

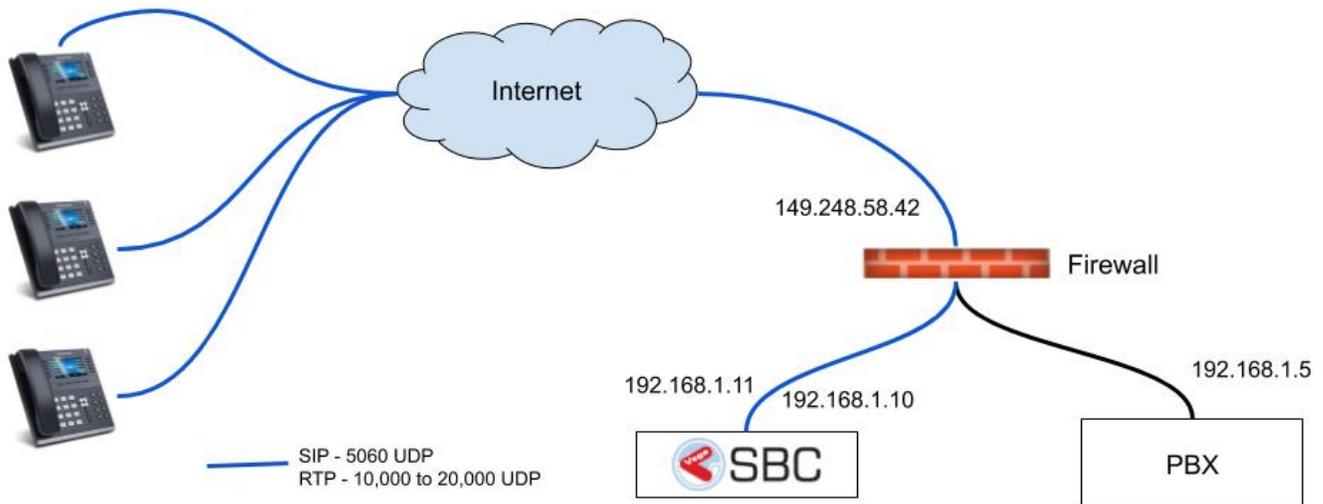
# Remote Phones

**SBC Public IP:** 149.248.58.42

**SBC Private IP #1:** 192.168.1.11 (Connection to Remote Phones - Public IP Ports Forwarded to this IP)

**SBC Private IP #2:** 192.168.1.10 (Connection to PBX)

**PBX Private IP:** 192.168.1.5



## Router Configuration

Ensure the following ports are open or forwarded to the public IP of the SBC.

- 5060 UDP
- 10,000 to 20,000 UDP

## SBC Configuration

1) Go to **Configuration IP Settings Access Control Lists** and create a new Access Control List called ACL. Set the default policy to Deny. Add the PBX IP as a ACL node as shown below. Ensure the policy is Allow and the prefix is 32 as shown below. Replace 192.168.1.5 with the private IP of your PBX.



The Email Notification is disabled.

ACL - Switchvox

Default Policy **Deny**

Edit

Cancel

ACL Nodes

Q [ ] 10 Showing 1 to 1 of 1 entries

Policy	IP Address	Prefix
Allow	192.168.1.5	32

Add

2) Go to **Configuration Signalling SIP Profiles** and add a SIP Profile called External. Select the external facing private IP that the public IP is forwarded to. In this example 149.248.58.42 is forwarded to 192.168.1.11. Then put the public IP in **External SIP IP Address** and **External RTP IP Address** as shown below. Then ensure SIP Trace is enabled.

**Profile - External**

General

Display Name: External

User Agent: NetBorder Session Controller

SIP IP Address: eth1 - 192.168.1.11

External SIP IP Address: 149.248.58.42

Port: 5060

Transport: UDP+TCP

Outbound Proxy:

RTP IP address: (SIP Profile)

External RTP IP address: 149.248.58.42

Inbound Bypass Media: Disable

Inbound Media Profile: default

Outbound Media Profile: default

SIP Trace: **Enable**

SIP Capture: Disable

Strict Security: Disable

3) Next in the Authentication section disable Authenticate Calls. Then set the Network Validation ACL to IP Address as shown below. The Network Validation ACL only allows Registration messages through until the device registers. This means only Registrations are allowed from any IP, and everything else is blocked. Then in step #18 below we create a firewall rule to block multiple failed Registrations. Which ensures hackers can't keep sending countless attempts to Register.

**Authentication**

Authenticate Calls **Disable** ⓘ

Accept Blind Authentication **Disable** ⓘ

Authenticate Requests **Disable** ⓘ

Network Validation ACL **IP Address** ⓘ

ACL for Inbound Calls **Used**

ACL for Registration **Used**

4) In the NAT Traversal section set the options exactly as shown below. These fix all the problems NAT can cause. Since the remote phone can be behind any router, its important these are all enabled as shown below.

**NAT Traversal**

NAT ACL **RFC1918** ⓘ

Ping NAT Registrations **Enable** ⓘ

Symmetric Response Routing **Force Always** ⓘ

RTP Auto Adjust **Enable** ⓘ

Aggressive NAT Detection **Enable** ⓘ

5) Create a second SIP profile called Internal as shown below. Selecting the internal side private IP, enabling SIP trace and enabling Strict Security.

**Profile - Internal**

General

Display Name: Internal

User Agent: NetBorder Session Controller

SIP IP Address: eth1 - 192.168.1.10

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

SIP Capture: Disable

Strict Security: Enable

6) In the Authentication section Disable Authenticate Calls. Then move the ACL over to the Used box for both Inbound calls, and Registrations. This only permits SIP requests from IPs in the ACL.

**Authentication**

Authenticate Calls: Disable

Accept Blind Authentication: Disable

Authenticate Requests: Disable

Network Validation ACL: Disable

ACL for Inbound Calls: Used

ACL:

Available:

ACL for Registration: Used

ACL:

Available:

7) Next go to **Configuration Signalling SIP Trunks** and create a new trunk called PBX. Set the Domain to the IP of the PBX, and then ensure the SIP Profile is set to Internal. Once done save the SIP trunk.

Trunk - Swvx\_trunk

General

Display Name

Domain

User Name

Authentication User Name

Password

From User

From Domain

Transparent CallerID

Proxy Address

Outbound Proxy Address

Transport

Secure Media

Contact Host

Contact Parameters

OPTIONS Ping Frequency

OPTIONS Max Ping

OPTIONS Min Ping

Allow Port in Gateway Identity

SIP Profile

Inbound Media Profile

Outbound Media Profile

8) Next go to **Configuration Signalling Domains** and create a new domain. The Domain will be the public IP of the SBC. Put the Domain into the Display Name as shown below. Then enable forward registration. Set the forward SIP profile to Internal. Then move the PBX trunk over to the used box as shown below. Then save once done.

**Note:** In some cases you may want to set the Force Expires time. Setting this will allow you to shorten the time that devices stay Registered. If phones are constantly changing between networks, then a shorter Register time such as 300 seconds or less is a good idea. This way the SBC always has the most current location of the phone.

Domain - Domain\_119

Display Name: 149.248.58.42

Multiple registrations: Disable

Forward Registration / Authentication: Enable

Forward SIP profile: Internal

Trunk List

Used	Available
PBX	

Force Expires:

Block IP On Unresponsive Challenged Registration: Disable

IP Blocking duration: 60

Forward Refer Headers: Enable

Forward Registration Origination Network Info: Disable

Server Error Codes: 408

Save Cancel

9) Now that the domain is made, go to **Configuration Signalling SIP Profiles External** and click the **Bind** button. A popup will come up, simply select the domain made in the previous step.

Profile - Profile\_71

Profile Name: External

User Agent: NetBorder Session Controller

Routing Plan: External

SIP IP Address: eth1 - 192.168.1.11

Port: 5060

Transport: UDP+TCP

Network Validation ACL: IP Address

Edit Cancel

---

Domain

Showing 1 to 1 of 1 entries

Domain
149.248.58.42

Unbind

Bind

10) Go to **Configuration Routing Call Routing** and create a new **Basic** rule called External.

Basic Call Routing - External	
Display Name	External
Description	
Trace Call	Disable
Default Response	404
<input type="button" value="Edit"/> <input type="button" value="Cancel"/>	

Rule
No Rule
<input type="button" value="Add"/>

11) Next Add a new rule as shown below. This rule will route all External calls from the remote phones to the PBX.

Rule - Rule_117	
Condition	
Description	<input type="text"/> Rank 10
Matching	All Stop Policy Stop On Success
Condition	Standard Information Name Destination Address Expression (*)
Actions to perform if condition matches	
Action	Bridge to Trunk Trunk PBX Destination S1
Actions to perform if condition doesn't match	
Action	( Please Select One )
<input type="button" value="Save"/> <input type="button" value="Save &amp; Apply"/> <input type="button" value="Cancel"/>	

12) Go to **Configuration Routing Call Routing** and create a new **Basic** rule called Internal.

Basic Call Routing - Internal	
Display Name	Internal
Description	
Trace Call	Disable
Default Response	404
<input type="button" value="Edit"/> <input type="button" value="Cancel"/>	

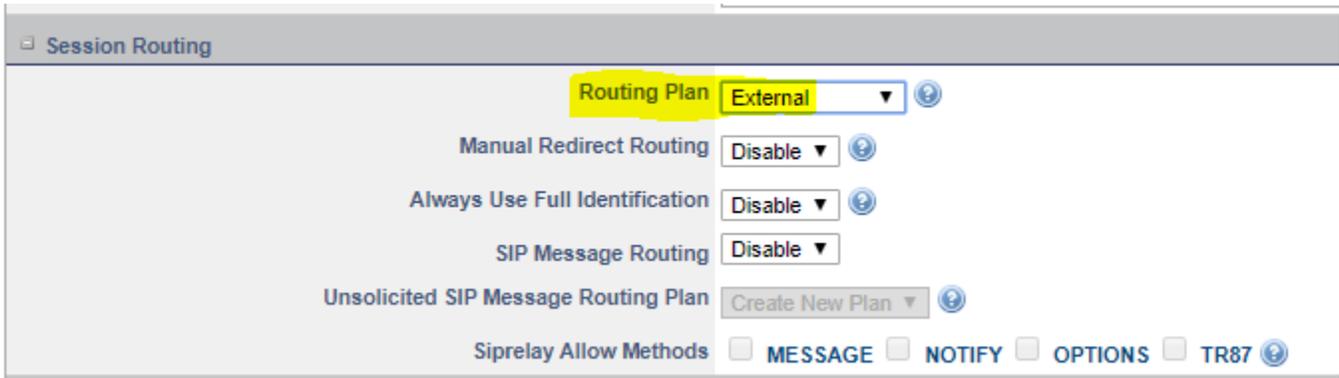
  

Rule
No Rule
<input type="button" value="Add"/>

13) Next Add a new rule as shown below. This rule will route all Internal calls to the Registered users.

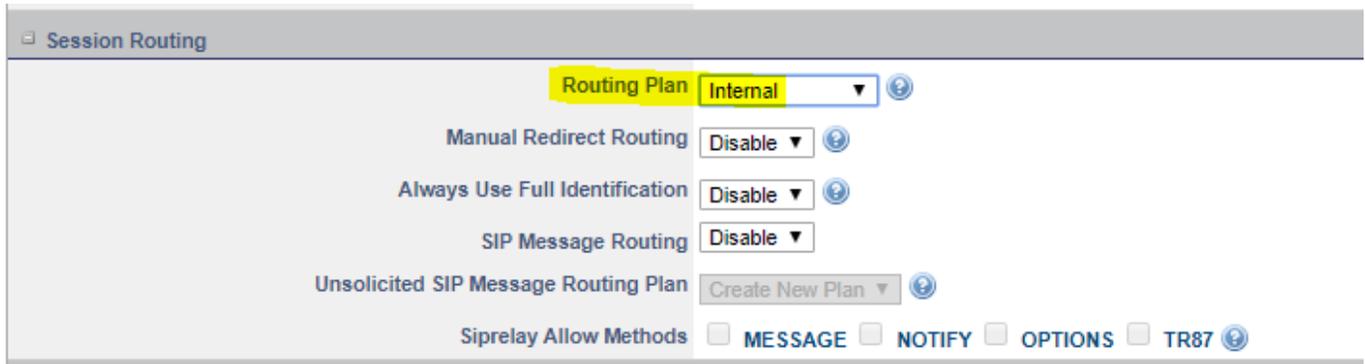
Rule - Rule_97	
Condition	
Description	<input type="text"/> Rank 10
Matching	All Stop Policy Stop On Success
Condition	Standard Information Name Destination Address Expression (*)
Actions to perform if condition matches	
Action	Bridge to Contact Profile External Domain 149.248.56.42 Destination S1
Actions to perform if condition doesn't match	
Action	( Please Select One )
<input type="button" value="Save"/> <input type="button" value="Save &amp; Apply"/> <input type="button" value="Cancel"/>	

14) Go to **Configuration Signalling SIP Profiles** and Modify the External SIP profile. Then on the following page click Edit. At this point scroll to the bottom and set the Routing Plan to External.



The screenshot shows the 'Session Routing' configuration page for an External SIP profile. The 'Routing Plan' dropdown is highlighted in yellow and set to 'External'. Other settings include 'Manual Redirect Routing', 'Always Use Full Identification', and 'SIP Message Routing', all set to 'Disable'. The 'Unsolicited SIP Message Routing Plan' is set to 'Create New Plan'. Under 'Siprelay Allow Methods', the checkboxes for 'MESSAGE', 'NOTIFY', 'OPTIONS', and 'TR87' are all unchecked.

15) Go to **Configuration Signalling SIP Profiles** and Modify the Internal SIP profile. Then on the following page click Edit. At this point scroll to the bottom and set the Routing Plan to Internal.



The screenshot shows the 'Session Routing' configuration page for an Internal SIP profile. The 'Routing Plan' dropdown is highlighted in yellow and set to 'Internal'. Other settings include 'Manual Redirect Routing', 'Always Use Full Identification', and 'SIP Message Routing', all set to 'Disable'. The 'Unsolicited SIP Message Routing Plan' is set to 'Create New Plan'. Under 'Siprelay Allow Methods', the checkboxes for 'MESSAGE', 'NOTIFY', 'OPTIONS', and 'TR87' are all unchecked.

16) To configure the Intrusion Detection or IDS simply go to **Configuration Security Intrusion Detection** and select the following 4 rule groups as shown below. We will be isolating the webUI from the internet, so there is no need for the other rules. Once done click the update button at the bottom to save changes.

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

17) Next go to **Configuration Security SIP Firewall** and edit the default rule **Fail\_Call\_Block**. This rule will block any IP that fails 10 times over a 30 minute period. By default the rule only blocks for 60 minutes, but it is best to change this to forever. To do this change the Action Parameter to 0 as shown below.

This rule can be adjusted if you find there is too many users being blocked by this. Also note if you have multiple phones a remote site, the block can take down the whole site. To avoid this, put any known remote site IPs in the "Source IP White List Filter", and separate the IPs by commas if there is more than one.



Rules - Fail\_Call\_Block

SIP Request Method: INVITE

Failed Attempts: 10

Interval: 30

Source IP White List Filter: [Empty]

Source IP Filter: [Empty]

SIP Profile Filter: (None)

Account Registration Filter: [Empty]

User Agent Filter: [Empty]

SIP Response Code Filter: 403

Action: Block IP

Action Parameter: 0

Comments: Failed inbound call with SIP 403, block IP forever

Save Cancel

18) Next we need to do the same rule as the previous step, but this time for Registrations. Just as mentioned in the previous step you can white list IPs of known remote sites. Once done save to complete the SIP Firewall setup.

This rule can be adjusted if you find there is too many users being blocked by this. Also note if you have multiple phones a remote site, the block can take down the whole site. To avoid this, put any known remote site IPs in the "Source IP White List Filter", and separate the IPs by commas if there is more than one.

Home / Configuration / Security / SIP Firewall / Fail\_Reg\_Block

The Email Notification is disabled.

**Rules - Fail\_Reg\_Block**

SIP Request Method: REGISTER

Failed Attempts: 10

Interval: 30

Source IP White List Filter:

Source IP Filter:

SIP Profile Filter: (None)

Account Registration Filter:

User Agent Filter:

SIP Response Code Filter: 403

Action: Block IP

Action Parameter: 0

Comments: Failed Registration with 403; block IP forever

19) If you do have an IP blocked by the IDS you can go to **Overview Security Intrusion Detection Status** to see if its blocked. It will be shown at the bottom there, and you will have the ability to unblock the IP. You can also add known IPs to the Exempt list so the IDS doesn't block them. Keep in mind, the Exempt list for the IDS is different then the White list for the SIP firewall as mentioned in Step #17. You should put known remote site IPs in both locations.

Home / Overview / Security / Intrusion Detection Status

**Exempt List**

IP Address	Action
10.0.0.0/8	<input type="button" value="Delete"/>
172.16.0.0/12	<input type="button" value="Delete"/>
192.168.0.0/16	<input type="button" value="Delete"/>
<input style="width: 100%;" type="text"/>	<input type="button" value="Add"/>

**Intrusion Prevention - Active Block List**

ID	Blocked IP	Date	Time	Time Remaining	Action
Report is empty.					

20) If the IP isn't blocked by the IDS, then it can be blocked by the SIP Firewall configured in steps #17/18. If the IP is blocked you will see it in the list as shown below. You can unblock the IP by pressing the unblock button.



The Email Notification is disabled.

Edit

#### Blocked IPs

IP	Block Time	Block Expiration	Blocking Rule	
141.98.10.33	2020-02-27 14:55:28	2020-02-27 15:55:28	Fail_Call_Block	Unlock

21) Last step to security is configuring both the webUI and SSH to only listen on the internal network. To do this go to **System Server Web** and set the Network Interface to the private network, then save changes.



The Email Notification is disabled.

#### Web Server

Network Interface

HTTP port

HTTPS port

Protocol

Save

22) Go to **System Server Secure Shell** to do the same for SSH. Setting the Network Interface to the private IP.



The Email Notification is disabled.

#### Secure Shell

Network Interface

Port

Save

23) The SBC at this point is completely configured. Ensure you apply changes and start the SBC. Once the SBC starts take a **configuration backup** as shown at <https://wiki.sangoma.com/display/SBC/Backup+and+Restore>.

24) If there is any issues please contact Sangoma support with the info up at <https://wiki.sangoma.com/display/SBC/How+To+Capture+Logs>. To open a ticket please go to <https://support.sangoma.com>.

