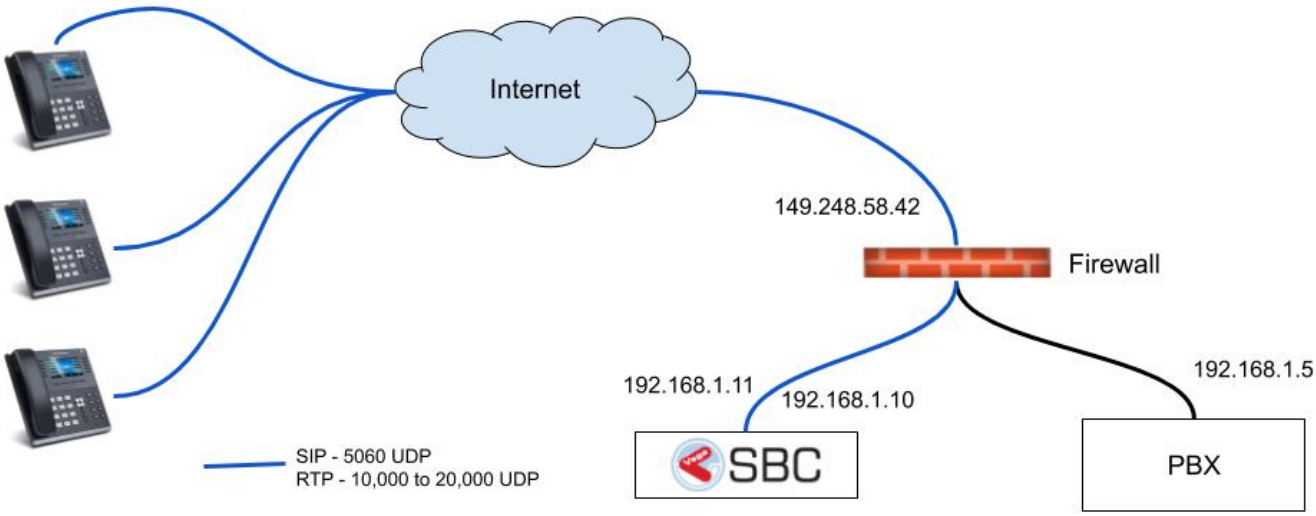
Remote Phones

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



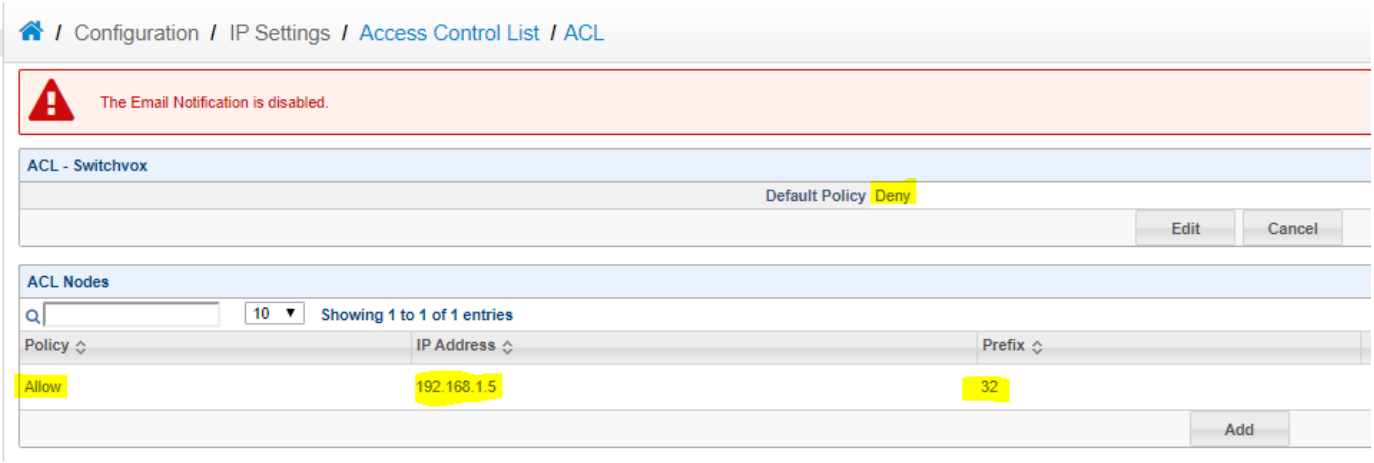
Router Configuration

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

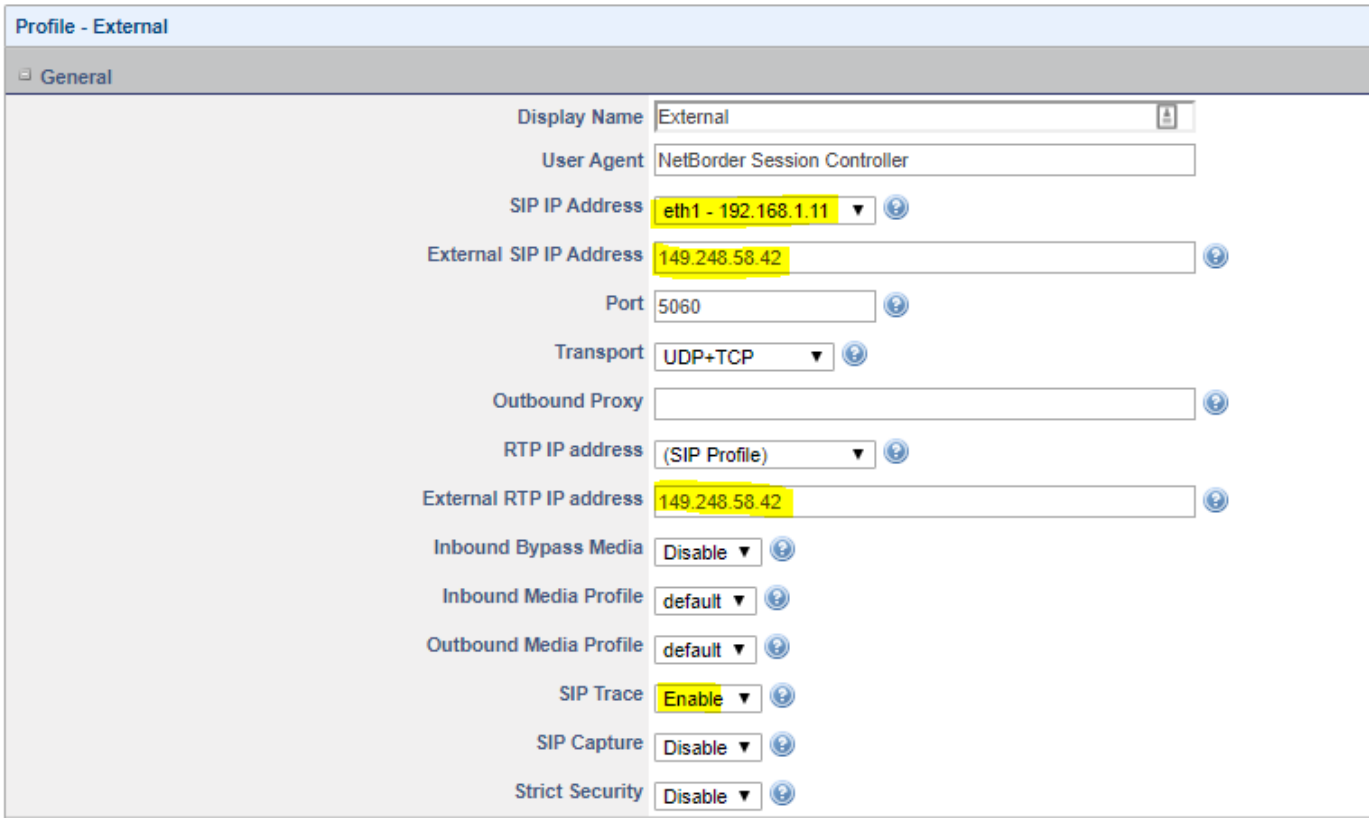
- **5060 UDP**
- **10,000 to 20,000 UDP**

SBC Configuration

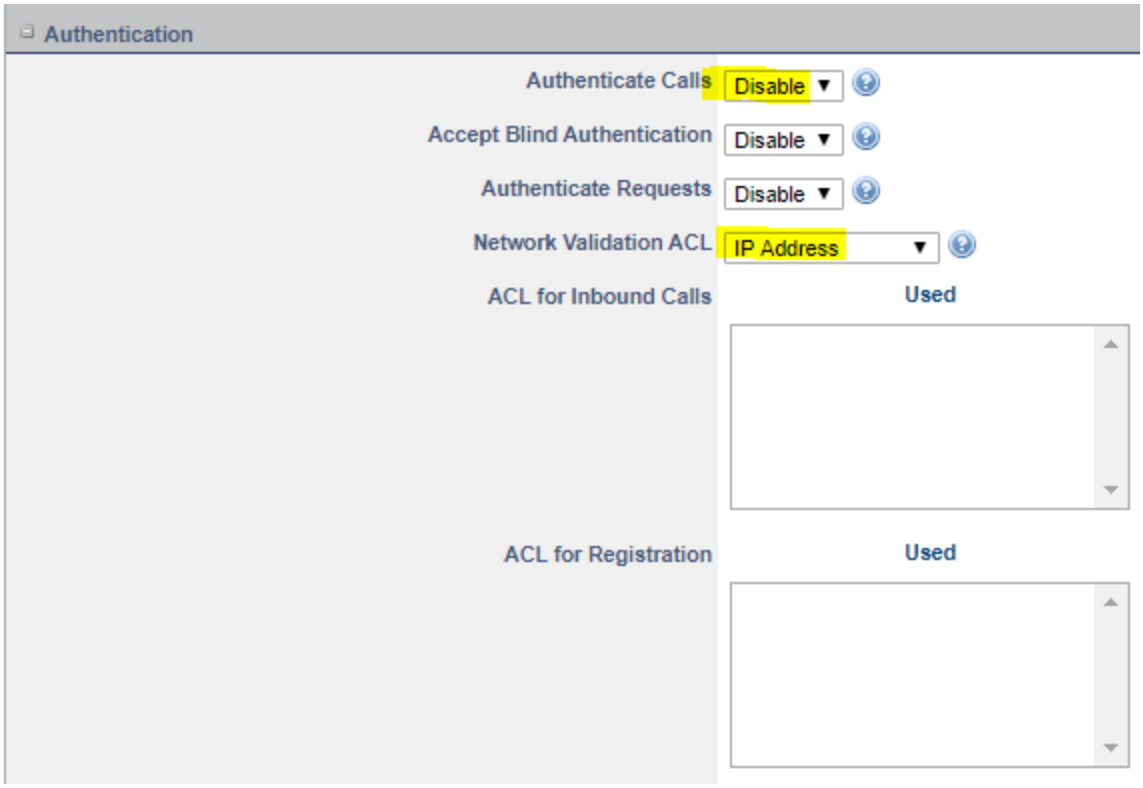
1) Go to **Configuration IP Settings Access Control Lists** and create a new Access Control List called ACL. Set the default policy to Deny. Add the PBX IP as a ACL node as shown below. Ensure the policy is Allow and the prefix is 32 as shown below. Replace 192.168.1.5 with the private IP of your PBX.



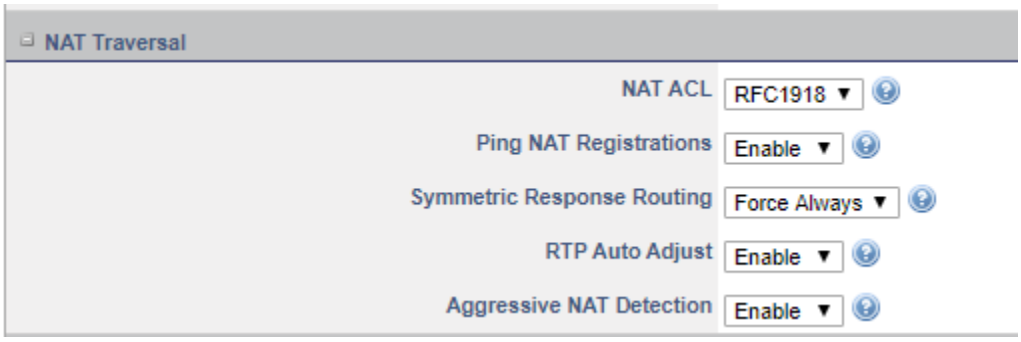
2) Go to **Configuration Signalling SIP Profiles** and add a SIP Profile called External. Select the external facing private IP that the public IP is forwarded to. In this example 149.248.58.42 is forwarded to 192.168.1.11. Then put the public IP in **External SIP IP Address** and **External RTP IP Address**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



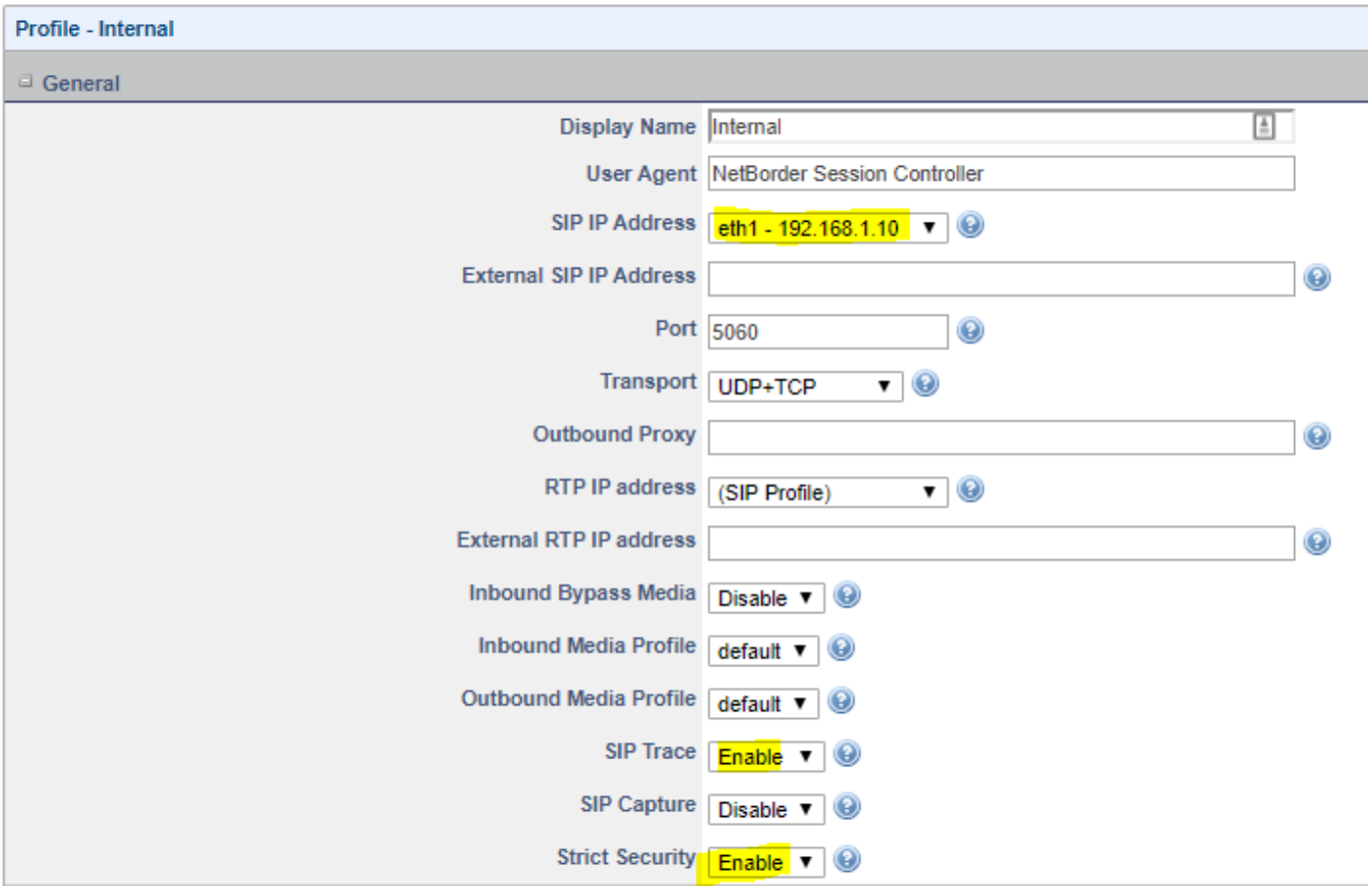
3) Next in the Authentication section disable Authenticate Calls. Then set the Network Validation ACL to IP Address as shown below. The Network Validation ACL only allows Registration messages through until the device registers. This means only Registrations are allowed from any IP, and everything else 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.



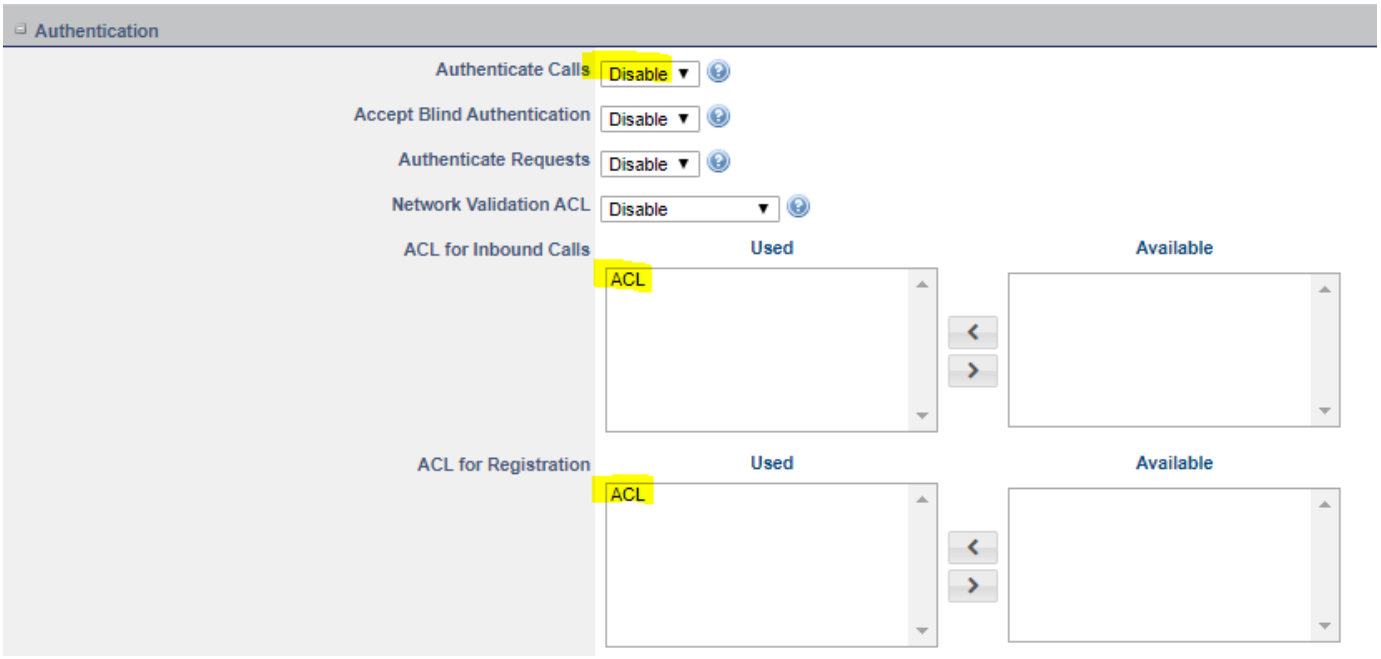
4) In the NAT Traversal section set the options exactly as shown below. These fix all the problems NAT can cause. Since the remote phone can be behind any router, its important these are all enabled as shown below.



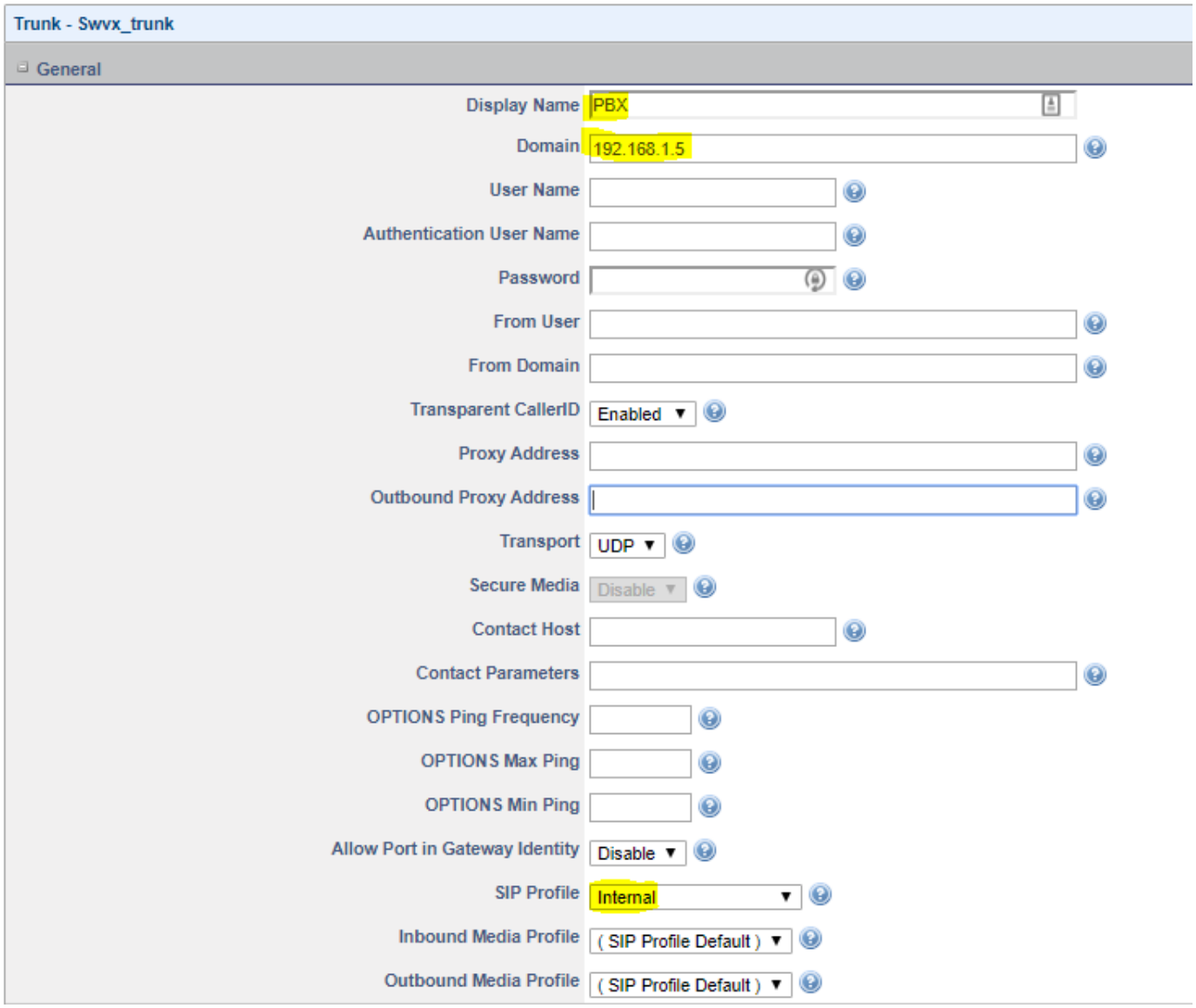
5) Create a second SIP profile called Internal as shown below. Selecting the internal side private IP, enabling SIP trace and enabling Strict Security.



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.

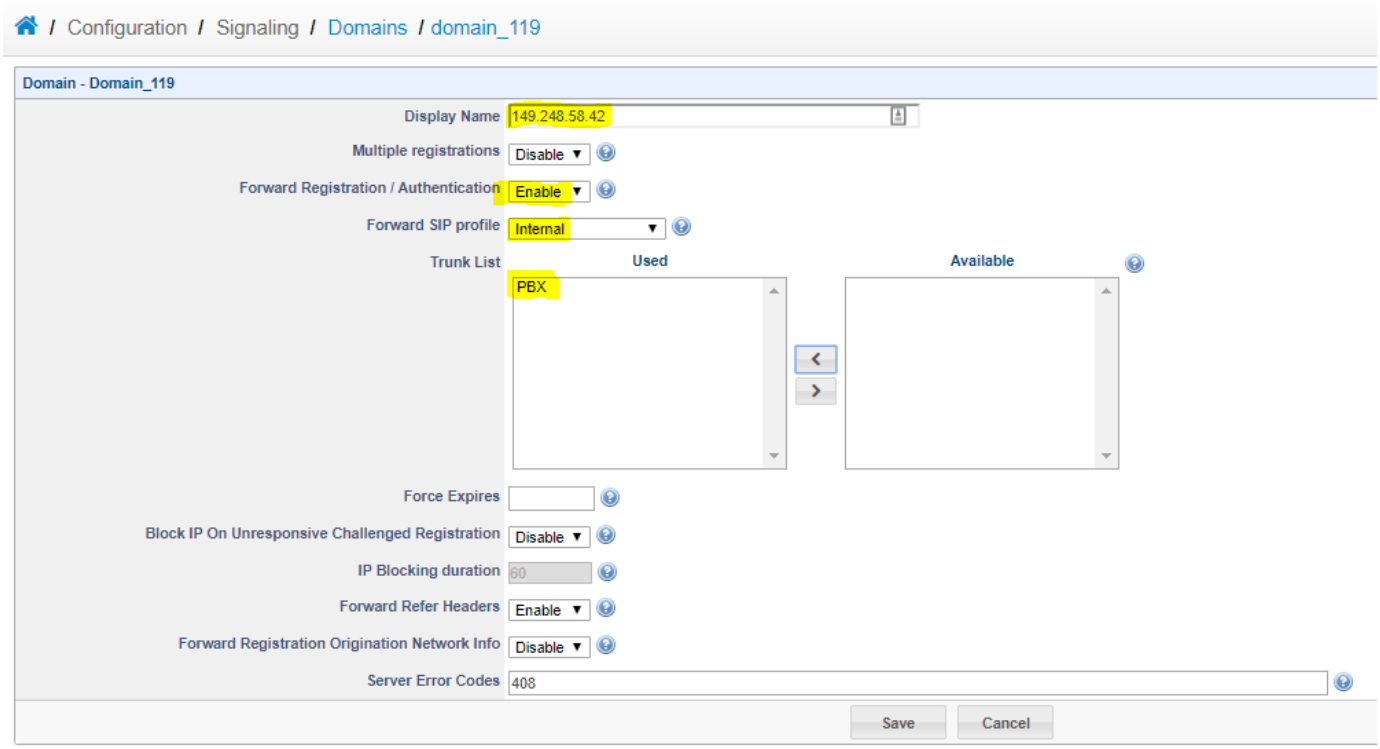


7) Next go to **Configuration Signalling SIP Trunks** and create a new trunk called PBX. Set the Domain to the IP of the PBX, and then ensure the SIP Profile is set to Internal. Once done save the SIP trunk.

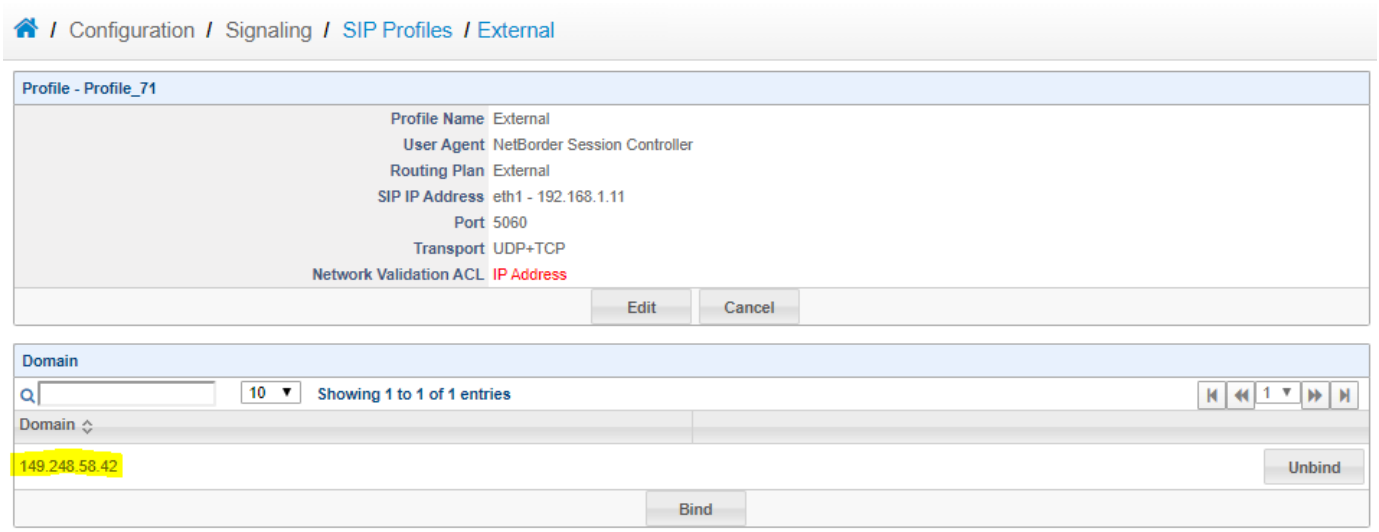


8) Next go to **Configuration Signalling Domains** and create a new domain. The Domain will be the public IP of the SBC. Put the Domain into the Display Name as shown below. Then enable forward registration. Set the forward SIP profile to Internal. Then move the PBX trunk over to the used box as shown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

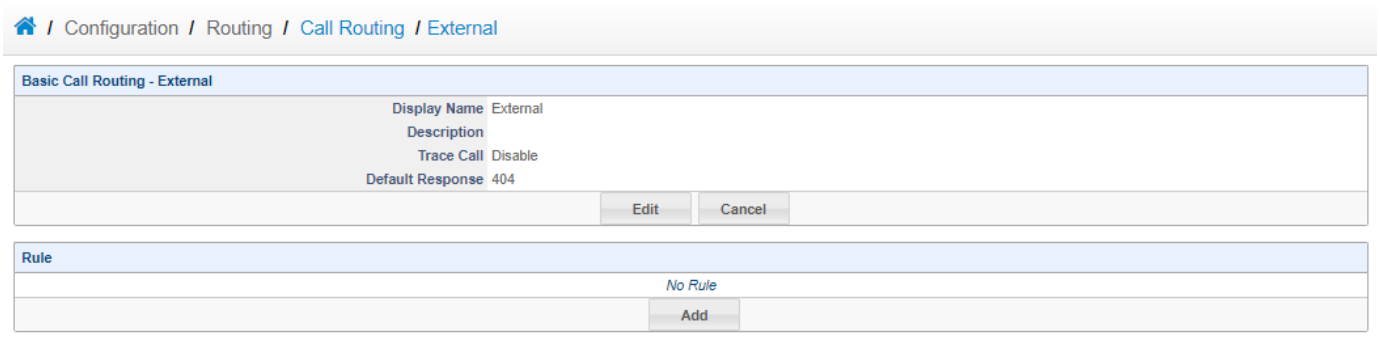
Note: In some cases you may want to set the Force Expires time. Setting this will allow you to shorten the time that devices stay Registered. If phones are constantly changing between networks, then a shorter Register time such as 300 seconds or less is a good idea. This way the SBC always has the most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



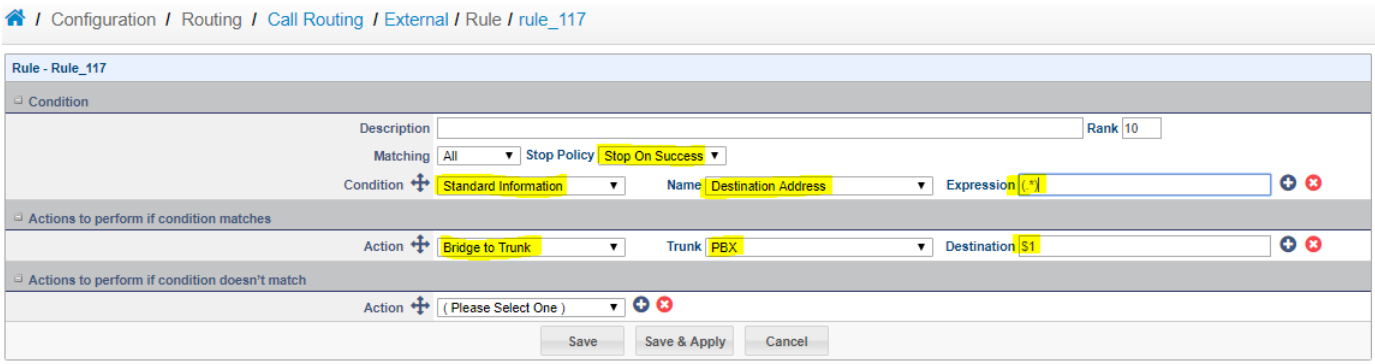
9) Now that the domain is made, go to **Configuration Signalling SIP Profiles External** and click the **Bind button**. A popup will come up, simply select the domain made in the previous step.



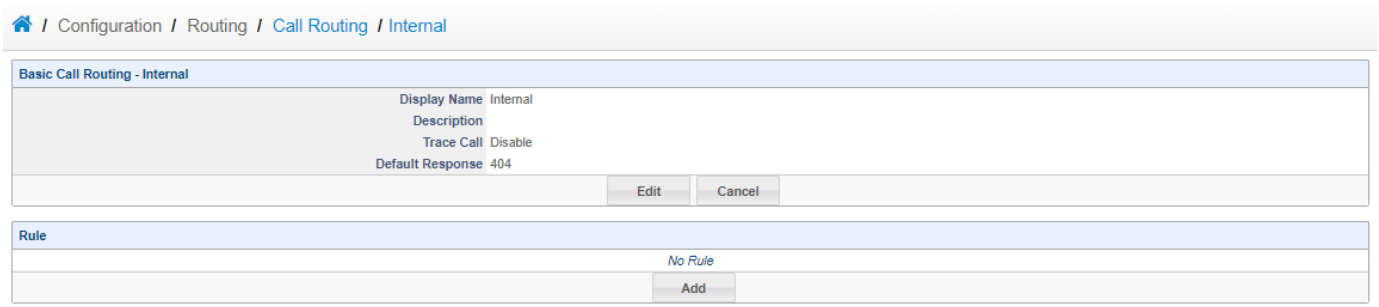
10) Go to **Configuration Routing Call Routing** and create a new **Basic** rule called External.



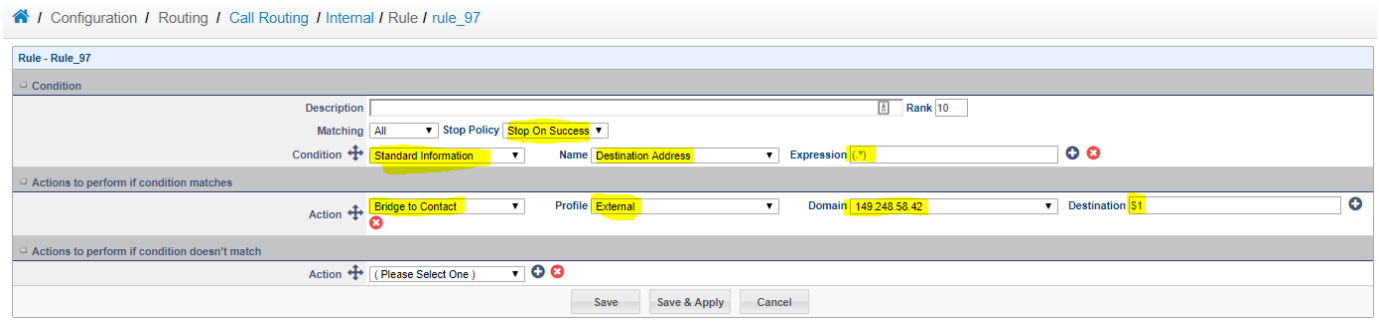
11) Next Add a new rule as shown below. This rule will route all External calls from the remote phones to the PBX.



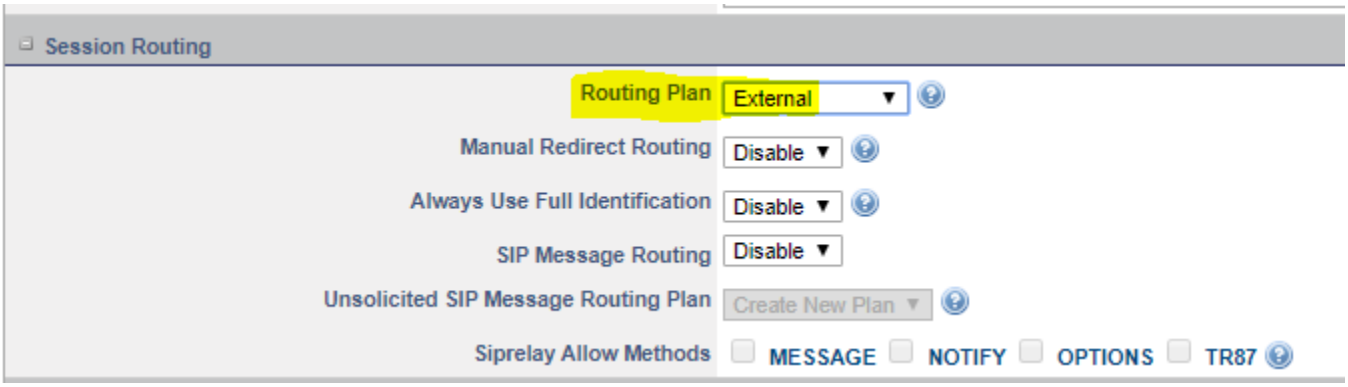
12) Go to **Configuration Routing Call Routing** and create a new **Basic** rule called Internal.



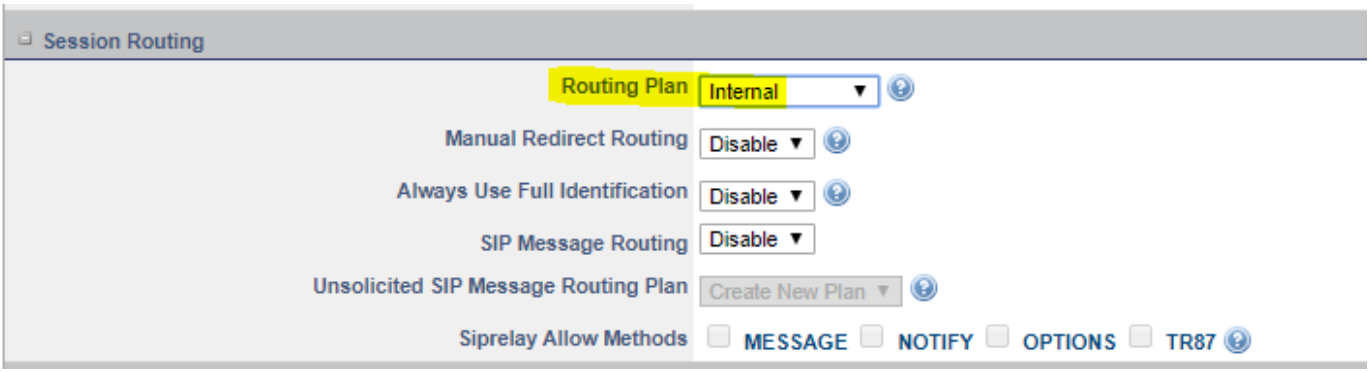
13) Next Add a new rule as shown below. This rule will route all Internal calls to the Registered users.



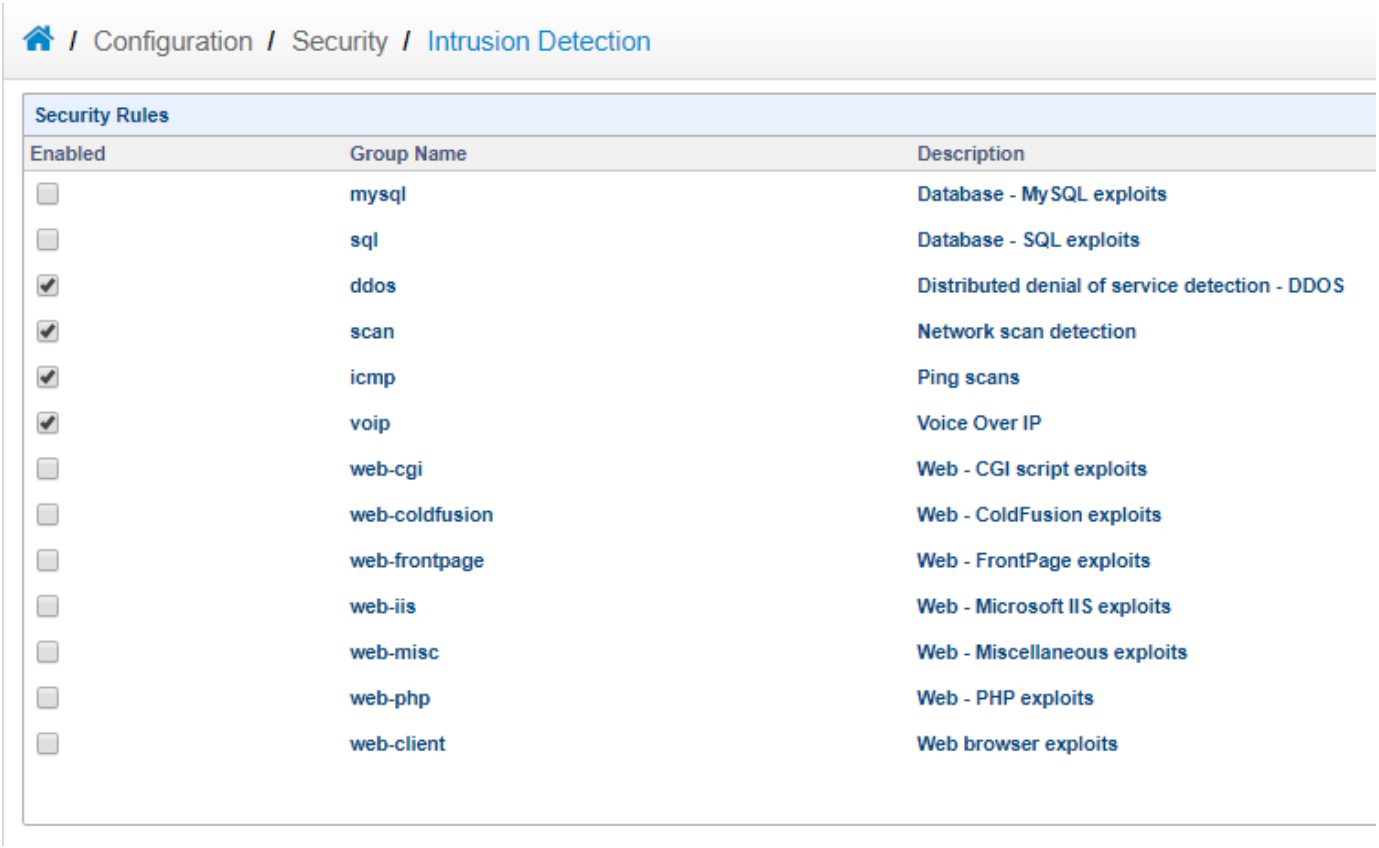
14) Go to **Configuration Signalling SIP Profiles** and Modify the External SIP profile. Then on the following page click Edit. At this point scroll to the bottom and set the Routing Plan to External.



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.

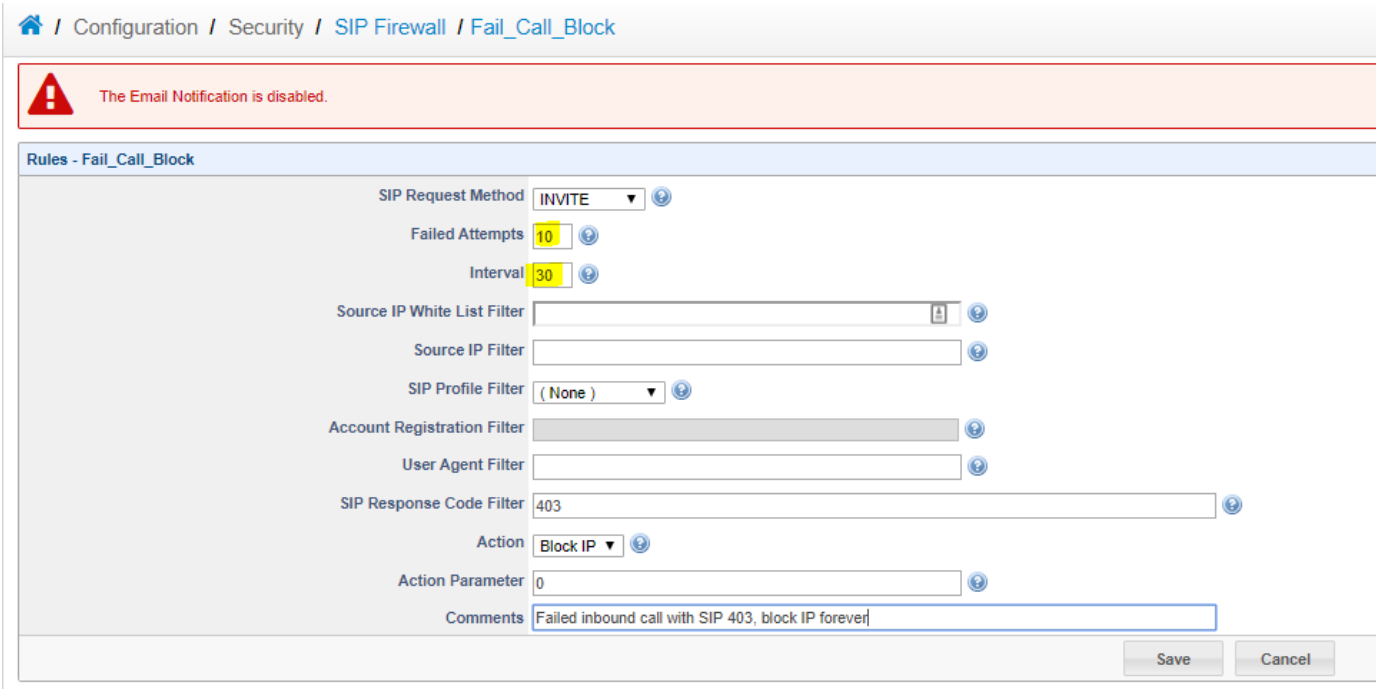


16) To configure the Intrusion Detection or IDS simply go to **Configuration Security Intrusion Detection** and select the following 4 rule groups as shown below. We will be isolating the webUI from the internet, so there is no need for the other rules. Once done click the update button at the bottom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



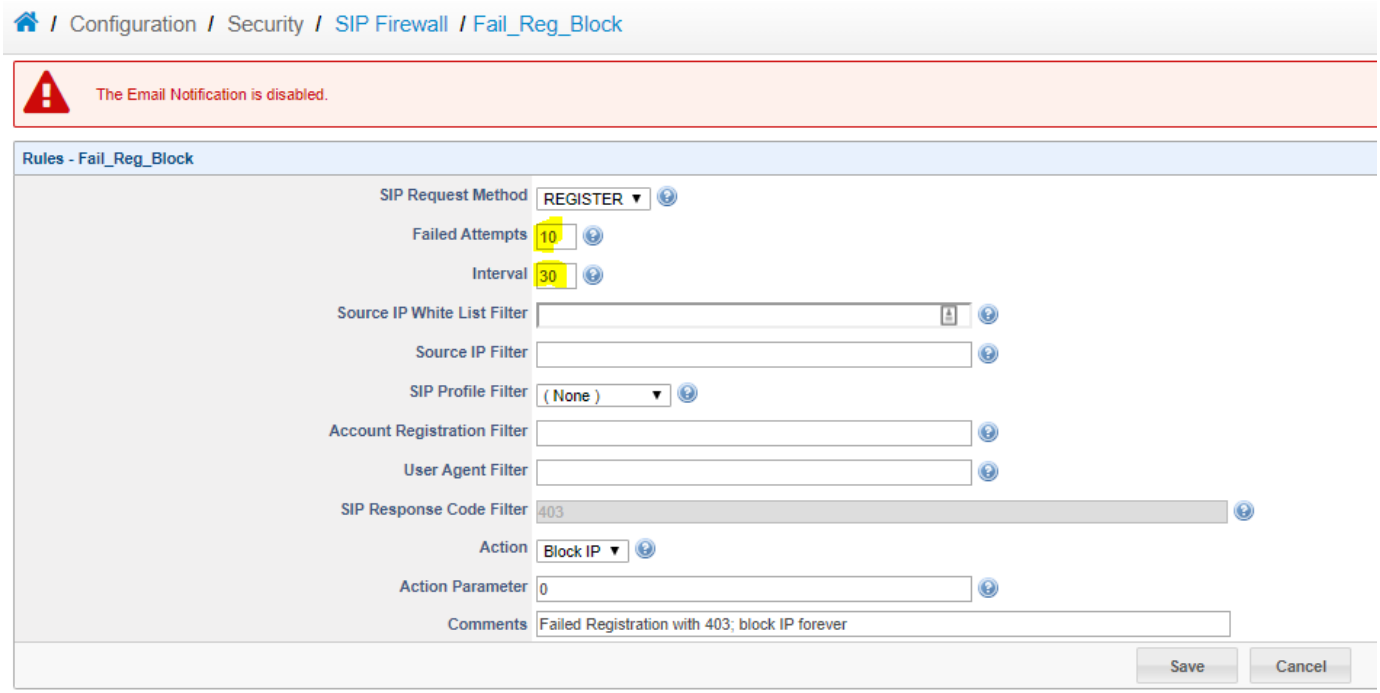
17) Next go to **Configuration Security SIP Firewall** and edit the default rule **Fail_Call_Block**. This rule will block any IP that fails 10 times over a 30 minute period. By default the rule only blocks for 60 minutes, but it is best to change this to forever. To do this change the Action Parameter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

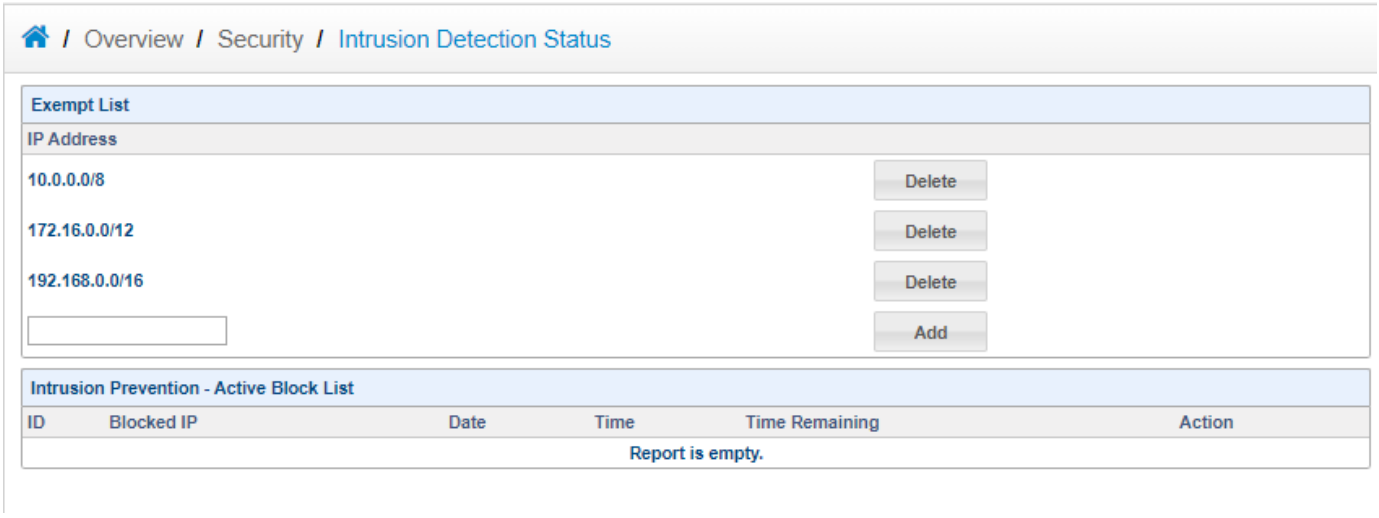


18) Next we need to do the same rule as the previous step, but this time for Registrations. Just as mentioned in the previous step you can white list IPs of known remote sites. Once done save to complete the SIP Firewall setup.

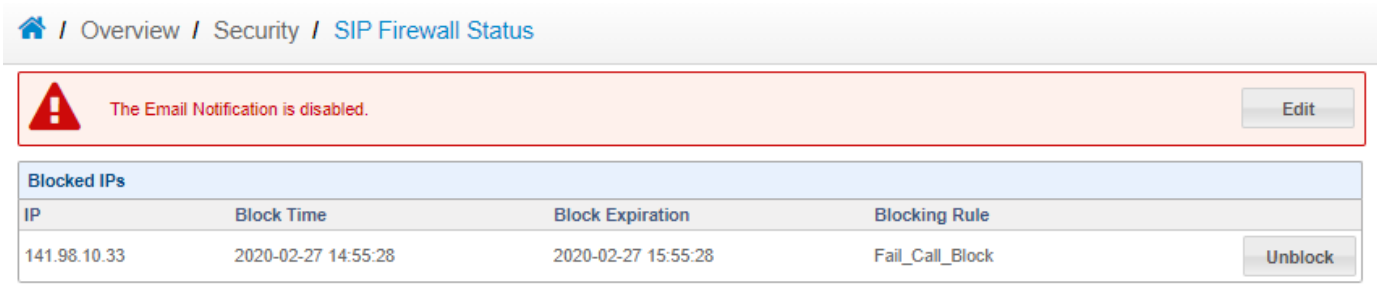
This rule can be adjusted if you find there is too many users being blocked by this. Also note if you have multiple phones a remote site, the block can take down the whole site. To avoid this, put any known remote site IPs in the "Source IP White List Filter", and separate the IPs by commas if there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



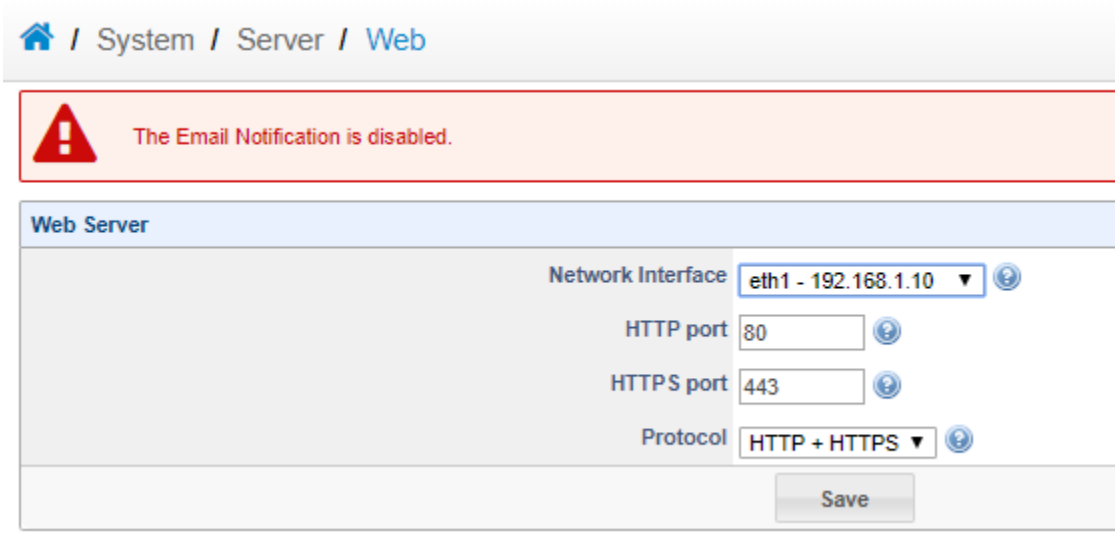
19) If you do have an IP blocked by the IDS you can go to **Overview Security Intrusion Detection Status** to see if its blocked. It will be shown at the bottom there, and you will have the ability to unblock the IP. You can also add known IPs to the Exempt list so the IDS doesn't block them. Keep in 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.



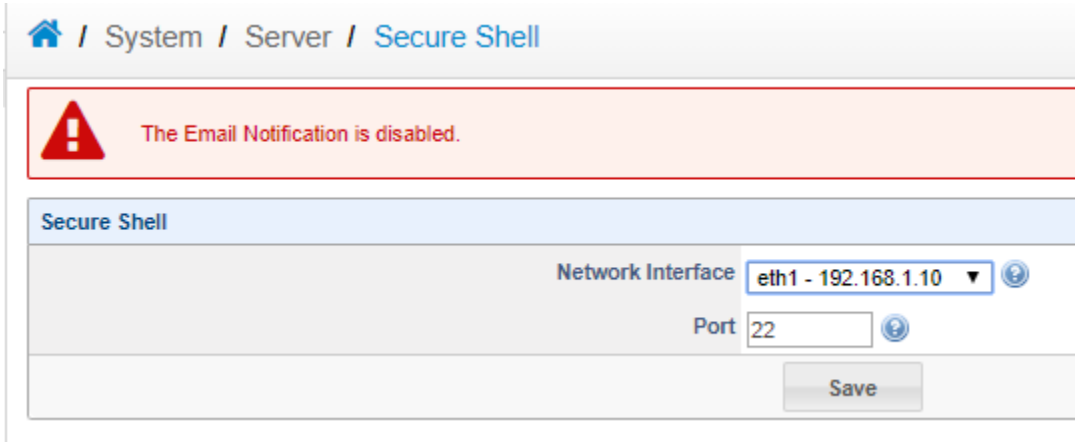
20) If the IP isn't blocked by the IDS, then it can be blocked by the SIP Firewall configured in steps #17/18. If the IP is blocked you will see it in the list as shown below. You can unblock the IP by pressing the unblock button.



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.



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



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.