must be the same IP as configured on both the SIP Interface and Steering Pool
- The public IP address must be the public IP address of the NAT device

Here is an example configuration with SBC Behind NAT SPL config.

The SPL is applied to the Google side SIP interface.

GUI Path: session-router/sip-interface

ACL Path: config t→session-router→sip-interface

HeaderNatPublicSipIfIp=52.151.236.203,HeaderNatPrivateSipIfIp=10.1.3.4

HeaderNatPublicSipIfIp is the public interface ip

HeaderNatPrivateSipIfIp is the private ip.
You will need to apply these options to every sip interface on the SBC that is connected through a NAT.
12 ACLI Running Configuration

Below is a complete output of the running configuration used to create this application note. This output includes all the configuration elements used in our examples, including some of the optional configuration features outlined throughout this document. Be aware that not all parameters may be applicable to every Oracle SBC setup, so please take this into consideration if planning to copy and paste this output into your SBC.

```
certificate-record
  name          DigiCertRoot
  common-name   DigiCert Global Root CA

certificate-record
  name          DigiCertTLSRSA
  organization  DigiCert Inc
  unit          www.digicert.com
  common-name   DigiCert TLS RSA SHA256 2020 CA1

certificate-record
  name          GTSRootR1
  state         CA
  organization  Google Trust Services LLC
  common-name   GTS Root R1

certificate-record
  name          GlobalSignRoot
  state         CA
  organization  GlobalSign
  common-name   GlobalSign Root

certificate-record
  name          SBCCertificateforGoogleVoice
  state         TX
  locality      Austin
  common-name   solutionslab.cgbuburlington.com
  extended-key-usage-list
    serverAuth
    clientAuth

codec-policy
  name          GoogleVoiceCodecPolicy
  allow-codecs  * PCMU:NO
  add-codecs-on-egress
  order-codecs  PCMA *

codec-policy
  name          SipTrunkCodecs
  allow-codecs  * PCMA:NO
  add-codecs-on-egress
  order-codecs  PCMU
                OPUS PCMU *

filter-config
  name          all
  user          *

http-server
  name          webServerInstance
  http-interface-list
    GUI

ice-profile
  name          ice

local-policy
  from-address  *
  to-address    *
  source-realm  GoogleVoice
```
<table>
<thead>
<tr>
<th>Policy Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>next-hop</td>
<td>10.1.2.10</td>
</tr>
<tr>
<td>realm</td>
<td>SIPTrunk</td>
</tr>
<tr>
<td>action</td>
<td>replace-uri</td>
</tr>
<tr>
<td>from-address</td>
<td>*</td>
</tr>
<tr>
<td>to-address</td>
<td>*</td>
</tr>
<tr>
<td>source-realm</td>
<td>SIPTrunk</td>
</tr>
<tr>
<td>next-hop</td>
<td>siplink.telephony.goog</td>
</tr>
<tr>
<td>realm</td>
<td>GoogleVoice</td>
</tr>
<tr>
<td>action</td>
<td>replace-uri</td>
</tr>
<tr>
<td>from-address</td>
<td>*</td>
</tr>
<tr>
<td>to-address</td>
<td>*</td>
</tr>
<tr>
<td>source-realm</td>
<td>GoogleVoice</td>
</tr>
</tbody>
</table>

**Media Manager**

**Policy Attribute**

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>replace-uri</td>
</tr>
<tr>
<td>from-address</td>
<td>*</td>
</tr>
<tr>
<td>to-address</td>
<td>*</td>
</tr>
<tr>
<td>source-realm</td>
<td>GoogleVoice</td>
</tr>
</tbody>
</table>

**Media Security Policy**

**Policy Attribute**

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>inbound</td>
<td>SDES</td>
</tr>
<tr>
<td>mode</td>
<td>srtp</td>
</tr>
<tr>
<td>protocol</td>
<td>sdes</td>
</tr>
<tr>
<td>outbound</td>
<td>SDES</td>
</tr>
<tr>
<td>mode</td>
<td>srtp</td>
</tr>
<tr>
<td>protocol</td>
<td>sdes</td>
</tr>
</tbody>
</table>

**Network Interface**

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>s0p0</td>
</tr>
<tr>
<td>ip-address</td>
<td>10.1.2.4</td>
</tr>
<tr>
<td>netmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>gateway</td>
<td>10.1.2.1</td>
</tr>
</tbody>
</table>

**Network Interface**

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>s1p0</td>
</tr>
<tr>
<td>ip-address</td>
<td>10.1.3.4</td>
</tr>
<tr>
<td>netmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>gateway</td>
<td>10.1.3.4</td>
</tr>
<tr>
<td>dns-ip-primary</td>
<td>8.8.8.8</td>
</tr>
<tr>
<td>dns-ip-backup1</td>
<td>8.8.4.4</td>
</tr>
<tr>
<td>dns-domain</td>
<td>solutionslab.cgbuburlington.com</td>
</tr>
</tbody>
</table>

**Physical Interface**

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>s0p0</td>
</tr>
<tr>
<td>operation-type</td>
<td>Media</td>
</tr>
</tbody>
</table>

**Physical Interface**

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>s1p0</td>
</tr>
<tr>
<td>operation-type</td>
<td>Media</td>
</tr>
<tr>
<td>port</td>
<td>0</td>
</tr>
<tr>
<td>slot</td>
<td>1</td>
</tr>
</tbody>
</table>

**Realm Config**

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>identifier</td>
<td>GoogleVoice</td>
</tr>
<tr>
<td>network-interfaces</td>
<td>s1p0:0.4</td>
</tr>
<tr>
<td>mm-in-realm</td>
<td>enabled</td>
</tr>
<tr>
<td>media-security-policy</td>
<td>GoogleMediaSecurity</td>
</tr>
<tr>
<td>teams-fqdn</td>
<td>solutionslab.cgbuburlington.com</td>
</tr>
<tr>
<td>teams-fqdn-in-uri</td>
<td>enabled</td>
</tr>
<tr>
<td>access-control-trust-level</td>
<td>high</td>
</tr>
<tr>
<td>codec-policy</td>
<td>GoogleVoiceCodecPolicy</td>
</tr>
</tbody>
</table>
realm-config
identifier SIPTrunk
network-interfaces s0p0:0.4
mm-in-realm enabled
media-sec-policy PSTNNonSecure
access-control-trust-level high
codec-policy SipTrunkCodecs
sdes-profile
name GoogleVoiceSRTP
session-agent
hostname 10.1.2.10
ip-address 10.1.2.10
realm-id SIPTrunk
ping-interval 30
ping-response enabled
session-agent
hostname siplink.telephony.goog
port 5672
transport-method StaticTLS
realm-id GoogleVoice
ping-method OPTIONS
ping-interval 30
ping-send-mode keepalive
ping-response enabled
session-timer-profile
name googletimer
sip-config
home-realm-id GoogleVoice
registrar-domain *
registrar-host *
registrar-port 5060
options inmanip-before-validate
max-udp-length=0
allow-pani-for-trusted-only disabled
add-ue-location-in-pani disabled
npli-upon-register disabled
sip-interface
realm-id GoogleVoice
sip-port
address 10.1.3.4
port 5061
transport-protocol TLS
tls-profile GoogleVoiceTLSProfile
allow-anonymous agents-only
out-manipulationid
session-timer-profile
name googletimer
sip-interface
realm-id SIPTrunk
sip-port
address 10.1.2.4
allow-anonymous agents-only
sip-manipulation
name GoogleOutManip
header-rule
name ReqURIHost
header-name Request-URI
action | manipulate
---|---
msg-type | request
methods | INVITE,OPTIONS

element-rule
  name | ReqURIHost
  type | uri-host
  action | replace
  new-value | "trunk.sip.voice.google.com"

element-rule
  name | ReqURIPort
  type | uri-port
  action | replace
  new-value | $REMOTE_PORT

header-rule
  name | GoogleXHeader
  header-name | X-Googe-Pbx-Trunk-Secret-Key
  action | add
  msg-type | request
  methods | Invite,OPTIONS
  new-value | "a7e6efa4-60a7-45f7-bddb-fb428897c0ce"

header-rule
  name | ToHost
  header-name | TO
  action | manipulate
  msg-type | request
  methods | Invite,Options
  element-rule
    name | tohost
    type | uri-host
    action | replace
    new-value | "trunk.sip.voice.google.com"
  element-rule
    name | toport
    type | uri-port
    action | replace
    new-value | $REMOTE_PORT

steering-pool
  ip-address | 10.1.3.4
  start-port | 20000
  end-port | 20999
  realm-id | GoogleVoice

steering-pool
  ip-address | 10.1.2.4
  start-port | 10000
  end-port | 10999
  realm-id | SIPTrunk

system-config
tls-profile
  name | GoogleVoiceTLSProfile
  end-entity-certificate | SBCCertificateforGoogleVoice
  trusted-ca-certificates | GTSRootR1
  GlobalSignRoot
  mutual-authenticate | enabled