# SIP Trunking

Overview

The SIP Trunking use case allows your PBX to safely connect over the internet to an ITSP. The SBC in this scenaro is providing 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 Remote Phone Support but for simplicity the example below concentrates on SIP trunking.

(Under Construction)
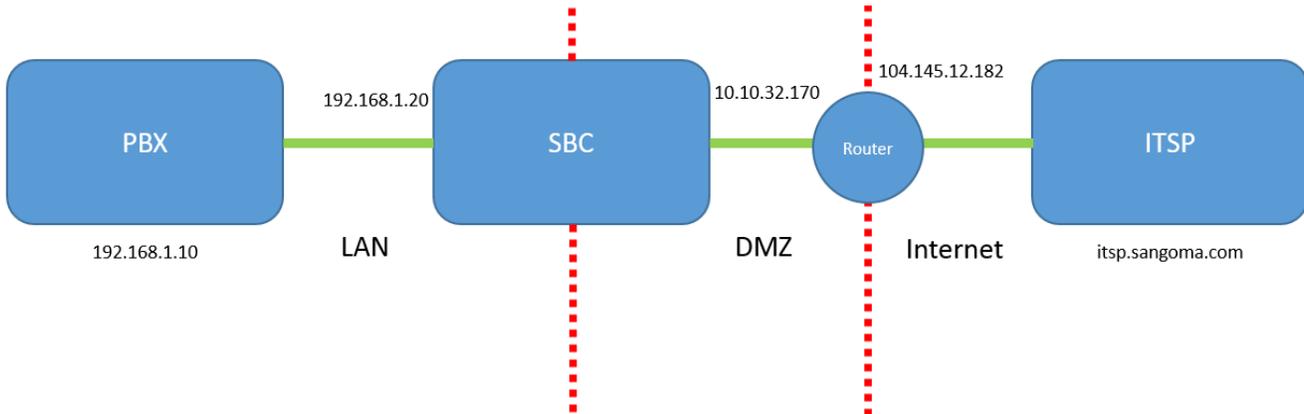
PBX IP: 192.168.1.10
SBC LAN IP: 192.168.1.20
SBC DMZ IP: 10.10.32.170
SBC Public IP: 104.145.12.182
ITSP FQDN: itsp.sangoma.com

1) Network Setup (here)

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.

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

🏠 / 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

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

🏠 / 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   ⏮ ◀◀ 1 ▾ ▶▶ ⏭

	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.

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

2) SIP Profile Configuration

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

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

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.

4. Next add a new profile called external.
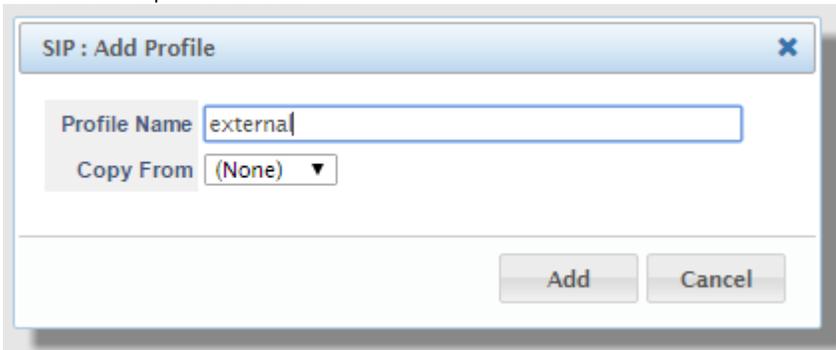
SIP : Add Profile   ✕

Profile Name external

Copy From (None) ▼

[Add]   [Cancel]

5. 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.
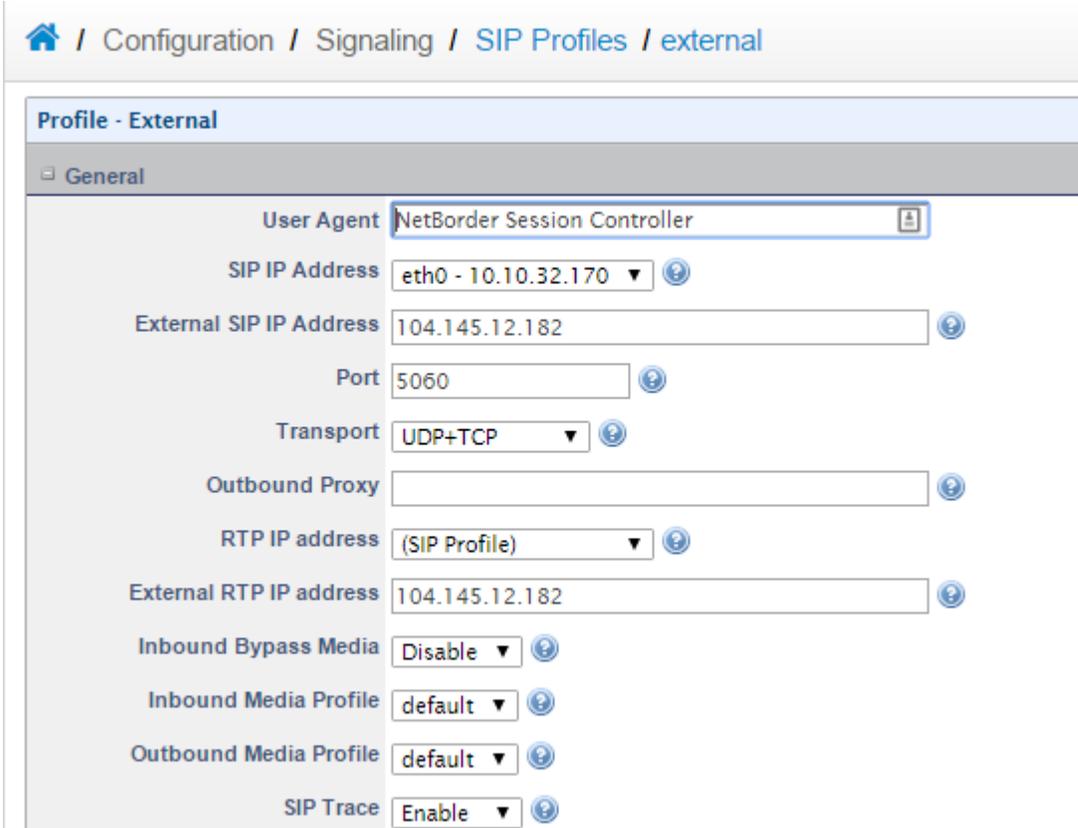
🏠 / Configuration / Signaling / SIP Profiles / external

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 ▼

6. Next disable authenticate calls as we did with the internal SIP profile.
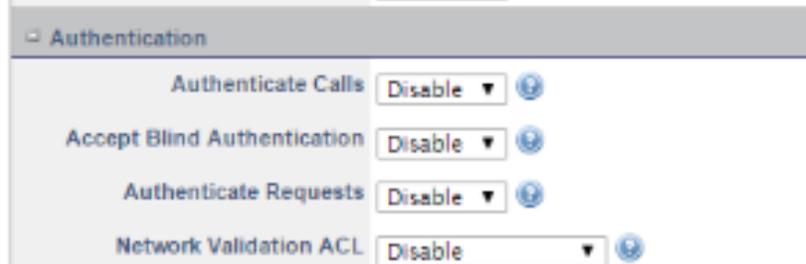
Authentication

Authenticate Calls	Disable ▼
Accept Blind Authentication	Disable ▼
Authenticate Requests	Disable ▼
Network Validation ACL	Disable ▼

3) Adding SIP Trunk to PBX and ITSP

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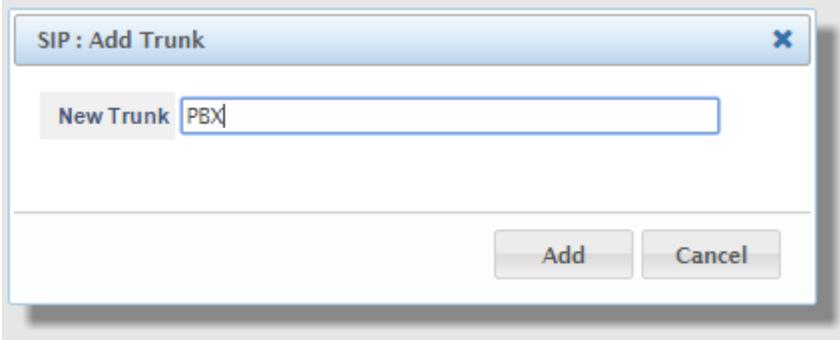
SIP : Add Trunk   ✖

New Trunk [PBX]

[Add]   [Cancel]

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.
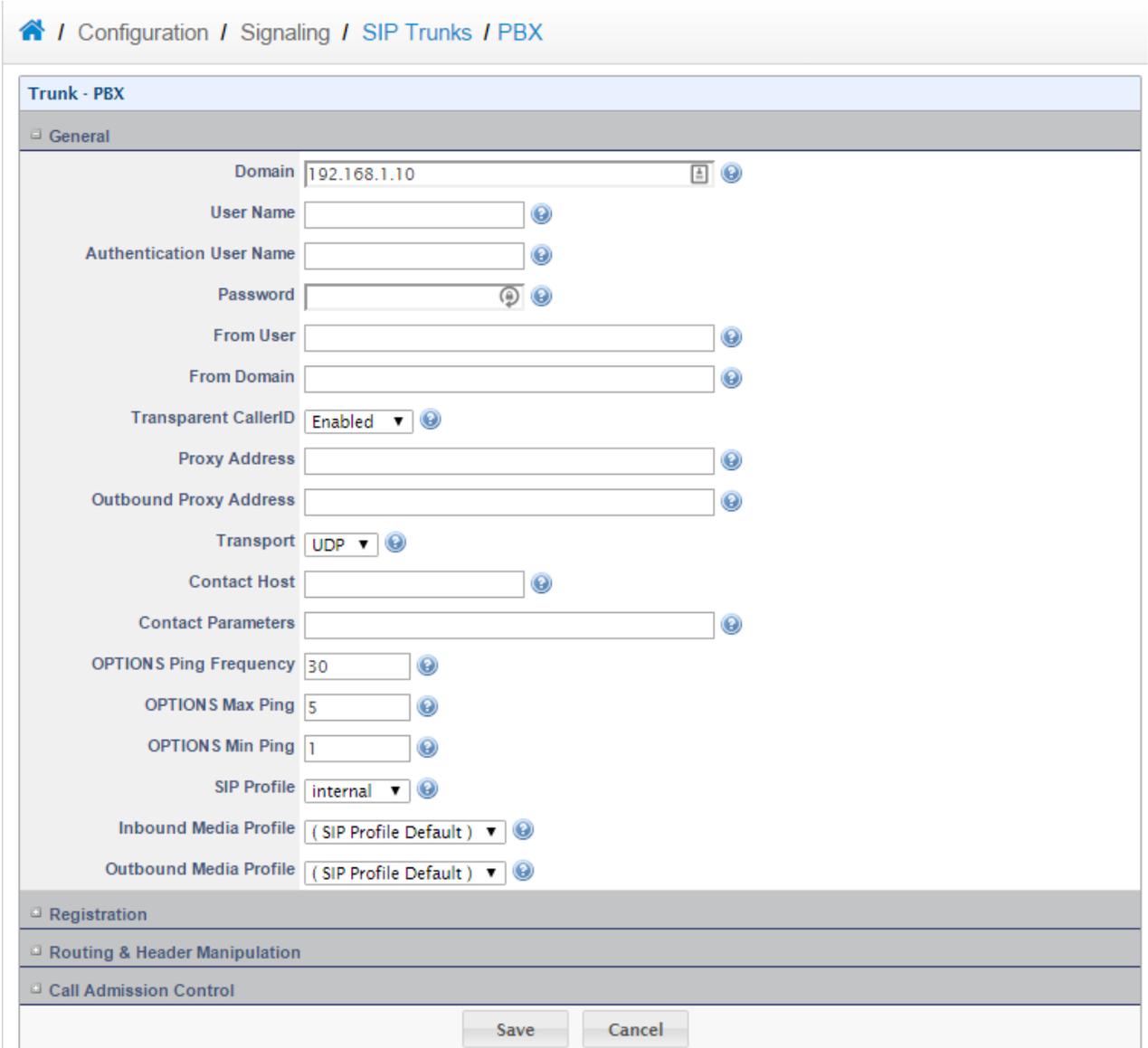
🏠 / Configuration / Signaling / SIP Trunks / PBX

Trunk - PBX

▭ General

Domain	192.168.1.10
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	30
OPTIONS Max Ping	5
OPTIONS Min Ping	1
SIP Profile	internal ▾
Inbound Media Profile	(SIP Profile Default) ▾
Outbound Media Profile	(SIP Profile Default) ▾

▭ Registration

▭ Routing & Header Manipulation

▭ Call Admission Control

[Save]   [Cancel]

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.
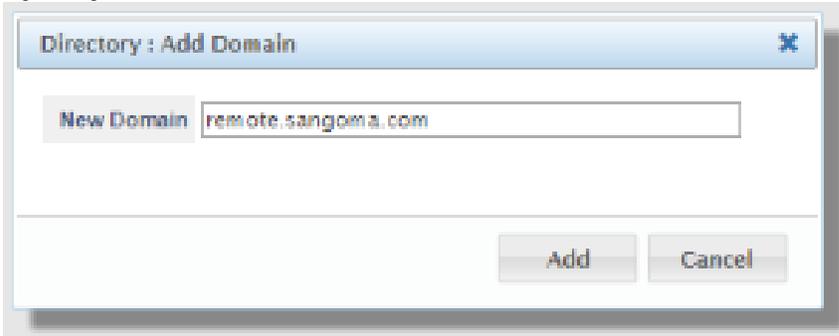
Directory : Add Domain ✖

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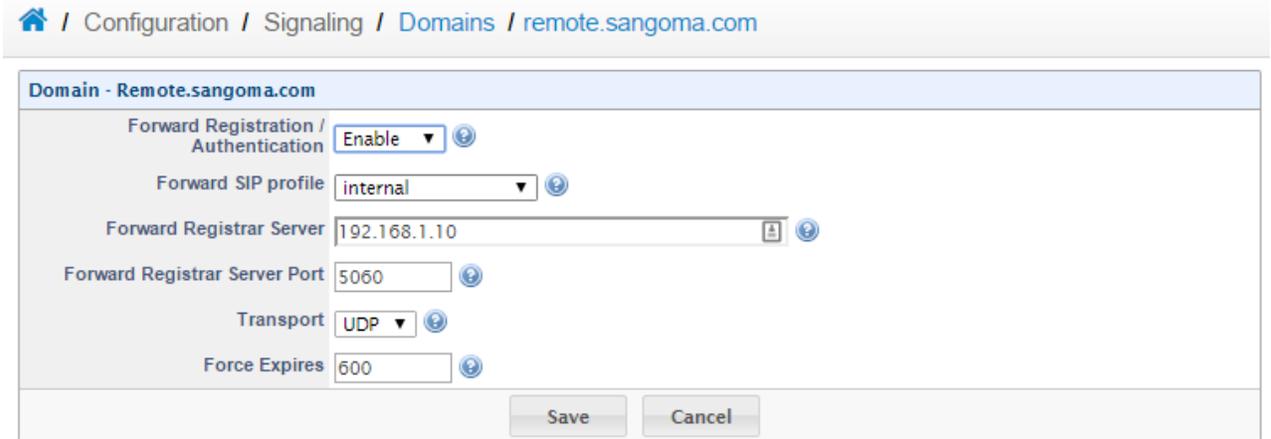
🏠 / Configuration / Signaling / Domains / remote.sangoma.com

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.

🏠 / Configuration / Signaling / SIP Profiles

Profile

🔍 [   ]   10 ▼   Showing 1 to 2 of 2 entries |◄ ◄◄ 1 ▼ ►► ►|

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.

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

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

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.

4. In the new rule change the stop policy to Stop On Failure. Add the condition below to verify all internal calls orginate 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.

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) ▾		

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

5. 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.

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) ▾		

Actions to perform if condition matches

Action	Custom ▾	Application bridge	Data ${sofia_contact(external/$1@remote.sa
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

6. 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.

🏠 / Configuration / Routing / Call Routing / external / Rule / rule_64

Rule - Rule_64

▫ **Condition**

Description	[ ] ⬆ Rank [10]
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 [$1]
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]

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

🏠 / Configuration / Signaling / SIP Profiles

Profile

🔍 [   ] [10 ▼]   Showing 1 to 2 of 2 entries   ⏮ ◀◀ [1 ▼] ▶▶ ⏭

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]

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

Accept Blind Authentication	Disable ▼ ❸
Authenticate Requests	Disable ▼ ❸
Network Validation ACL	Disable ▼ ❸

□ QoS

SIP TOS Value	❸
RTP TOS Value	❸

□ NAT Traversal

NAT ACL	(None) ▼ ❸
Ping NAT Registrations	Disable ▼ ❸
Symmetric Response Routing	Enable ▼ ❸
RTP Auto Adjust	Disable ▼ ❸
Aggressive NAT Detection	Disable ▼ ❸

□ Load Limits

Enable Load Limiting	Enable ▼ ❸
Max Concurrent Sessions	❸
CPU High Threshold	90 ❸
CPU Low Threshold	80 ❸
Reject Response Code	503 ❸
Reject Message	Service Unavailable ❸

□ Session Routing

Routing Plan	internal ▼ ❸
Manual Redirect Routing	Disable ▼ ❸
Always Use Full Identification	Disable ▼ ❸

□ Header Manipulation

Ingress	(None) ▼
Egress	(None) ▼

Save   Cancel

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.

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

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

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

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

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

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

/ Configuration / Security / Intrusion Detection

Security Rules			
Enabled	Group Name	Description	Number of Rules
✔	mysql	Database - MySQL exploits	6
✔	sql	Database - SQL exploits	8
✔	ddos	Distributed denial of service detection - DDOS	1
✔	scan	Network scan detection	4
✔	icmp	Ping scans	13
✔	voip	Voice Over IP	188
✔	web-cgi	Web - CGI script exploits	7
✔	web-coldfusion	Web - ColdFusion exploits	44
✔	web-frontpage	Web - FrontPage exploits	38
✔	web-iis	Web - Microsoft IIS exploits	7
✔	web-misc	Web - Miscellaneous exploits	116
✔	web-php	Web - PHP exploits	13
✔	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.

🏠 / 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.

🏠 / System / Server / Web

Web Server

Network Interface	eth1 - 192.168.1.20 ▾ ❓
HTTP port	80 ❓
HTTPS port	443 ❓
Protocol	HTTP + HTTPS ▾ ❓

Save

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.

🏠 / System / Server / Secure Shell

Secure Shell

Network Interface	eth1 - 192.168.1.20 ▾ ❓
Port	22 ❓

Save

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

🏠 / System / Management / Backup - Restore

⬆ Upload   🗃 Backup

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	System-Backup-Sept-1-2015
Backup Type	System Backup ▾

Backup   Cancel