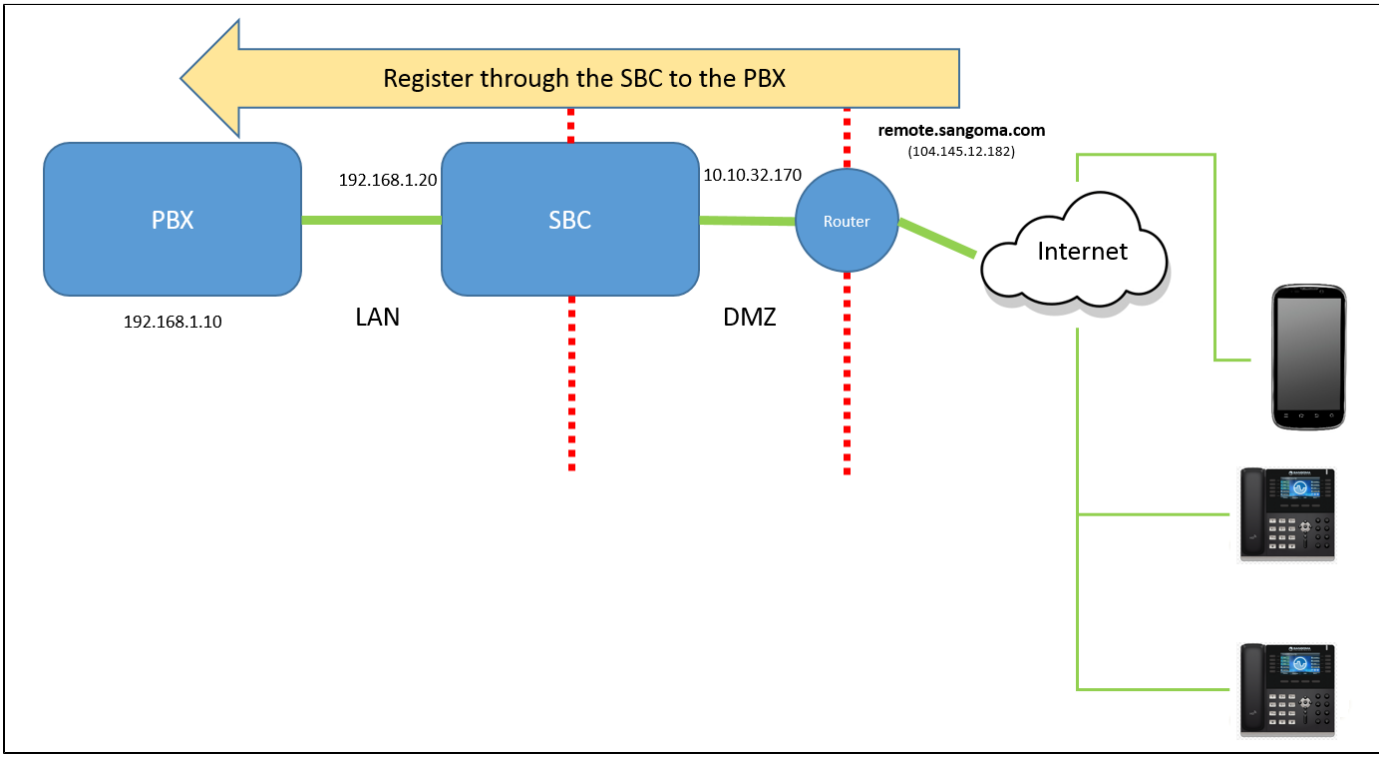
Remote Phone Support

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 scenaro 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.

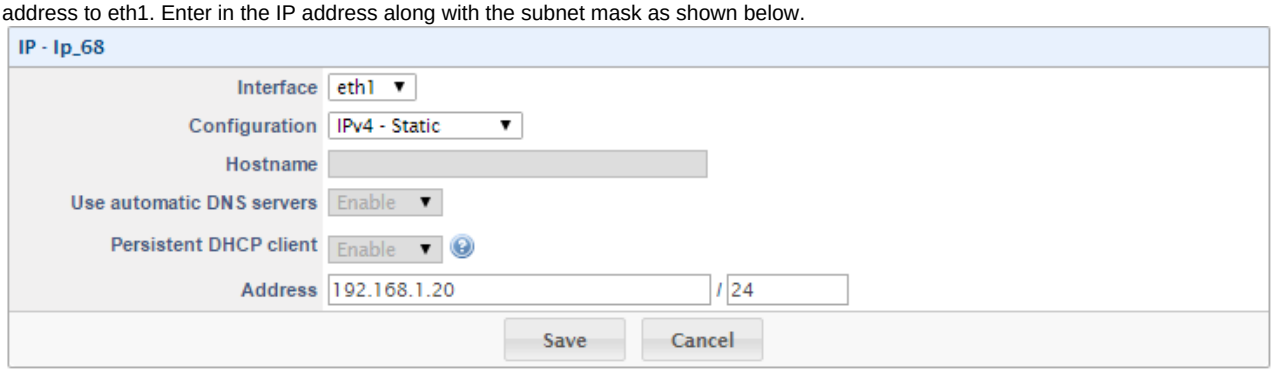


PBX IP: 192.168.1.10
SBC LAN IP: 192.168.1.20
SBC DMZ IP: 10.10.32.170
SBC Public IP: 104.145.12.182
SBC FQDN: remote.sangoma.com

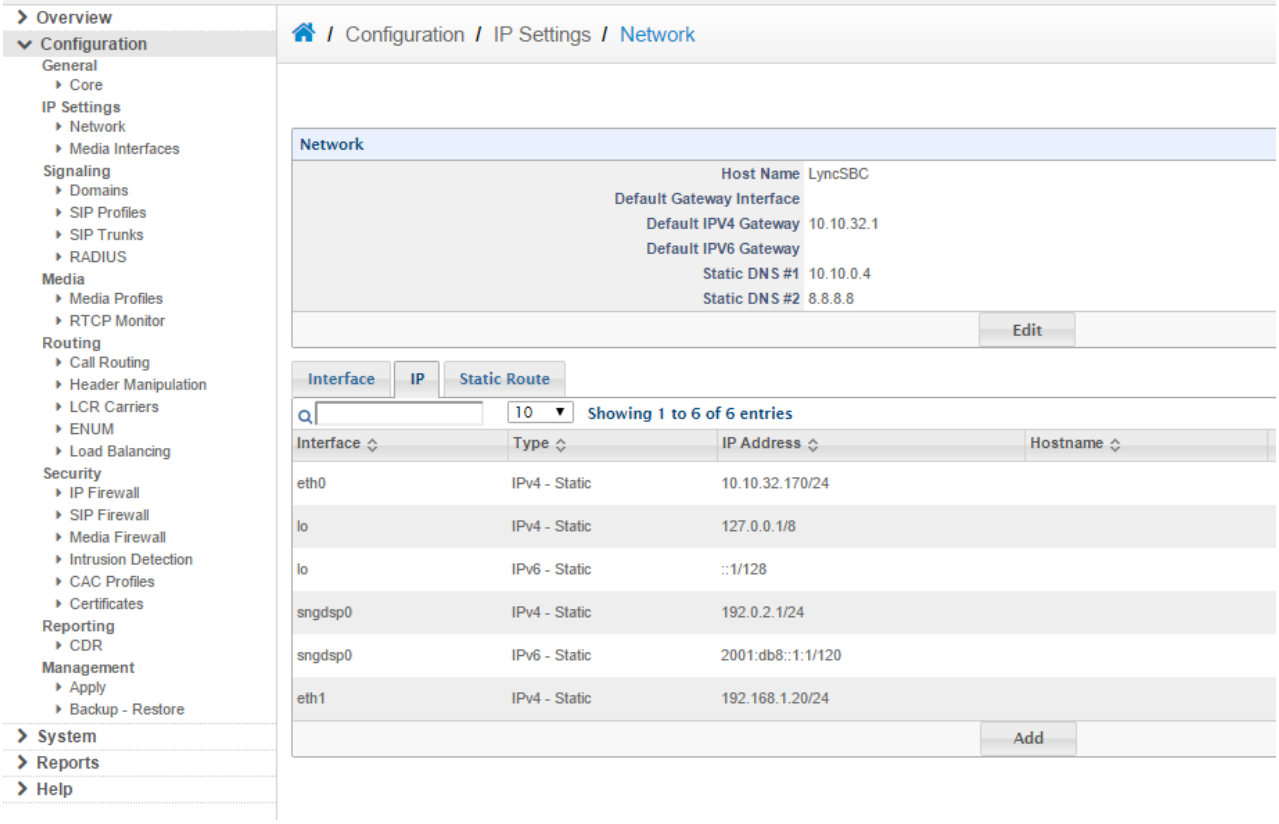
---

1) Network Setup

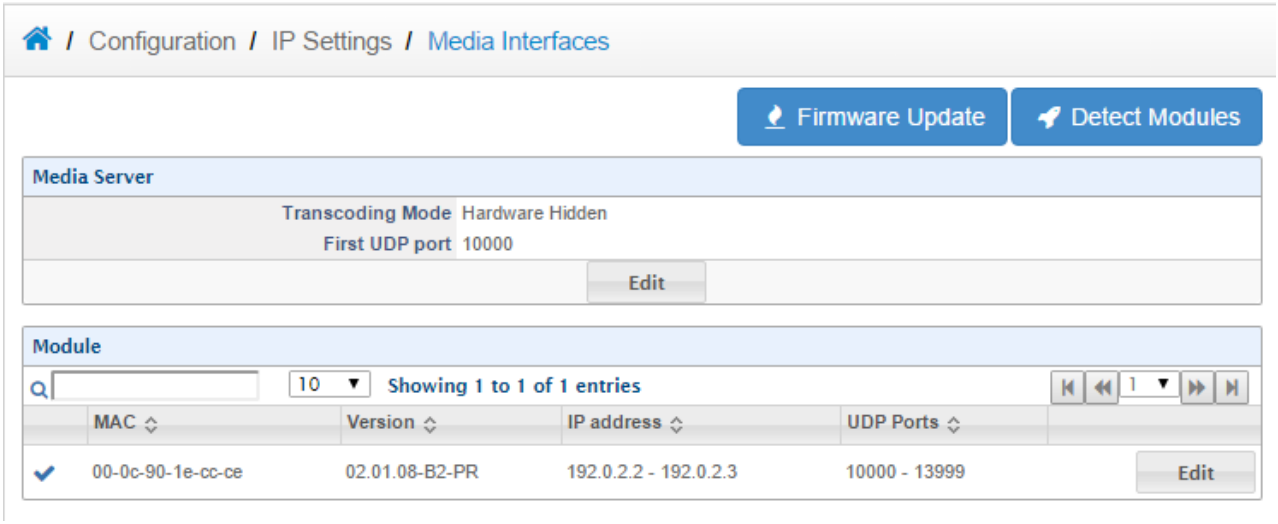
1. Go to Configuration->IP Settings->Network and then edit eth0 and assign the DMZ IP address. Next click the Add button to add an IP address to eth1. Enter in the IP address along with the subnet mask as shown below.



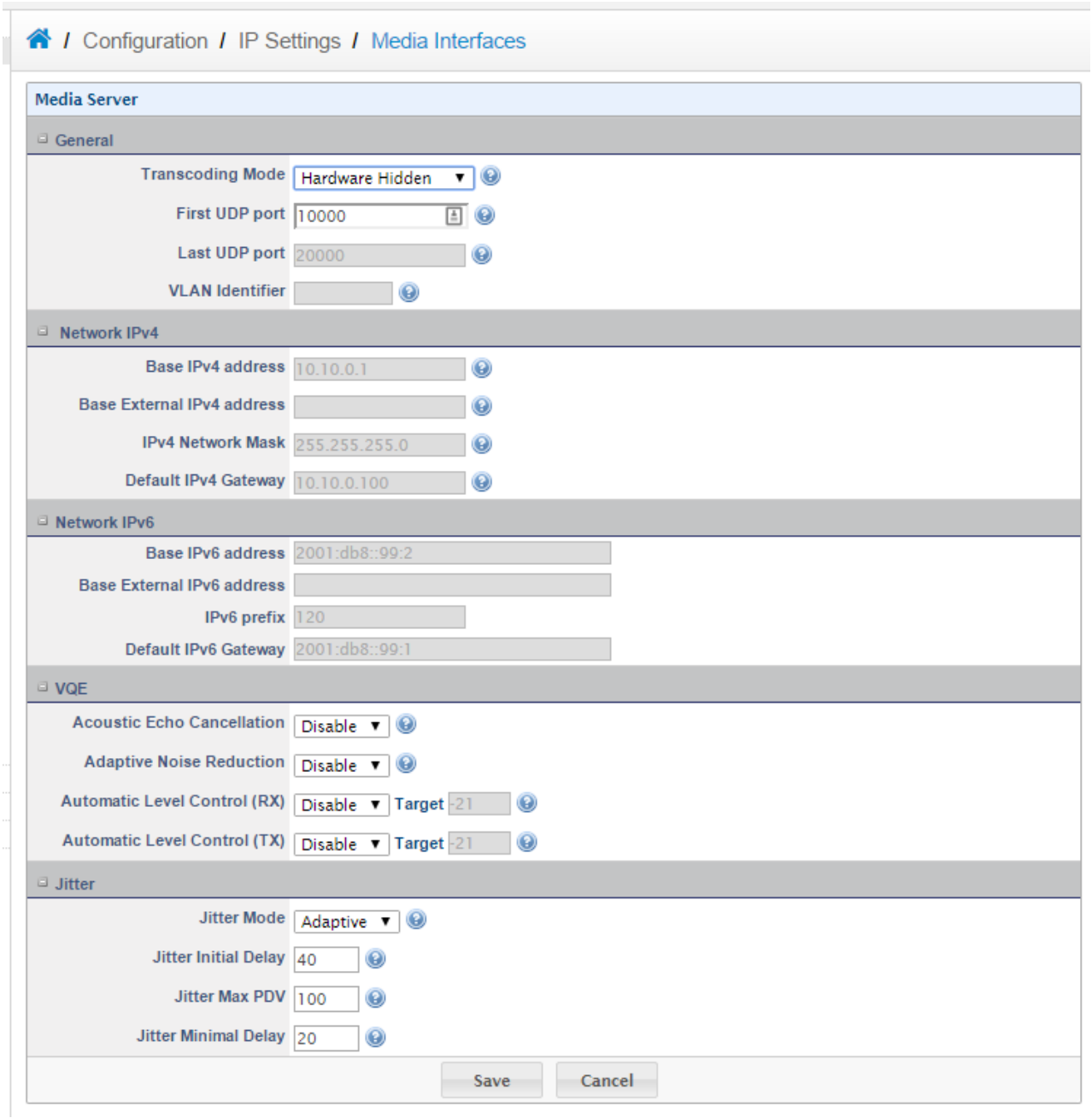
2. Once completed you will now have an IP address on eth0 and eth1.



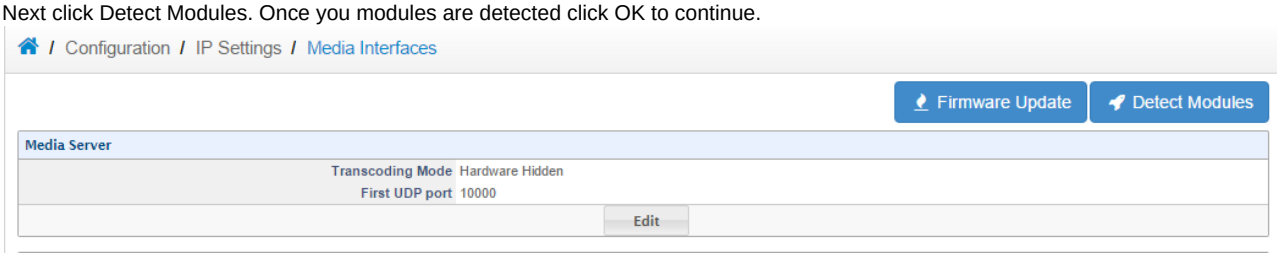
3. Next go to Configuration -> IP Settings -> Media Interfaces and click Edit.



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

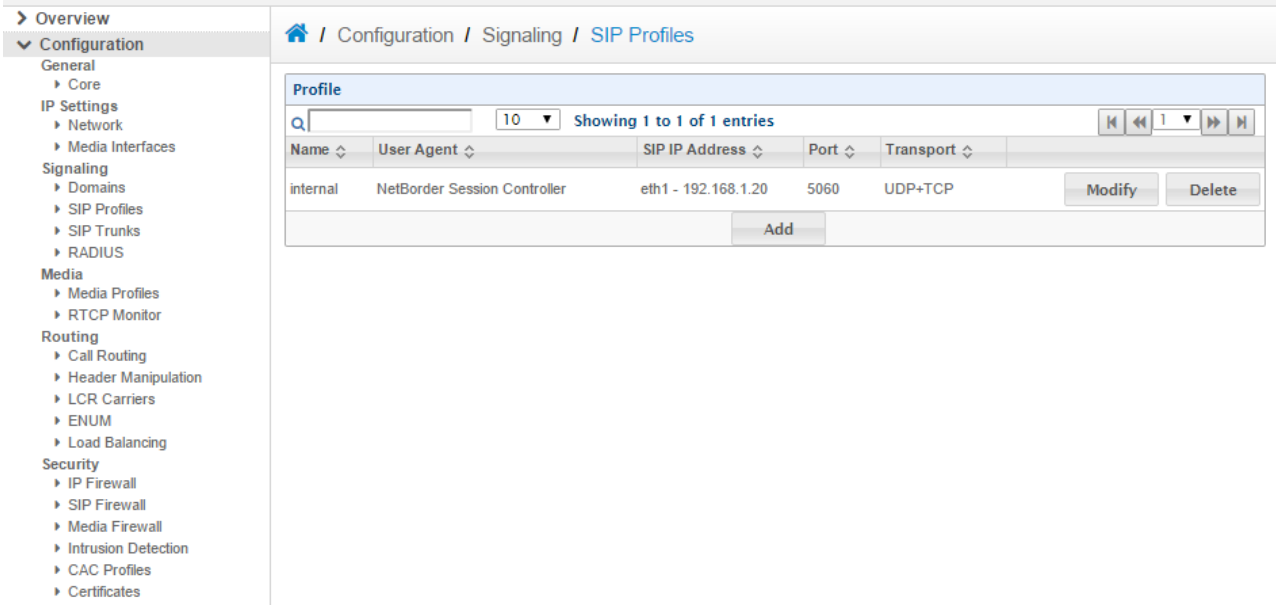


5. Next click Detect Modules. Once you modules are detected click OK to continue.

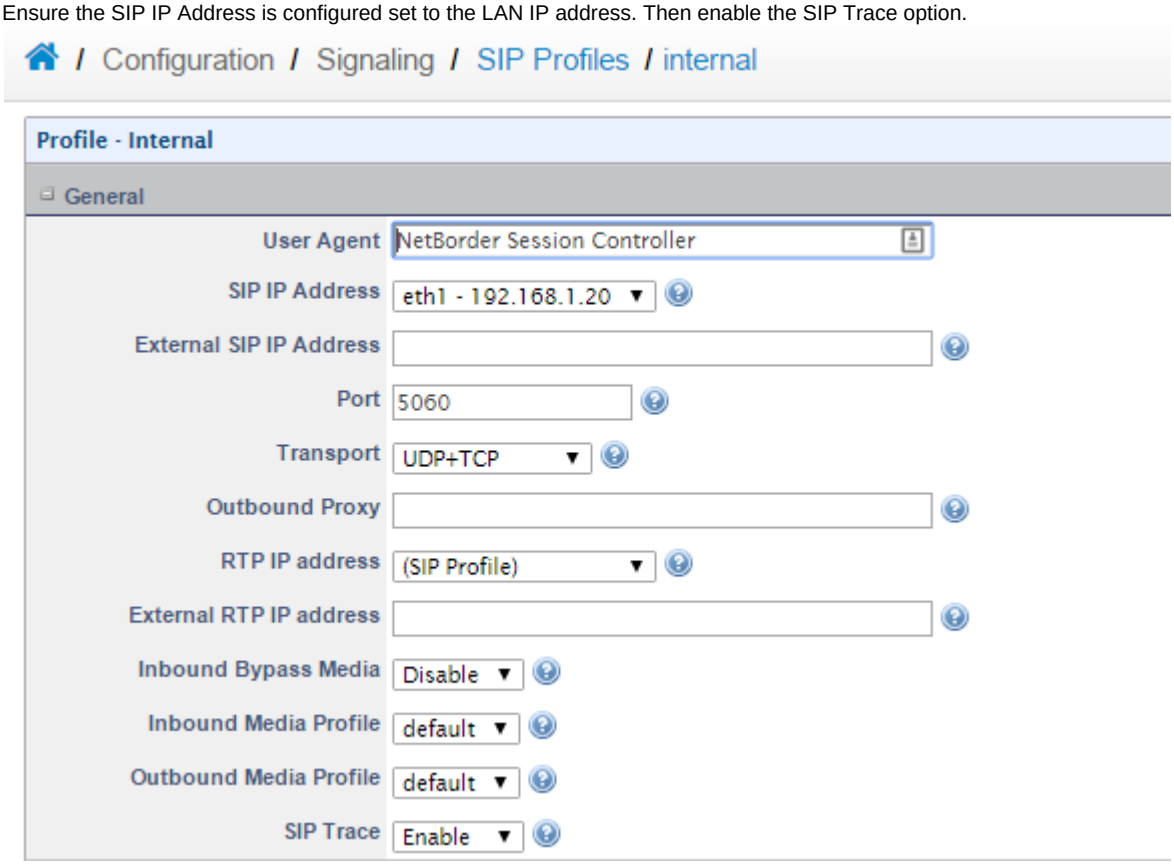


2) SIP Profile Configuration

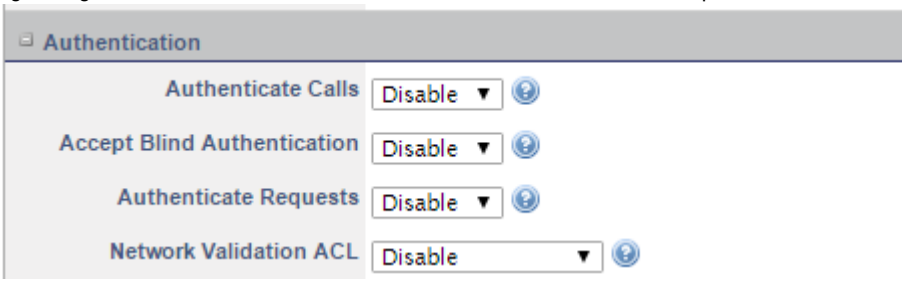
1. Go to Configuration -> Signaling -> SIP Profiles and click Modify next to the default internal SIP profile.



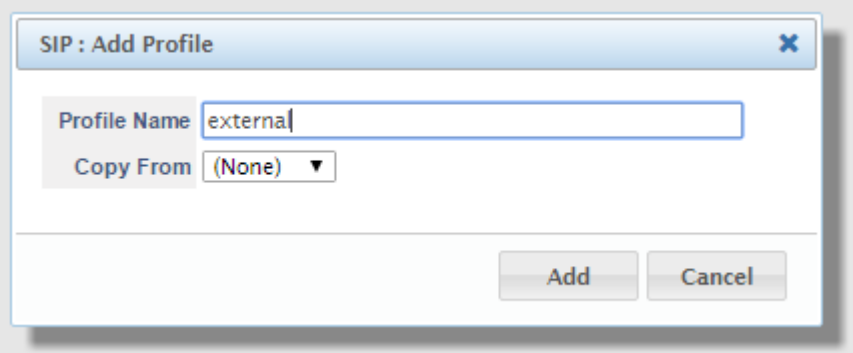
2. Ensure the SIP IP Address is configured set to the LAN IP address. Then enable the SIP Trace option.



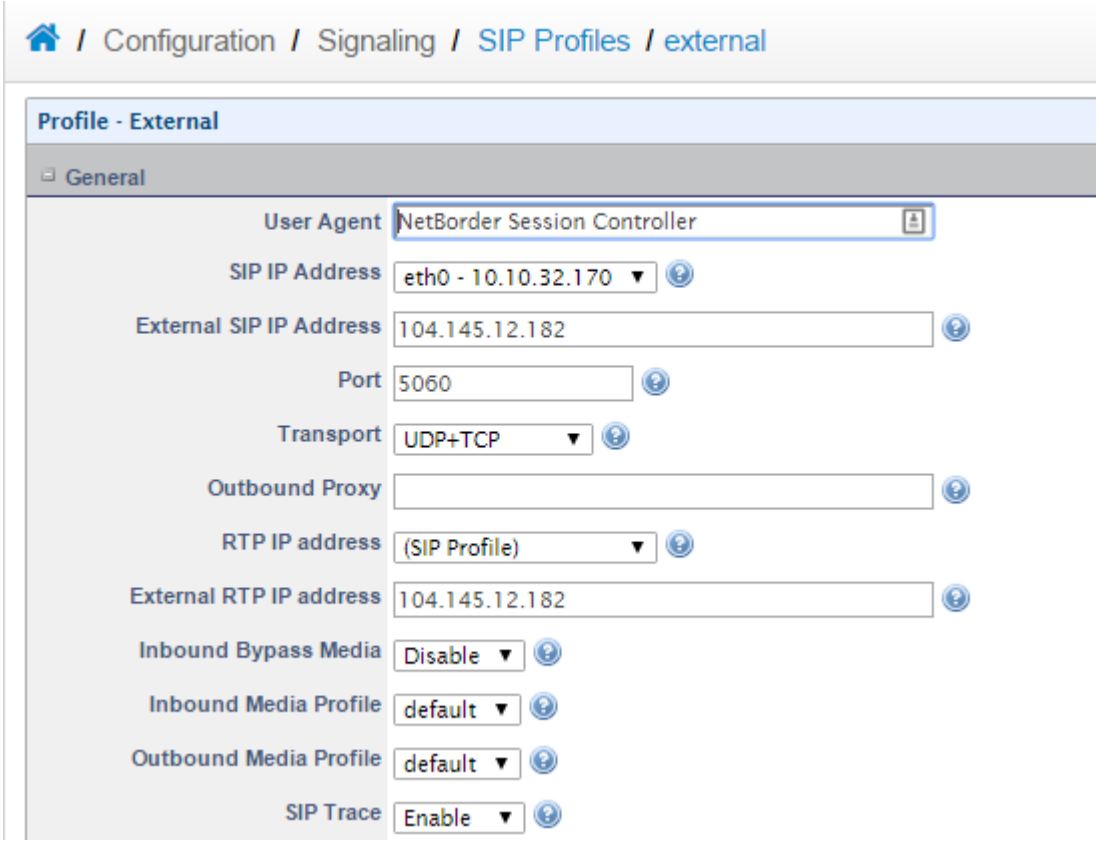
3. Next scroll down to the Authentication section and disable Authenticate Calls. This option is only required when remote phones are registering to a local SIP account on the SBC. Once done save the internal profile.



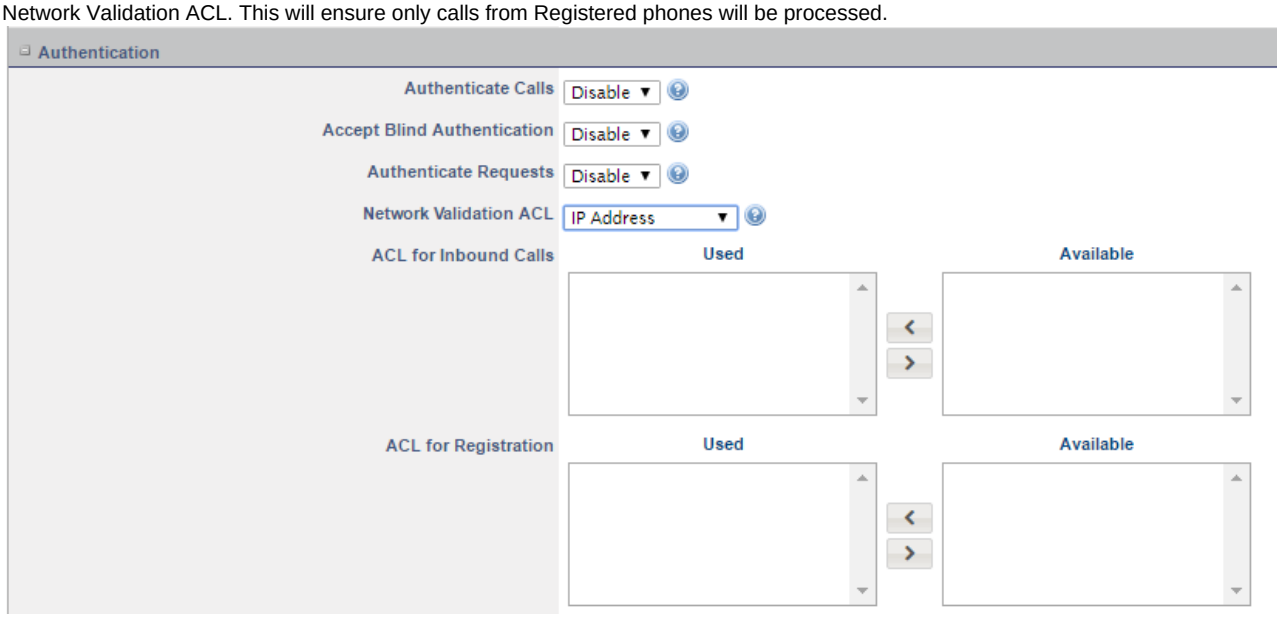
4. Next add a new profile called external.



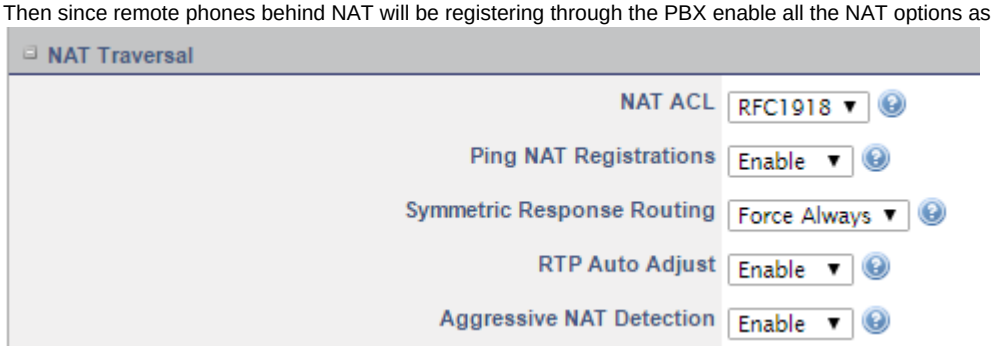
5. In the External SIP profile set the External SIP IP Address and External RTP IP Address to the public IP. As well enable the SIP Trace option.



6. 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.



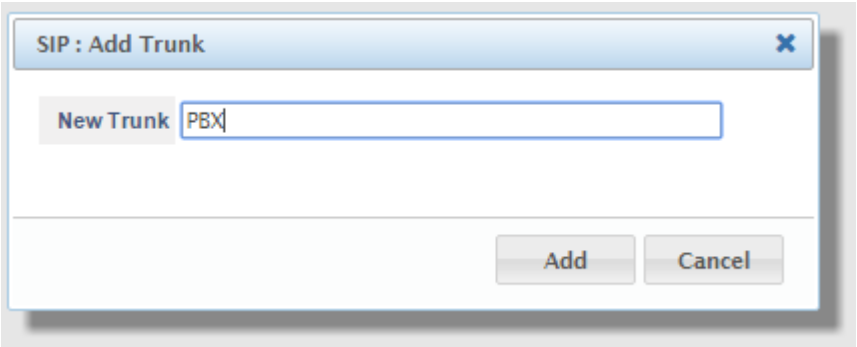
7. Then since remote phones behind NAT will be registering through the PBX enable all the NAT options as shown below.



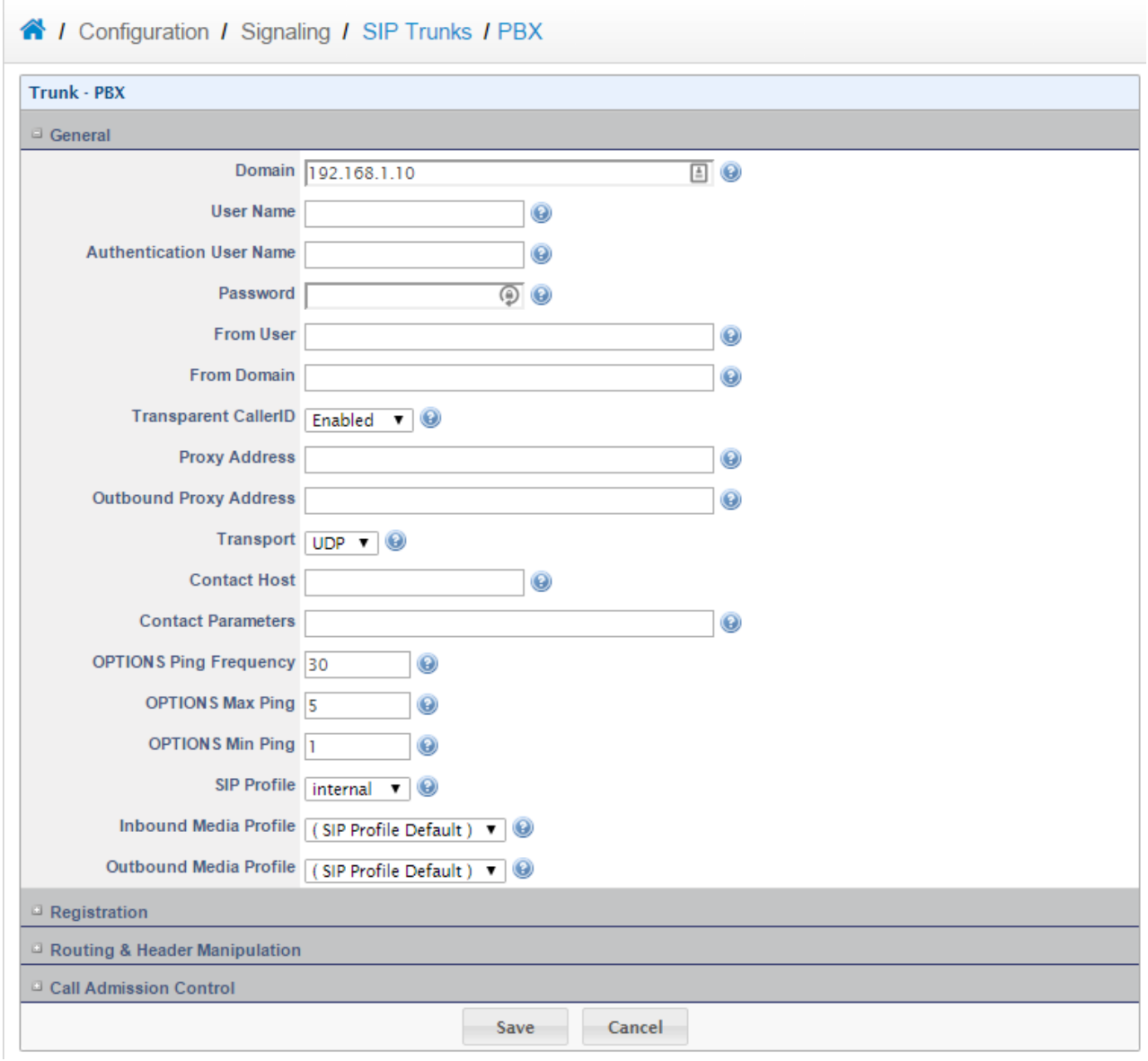
---

3) Adding SIP Trunk to PBX

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

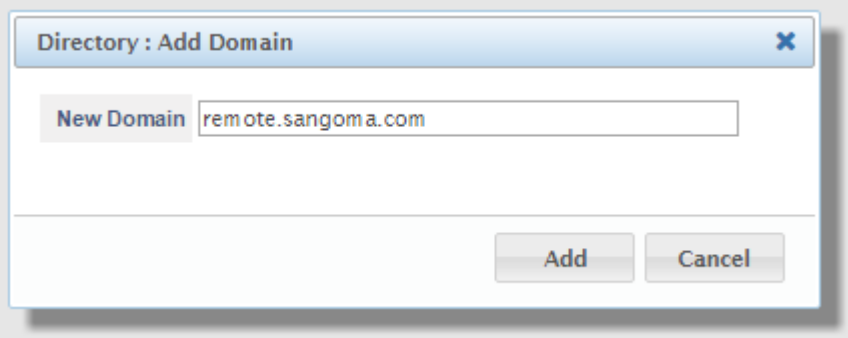


2. Set the Domain to be the IP address of the PBX. Enable OPTIONS by setting the Frequency and Max/Min Pings as shown below. Once done click Save.

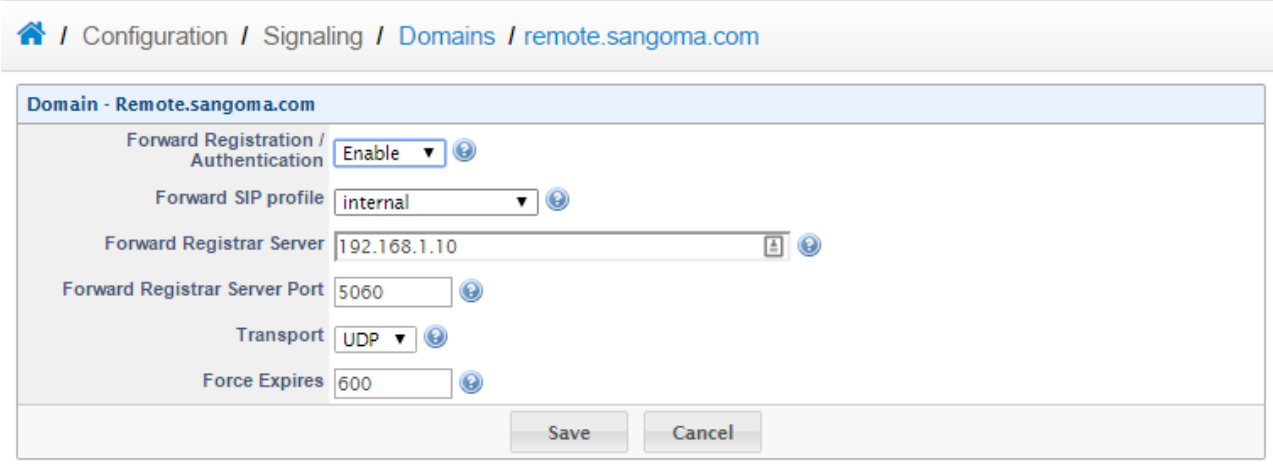


4) Configuring the SIP Domain

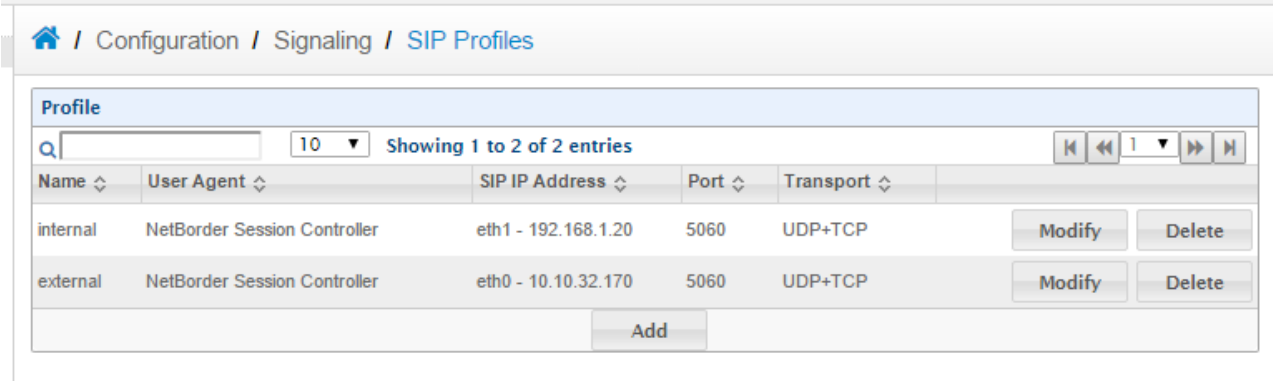
1. Go to Configuration -> Signaling -> Domains and click Add. Set the name of the domain to the FQDN or IP the remote phones will be registering to.



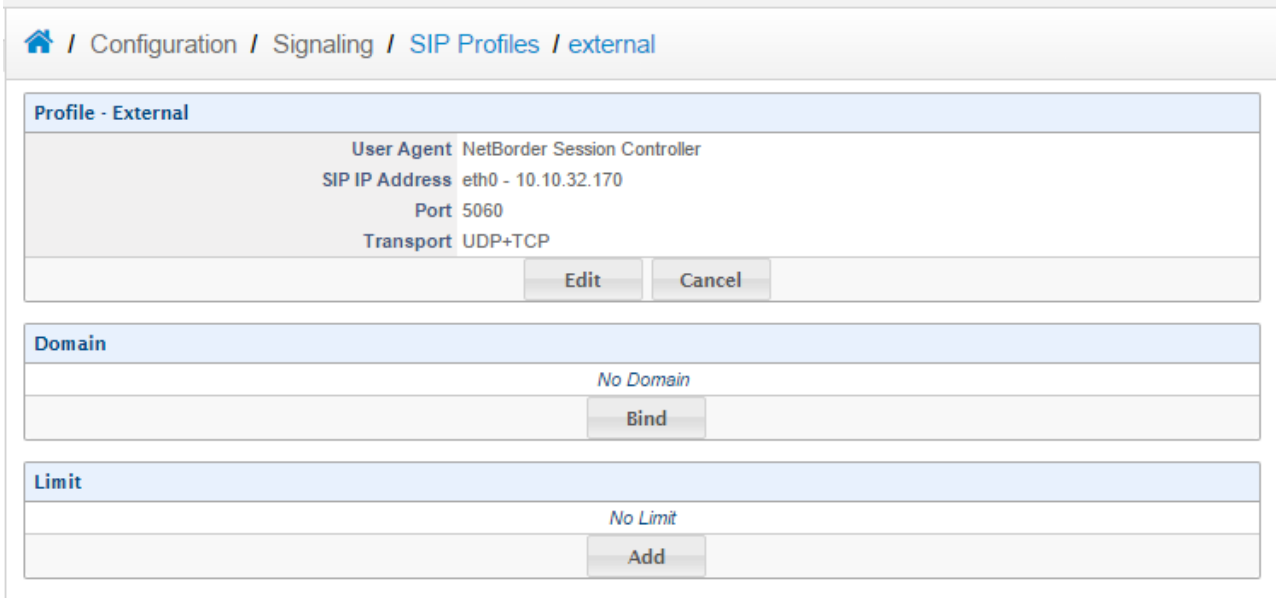
2. Next enable Forward Registration/Authentication as shown below. Set the Forward SIP profile to Internal. Then it is recommended to Force the Expires time to around 300-600 seconds; this will force the phones to register every 5-10 minutes. The short time period will ensure the registration information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



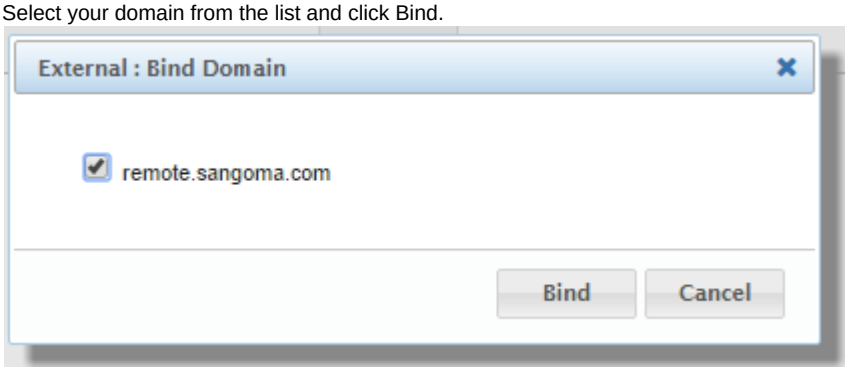
3. Next go to Configuration -> Signaling -> SIP Profiles and click Modify on the External SIP Profile.



4. Then click Bind under the Domain section.



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

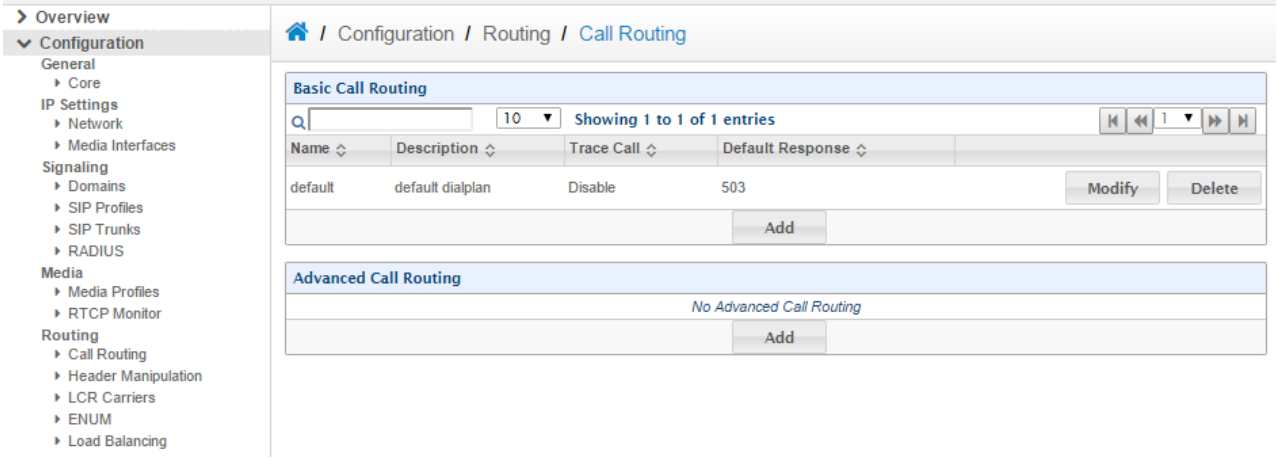


6. Your domain will now be bound to the SIP profile. This will allow Remote phones to register to your External SIP Profile.

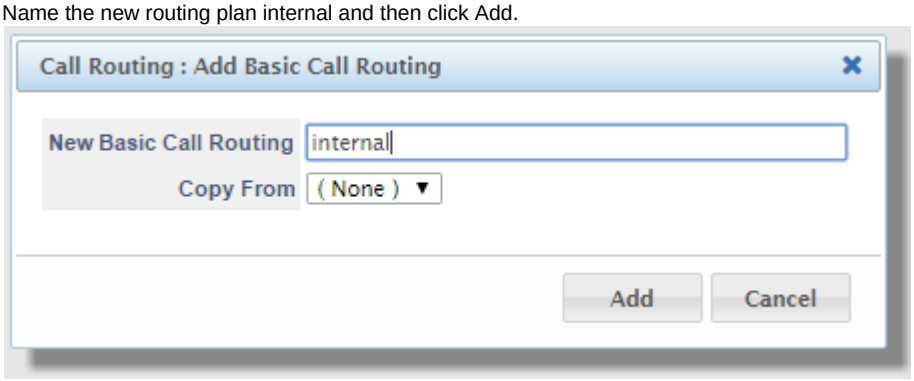
---

5) Configuring the Call Routing

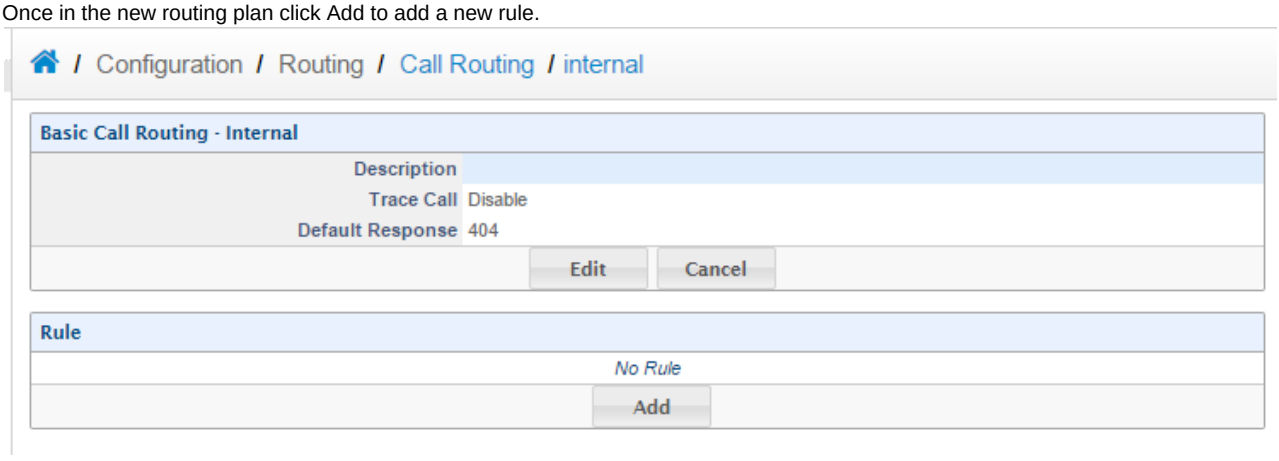
1. Go to Configuration -> Routing -> Call Routing and then click the Add button in the Basic Call Routing section to add a new routing plan.



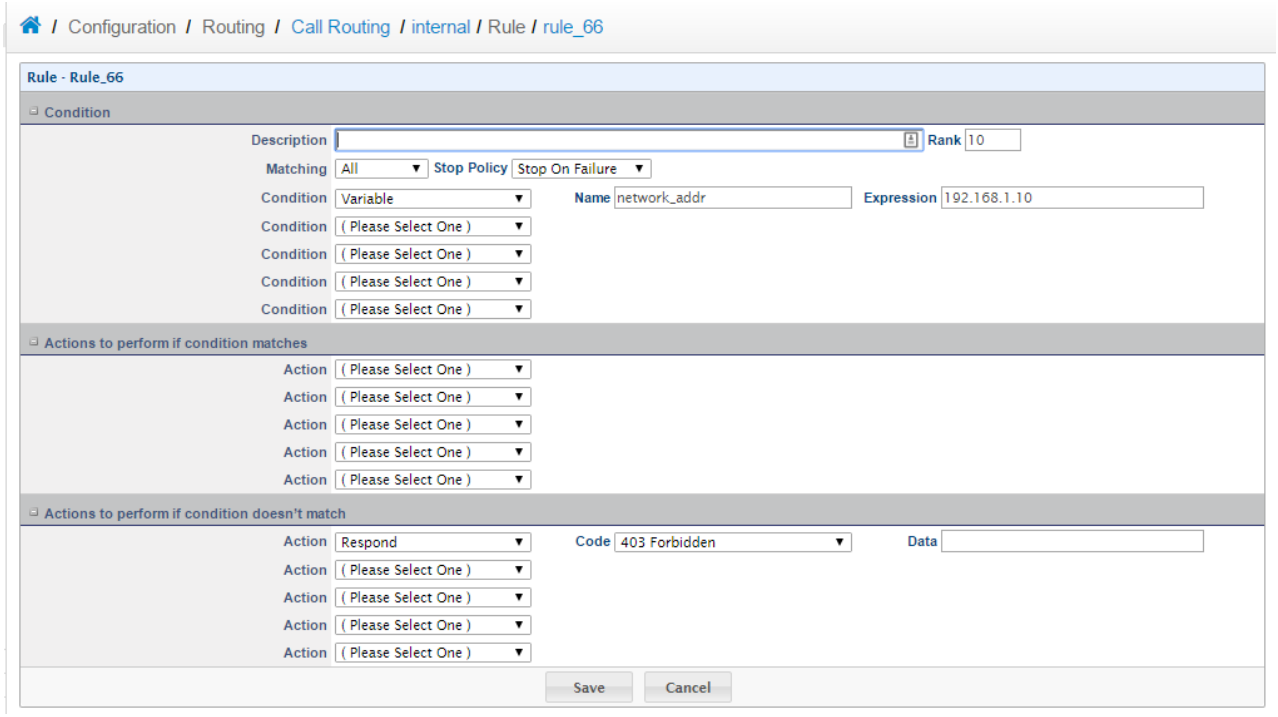
2. Name the new routing plan internal and then click Add.



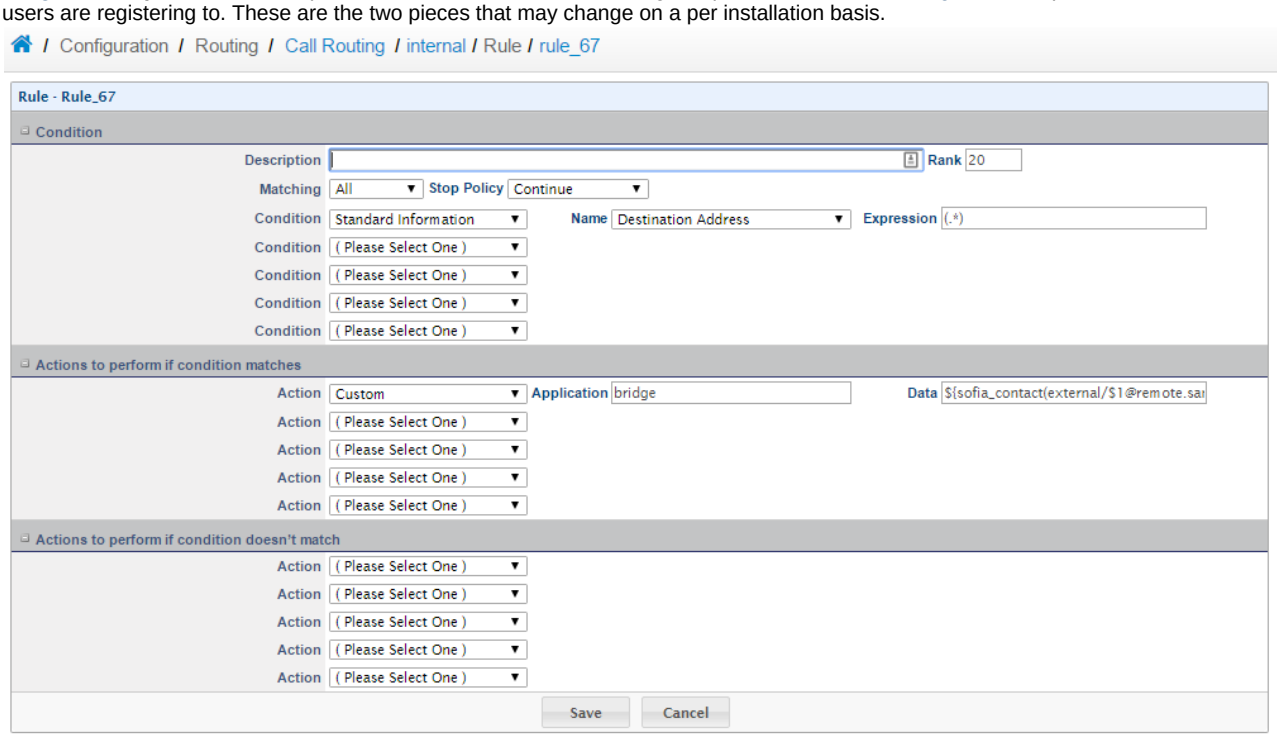
3. Once in the new routing plan click Add to add a new rule.



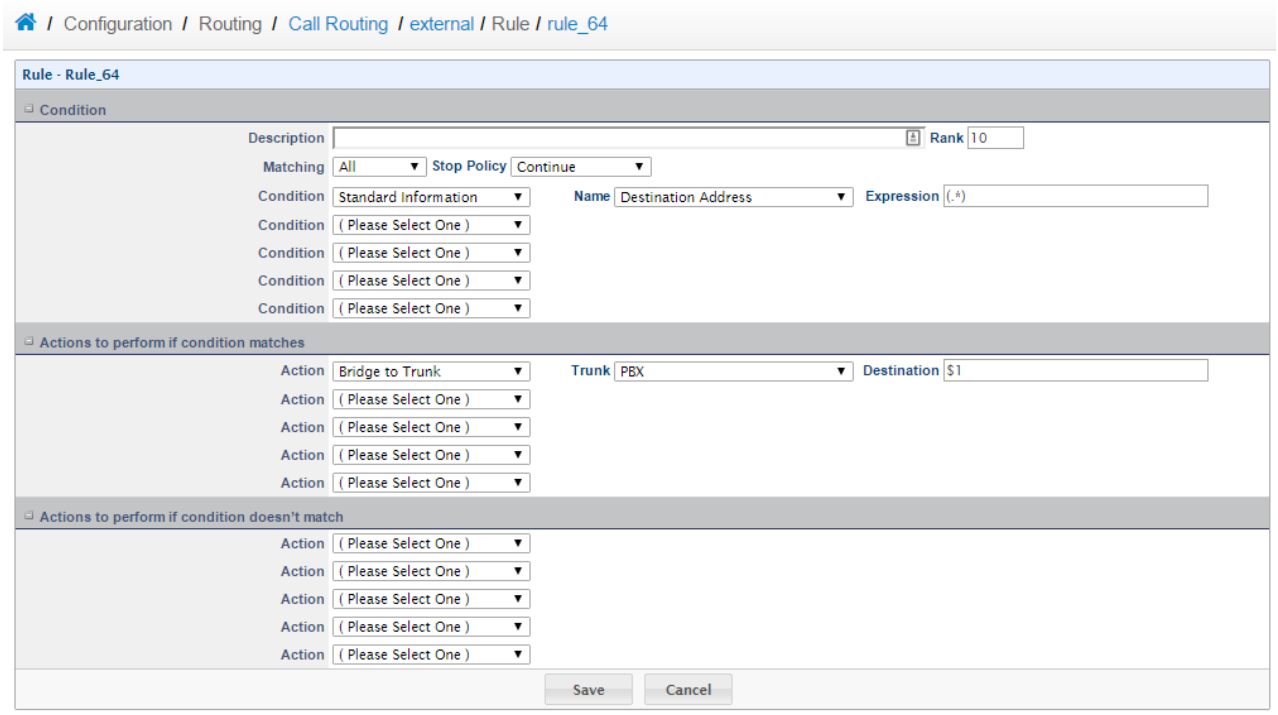
4. In the new rule change the stop policy to Stop On Failure. Add the condition below to verify all internal calls orginate from the PBX's IP address. To do this use the network_addr variable as shown below. Ensure the actions to perform if the condition doesn't match is set to respond with a 403. Once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



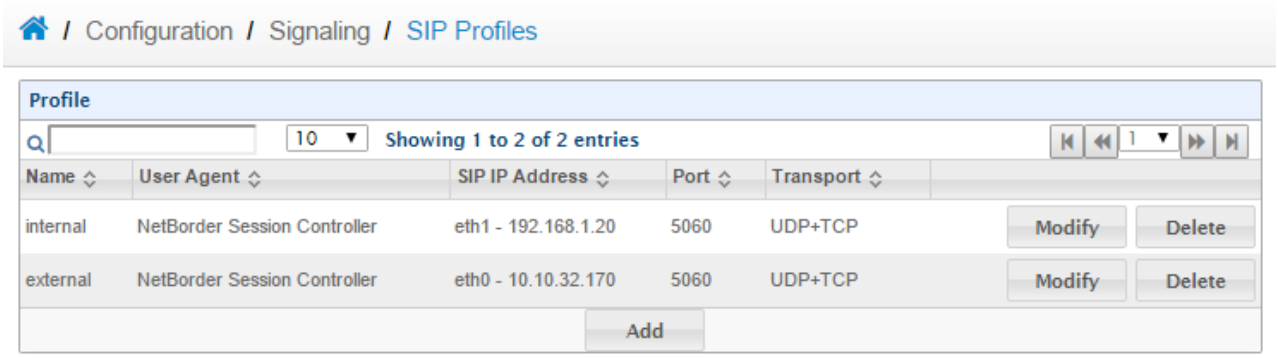
5. Next click Add to add a new rule. In the new rule set the condition based off the Destination Address. The condition will be (.*). The action will need to be a custom action and the application will be bridge. The data will be **${sofia_contact(external/$1@remote.sangoma.com)** . The "external" part 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.



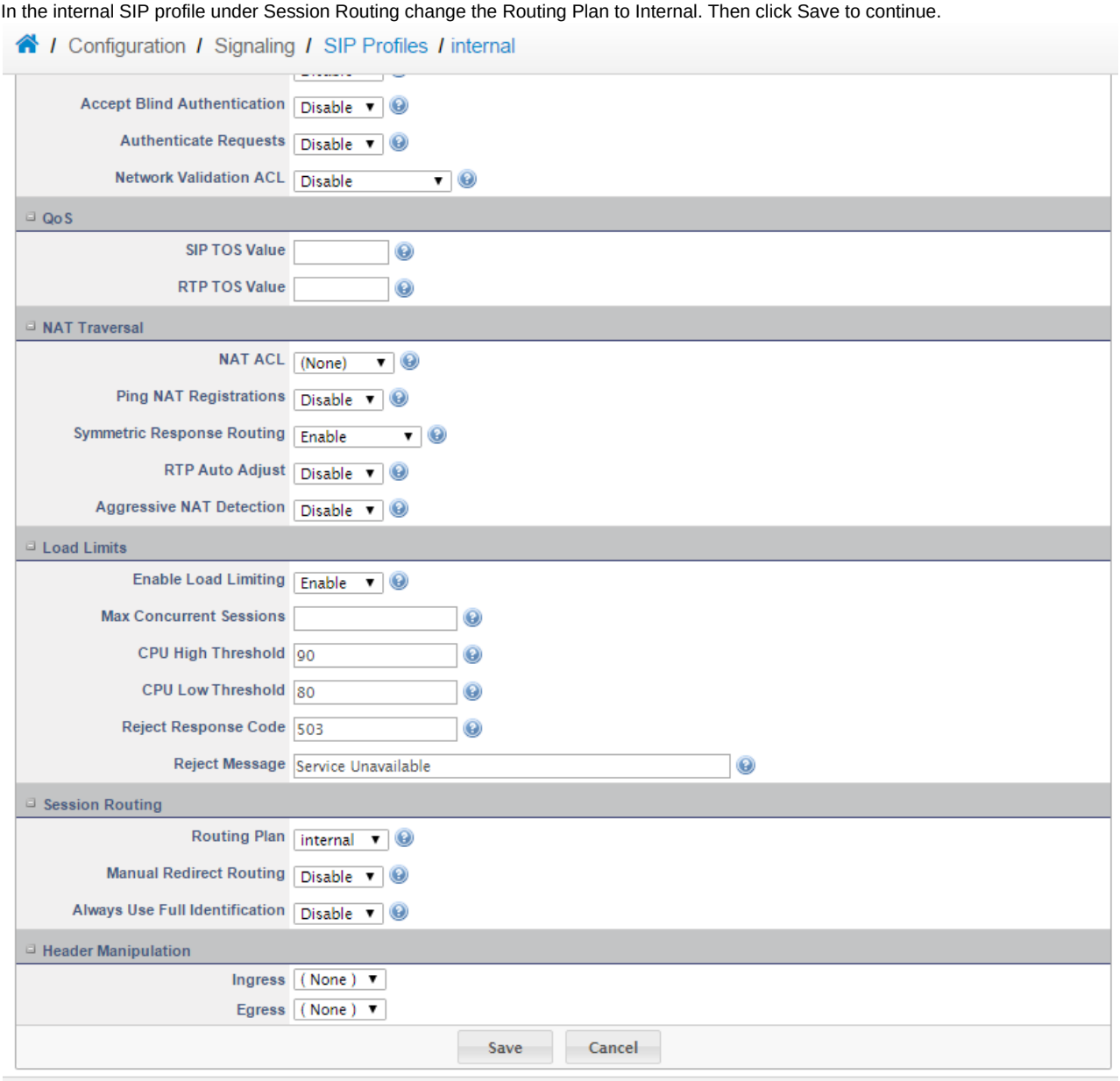
6. Next go back to the call routing and add a new routing plan as we did in step 1-2 above. Name the new routing plan external. This will be used for the external SIP profile. In the new routing plan add only one rule. The condition will be (.*) and based on the Destination Address. Then the action will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



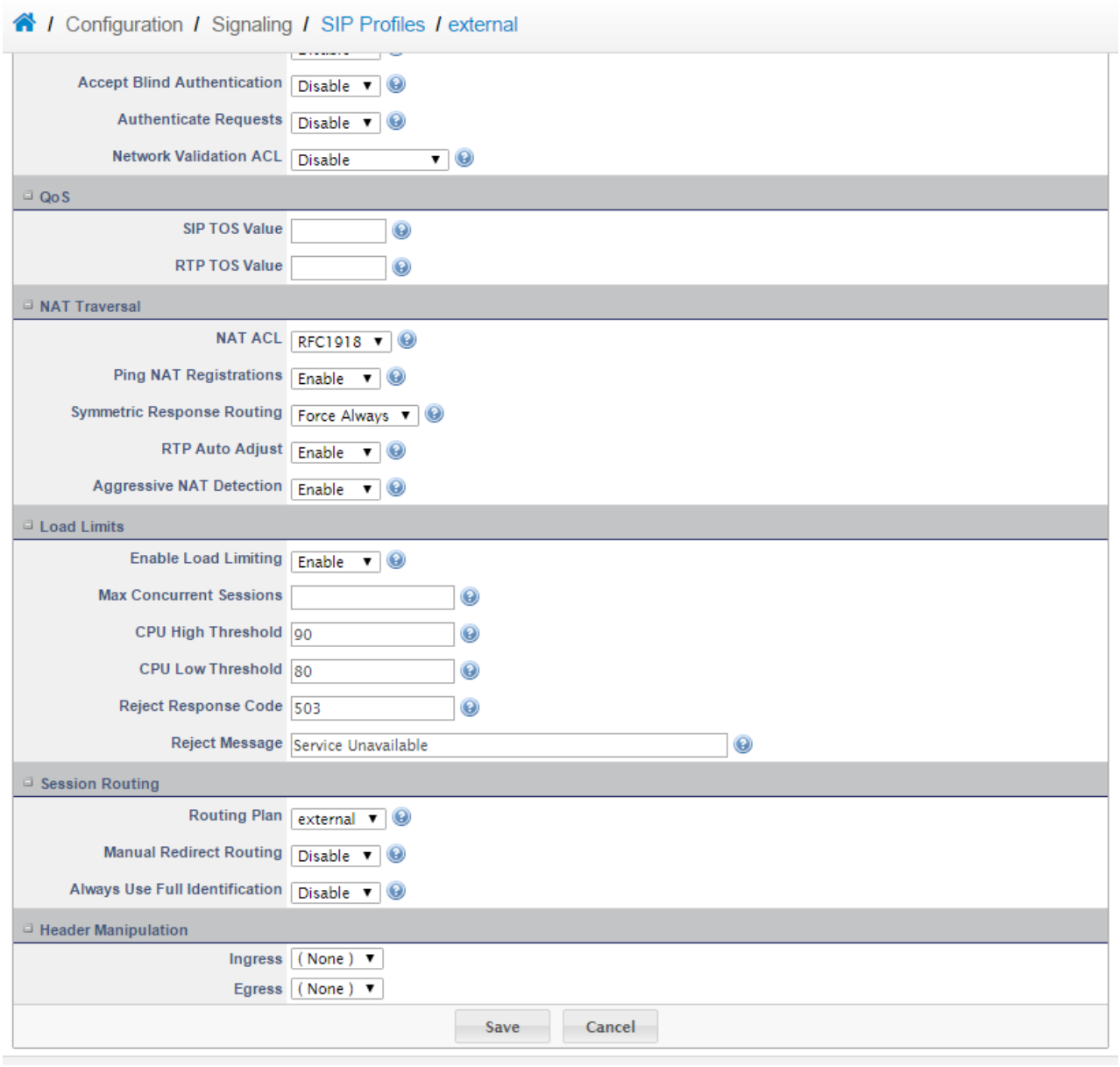
7. Now that both routing plans are made go to Configuration -> Signaling -> SIP Profiles and modify the internal SIP profile.



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



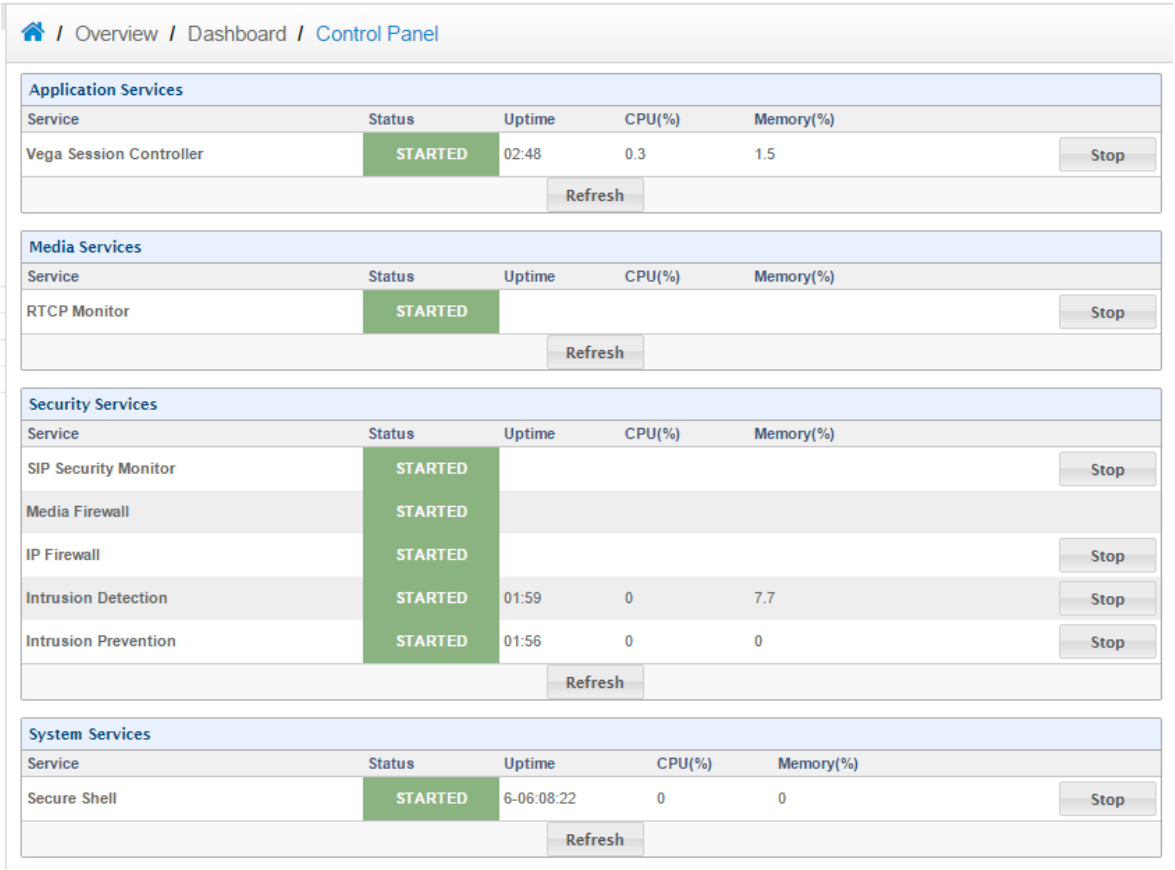
9. Next go back to Configuration -> Signaling -> SIP Profiles and this time click Modify next to the External SIP profile. Once in the External SIP profile, go to the Session Routing section and change the Routing Plan to External. Then click Save.



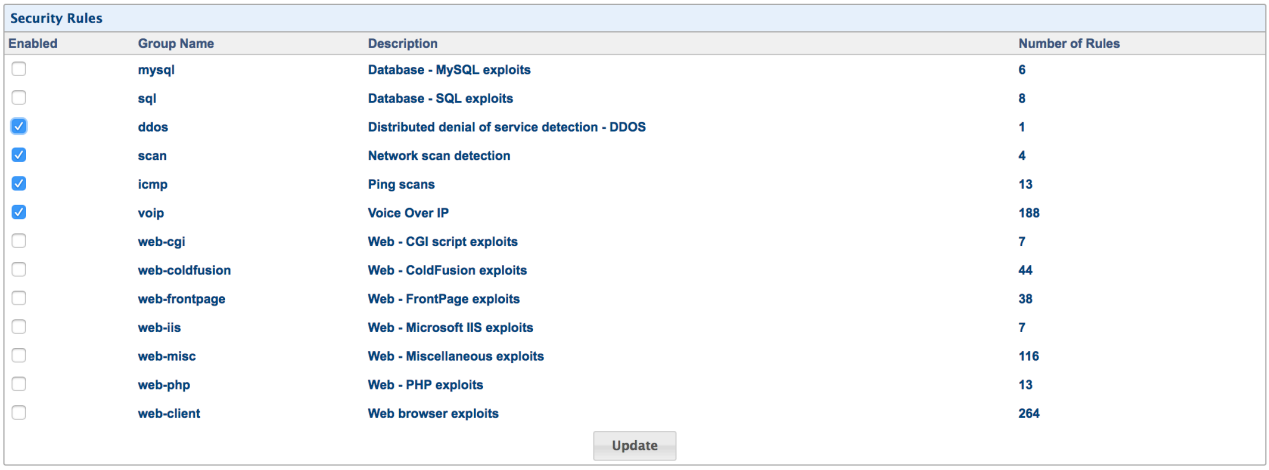
6) Finalizing the Installation

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

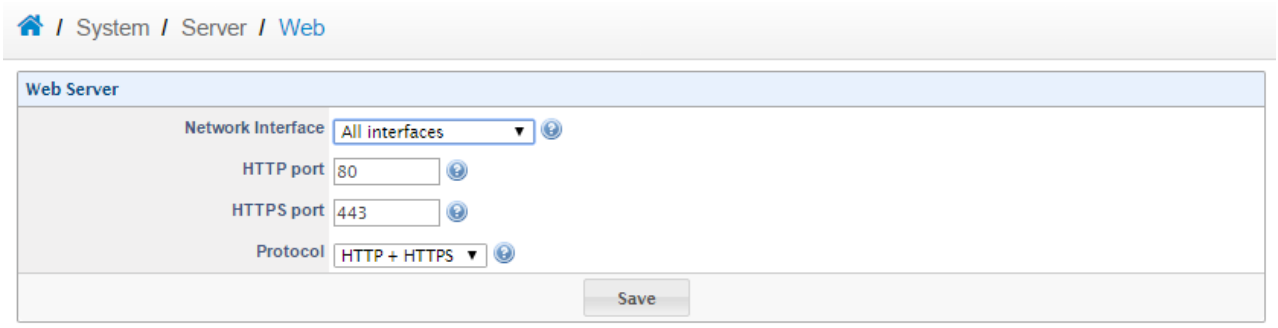
4. Intrusion Prevention



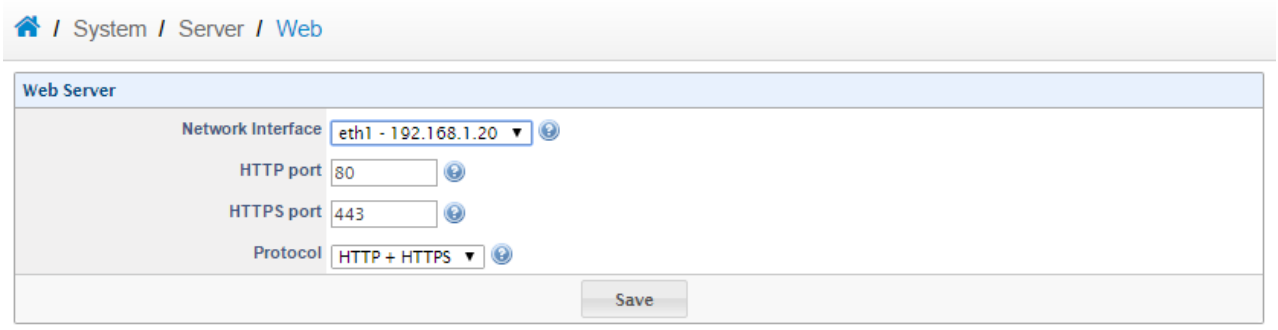
2. Enable ddos, scan, icmp and voip IDS rules rules by going to Configuration -> Security -> Intrusion Detection and ensuring all are checked. Once done click Update to apply the changes.



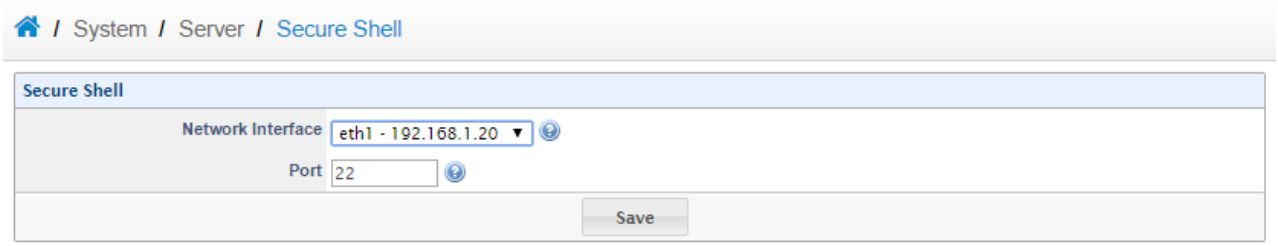
3. Next go to System -> Server -> Web and change the Network Interface from All interfaces to only the internal network interface.



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



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