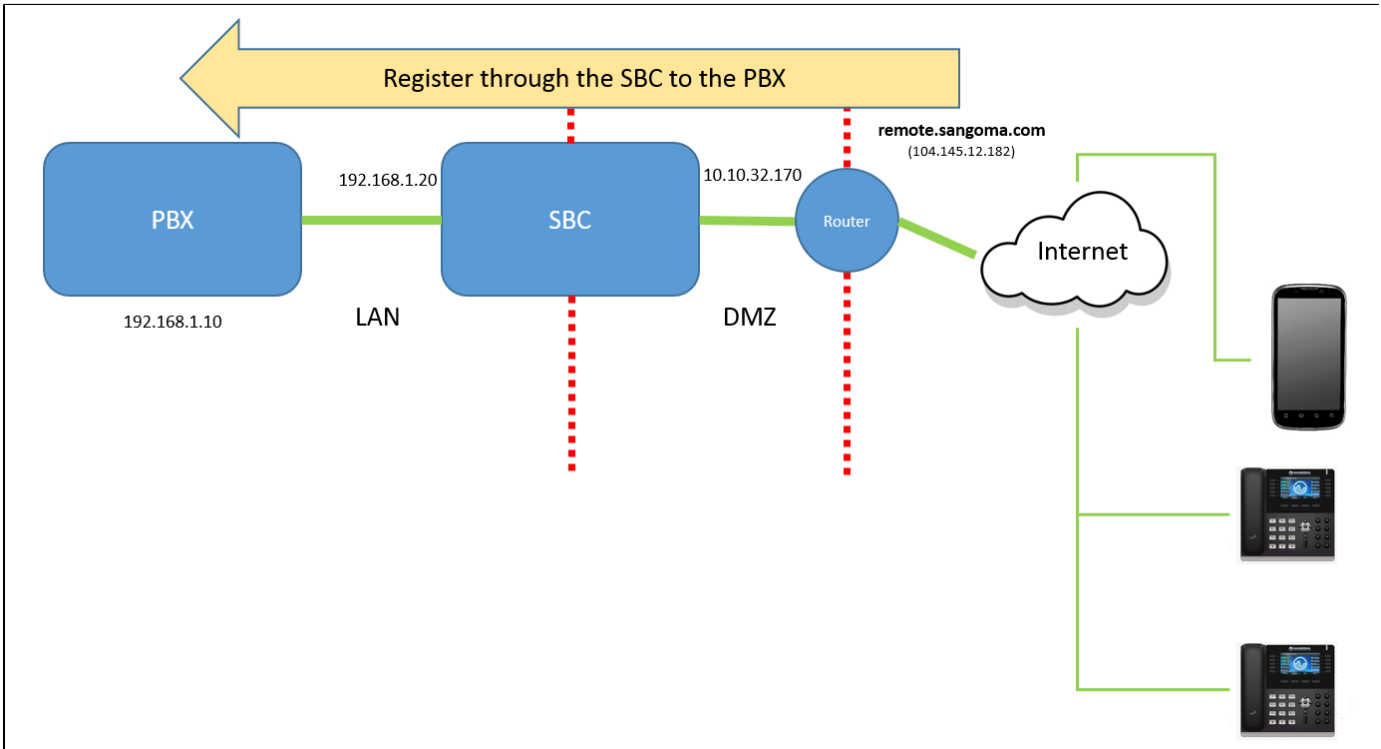


Remote Phone Support

Overview

The Remote Phone Support use case allows remote phones - employees working from home, or using a SIP client on their mobile phone - to register through the SBC to the PBX so the users can use their normal office extensions as if they were sitting in the office. The SBC in this scenario is providing far-end NAT traversal for the remote phones as well as enhanced security for the corporate network without the need to set up VPN tunnels. Note that the SBC can be used at the same time to perform SIP trunking interconnection but for simplicity the example below concentrates on remote access.



PBX IP: 192.168.1.10
SBC LAN IP: 192.168.1.20
SBC DMZ IP: 10.10.32.170
SBC Public IP: 104.145.12.182
SBC FQDN: remote.sangoma.com

1) Network Setup

1. Go to Configuration->IP Settings->Network and then edit eth0 and assign the DMZ IP address. Next click the Add button to add an IP address to eth1. Enter in the IP address along with the subnet mask as shown below.

IP - Ip_68	
Interface	eth1
Configuration	IPv4 - Static
Hostname	
Use automatic DNS servers	Enable
Persistent DHCP client	Enable
Address	192.168.1.20 / 24
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

2. Once completed you will now have an IP address on eth0 and eth1.

[Home](#) / [Configuration](#) / [IP Settings](#) / [Network](#)

Network

	Host Name	LyncSBC
Default Gateway Interface	Default IPv4 Gateway	10.10.32.1
Default IPv6 Gateway	Static DNS #1	10.10.0.4
	Static DNS #2	8.8.8.8

[Edit](#)

[Interface](#) | [IP](#) | [Static Route](#)

10 ▼ Showing 1 to 6 of 6 entries

Interface	Type	IP Address	Hostname
eth0	IPv4 - Static	10.10.32.170/24	
lo	IPv4 - Static	127.0.0.1/8	
lo	IPv6 - Static	::1/128	
sngdsp0	IPv4 - Static	192.0.2.1/24	
sngdsp0	IPv6 - Static	2001:db8::1:1/120	
eth1	IPv4 - Static	192.168.1.20/24	

[Add](#)

[System](#)
[Reports](#)
[Help](#)

3. Next go to Configuration -> IP Settings -> Media Interfaces and click Edit.

[Home](#) / [Configuration](#) / [IP Settings](#) / [Media Interfaces](#)

[Firmware Update](#)
[Detect Modules](#)

Media Server

Transcoding Mode	Hardware Hidden
First UDP port	10000

[Edit](#)

Module

10 ▼ Showing 1 to 1 of 1 entries

	MAC	Version	IP address	UDP Ports
✓	00-0c-90-1e-cc-ce	02.01.08-B2-PR	192.0.2.2 - 192.0.2.3	10000 - 13999

[Edit](#)

4. Change the Transcoding Mode to Hardware Hidden mode. Then click Save.

Home / Configuration / IP Settings / Media Interfaces

Media Server

General

Transcoding Mode: Hardware Hidden

First UDP port: 10000

Last UDP port: 20000

VLAN Identifier:

Network IPv4

Base IPv4 address: 10.10.0.1

Base External IPv4 address:

IPv4 Network Mask: 255.255.255.0

Default IPv4 Gateway: 10.10.0.100

Network IPv6

Base IPv6 address: 2001:db8::99:2

Base External IPv6 address:

IPv6 prefix: 120

Default IPv6 Gateway: 2001:db8::99:1

VQE

Acoustic Echo Cancellation: Disable

Adaptive Noise Reduction: Disable

Automatic Level Control (RX): Disable Target: -21

Automatic Level Control (TX): Disable Target: -21

Jitter

Jitter Mode: Adaptive

Jitter Initial Delay: 40

Jitter Max PDV: 100

Jitter Minimal Delay: 20

Save Cancel

5. Next click Detect Modules. Once you modules are detected click OK to continue.

Home / Configuration / IP Settings / Media Interfaces

Firmware Update Detect Modules

Media Server

Transcoding Mode: Hardware Hidden

First UDP port: 10000

Edit

2) SIP Profile Configuration

1. Go to Configuration -> Signaling -> SIP Profiles and click Modify next to the default internal SIP profile.

Configuration / Signaling / SIP Profiles

Profile

Showing 1 to 1 of 1 entries

Name	User Agent	SIP IP Address	Port	Transport	
internal	NetBorder Session Controller	eth1 - 192.168.1.20	5060	UDP+TCP	Modify Delete

Add

2. Ensure the SIP IP Address is configured set to the LAN IP address. Then enable the SIP Trace option.

Configuration / Signaling / SIP Profiles / internal

Profile - Internal

General

User Agent: NetBorder Session Controller

SIP IP Address: eth1 - 192.168.1.20

External SIP IP Address:

Port: 5060

Transport: UDP+TCP

Outbound Proxy:

RTP IP address: (SIP Profile)

External RTP IP address:

Inbound Bypass Media: Disable

Inbound Media Profile: default

Outbound Media Profile: default

SIP Trace: Enable

3. Next scroll down to the Authentication section and disable Authenticate Calls. This option is only required when remote phones are registering to a local SIP account on the SBC. Once done save the internal profile.

Authentication

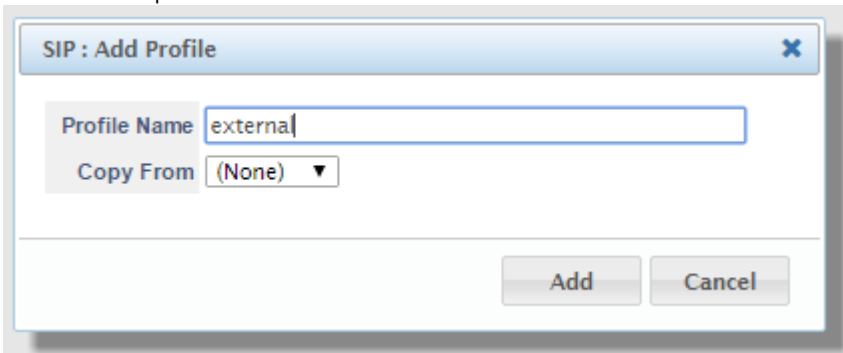
Authenticate Calls: Disable

Accept Blind Authentication: Disable

Authenticate Requests: Disable

Network Validation ACL: Disable

- Next add a new profile called external.



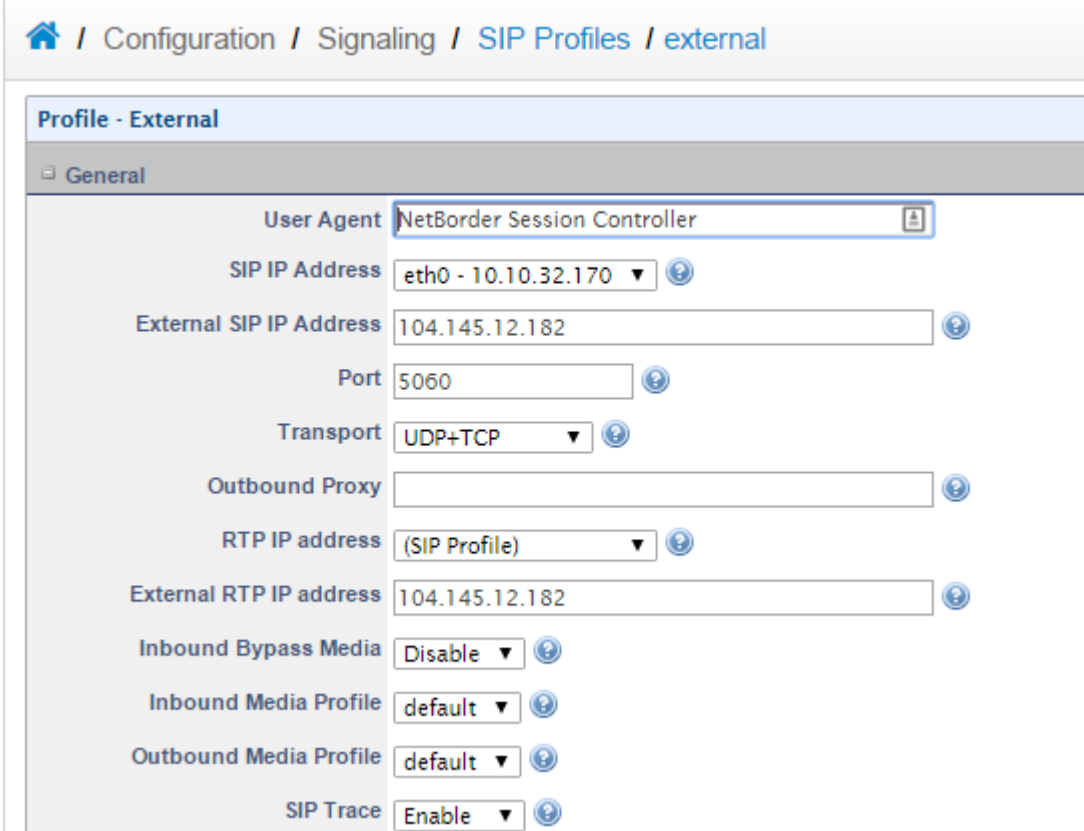
SIP : Add Profile

Profile Name: externa|

Copy From: (None) ▼

Add Cancel

- In the External SIP profile set the External SIP IP Address and External RTP IP Address to the public IP. As well enable the SIP Trace option.



Configuration / Signaling / SIP Profiles / external

Profile - External

General

User Agent: NetBorder Session Controller

SIP IP Address: eth0 - 10.10.32.170

External SIP IP Address: 104.145.12.182

Port: 5060

Transport: UDP+TCP

Outbound Proxy:

RTP IP address: (SIP Profile)

External RTP IP address: 104.145.12.182

Inbound Bypass Media: Disable

Inbound Media Profile: default

Outbound Media Profile: default

SIP Trace: Enable

- Next disable authenticate calls as we did with the internal SIP profile. Since the SIP profile is facing the internet we need to enable the Network Validation ACL. This will ensure only calls from Registered phones will be processed.

Authentication

Authenticate Calls: ⓘ

Accept Blind Authentication: ⓘ

Authenticate Requests: ⓘ

Network Validation ACL: ⓘ

ACL for Inbound Calls

Used: [] Available: []

ACL for Registration

Used: [] Available: []

- Then since remote phones behind NAT will be registering through the PBX enable all the NAT options as shown below.

NAT Traversal

NAT ACL: ⓘ

Ping NAT Registrations: ⓘ

Symmetric Response Routing: ⓘ

RTP Auto Adjust: ⓘ

Aggressive NAT Detection: ⓘ

3) Adding SIP Trunk to PBX

- Go to Configuration -> Signaling -> SIP Trunks and click Add. Name the SIP trunk PBX.

SIP : Add Trunk [X]

New Trunk:

2. Set the Domain to be the IP address of the PBX. Enable OPTIONS by setting the Frequency and Max/Min Pings as shown below. Once done click Save.

[Home](#) / [Configuration](#) / [Signaling](#) / [SIP Trunks](#) / [PBX](#)

Trunk - PBX

General

Domain	<input type="text" value="192.168.1.10"/>
User Name	<input type="text"/>
Authentication User Name	<input type="text"/>
Password	<input type="password"/>
From User	<input type="text"/>
From Domain	<input type="text"/>
Transparent CallerID	<input type="text" value="Enabled"/>
Proxy Address	<input type="text"/>
Outbound Proxy Address	<input type="text"/>
Transport	<input type="text" value="UDP"/>
Contact Host	<input type="text"/>
Contact Parameters	<input type="text"/>
OPTIONS Ping Frequency	<input type="text" value="30"/>
OPTIONS Max Ping	<input type="text" value="5"/>
OPTIONS Min Ping	<input type="text" value="1"/>
SIP Profile	<input type="text" value="internal"/>
Inbound Media Profile	<input type="text" value="(SIP Profile Default)"/>
Outbound Media Profile	<input type="text" value="(SIP Profile Default)"/>

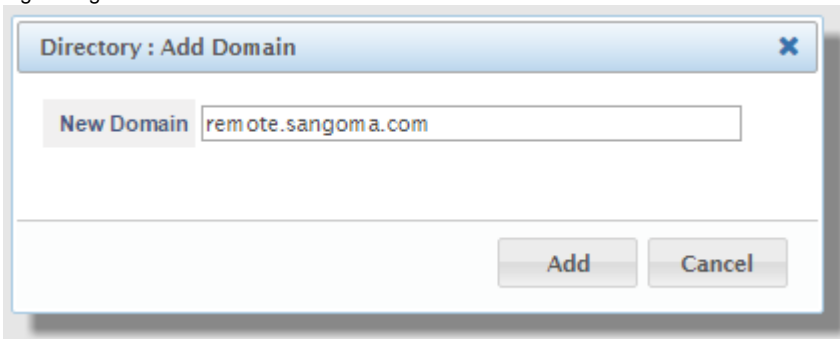
Registration

Routing & Header Manipulation

Call Admission Control

4) Configuring the SIP Domain

1. Go to Configuration -> Signaling -> Domains and click Add. Set the name of the domain to the FQDN or IP the remote phones will be registering to.

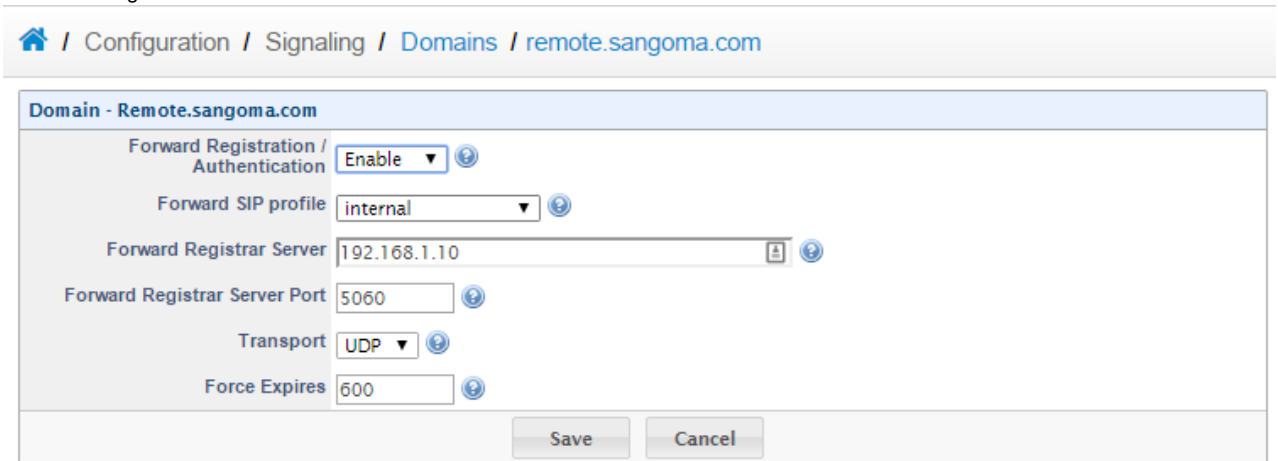


Directory : Add Domain

New Domain: remote.sangoma.com

Add Cancel

2. Next enable Forward Registration/Authentication as shown below. Set the Forward SIP profile to Internal. Then it is recommended to Force the Expires time to around 300-600 seconds; this will force the phones to register every 5-10 minutes. The short time period will ensure the registration information is current and correct.



Home / Configuration / Signaling / Domains / remote.sangoma.com

Domain - Remote.sangoma.com

Forward Registration / Authentication: Enable

Forward SIP profile: internal

Forward Registrar Server: 192.168.1.10

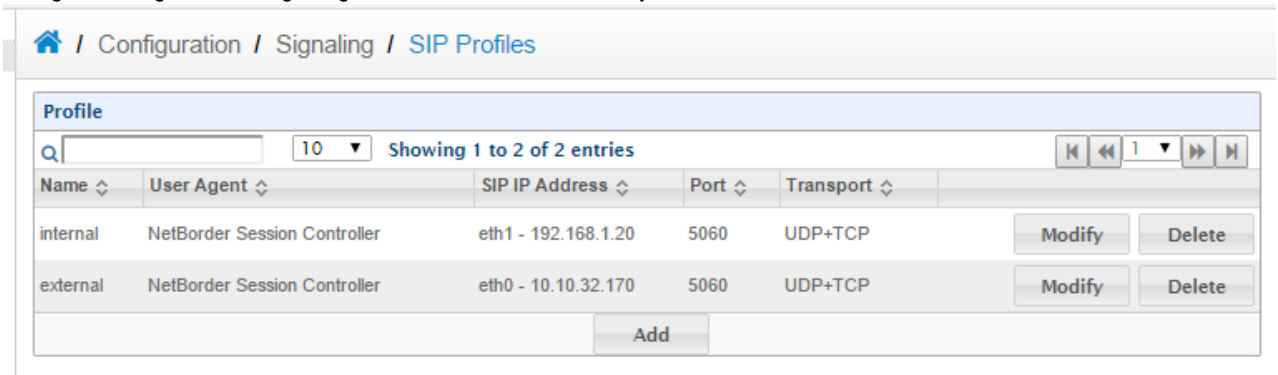
Forward Registrar Server Port: 5060

Transport: UDP

Force Expires: 600

Save Cancel

3. Next go to Configuration -> Signaling -> SIP Profiles and click Modify on the External SIP Profile.



Home / Configuration / Signaling / SIP Profiles

Profile

Showing 1 to 2 of 2 entries

Name	User Agent	SIP IP Address	Port	Transport	
internal	NetBorder Session Controller	eth1 - 192.168.1.20	5060	UDP+TCP	Modify Delete
external	NetBorder Session Controller	eth0 - 10.10.32.170	5060	UDP+TCP	Modify Delete

Add

4. Then click Bind under the Domain section.

The screenshot shows the configuration page for the 'external' SIP profile. The breadcrumb path is 'Home / Configuration / Signaling / SIP Profiles / external'. The page is divided into three sections: 'Profile - External', 'Domain', and 'Limit'.
- The 'Profile - External' section shows: User Agent: NetBorder Session Controller, SIP IP Address: eth0 - 10.10.32.170, Port: 5060, and Transport: UDP+TCP. There are 'Edit' and 'Cancel' buttons.
- The 'Domain' section shows 'No Domain' and a 'Bind' button.
- The 'Limit' section shows 'No Limit' and an 'Add' button.

5. Select your domain from the list and click Bind.

The dialog box titled 'External : Bind Domain' has a close button (X) in the top right corner. It contains a list with one entry: 'remote.sangoma.com' with a checked checkbox. At the bottom, there are 'Bind' and 'Cancel' buttons.

6. Your domain will now be bound to the SIP profile. This will allow Remote phones to register to your External SIP Profile.

The screenshot shows the 'Domain' section of the configuration page. It features a search bar, a dropdown menu set to '10', and the text 'Showing 1 to 1 of 1 entries'. Below this is a table with one entry: 'remote.sangoma.com'. To the right of this entry is an 'Unbind' button. At the bottom of the table area is a 'Bind' button.

5) Configuring the Call Routing

1. Go to Configuration -> Routing -> Call Routing and then click the Add button in the Basic Call Routing section to add a new routing plan.

2. Name the new routing plan internal and then click Add.

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

- In the new rule change the stop policy to Stop On Failure. Add the condition below to verify all internal calls originate from the PBX's IP address. To do this use the network_addr variable as shown below. Ensure the actions to perform if the condition doesn't match is set to respond with a 403. Once done click Save to continue.

Configuration / Routing / Call Routing / internal / Rule / rule_66

Rule - Rule_66

Condition

Description: [] Rank: 10

Matching: All Stop Policy: Stop On Failure

Condition: Variable Name: network_addr Expression: 192.168.1.10

Condition: (Please Select One)

Condition: (Please Select One)

Condition: (Please Select One)

Condition: (Please Select One)

Condition: (Please Select One)

Actions to perform if condition matches

Action: (Please Select One)

Action: (Please Select One)

Action: (Please Select One)

Action: (Please Select One)

Action: (Please Select One)

Actions to perform if condition doesn't match

Action: Respond Code: 403 Forbidden Data: []

Action: (Please Select One)

Action: (Please Select One)

Action: (Please Select One)

Action: (Please Select One)

Save Cancel

- Next click Add to add a new rule. In the new rule set the condition based off the Destination Address. The condition will be (.*). The action will need to be a custom action and the application will be bridge. The data will be `$(sofia_contact(external/$1@remote.sangoma.com))`. The "external" part is the name of the external facing SIP profile. The "remote.sangoma.com" part is the domain the users are registering to. These are the two pieces that may change on a per installation basis.

Configuration / Routing / Call Routing / internal / Rule / rule_67

Rule - Rule_67

Condition

Description: [] Rank: 20

Matching: All Stop Policy: Continue

Condition: Standard Information Name: Destination Address Expression: (.*)

Condition: (Please Select One)

Condition: (Please Select One)

Condition: (Please Select One)

Condition: (Please Select One)

Condition: (Please Select One)

Actions to perform if condition matches

Action: Custom Application: bridge Data: \$(sofia_contact(external/\$1@remote.sangoma.com))

Action: (Please Select One)

Action: (Please Select One)

Action: (Please Select One)

Action: (Please Select One)

Actions to perform if condition doesn't match

Action: (Please Select One)

Action: (Please Select One)

Action: (Please Select One)

Action: (Please Select One)

Action: (Please Select One)

Save Cancel

- Next go back to the call routing and add a new routing plan as we did in step 1-2 above. Name the new routing plan external. This will be used for the external SIP profile. In the new routing plan add only one rule. The condition will be (.*) and based on the Destination Address. Then the action will be bridge to trunk. The Trunk will be the SIP trunk named PBX with the destination \$1 as shown below.

[Home](#) / [Configuration](#) / [Routing](#) / [Call Routing](#) / [external](#) / [Rule](#) / [rule_64](#)

Rule - Rule_64

Condition

Description Rank

Matching All Stop Policy Continue

Condition Standard Information Name Destination Address Expression

Condition (Please Select One)

Condition (Please Select One)

Condition (Please Select One)

Condition (Please Select One)

Actions to perform if condition matches

Action Bridge to Trunk Trunk PBX Destination

Action (Please Select One)

Action (Please Select One)

Action (Please Select One)

Action (Please Select One)

Actions to perform if condition doesn't match

Action (Please Select One)

Action (Please Select One)

Action (Please Select One)

Action (Please Select One)

Action (Please Select One)

- Now that both routing plans are made go to Configuration -> Signaling -> SIP Profiles and modify the internal SIP profile.

[Home](#) / [Configuration](#) / [Signaling](#) / [SIP Profiles](#)

Profile

10 Showing 1 to 2 of 2 entries ⏪ ⏩ 1 ⏪ ⏩

Name	User Agent	SIP IP Address	Port	Transport	Modify	Delete
internal	NetBorder Session Controller	eth1 - 192.168.1.20	5060	UDP+TCP	Modify	Delete
external	NetBorder Session Controller	eth0 - 10.10.32.170	5060	UDP+TCP	Modify	Delete

8. In the internal SIP profile under Session Routing change the Routing Plan to Internal. Then click Save to continue.

[Home](#) / [Configuration](#) / [Signaling](#) / [SIP Profiles](#) / [internal](#)

Accept Blind Authentication	Disable	?
Authenticate Requests	Disable	?
Network Validation ACL	Disable	?
QoS		
SIP TOS Value		?
RTP TOS Value		?
NAT Traversal		
NAT ACL	(None)	?
Ping NAT Registrations	Disable	?
Symmetric Response Routing	Enable	?
RTP Auto Adjust	Disable	?
Aggressive NAT Detection	Disable	?
Load Limits		
Enable Load Limiting	Enable	?
Max Concurrent Sessions		?
CPU High Threshold	90	?
CPU Low Threshold	80	?
Reject Response Code	503	?
Reject Message	Service Unavailable	?
Session Routing		
Routing Plan	internal	?
Manual Redirect Routing	Disable	?
Always Use Full Identification	Disable	?
Header Manipulation		
Ingress	(None)	?
Egress	(None)	?

9. Next go back to Configuration -> Signaling -> SIP Profiles and this time click Modify next to the External SIP profile. Once in the External SIP profile, go to the Session Routing section and change the Routing Plan to External. Then click Save.

[Home](#) / [Configuration](#) / [Signaling](#) / [SIP Profiles](#) / external

Accept Blind Authentication	Disable
Authenticate Requests	Disable
Network Validation ACL	Disable
QoS	
SIP TOS Value	
RTP TOS Value	
NAT Traversal	
NAT ACL	RFC1918
Ping NAT Registrations	Enable
Symmetric Response Routing	Force Always
RTP Auto Adjust	Enable
Aggressive NAT Detection	Enable
Load Limits	
Enable Load Limiting	Enable
Max Concurrent Sessions	
CPU High Threshold	90
CPU Low Threshold	80
Reject Response Code	503
Reject Message	Service Unavailable
Session Routing	
Routing Plan	external
Manual Redirect Routing	Disable
Always Use Full Identification	Disable
Header Manipulation	
Ingress	(None)
Egress	(None)

6) Finalizing the Installation

1. Go to Overview -> Dashboard -> Control Panel and start the following services.
 1. Vega Session Controller
 2. IP Firewall
 3. Intrusion Detection

4. Intrusion Prevention

Home / Overview / Dashboard / Control Panel

Application Services				
Service	Status	Uptime	CPU(%)	Memory(%)
Vega Session Controller	STARTED	02:48	0.3	1.5
Refresh				

Media Services				
Service	Status	Uptime	CPU(%)	Memory(%)
RTCP Monitor	STARTED			
Refresh				

Security Services				
Service	Status	Uptime	CPU(%)	Memory(%)
SIP Security Monitor	STARTED			
Media Firewall	STARTED			
IP Firewall	STARTED			
Intrusion Detection	STARTED	01:59	0	7.7
Intrusion Prevention	STARTED	01:56	0	0
Refresh				

System Services				
Service	Status	Uptime	CPU(%)	Memory(%)
Secure Shell	STARTED	6-06:08:22	0	0
Refresh				

2. Enable ddos, scan, icmp and voip IDS rules rules by going to Configuration -> Security -> Intrusion Detection and ensuring all are checked. Once done click Update to apply the changes.

Security Rules			
Enabled	Group Name	Description	Number of Rules
<input type="checkbox"/>	mysql	Database - MySQL exploits	6
<input type="checkbox"/>	sql	Database - SQL exploits	8
<input checked="" type="checkbox"/>	ddos	Distributed denial of service detection - DDOS	1
<input checked="" type="checkbox"/>	scan	Network scan detection	4
<input checked="" type="checkbox"/>	icmp	Ping scans	13
<input checked="" type="checkbox"/>	voip	Voice Over IP	188
<input type="checkbox"/>	web-cgi	Web - CGI script exploits	7
<input type="checkbox"/>	web-coldfusion	Web - ColdFusion exploits	44
<input type="checkbox"/>	web-frontpage	Web - FrontPage exploits	38
<input type="checkbox"/>	web-iis	Web - Microsoft IIS exploits	7
<input type="checkbox"/>	web-misc	Web - Miscellaneous exploits	116
<input type="checkbox"/>	web-php	Web - PHP exploits	13
<input type="checkbox"/>	web-client	Web browser exploits	264
Update			

3. Next go to System -> Server -> Web and change the Network Interface from All interfaces to only the internal network interface.

Home / System / Server / Web

Web Server	
Network Interface	All interfaces
HTTP port	80
HTTPS port	443
Protocol	HTTP + HTTPS
Save	

4. In this example eth1 is the internal network interface. Once done click Save.

[Home](#) / [System](#) / [Server](#) / [Web](#)

Web Server

Network Interface	<input type="text" value="eth1 - 192.168.1.20"/>
HTTP port	<input type="text" value="80"/>
HTTPS port	<input type="text" value="443"/>
Protocol	<input type="text" value="HTTP + HTTPS"/>

5. 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.

[Home](#) / [System](#) / [Server](#) / [Secure Shell](#)

Secure Shell

Network Interface	<input type="text" value="eth1 - 192.168.1.20"/>
Port	<input type="text" value="22"/>

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

[Home](#) / [System](#) / [Management](#) / [Backup - Restore](#)

7. 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.

Vega Session Controller : Backup

Backup Name	<input type="text" value="System-Backup-Sept-1-2015"/>
Backup Type	<input type="text" value="System Backup"/>

Vega Session Controller : Backup

Backup Name	<input type="text" value="System-Backup-Sept-1-2015"/>
Backup Type	<input type="text" value="System Backup"/>