

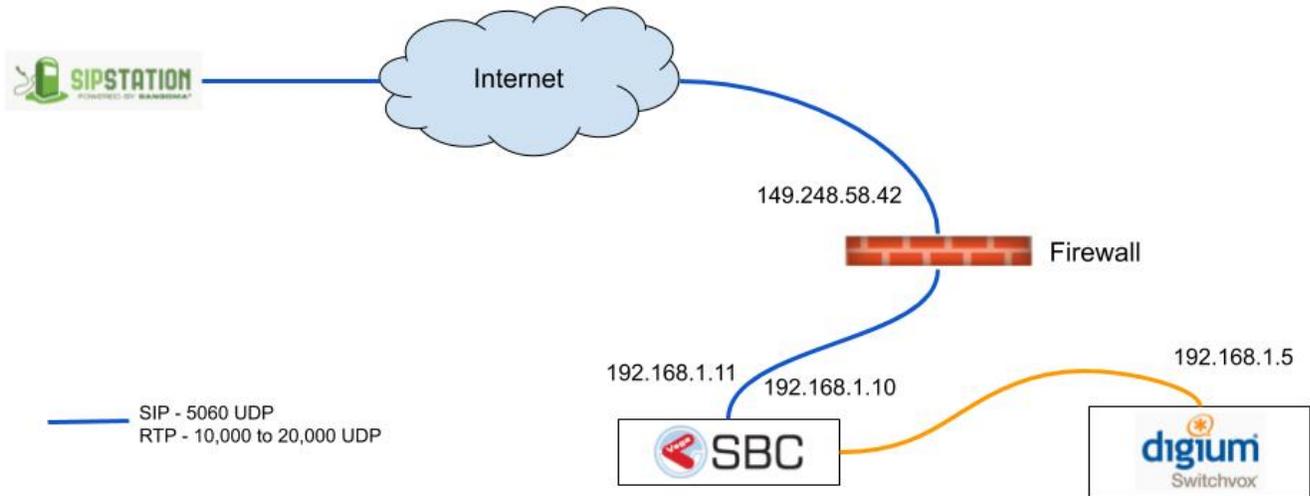
Switchvox - SIP Trunking

Switchvox Private IP: 192.168.1.5

SBC Public IP: 149.248.58.42

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

SBC Private IP #2: 192.168.1.10 (Connection to Switchvox)



Router Configuration

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

SBC Public IP Ports

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

SBC Configuration

1) Go to **Configuration IP Settings Access Control List** and add a new list called ACL. Ensure the default policy is Deny, and then add both the IP of Switchvox, and the IP(s) of your ITSP. Ensure the prefix is /32 to only allow the single IP.

Note: In this case the ITSP is Sangoma's SIP Station. The FQDN's are trunk1.freepbx.com and trunk2.freepbx.com. Check with your ITSP if you need the IPs.



The Email Notification is disabled.

ACL - ACL

Default Policy Deny

Edit

Cancel

ACL Nodes

Showing 1 to 3 of 3 entries

Policy	IP Address	Prefix
Allow	192.168.1.5	32
Allow	192.159.66.3	32
Allow	162.253.134.142	32

Add

2) Go to **Configuration Signaling SIP Profiles** and add a new SIP profile called External_ITSP. Select the private IP that the public IP ports are forwarded to. In this example 149.248.58.42 is forwarded to 192.168.1.11. Then put the public IP of the SBC in **External SIP IP Address** and **External RTP IP Address** as shown below. Then ensure SIP Trace is enabled, as well as Strict Security as shown below.



The Email Notification is disabled.

Profile - External_ITSP

General

Display Name: External_ITSP

User Agent: NetBorder Session Controller

SIP IP Address: eth - 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

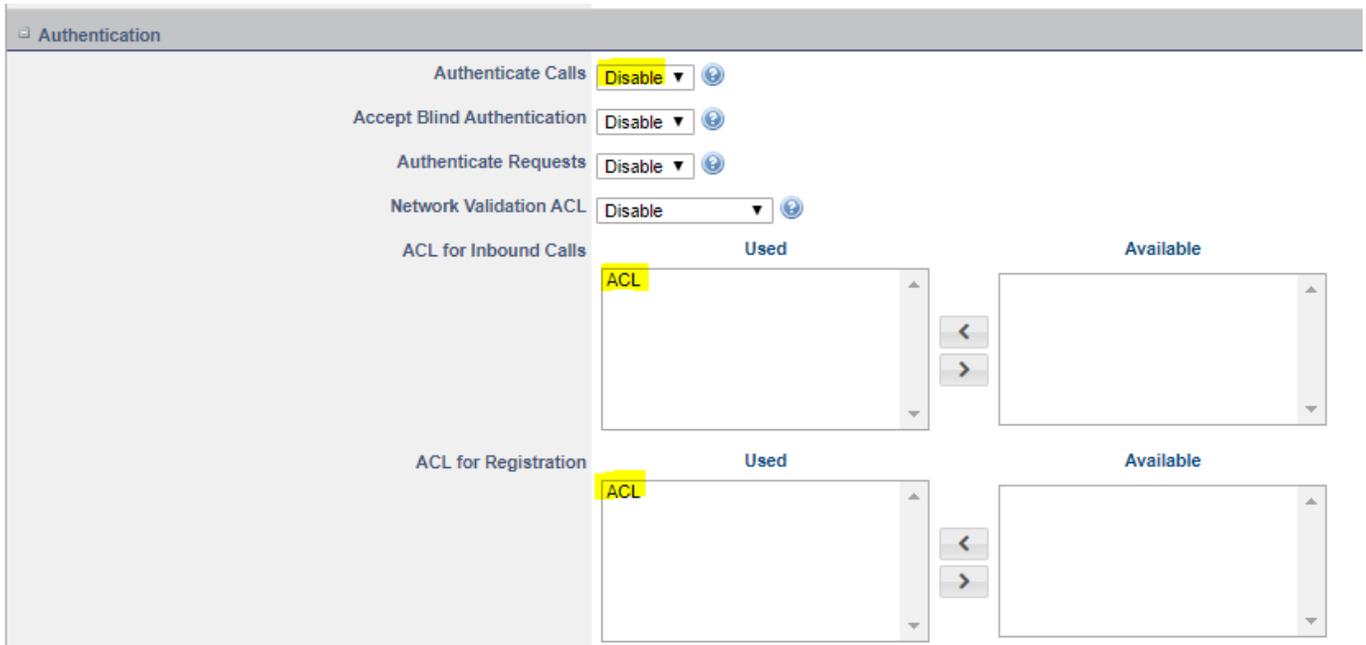
Outbound Media Profile: default

SIP Trace: Enable

SIP Capture: Disable

Strict Security: Enable

3) In the Authentication section Disable authenticate calls, and add the ACL list created previously to both inbound calls and registrations as shown below.



4) Go to **Configuration Signalling SIP Profiles** and add a new SIP profile called Internal_ITSP. Selecting the private IP, enabling SIP trace and enabling Strict Security.



The Email Notification is disabled.

Profile - Internal_ITSP

General

Display Name	Internal_ITSP
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

5) In the Authentication section Disable authenticate calls, and add the ACL list created previously to both inbound calls and registrations as shown below.

Authentication

Authenticate Calls **Disable** ?

Accept Blind Authentication **Disable** ?

Authenticate Requests **Disable** ?

Network Validation ACL **Disable** ?

ACL for Inbound Calls

Used	Available
ACL	

ACL for Registration

Used	Available
ACL	

6) Go to **Configuration Signalling SIP Trunks** and create a new SIP trunk called swvx_itsp. This trunk will point to your Switchvox PBX. Put the IP of the Switchvox in the domain, and ensure the SIP profile is set to Internal_ITSP. As well ensure Registration is Disabled.



The Email Notification is disabled.

Trunk - Swvx_itsp

General

Display Name	swvx_itsp
Domain	192.168.1.5
User Name	
Authentication User Name	
Password	
From User	
From Domain	
Transparent CallerID	Enabled
Proxy Address	
Outbound Proxy Address	
Transport	UDP
Secure Media	Disable
Contact Host	
Contact Parameters	
OPTIONS Ping Frequency	
OPTIONS Max Ping	
OPTIONS Min Ping	
Allow Port in Gateway Identity	Disable
SIP Profile	Internal_ITSP
Inbound Media Profile	(SIP Profile Default)
Outbound Media Profile	(SIP Profile Default)

Registration

Registration	Disable
Registrar Proxy Address	

7) Create another SIP trunk called Trunk1. This will go to trunk1.freepbx.com. Enter the username and password. Set the SIP profile to External_ITSP and enable Registration.



The Email Notification is disabled.

Trunk - Trunk1

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

Registration

Registration

Registrar Proxy Address

Register To: Header

8) Create another SIP trunk called Trunk2. This will go to trunk2.freepbx.com. Enter the username and password. Set the SIP profile to External_ITSP and enable Registration.

Note: Some ITSP's may only have 1 SIP Trunk. If this is the case skip this step.



The Email Notification is disabled.

Trunk - Trunk2

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

Registration

Registrar Proxy Address

9) Go to **Configuration Routing Call Routing** and create a new routing plan called External_ITSP. Then make a new rule as shown below. Ensure the Stop policy is set as shown below, and the trunk is set to swvx_itsp.

Expression: (.*)

Destination: \$1

 The Email Notification is disabled.

Rule - Rule_83

Condition

Description: [] 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: swvx_itsp Destination: S1

Actions to perform if condition doesn't match

Action: (Please Select One)

Save Save & Apply Cancel

10) Go to **Configuration Routing Call Routing** and create a another new routing plan called Internal_ITSP. If your provider only has a single trunk, then you can use the same rule as in step #9, but select your providers trunk. If you are using SIP Station or any other provider with two trunks, then use the rule below. This will allow fail over to work; where the call will go to trunk1, and if that is down, then it will go to trunk2.

Action 1: hangup_after_bridge
Value 1: true

Action 2: continue_on_fail
Value 2: NORMAL_TEMPORARY_FAILURE,USER_BUSY,NO_ANSWER,NO_USER_RESPONSE,NO_ROUTE_DESTINATION, NETWORK_OUT_OF_ORDER,CALL_REJECTED,DESTINATION_OUT_OF_ORDER,NORMAL_CIRCUIT_CONGESTION

Action 3: bridge
Value 3: sip/trunk/Trunk1/\$1

Action 4: bridge
Value 4: sip/trunk/Trunk2/\$1

 The Email Notification is disabled.

Rule - Rule_87

Condition

Description: [] Rank: 10

Matching: All Stop Policy: Stop On Success

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

Actions to perform if condition matches

Action	Set Variable	Name	hangup_after_bridge	Value	true
Action	Set Variable	Name	continue_on_fail	Value	NORMAL_TEMPORARY_FAILURE,USER_BUSY,NO_ANSWER,NO_USER_RESPONSE,NO_ROUTE_DESTINATION, NETWORK_OUT_OF_ORDER,CALL_REJECTED,DESTINATION_OUT_OF_ORDER,NORMAL_CIRCUIT_CONGESTION
Action	Custom	Application	bridge	Data	sip/trunk/Trunk1/\$1
Action	Custom	Application	bridge	Data	sip/trunk/Trunk2/\$1

Actions to perform if condition doesn't match

Action: (Please Select One)

Save Save & Apply Cancel

10) Go to **Configuration Signalling SIP Profiles External_ITSP** and modify and then edit the profile. Scroll to the bottom and set the Routing plan to External_ITSP.

Load Limits

Enable Load Limiting: Enable

Max Concurrent SIP Sessions: []

CPU High Threshold: 90

CPU Low Threshold: 80

Reject Response Code: 503

Reject Message: Service Unavailable

Session Routing

Routing Plan: External_ITSP

Manual Redirect Routing: Disable

Always Use Full Identification: Disable

SIP Message Routing: Disable

Unsolicited SIP Message Routing Plan: Create New Plan

Siprelay Allow Methods: MESSAGE NOTIFY OPTIONS TR87

Header Manipulation

Ingress: (None)

Egress: (None)

Save Cancel

11) Go to **Configuration Signalling SIP Profiles Internal_ITSP** and modify and then edit the profile. Scroll to the bottom and set the Routing plan to Internal_ITSP.

Load Limits

Enable Load Limiting: ⓘ

Max Concurrent SIP Sessions: ⓘ

CPU High Threshold: ⓘ

CPU Low Threshold: ⓘ

Reject Response Code: ⓘ

Reject Message: ⓘ

Session Routing

Routing Plan: ⓘ

Manual Redirect Routing: ⓘ

Always Use Full Identification: ⓘ

SIP Message Routing: ⓘ

Unsolicited SIP Message Routing Plan: ⓘ

Siprelay Allow Methods: MESSAGE NOTIFY OPTIONS TR87 ⓘ

Header Manipulation

Ingress: ⓘ

Egress: ⓘ

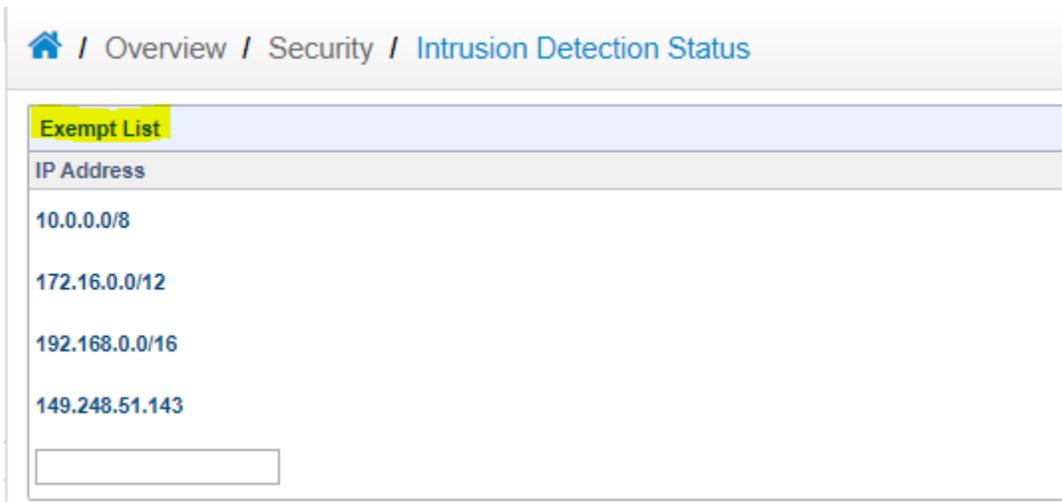
12) To configure the Intrusion Detection or IDS simply go to **Configuration Security Intrusion Detection** and select the following 4 rule groups as shown below. We will be isolating the webUI from the internet, so there is no need for the other rules. Once done click the update button at the bottom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

Home / Configuration / Security / Intrusion Detection

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

13) Go to **Overview Security Intrusion Detection Status** and then ensure the Switchvox IP is in the list. In this case the Switchvox is 192.168.1.5, which falls in the 192.168.0.0/16 range, which is part of the default config. In most cases this step can be skipped, as all private addresses are included here by default.

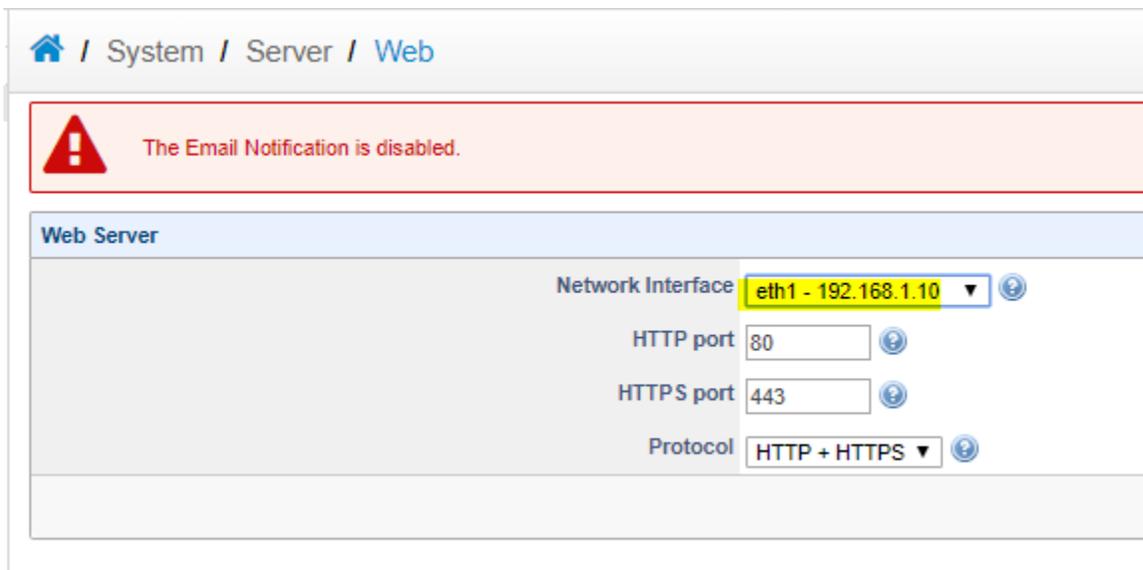


The screenshot shows a web interface with a breadcrumb trail: [Home](#) / [Overview](#) / [Security](#) / [Intrusion Detection Status](#). Below the breadcrumb is a section titled "Exempt List" with a table header "IP Address". The table contains the following entries:

IP Address
10.0.0.0/8
172.16.0.0/12
192.168.0.0/16
149.248.51.143

There is an empty input field at the bottom of the list.

14) 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 screenshot shows a web interface with a breadcrumb trail: [Home](#) / [System](#) / [Server](#) / [Web](#). A red warning banner at the top states: "The Email Notification is disabled." Below this is the "Web Server" configuration section with the following settings:

Network Interface	eth1 - 192.168.1.10
HTTP port	80
HTTPS port	443
Protocol	HTTP + HTTPS

15) 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 ?

Switchvox Configuration

1) Go to **Setup Call Routing VoIP Providers** and create a new Provider called SBC. Put anything into the Your Account ID and Your Password as a place holder. The put the IP of the SBC into the Hostname/IP Address field. Use the second IP assigned to the SBC. The one that doesn't have the public IP forwarded to it.

Modify SIP Provider ?



Provider Information



Peer Settings



Caller ID Settings



Connection Settings

SIP Provider Information ?

SIP Provider Name

Your Account ID

Your Password
Leave blank to keep current password.

Hostname/IP Address

Callback Extension

Default Fax Extension

DTMF Mode

Save SIP Provider ✓

2) Go to **Setup Call Routing Outgoing Calls** and ensure the new Provider called SBC is assigned to the correct routes as shown below.

Outgoing Calls ⓘ

Outgoing Call Rules | Caller ID Rules | Call Diagnostics

Create Outgoing Call Rule

Outgoing Call Rules

Showing: International to Internal (7 total)

Move	Name	Pattern To Match	Outgoing Type	Call Using	Note	Actions
↕ ₁	International	Begins with 9011 and the remainder is 7 to 13 digits in length	SIP Provider	SBC		
↕ ₂	1-900 Numbers	Begins with 91(900 976) and the remainder is 7 digits in length.	SIP Provider	SBC		
↕ ₃	Toll Free	Begins with 91(800 888 877 866 855 844) and the remainder is 7 digits in length.	SIP Provider	SBC		
↕ ₄	Long Distance	Begins with 91 and the remainder is 10 digits in length.	SIP Provider	SBC		
↕ ₅	Local	Begins with 9 and the remainder is 7 digits in length.	SIP Provider	SBC		
↕ ₆	911	Number exactly matches 911.	SIP Provider	SBC		
↕ ₇	Internal	Any local extension.	Internal			

3) Go to **Setup Call Routing Incoming Calls** and set the the destination. Here we have simply just sent the calls to an extension as an example.

Incoming Calls ⓘ

DID Routes | Caller ID Rules

Create Single DID Route | Create Ranged DID Route

Incoming DID Routes

Showing: Default to Unknown VOIP (2 total)

Move	Route Type	Name	Details	Note	Actions
	Default	Default	Route all calls on unmatched numbers from SIP Provider SBC to extension 500		
	Unknown VOIP	Unknown VOIP	Route all VOIP calls from any unknown host to Busy Signal.		

4) If there is any issues support will need the info up at <https://wiki.sangoma.com/display/SBC/How+To+Capture+Logs> when reporting an issue related to the SBC.