FreePBX-PBXact Trunking Configuration

Overview

This document will guide you through the process of configuring the Session Border Controllers to work with FreePBX or PBXact. There are two major applications - 1) SIP Trunking solutions, 2) Remote Phone solutions. This document describes the configuration of SIP Trunking.

Introduction

For Trunking solutions, SBC to FreePBX - PBXact Configuration Guide provides detailed information about the configuration requirements in the SMB SBC, Vega SBC, Netborder SBC and the Software VM SBC. A typical deployment connects SIP Trunking Service Provider across Internet or other networks into the SBC, where the SBC provides Security, Routing, Interoperability and more, then delivers the SIP Trunk call to the FreePBX - PBXact IP-PBX. Using SIP Protocol the SBC and the FreePBX - PBXact create a Trunk together.

SIP Trunking

Bringing SIP Trunks from SIP Trunking Service Providers into the SBC and then deliver the SIP Trunk calls to the FreePBX - PBXact.

FreePBX - PBXact IP: 192.168.77.112
SBC LAN IP: 192.168.77.124
SBC DMZ IP: 10.10.32.170
SBC Public WAN IP: 104.145.12.182
ITSP FQDN: itsp.sangoma.com

Note: In the following configuration example, this is a DMZ-LAN setup of the SBC, and the FreePBX-PBXact is located on a Private LAN. This is one of many different network topologies that the SBC supports. Not all network topologies will be documented in the document, please consult other Wikis for slight changes in deployment styles of the SBC. Slight changes in configuration from this example to other network topologies are expected.
FreePBX-PBXact Configuration

General Configuration

The FreePBX-PBXact will typically have a Static IP or Fully Qualified Domain Name. In this configuration we are defining the SBC as a Trunk, then assigning a Outgoing Calls and Incoming Calls to/from the SBC.

Trunks

Open the Trunks Module. (Connectivity > Trunks)

Click Add Trunk. Select Add SIP (Chan_sip) Trunk

Note: "SIP (chan_pjsip) Trunk" works as well. But the configuration is not documented here.
Under General complete the following information:

- **Trunk Name**: Any Name - for example SBC-Trunk.124
- **Outbound CallerID**: Defined the default Outbound CallerID.
- **CID Options**: Outbound CallerID options. Allow Any CID will allow CallerID settings in other Modules. Some providers may restrict to only one, when this is the case “Force Trunk CID” should be selected.
- **Maximum Channels**: Optional. Controls the maximum number of outbound channels (simultaneous calls) that can be used on this trunk. ONLY limits outbound calls.
- **Disable Trunk**: No. But at anytime you want to turn off the trunk you can select Yes.

Under SIP Settings complete the following information in the Outgoing Tab

- **Trunk Name**: Enter any name

Under SIP Settings complete the following information in the Outgoing Tab Peer Details

- **host**=192.168.77.124 - This is the IP Address of the SBC Internal LAN interface
- **port**=5060 - This is the Port of the SIP Profile on the SBC Internal LAN Interface
- **type**=peer - We are creating a Peer relationship with the SBC, no Registrations - IP Authentication only
- **disallow**=all - Disallow all codecs
- **allow**=ulaw - Then define the list of codecs to send to the SBC
- **context**=from-pstn - Define the Asterisk Context as from-pstn
- **sendrpid**=yes - Optional. Turn on the use of sendrpid
- **trustrpid**=yes - Optional. Turn on the Asterisk to trust the RPID
- **dtmfmode**=rfc2833 - Use rfc2833 for DTMF
**Note:** When Peer is selected, the FreePBX-PBXact Admin GUI doesn’t report on the state of that peer, so it shows up as Unmonitored in the Server>Connection Status>VoIP Providers.
Click “Submit”

Inbound Routes

Open the Inbound Routes. (Connectivity > Inbound Routes)

Click Add Inbound Route.

Under Single DID Route Settings complete the following information:

- **Description**: Any Description - SBC
- **DID Number**: Enter in the DID (or range) being delivered from the SBC
- **CallerID Number**: This is a filter, to match for the Source CallerID
- **Alert Info**: Optional. Change the Ringer type
- **Set Destination**: Select the Destination to ring when a voice call comes in over this SBC or channel. The destination can be any extension type (your receptionist’s phone, an IVR, Queues, etc.).
Click “Submit”

Outbound Routes

Open the Outbound Routes. (Connectivity > Outbound Routes)

Click Add Outbound Route
When Outbound Route, there are general Route Settings and Dial Patterns.

- **Route Name**: Give it any name
- **Route CID**: Optional. If there is any Outbound CallerID that is specific to this Route
- **Override Extension**: Optional. Yes, if you want the Route CallerID to override the Extension CallerID
- **Route Password**: Optional. Enter a PIN if you want this Outbound Route PIN protected.
- **Trunk Sequence for Matched Routes**: Select the SBC trunk created earlier
Run through the Dial Plan Wizard. Or configure your Dial Plan.
SBC Configuration

General Configuration

The following configuration will focus on the FreePBX-PBXact to SBC requirements. It is only half of the configuration needed for proper operation, as the SIP Trunking Service Provider will also need to be configured, along with the External WAN interface and external SIP Profiles and related configuration. The document will reference the SIP Trunking Service Provider but not show how to configure the provider. There are other Wiki's that document how to configure SIP Trunking with SIP Trunking Service Providers.
FreePBX-PBXact IP: 192.168.77.112
SBC LAN IP: 192.168.77.124
SBC DMZ IP: 10.10.32.170
SBC Public IP: 104.145.12.182
ITSP FQDN: itsp.sangoma.com

**Note:** In the following configuration example, this is a DMZ-LAN setup of the SBC, and the FreePBX-PBXact is located on a Private LAN. This is one of many different network topologies that the SBC supports. Not all network topologies will be documented in the document, please consult other Wikis for slight changes in deployment styles of the SBC. Slight changes in configuration from this example to other network topologies are expected.

### IP Settings | Network

The default IP Address of the SBC is 192.168.168.2 root/sangoma The IP Address needs to be changed and a new admin user created.

Go to Configuration | IP Settings | Network

Press “Add” to add a DMZ IP Address

- **Interface:** Select Eth1
- **Configuration:** Select IPv4 - Static
- **Address:** Enter the DMZ interface IP Address / Mask.

Press Save
Press "Add" to add a LAN IP Address

- **Interface**: Select Eth0
- **Configuration**: Select IPv4 - Static
- **Address**: Enter the LAN interface IP Address / Mask.

Press Save

Once completed you will now have an IP address on eth0 for LAN and eth1 for DMZ.

Press "Edit" to configure the Default Gateway and Hostname
Configure the Network

- **Host Name**: Enter a FQDN
- **Default Gateway Interface**: Select eth1, the default gateway is always the way to the Internet
- **Default IPV4 Gateway**: Enter the IP Address of the Default Gateway
- **Static DNS #1**: Enter the IP Address of the Primary DNS Server
- **Static DNS #2**: Enter the IP Address of the Secondary DNS Server
At this point you can access the SBC from the New LAN IP Address.

**IP Settings | Media Interfaces**

Go to Configuration | IP Settings | Media Interfaces

Click Edit.
Ensure the Transcoding Mode is to Hardware Hidden mode for all Vega SBC and Netborder SBC. Then click Save.

Note: For SMB SBC and Software VM SBC the Transcoding Mode is to Software. The click Save.
Next click Detect Modules. Once you modules are detected click OK to continue.
IP Settings | Access Control Lists

Go to Configuration | IP Settings | Access Control Lists

Access Control Lists are a list of IP Address(es) that can have an Allow or Deny policy. Typical practice is to have a Default Policy to Deny all traffic, then Allow specific Hosts and Subnets. Both local trusted LAN traffic and Internet WAN traffic need to be defined separately.

Default

Local LAN Internal Network ACL

Within the ACL box, click Add.

Give the ACL a name.

Set the Default Policy to Deny. Press Save
Within the ACL Box, press Add

Add the local Subnet, where the FreePBX-PBXact resides. Add any additional networks within the LAN environment.

- **Policy**: Set to Allow
- **IP Address**: Enter the LAN Network Address or IP Address and Mask

Internet WAN External Network ACL

Within the ACL box, click Add.

Give the ACL a name.
Set the Default Policy to Deny. Press Save.

Within the ACL Box, press Add.

Add the local Subnet, where the FreePBX-PBXact resides. Add any additional networks within the LAN environment.

- **Policy**: Set to Allow
- **IP Address**: Here you will need a list of any IP Address(es) used by the SIP Trunk Service Provider - Enter the Network Address or IP Address and Mask

**Signaling | SIP Profile**

Two SIP Profiles are needed. One for the LAN side - for 'Internal' communications with the FreePBX-PBXact, and another for the WAN side - for 'External' communication with the SIP Trunk Service Provider.

Go to Configuration | Signaling | SIP Profiles

A default "internal" SIP Profile will be present. You can Delete it - then Add a new Profile OR Modify it.
Setup an Internal SIP Profile

Click Modify next to the default internal SIP profile.

This SIP Profile is used for assigning the SBC’s LAN IP to a SIP Profile. This is where the FreePBX-PBXact will communicate with the SBC. IP Address, Port, Transport and other interop settings are defined here. Not all SIP Profile settings are required. Here are the highlights:

- **Display Name**: Give the SIP Profile a name. PBXact_Internal
- **User Agent**: This is the name displayed on the User-Agent Header. Does not need changing.
- **SIP IP Address**: Select the LAN IP Address of the SBC
- **Port**: Port 5060 is default.
- **Transport**: Select the Transport you want to use, UDP+TCP is default. Or individually UDP or TCP.
- **SIP Trace**: Optional. Enable. It is useful when you have a problem.
- **Strict Security**: Optional. Enable when strict security is required, here all traffic from non whitelisted and/or registered IP addresses, on that SIP Profile, will be blocked. This means that with this feature enabled you need to assign ACLs or register endpoints in order to be able to make calls through the profile. Enabling in SIP Trunking solutions, allows the SBC to lock down to specific SIP Peers.
- **Authenticate Calls**: Select Disable.
- **ACL for Inbound Calls**: From the available list, select and use the Arrow key to move over the Local_LAN_Internal_ACL list created earlier.
Setup an External SIP Profile

Click Add to create a new SIP profile for the External SIP communications.

This SIP Profile is used for assigning the SBC’s DMZ IP to a SIP Profile - the WAN IP address of the Firewall will be NAT’d through to the DMZ IP of the SBC. This is where the SIP Trunk Service Provider will communicate with the SBC. IP Address. Port. Transport and other interop settings are defined here. Not all SIP Profile settings are required, here are the highlights:

- **Display Name**: Give the SIP Profile a name. ServiceProvider_EXTERNAL
- **User Agent**: This is the name displayed on the User-Agent Header. Does not need changing.
- **SIP IP Address**: Select the LAN IP Address of the SBC
- **External SIP IP Address**: Enter in the WAN IP Address of the Firewall/Router. This setting is only used when the SBC is behind a Firewall/Router.
- **Port**: Port 5060 is default.
- **Transport**: Select the Transport you want to use, UDP+TCP is default. Or individually UDP or TCP.
- **RTP IP address**: If different than the SIP IP Address, select the IP here.
- **External RTP IP address**: Enter in the WAN IP Address of the Firewall/Router. This setting is only used when the SBC is behind a Firewall/Router.
- **SIP Trace**: Optional. Enable. It is useful when you have a problem.
- **Strict Security**: Optional. Enable when strict security is required, here all traffic from non whitelisted and/or registered IP addresses, on that SIP Profile, will be blocked. This means that with this feature enabled you need to assign ACLs or register endpoints in order to be able to make calls through the profile. Enabling in SIP Trunking solutions, allows the SBC to lock down to specific SIP Peers.
- **Authenticate Calls**: Select Disable.
- **ACL for Inbound Calls**: From the Available list, select and use the Arrow key to move over the Internet_WAN_External_ACL list created earlier.
Press Save
Two SIP Trunks Profiles are needed. One for the FreePBX-PBXact and another for the SIP Trunk Service Provider. SIP Trunks Profile is where the Peer attributes are configured.

**Setup the FreePBX-PBXact in a SIP Trunk Profile**

Go to Configuration -> Signaling -> SIP Trunks

Click Add

The following parameters define the location and behavior specific to the FreePBX-PBXact:

- **Display Name**: Give any Name. PBXact
- **Domain**: Enter the IP Address or FQDN of the FreePBX-PBXact
- **User Name**: Not required.
- **Authentication User Name**: Not Required.
- **Password**: Not Required.
- **From User**: Not Required.
- **From Domain**: Not Required.
- **Transparent CallerID**: Select Enabled.
- **Transport**: Select UDP
- **OPTIONS Ping Frequency**: Optional: Enter 60 for 60 Seconds
- **OPTIONS Max Ping**: Optional: Enter 5 for 5 tries
- **OPTIONS Min Ping**: Optional: Enter 5 for 5 tries
- **SIP Profile**: Select the "PBXact_Internal" SIP Profile created earlier
Setup the SIP Trunking Service Provider in a SIP Trunk Profile

Go to Configuration -> Signaling -> SIP Trunks

Click Add

The following parameters define the location and behavior specific to the SIP Trunking Service Provider:

- **Display Name**: Give any Name. ITSP
- **Domain**: Enter the IP Address or FQDN of the SIP Trunking Service Provider. itsp.sangoma.com
- **User Name**: Specific to Service Provider requirements.
- **Authentication User Name**: Specific to Service Provider requirements.
- **Password**: Specific to Service Provider requirements.
- **From User**: Specific to Service Provider requirements.
- **From Domain**: Specific to Service Provider requirements.
- **Transparent CallerID**: Select Enabled.
- **Transport**: Select UDP
- **OPTIONS Ping Frequency**: Optional: Enter 60 for 60 Seconds
- **OPTIONS Max Ping**: Optional: Enter 5 for 5 tries
- **OPTIONS Min Ping**: Optional: Enter 5 for 5 tries
- **SIP Profile**: Select the "ServiceProvider_External" SIP Profile created earlier

The image shows a configuration page for a trunk with fields for Domain, User Name, Authentication User Name, Password, From User, From Domain, Transparent CallerID (Enabled), Proxy Address, Outbound Proxy Address, Transport (UDP), Contact Host, Contact Parameters, OPTIONS Ping Frequency, OPTIONS Max Ping, OPTIONS Min Ping, Allow Port in Gateway Identity (Disable), SIP Profile (ServiceProvider_External), Inbound Media Profile, and Outbound Media Profile. The page also has options for Registration, Routing & Header Manipulation, and Call Admission Control.

Press Save
The SBC will require two Call Route Dial Plans. One Dial Plan to send calls from the FreePBX-PBXact to the SIP Trunking Service Provider, and another Dial Plan to send calls from the SIP Trunking Service Provider to the FreePBX-PBXact.

Go to Configuration | Routing | Call Routing

**Outbound Calling**

Click the Add button in the Basic Call Routing section to add a new routing plan.

Give the Dial Plan a name. Outbound_Calling - then click Add.

**Basic Call Routing Setup**

- **Display Name**: Give any name: Outbound_Calling
- **Description**: Give any description. Outbound_Calling
- **Trace Call**: Enable is helpful when problems occur.
- **Default Response**: Select 404
Once in the new routing plan click Add to add a new rule.

This very next Dial Plan Rule is a redundant Dial Plan, when ACL is in place. But this shows some extra flexibility in the Dial Plan to check various attributes of a call that are not related to the SIP Protocol. This example is a Check IP Address. If the IP Address does not match, the SBC will respond with a 403 Forbidden. And then not process any remaining rules in the Dial Plan.

- **Description**: Enter a description. Check IP
- **Rank**: Enter 10. Dial Plan rules start at 1 and search up, starting at 10 lets you add more Rules below in the future.
- **Matching**: Select ALL. This will make the Rule look for all of the Conditions
- **Stop Policy**: Select “Stop on Failure”. If the condition is not matched, then no more Rules will be processed.
- **Condition**: Select “SIP Call Information” - this has a selection of parameters specific to call information
- **Name**: Select “Remote Network IP”. This is the Source IP Address.
- **Expression**: Enter the IP Address of the FreePBX-PBXact. 192.168.77.112
- **Actions to perform if condition matches**: **Action**: Nothing entered here, we are only looking for the Unmatch.
- **Actions to perform if condition doesn’t match**: **Action**: Select “Respond”. **Code**: Select “403 Forbidden”
Press Save

Once "Check IP" in saved, click Add to insert another Dial Plan Rule.

This next Dial Plan Rule is most important, as it 'bridges' the Outbound Call from the FreePBX-PBXact to the SIP Trunking Service Provider - SIP Trunk Profile that was defined earlier.

- **Description**: Enter a description. Bridge to Service Provider
- **Rank**: Enter 20. Using 20 lets you add more Rules in between 10 and 20 in the future.
- **Matching**: Select ALL. This will make the Rule look for all of the Conditions
- **Stop Policy**: Select "Stop on Success". If the condition is matched, then no more Rules will be processed.
- **Condition**: Select "Standard Information" - this has a selection of most popular parameters
- **Name**: Select "Destination Address". This is the Dialed Number in the R-URI address.
- **Expression**: Enter (\.*). Open Parenthesis Dot Asterisk Close Parenthesis - a Regular Expression to define to match any number dialed for the ITSP destination. **Destination**: Enter $1 This mean use first variable within the first set of Parenthesis defined in the expression.
- **Actions to perform if condition doesn’t match**: **Action**: Not Selected.

Press Save

Your Call Routing should now look like this for Outbound Calls to the SIP Trunking Service Provider.
Inbound Calling

Click the Add button in the Basic Call Routing section to add a new routing plan.

Give the Dial Plan a name. Inbound_Calling - then click Add.

Basic Call Routing Setup

- **Display Name**: Give any name: Inbound_Calling
**Description**: Give any description. *Inbound_Calling*

**Trace Call**: Enable is helpful when problems occur.

**Default Response**: Select 404

Once in the new routing plan click Add to add a new rule.

This very next Dial Plan Rule is a redundant Dial Plan, when ACL is in place. But this shows some extra flexibility in the Dial Plan to check various attributes of a call that are not related to the SIP Protocol. This example is a Check IP Address. If the IP Address does not match, the SBC will respond with a 403 Forbidden. And then not process any remaining rules in the Dial Plan.

- **Description**: Enter a description. Check IP
- **Rank**: Enter 10. Dial Plan rules start at 1 and search up, starting at 10 lets you add more Rules below in the future.
- **Matching**: Select ALL. This will make the Rule look for all of the Conditions
- **Stop Policy**: Select "Stop on Failure". If the condition is not matched, then no more Rules will be processed.
- **Condition**: Select "SIP Call Information" - this has a selection of parameters specific to call information
- **Name**: Select "Remote Network IP". This is the Source IP Address
- **Expression**: Enter the IP Address of the SIP Trunking Service Provider. 4.8.16.32
- **Actions to perform if condition matches**: Action: Nothing entered here, we are only looking for the Unmatch.
- **Actions to perform if condition doesn’t match**: Action: Select "Respond.  Code: Select "403 Forbidden"
Press Save

Once “Check IP” in saved, click Add to insert another Dial Plan Rule.

This next Dial Plan Rule is most important, as it ‘bridges’ the Inbound Call from the SIP Trunking Service Provider to the FreePBX-PBXact - SIP Trunk Profile that was defined earlier.

- **Description**: Enter a description. Bridge to PBXact
- **Rank**: Enter 20. Using 20 lets you add more Rules in between 10 and 20 in the future.
- **Matching**: Select ALL. This will make the Rule look for all of the Conditions
- **Stop Policy**: Select “Stop on Success”. If the condition is matched, then no more Rules will be processed.
- **Condition**: Select “Standard Information” - this has a selection of most popular parameters
- **Name**: Select “Destination Address”. This is the Dialed Number in the R-URI address.
- **Expression**: Enter (.*). Open Parenthesis Dot Asterisk Close Parenthesis - a Regular Expression to define to match any number dialed
- **Actions to perform if condition matches**: **Action**: Bridge to Trunk. Trunk: Select “PBXact” - this is the SIP Trunk Profile defined earlier for the PBXact destination. **Destination**: Enter $1 This mean use first variable within the first set of Parenthesis defined in the expression.
- **Actions to perform if condition doesn’t match**: **Action**: Not Selected.

Press Save

Your Call Routing should now look like this for Inbound Calls to the FreePBX-PBXact.
Two SIP Profiles were created earlier. We need to go back and assign the appropriate Call Routing Dial Plan to the correct SIP Profile. The Inbound_Calling Dial Plan is assigned to the ServiceProvider_External SIP Profile, as calls from the SIP Trunking Service Provider will be going Inbound_Calls to bridge to the FreePBX-PBXact. And the other direction, the FreePBX-PBXact will call the PBXact_Internal SIP Profile which will go to the Outbound_Calling Dial Plan, which will bridge the call to the SIP Trunking Service Provider.

Now that both routing plans are made go to Configuration | Signaling | SIP Profiles and modify the PBXact_Internal SIP profile.

Under Session Routing change the Routing Plan to Outbound_Calling. Then click Save to continue.
Modify the ServiceProvider_External SIP profile.

Under Session Routing change the Routing Plan to Inbound_Calling. Then click Save to continue.

Apply Configuration

You are Done. Time to save your efforts.
Finalizing the Installation

Starting the SBC application and other useful features on the SBC.

Go to Overview -> Dashboard -> Control Panel and Start the following services.
Enable all IDS rules by going to Configuration -> Security -> Intrusion Detection and ensuring all are checked. Once done click Update to apply the changes.
Next go to System -> Server -> Web and change the Network Interface from All interfaces to only the internal network interface.

In this example eth1 is the internal network interface. Once done click Save.
Next go to System -> Server -> Web and change the Network Interface from All interfaces to only the internal network interface. Now both the web server and SSH will only be available on your internal network.

Since the configuration is now completed get a backup. Go to System -> Management -> Backup-Restore and click Backup.

Name the file accordingly and click backup to download a copy. Ensure you keep this safe somewhere and always take a new backup after each change made to the SBC.