

Sangoma SBC Interoperability with Sipxcom High Availability

- Introduction
- Step 1 - Plan Your SBC Configuration
- Step 2 - Set Port Forward and Outbound NAT on Pfsense
- Step 3 - Sipxcom Configuration to Support SBC
 - Create an Unmanaged Gateway
 - Assign the SBC Unmanaged Gateway to Dial Plan
 - NAT Traversal Settings
 - Change Firewall Settings for SAA/BLA
- Step 4 - Configuring the Sangoma SBC
 - Pointing the SBC DNS Addresses at Sipxcom HA Servers
 - Create G.711 Media Profile for the ITSP
 - Build the SIP Profiles
 - Build the SIP Trunks
- Step 6 - Build the SBC Dialplans
- Step 7 - Test Your SBC Configuration

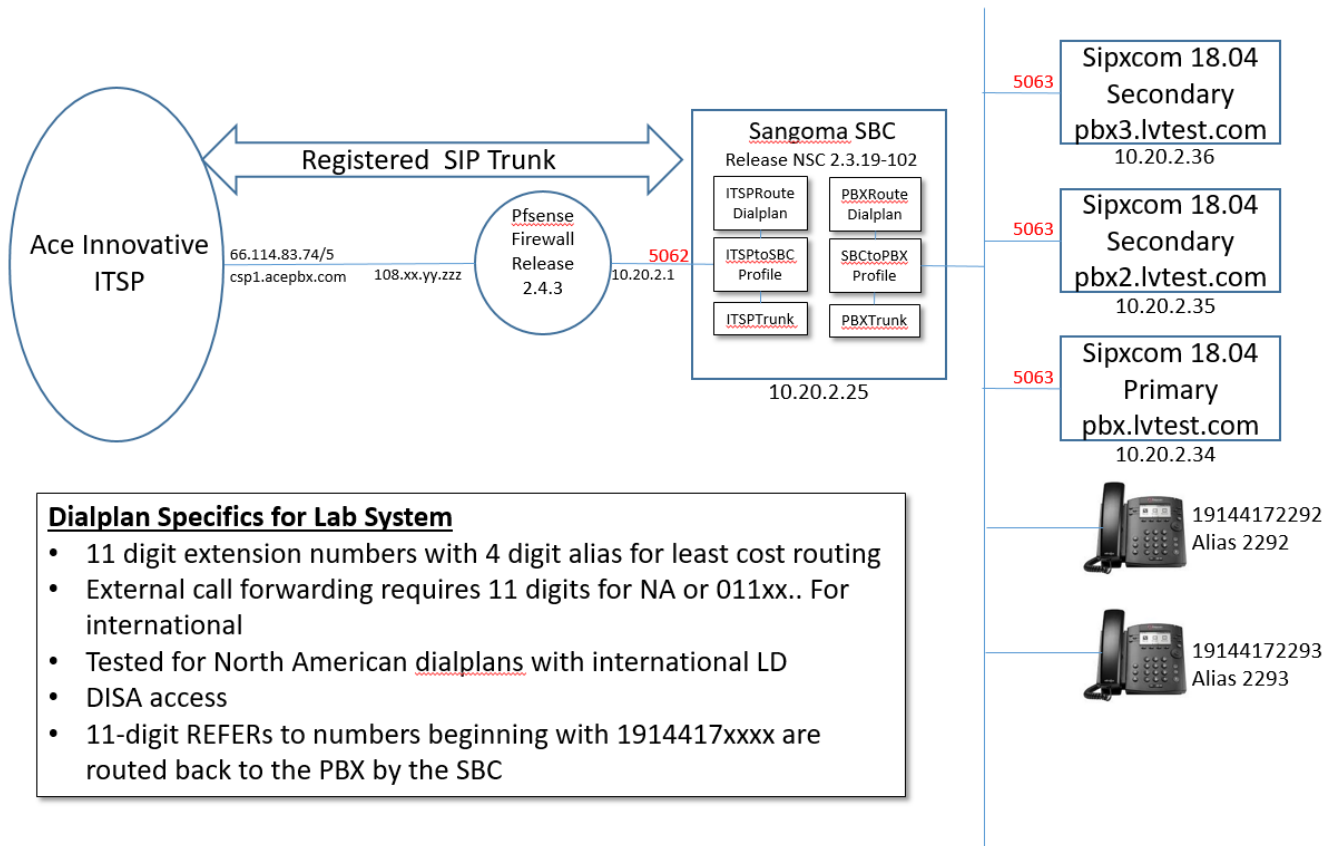
Introduction

This document provides an overview for configuring the Sangoma Session Border Controller (SBC) with the Sipxcom High Availability (HA) configuration. The following telephony features have been lab-tested with this configuration:

- Consultative and blind transfer of incoming and outgoing external calls from Polycom phones
- Call forwarding via the web portal
- DISA access - only works when the primary server is available
- Incoming and outgoing calls using a shared line with bridged line appearance (BLA) - only works when the primary server is available.

This document assumes working knowledge of Sipxcom HA, the Sangoma SBC, SIP, basic Freeswitch concepts, and regex expressions.

Step 1 - Plan Your SBC Configuration



Per the above reference diagram, the Sangoma SBC sits behind Pfsense in a private network. Given that the Pfsense firewall protects the private network from malicious public Internet traffic, the SBC firewall was turned off. The Sangoma SBC has several high availability and clustering settings - those settings were not tested or validated with the Siprocom HA configuration.

Siprocom 18.04 and Sangoma NSC 2.3.19-102 releases were used in the lab testing. The Siprocom HA cluster has 3 servers - one primary and two secondary servers; it also uses the lptest.com SIP realm for failover. The Siprocom default DNS settings were used during testing where phone registrations are spread evenly across all three servers in the HA cluster. The user extensions for the lab phones are 11-digit extensions (North American Dialplan) with 4 digit aliases that facilitates least-cost PSTN routing. For transfer testing, the Mongo Registrar was queried to ascertain successful call transfers through the SBC occurred to internal phones registered to different HA servers.

For incoming external calls that use DISA or calls that are transferred back out to the PSTN via a Polycom phone (e.g. cell phone), the SBC dialplan facing the Internet Telephony Service provider (ITSP) must distinguish between a call transfer going out to the PSTN versus a call being transferred to another user extension within Siprocom (remember that the Siprocom user extensions are 11 digits). When the SIP REFER is received as a result of a DISA call or call transfer, Siprocom issues a REFER back out to the SBC. The SBC looks at the 11-digit number in the REFER-TO header - if the number begins with 1914417xxxx then the subsequent INVITE is sent back to the PBX.

In the SBC, the **ITSPtoSBC** SIP Profile is first defined for incoming external calls that assigns the 5062 port number that the profile will act upon. This profile is then linked to the **ITSPTrunk** SIP trunk which defines the far endpoint of the trunk, and optionally, whether the SIP trunk is registered along with registration credentials. Finally the **ITSPRoute** dialplan is defined and mapped to the profile that determines how the incoming call will be routed. There is the **SBCtoPBX** SIP profile, **SBCtoPBX** trunk, and **PBXRoute** dialplan with port 5063 that processes incoming calls from Siprocom.

This wiki page provides good guidance on building dialplans using the Sangoma SBC <https://wiki.sangoma.com/display/SBC/SIP+Refer+Handling>. It is important to understand how the SBC processes REFERs. If an incoming external call arrives at the SBC, is routed to Siprocom, and is then call-transferred, the REFER coming back from Siprocom is processed by the **ITSPtoSBC** SIP profile and corresponding ITSPRoute dialplan, as that is where the original call is anchored. Likewise if a Siprocom user placed an external call to the ITSP and the call is transferred, the incoming REFER to the SBC is processed by the **SBCtoPBX** Profile and **PBXRoute** dialplan as that is where the original call is anchored.

Step 2 - Set Port Forward and Outbound NAT on Pfsense

The Internet Telephony Service Provider used for Siprocom HA and Sangoma SBC interoperability testing has its servers in the 66.114.83.0/24 class C sub-network range. For incoming traffic from the ITSP, Pfsense must be configured to allow all incoming traffic from this subnetwork destined for the public IP address of **108.xx.yy.zzz** with the port ranges of **5062-65535** to be forwarded to the SBC in the private network with the IP address of **10.20.2.25**. It should be noted that the Pfsense WAN interface supports multiple public IP addresses and by leveraging the Pfsense Virtual IP address feature, the **108.xx.yy.zzz** address has been reserved for SBC traffic.

For outbound traffic from the SBC to the ITSP, Pfsense must be programmed to NAT outgoing traffic from **10.20.2.25** to the public IP address reserved for SBC traffic - this is done via a mapping entry on the Pfsense **Firewall->NAT->Outbound** menu.

The screenshot shows the Pfsense configuration interface for Firewall > NAT > Port Forward. The 'Port Forward' tab is selected and highlighted with a red box. Below it, a table lists a rule for forwarding traffic from the WAN interface (TCP/UDP) from source address 66.114.83.0/24 to destination address 108.xx.yy.zzz on ports 5062-65535, NATting it to 10.20.2.25 on ports 5062-65535. The description is 'Sangoma SBC'.

Below the Port Forward section, the 'Firewall / NAT / Outbound' menu is shown, with the 'Outbound' tab selected and highlighted with a red box. Under 'Outbound NAT Mode', the 'Manual Outbound NAT rule generation' option is selected with a radio button. The other options are 'Automatic outbound NAT rule generation (IPsec passthrough included)', 'Hybrid Outbound NAT rule generation (Automatic Outbound NAT + rules below)', and 'Disable Outbound NAT rule generation (No Outbound NAT rules)'. A 'Save' button is visible below the mode selection.

At the bottom, the 'Mappings' section shows a mapping entry for the WAN interface, source 10.20.2.25/32, with destination and destination port set to asterisks, NAT address 108.xx.yy.zzz, and a checked 'Static Port' box. The description is 'LAN to WAN'.

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input checked="" type="checkbox"/> WAN	TCP/UDP	66.114.83.0/24	*	108.xx.yy.zzz	5062 - 65535	10.20.2.25	5062 - 65535	Sangoma SBC	

Mode	Description
<input type="radio"/> Automatic outbound NAT rule generation. (IPsec passthrough included)	
<input type="radio"/> Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)	
<input checked="" type="radio"/> Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)	
<input type="radio"/> Disable Outbound NAT rule generation. (No Outbound NAT rules)	

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input checked="" type="checkbox"/> WAN	10.20.2.25/32	*	*	*	108.xx.yy.zzz	*	<input checked="" type="checkbox"/>	LAN to WAN	

Step 3 - Sipxcom Configuration to Support SBC

The key configuration changes to support the SBC are in the following areas:

- Creation of unmanaged gateway to the SBC
- Assign the unmanaged gateway to a dial plan
- Change NAT Traversal settings
- Changing BLA/SAA Firewall setting to test incoming external calls on BLA-enabled lines

Create an Unmanaged Gateway

Create an unmanaged gateway to the SBC at 10.20.2.25 using TCP transport and port 5063.

GATEWAY DETAILS

Configuration	Gateway : <u>SBC / Unmanaged gateway</u>	
Caller ID	Enabled	<input checked="" type="checkbox"/>
Dial Plan	Name	<input type="text" value="SBC"/>
	Description	<input type="text"/>
	Address	<input type="text" value="10.20.2.25"/> <small>For a PSTN gateway: IP address of the gateway (example: 10.1.1 without NAT. For an ITSP SIP Trunk: External IP address or fully defined in the field below. For a Direct SIP Trunk: To interconnect</small>
	Port	<input type="text" value="5063"/>
	Transport protocol	<input type="text" value="TCP"/> <small>Set to force the SIP transport protocol. If set to auto the transport</small>
	Location	<input type="text" value="-- all --"/> <small>Defines the Location of this Gateway.</small>
	Shared	<input checked="" type="checkbox"/> <small>If checked this gateway can be used by any user in any location, preferred gateway, but the gateway can also be used by other use</small>
	<input type="button" value="OK"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Assign the SBC Unmanaged Gateway to Dial Plan

Assign the SBC unmanaged gateway to the appropriate dial plans such as the **Long Distance** Dialplan.

Enabled

Name
 Description

Permission
 Caller permission needed for this rule to succeed.

PSTN prefix
 Prefix dialed by the caller and dropped before the call is sent to the gateway.

Long distance prefix
 Prefix dialed by the caller and sent to the gateway.

Area codes

External number length
 Number of digits in the resulting number sent to the gateway. The PSTN prefix and the long distance prefix are not counted.

Schedule

Gateways

<input type="checkbox"/>	Name	Enabled	Address	Location	Model
<input type="checkbox"/>	SBC	Enabled	10.20.2.25	All	Unmanaged gateway

Move Up Move Down Remove

OK Apply Cancel

NAT Traversal Settings

In the System -> Nat Traversal Settings menus, disable the **Enable NAT Traversal** and **Server Behind NAT** options. Also change **Address Type** to **Specify IP address** and provision the Public IP address with the IP address of the SipXcom primary voice server. Repeat this step for each of the secondary servers (10.20.2.35 and 10.20.2.36).

EDIT NAT TRAVERSAL

NAT Traversal | pbx.louisavoice-lmabs.dyndns.org

NAT

Address type

Public IP address

SIP Port

TLS SIP Port

OK Apply Cancel

NAT TRAVERSAL

Settings

Server Config

Enable NAT Traversal

Server behind NAT

Media Relay Temperament

Reject Stray Packets

log_level

xml-rpc-port

Apply

Change Firewall Settings for SAA/BLA

By default, the firewall settings to allow 5170 traffic from the phones to Sipxcom are disabled - this is used by bridge line appearance (BLA) lines on Sipxcom. Go to the **System->Firewall** menu and change the **SAA/BLA TCP** and **UDP** firewall settings from **CLUSTER** to **PUBLIC**. This change allows BLA to work on shared lines using Polycom phones in order to perform interoperability testing with the Sangoma SBC.

SAA/BLA TCP	10.20.2.34 : 5170	<input type="text" value="PUBLIC"/>	<input type="checkbox"/>
SAA/BLA UDP	10.20.2.34 : 5170	<input type="text" value="PUBLIC"/>	<input type="checkbox"/>

Step 4 - Configuring the Sangoma SBC

The Vmware version of the Sangoma SBC was used for this interoperability testing work and assumes the SBC has already been installed and operational. The changes to support Sipxcom HA include:

- Pointing the SBC DNS addresses at Sipxcom HA servers
- Creating G.711 media profiles for the ITSP
- Build the SIP Profiles
- Build the SIP Trunks
- Build the Call Routing Dialplans

Pointing the SBC DNS Addresses at Sipxcom HA Servers

Go to the **Configuration->IP Settings->Network** menu on the SBC and validate the IP Address assigned to the **Eth0** interface and **default gateway** from the installation. Point the SBC DNS addresses to the three Sipxcom HA servers.

The screenshot shows the configuration page for the Network settings. At the top, there is a warning message: "The IP Firewall service is stopped." Below this, the Network configuration is displayed with the following values:

- Host Name: lvsbc.com
- Default Gateway Interface: (empty)
- Default IPv4 Gateway: 10.20.2.1
- Default IPv6 Gateway: (empty)
- Static DNS #1: 10.20.2.34
- Static DNS #2: 10.20.2.35
- Static DNS #3: 10.20.2.36

Below the network settings, there are tabs for "Interface", "IP", "Static Route", and "Source Policy Routing". The "Interface" tab is selected, showing a table of interfaces:

Interface	Type	IP Address
lo	IPv4 - Static	127.0.0.1/8
lo	IPv6 - Static	::1/128
eth0	IPv4 - Static	10.20.2.25/24

Create G.711 Media Profile for the ITSP

The ITSP used for interoperability testing with the PSTN only supports G.711 codecs. Go into the **Configuration->Media->Media Profiles** menu of the SBC and create an ITSP profile that only supports PCMU and PCMA codecs. The **aceprofile** will be assigned to the ITSP and PBX SIP profiles of the SBC.

Configuration / Media / Media Profiles

The IP Firewall service is stopped.

Profile

10 Showing 1 to 2 of 2 entries

Name	Codec List
default	PCMU 20ms, PT=0 PCMA 20ms, PT=8 G.729 20ms, PT=18 iLBC 15.20Kbps 20ms, PT=98 G.722 20ms, PT=9
aceprofile	PCMU 20ms, PT=0 PCMA 20ms, PT=8 PCMU 30ms, PT=0 PCMA 30ms, PT=8

Add

Build the SIP Profiles

From the planning diagram in step 1, there are two SIP Profiles required:

- **ITSPtoSBC** using Port **5062** - this SIP profile manages the traffic between the SBC and the ITSP
- **SBCtoPBX** using Port **5063** - this SIP profile manages the traffic between the SBC and Sipscom

These two profiles are first created so that they can then be linked to the SIP trunks. The SIP profiles will then be updated after the corresponding Call Routing dialplans have been created.

Configuration / Signaling / SIP Profiles

The IP Firewall service is stopped.

Profile

10 Showing 1 to 2 of 2 entries

Profile Name	User Agent	Routing Plan	SIP IP Address	Port	Transport
ITSPtoSBC	NetBorder Session Controller	ITSPRoute	eth0 - 10.20.2.25	5062	UDP+TCP
SBCtoPBX	NetBorder Session Controller	PBXRoute	eth0 - 10.20.2.25	5063	UDP+TCP

Add

Create the **ITSPtoSBC** profile using the default SBC profile settings except for the following fields:

- External SIP and RTP IP address fields are provisioned to **108.xx.yy.zzz** this is the public IP address assigned by PfSense for the SBC. This is required as the SBC is sitting behind the firewall and not directly connected to the Internet. The SBC will replace the source IP address for outgoing SIP packets to the ITSP with the public **108.xx.yy.zzz** IP address assigned to the SBC.
- Port number is **5062** (see architecture diagram in step 1 again)
- Transport is **UDP+TCP**
- Inbound and outbound media profiles are set to **aceprofile** (previous step) as the ITSP only supports G.711 codecs
- Validate that the Inbound **bypass Media option** is disabled - this means that all media goes through the SBC and simplifies troubleshooting.
- Enable the **Accept Blind Authentication** option



The IP Firewall service is stopped.

Profile - ITSPtoSBC

General

Display Name ITSPtoSBC

User Agent NetBorder Session Controller

SIP IP Address eth0 - 10.20.2.25

External SIP IP Address 108.xx.yy.zzz

Port 5062

Transport UDP+TCP

Outbound Proxy

RTP IP address (SIP Profile)

External RTP IP address 108.xx.yy.zzz

Inbound Bypass Media Disable

Inbound Media Profile aceprofile

Outbound Media Profile aceprofile

SIP Trace Enable

SIP Capture Disable

Strict Security Disable

Interoperability

100 Reliability Disable

3PCC Disable

3pcc Relay Alerting Disable

Request SIP DNS Caching Disable

Ignore 183 without SDP Disable

Allow Private Wire Info Enable

Create the **SBCtoPBX** profile using the default SBC profile settings except for the following fields:

- Port number is **5063** (see architecture diagram in step 1 again)
- Transport is **UDP+TCP**
- Inbound and outbound media profiles are set to **aceprofile** (previous step) as the ITSP only supports G.711 codecs
- Validate that the Inbound **bypass Media option** is disabled - this means that all media goes through the SBC and simplifies troubleshooting
- Enable the **Accept Blind Authentication** option



The IP Firewall service is stopped.

Profile - SBCToPBX

General

Display Name	SBCtoPBX
User Agent	NetBorder Session Controller
SIP IP Address	eth0 - 10.20.2.25
External SIP IP Address	
Port	5063
Transport	UDP+TCP
Outbound Proxy	
RTP IP address	(SIP Profile)
External RTP IP address	
Inbound Bypass Media	Disable
Inbound Media Profile	aceprofile
Outbound Media Profile	aceprofile
SIP Trace	Enable
SIP Capture	Disable
Strict Security	Disable

Interoperability

100 Reliability	Disable
3PCC	Disable
3pcc Relay Alerting	Disable
Request SIP DNS Caching	Disable
Ignore 183 without SDP	Disable
Allow Private Wire Info	Enable

Build the SIP Trunks

From the planning diagram in Step 1, there are two SIP trunks to be configured on the SBC:

- **ITSPTTrunk** - points to the ITSP nodes defined at csp1.acepbx.com. The Ace Innovative ITSP actually presents two SRV records when queried by DNS - the primary server at **66.114.83.74** and the secondary server at **66.114.83.75**.
- **PBXTrunk** - points to the Sipxcom HA cluster with the SIP realm of lvttest.com. The Sangoma SBC is able to process DNS SRV records.



The IP Firewall service is stopped.

Trunk		
Name	Domain	SIP Profile
PBXTrunk	lvtest.com	SBCToPBX
ITSPTrunk	csp1.acepbx.com	ITSPtoSBC

The SBC must be stopped prior to building the SIP Trunks and assigning the SIP Profile to the Trunk. The following configuration parameters are defined on the **ITSPTrunk** SIP Trunk:

- Domain name is the FQDN of the ITSP - in this case **csp1.acepbx.com**
- This is a registered SIP trunk, so User Name and Password credentials for the trunk are provided
- Map SIP Profile to the **ITSPtoSBC** profile
- Enable Registration on the SIP Trunk

Step 6 - Build the SBC Dialplans

Building the Call Routing Dialplans is an iterative process - for the lab system defined in step 1, two dialplans are defined:

- **ITSPRoute** - this dialplan will handle incoming calls from the ITSP to the SBC. Incoming INVITES and REFERS from the ITSP are processed by this call routing dialplan.
- **PBXRoute** - this dialplan will handle incoming calls from the PBX to the SBC. Incoming INVITES and REFERS from the PBX are processed by this call routing dialplan.

Go to the **Configuration->Call Routing** menu and build these two dialplans.

Configuration / Routing / Call Routing

The IP Firewall service is stopped.

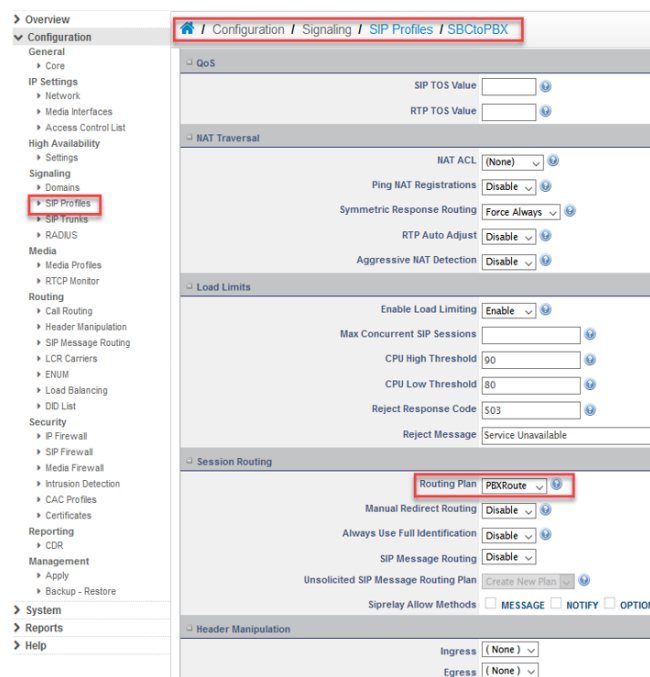
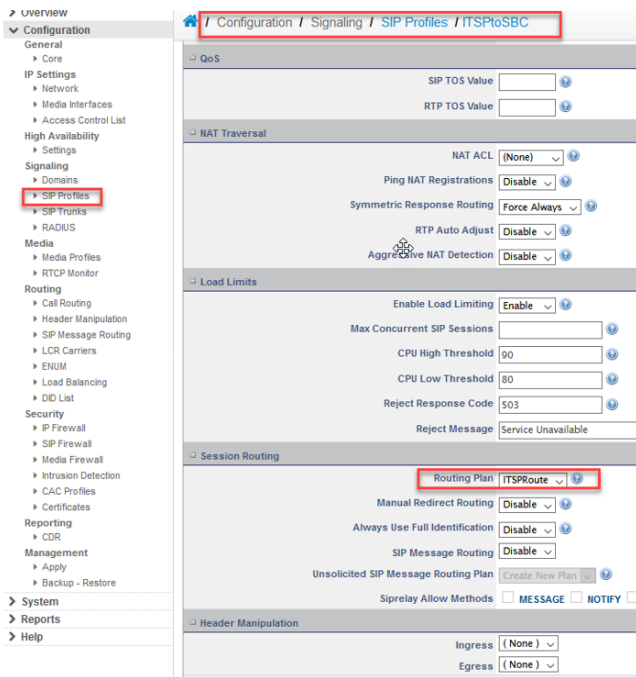
Basic Call Routing			
Display Name	Description	Trace Call	Default Response
ITSPRoute	Dialplan for calls from ITSP	Enable	404
PBXRoute	Dialplan for calls from PBX	Enable	404
<input type="button" value="Add"/>			

Advanced Call Routing	
<i>No Advanced Call Routing</i>	
<input type="button" value="Add"/>	

Once the call routing dialplans have been defined, they need to be mapped to the correct SIP profile as follows:

- In the **Configuration->Signaling->SIP Profile** menu, edit the **ITSPtoSBC** SIP profile, and in the Session Routing section, map the **ITSPRoute** dialplan to the profile, and save.
- Edit the **SBCToPBX** SIP profile, and in the Session Routing section, map the **PBXRoute** dialplan to the profile, and save.

Once these configurations are applied to the SBC, the rules for each dialplan can be defined and tested.



Before working through the details of the call routing dialplan rules, some simple call flow examples will provide clarity on the dialplan logic. Let's start with an incoming external call to 914-417-2292 (see architecture diagram in step 1), which is a Polycom phone behind Siprocom. Because the call originated from the ITSP, the SBC processes the call using the **ITSPtoSBC** SIP Profile and corresponding **ITSPRoute** dialplan. The 19144172292 user answers the call and transfers the call to 2293 (which is an alias of 19144172293). To complete the transfer, Siprocom issues a SIP REFER back to the SBC. Because the call being transferred originated from the ITSP, the **ITSPRoute** dialplan will process the REFER even though the REFER came from Siprocom. The REFER from Siprocom will have a **Refer-To:** header that begins with **sip:2293@lvttest.com;user=phone**; the SBC dialplan regex must parse this header, look at the **2293** destination address, and instruct the SBC to send an INVITE to **2293@lvttest.com** back to Siprocom in order to complete the call transfer.

Let's use the same call flow but instead of transferring the call to 2293, the 19144172292 user transfers the call to the full 11-digit extension **19144172293**. The REFER from Siprocom will have a **Refer-To:** header that begins with **sip:19144172293@lvttest.com;user=phone**; - the **ITSPRoute** dialplan must have a rule defined that sends the **SIP INVITE** for **19144172293** back to Siprocom and not to the ITSP.

The Siprocom **19144172292** user places an external call to the ITSP - because the call originated from Siprocom, the **SBCToPBX** SIP Profile and corresponding **PBXRoute** dialplan on the SBC processes the call. When the **19144172292** user transfers the call to **19144172293** or its **2293** alias, the **REFER** that is sent to the SBC is handled by the **SBCToPBX** SIP profile and **PBXRoute** dialplan as the original outgoing call is anchored to this path. The **PBXRoute** dialplan must have dialplan rules that correctly routes calls for **1914417xxx** and 4-digit aliases back to Siprocom.

Final example - Siprocom user **19144172292** has a call forwarding rule that forwards incoming calls to **16465551212** after 1 second. An external ITSP 9145551212 caller places a call to 19144172292. Siprocom after 1 second sends an INVITE back to the SBC with a Request-line URI of **INVITE sip:16465551212@10.20.2.25:5063** but the SIP TO: header has the original **sip:9144172292@lvttest.com** URI. Almost all SIP INVITES have Request-line URIs that are identical to the TO: header URI. However when call forwards are initiated by Siprocom due to a call forwarding rule, the telephone numbers in the R-URI header and To: headers are different - the SBC must account for this when a call forwarding rule is applied to a Siprocom user.

```

> Internet Protocol Version 4, Src: 10.20.2.34, Dst: 10.20.2.25
> Transmission Control Protocol, Src Port: 5060, Dst Port: 41098, Seq: 935, Ack: 1284, Len: 2133
> Session Initiation Protocol (INVITE)
  > Request-Line: INVITE sip:16465551212@10.20.2.25:5063;callgroup=19144172292;sipx-noroute=Voicemail;transport=tcp;sipxcs-lineid=1 SIP/2.0
  > Message Header
    > Record-Route: <sip:10.20.2.34:5060;lr;sipXecs-CallDest=AL%2CAL%2CLD;sipXecs-rs=%2Aauth%7E.%2Afrom%7ESz3S2FyeVvQdFp0UQ%60%60%2150055ea97e505caacf5acb90b50b0ea5>
    > Via: SIP/2.0/TCP 10.20.2.34;branch=z9hG4bK-XX-3630AVNdLbZ6ajjG0T6YwInAKA;sipxcs-lineid=1
    > Via: SIP/2.0/TCP 10.20.2.34;branch=z9hG4bK-XX-362c`hXLDzSS`P`hWa3JxFiaYg-MXWp_`vXjNRmPqBj78IvZQ
    > Via: SIP/2.0/TCP 10.20.2.34;branch=z9hG4bK-XX-3624_aIZQhZ0`B6GbxzYp_xTdQ~J3nB_urz01e_5vGkgwsyWg
    > Via: SIP/2.0/TCP 10.20.2.34;branch=z9hG4bK-XX-3615C01b03oyO`D6YcFJWsvKMQ~EiU3RtRORVHSuEGAk1RsAA
    > Via: SIP/2.0/TCP 10.20.2.25:5063;branch=z9hG4bK4cFpXvypQ78Dg
    Max-Forwards: 14
    > From: " 9145551212 " <sip:9144172275@10.20.2.25>;tag=K87KaryUjtZtQ
    > To: <sip:9144172292@lvttest.com>
    Call-Id: fccefdee-f17f-1236-328e-005056946706
    > Cseq: 124541577 INVITE
    > Contact: <sip:NetBorder_Session_Controller@10.20.2.25:5063;transport=tcp;gw=PBXTrunk;x-sipX-nonat>
    User-Agent: NetBorder_Session_Controller
    Allow: INVITE, ACK, BYE, CANCEL, OPTIONS, MESSAGE, UPDATE, INFO, REGISTER, REFER, NOTIFY, PUBLISH, SUBSCRIBE
    Supported: pw-info-package, path, replaces
    Allow-Events: talk, hold, presence, dialog, line-seize, call-info, sla, include-session-description, presence.winfo, message-summary, refer
    Content-Type: application/sdp
    Content-Disposition: session
    Content-Length: 283

```

The Call Routing dialplan rules for both the **ITSPRoute** and **PBXRoute** dialplans are identical except for dialplan rule 9. In the following dialplan rule illustration, rule number 4 is a best practice and checks that SIP signaling comes from either the Spxcom high availability servers or the ITSP - if not, processing stops with a SIP 405 error message and further dialplan processing terminates.

Dialplan rules 5 through 8 handle REFER processing - let's start with dialplan rule 5. In the dialplan assumptions documented in the architecture diagram in step 1, Spxcom users are 11 digits and follow the North American telephone numbering plan. The numbering plan also assumes that **9144170000-9144179999** are assigned to Spxcom users. If an external caller dialed 19144172292, the Spxcom user answered the call, and then transferred the call to 19144172294, the REFER back to the SBC from Spxcom would have **Refer-To** header of **19144172294@lvtest.com**. The regex in dialplan rule 5 checks whether the cialing number is 11 digits and begins with 1914417 - if it does, the regex populates the \$1 variable with the called number and then sends the subsequent INVITE to Spxcom.

Dialplan rules 6 and 7 go together and are a workaround to regex processing on the Sangoma SBC where some statements with multiple brackets fails to populate the \$1 variable. In dialplan rule number 6, a check is made on whether the incoming packet is a SIP REFER packet - if so, the **REFER-TO** variable is populated with the contents of the \$1 variable containing the called telephone number. The regex in dialplan 7 checks whether the called number in the **Refer-To**: header is an 11 digit long-distance number or international call beginning with 011 - if so, then the subsequent INVITE is sent to the ITSP using the **REFER-TO** variable.

Dialplan rule 8 covers the case of a REFER containing any other called number - e.g. user **19144172292** transfers the call to alias **2294**. The regex in this dialplan takes the the called number populated in the \$1 variable and sends the INVITE to Spxcom.

Note that dialplan processing stops for REFER dialplan rules 5, 7, and 8 if the matching condition was successful.

Further guidance on how to bridge REFERs with SIP Trunks is found here <https://wiki.freepbx.org/display/SBC/SIP+Refer+Handling>. This document provides useful regex examples for the Sangoma SBC <https://wiki.freepbx.org/display/SBC/Regular+Expressions+in+the+Dial+Plan>.

The final dialplan rule 9 forwards an incoming call from the ITSP to the Spxcom PBX, and vice-versa. In the **ITSPRoute** dialplan rule (illustrated), the called number is custom bridged to the **PBXTrunk** which connects to Spxcom. For an incoming call from Spxcom to the ITSP, the **PBXRoute** dialplan would custom bridge the call to the **ITSPTrunk** in rule 9. Note that in the conditional query for the SIP INVITE packet, the request-line URI is queried and populated in the \$1 variable by the underlying regex..

Rule	
#	Description
4	IF NOT MATCH Condition(Any,Variable[network_addr] = 10.20.2.34,Variable[network_addr] = 10.20.2.34,Variable[network_addr] = 10.20.2.34,Variable[network_addr] = 66.114.83.74,Variable[network_addr] = 66.114.83.75) THEN Respond[405 Method Not Allowed]=Invalid ITSP or PBX Address AND Stop On Failure
5	IF MATCH Condition(All,Variable[sip_refer_to] = ^.*sip:(1914417[0-9]{4})@(.*)\$) Custom[bridge]=sip/trunk/PBXTrunk/\$1 AND Stop On Success
6	IF MATCH Condition(All,Variable[sip_refer_to] = ^.*sip:[\+]?(\+)?@(.*)\$) Set Variable[REFER-TO]=\$1 AND Continue
7	IF MATCH Condition(Any,Variable[sip_refer_to] = ^.*sip:(1[2-9][0-9]{9})011.*@(.*)\$) Unset Variable[sip_refer_to] Export Variable[sip_force_full_to]=sip:\${REFER-TO} Custom[bridge]=sip/trunk/ITSPTrunk/\${REFER-TO} AND Stop On Success
8	IF MATCH Condition(All,Variable[sip_refer_to] = ^.*sip:[\+]?(\+)?@(.*)\$) Unset Variable[sip_refer_to] Export Variable[sip_force_full_to]=sip:\$1 Custom[bridge]=sip/trunk/PBXTrunk/\$1 AND Stop On Success
9	IF MATCH Condition(All,SIP Header Information[R-URI] = (.*)@(.*)\$) Custom[bridge]=sip/trunk/PBXTrunk/\$1 AND Continue

Step 7 - Test Your SBC Configuration

Session Border controllers, and dialplan configurations (regex plans in particular) are detailed - a simple misspelling or an errant forward-slash in a trunk bridging operation can be problematic to trouble-shoot. In putting together this document, the following tests were performed to validate the configuration:

- Incoming ITSP call into Spxcom - long-distance and international
- Outgoing external call - long-distance and international
- Incoming ITSP call into Spxcom, answer call on one Polycom phone, and then test call transfer consultative and blind:
 - To another Polycom phone within Spxcom using a 11-digit Spxcom user number
 - To another Polycom phone within Spxcom using a Spxcom alias
 - To an external North American number from the Polycom phone
 - To an external international number from the Polycom phone
 - To an external North American number using the external phone connected through the ITSP
 - To an external international number using the external phone connected through the ITSP
- Outgoing Spxcom to an ITSP, call is answered, and then test call transfer consultative and blind:
 - To another Polycom phone within Spxcom using a 11-digit Spxcom user number
 - To another Polycom phone within Spxcom using a Spxcom alias
 - To an external North American number from the Polycom Phone
 - To an external international number from the Polycom phone
 - To an external North American number using the external phone connected through the ITSP
 - To an external international number using the external phone connected through the ITSP
- Incoming internal and external calls into Spxcom user, then call forward (from portal) to North American and International numbers
- Incoming internal and external calls into DISA, which then places call to internal, North America, and International numbers

- Incoming external calls into Sipxcom user enabled with bridged line appearance, answer call and check whether other BLA lines are flashing red, place call on hold, and pick up call on another phone.

The primary Sipxcom server in the high availability cluster was powered off, and the above tests were repeated. The tests using DISA (Authorization codes) and bridged line appearance failed as these features are only available when the primary server is operational - all other calls were successfully completed.