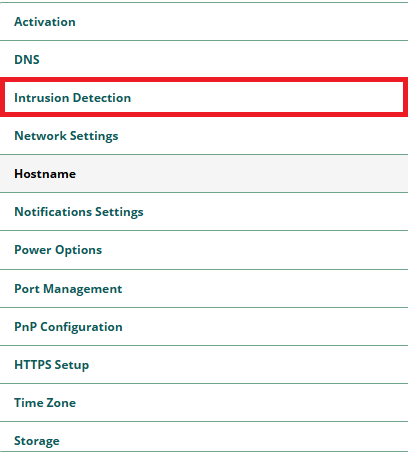
Как настроить Intrusion Detection, он же IP Tables, он же Whitelist в freePBX ?

Заходим в Admin – System Admin – Intrusion Detection.



10) Настроим **Intrusion Detection,** он же **IP Tables**, он же **Whitelist**.

*Данная штука очень полезна, она помогает защититься от спам-траффика, или брутфорс-атак.*

*Также, сюда имеет смысл добавить доверенные сети и IP адреса, точечно.*

Status всегда должен быть **running**

Также можно совершать перезагрузку (Restart)

Ban Time: 86400 (сутки) – время, в течении которого IP адрес будет забанен (указывается в секундах)

Max Retry: 8 - это количество попыток при подключении к АТС, которое пользователь сможет осуществить в течении параметра Find Time (ниже)

Find Time: 600 (секунд)  
*То есть, в течении 10 минут (600 сек.) нам дают 8 попыток. Если неправильно – мы попадаем в бан.*

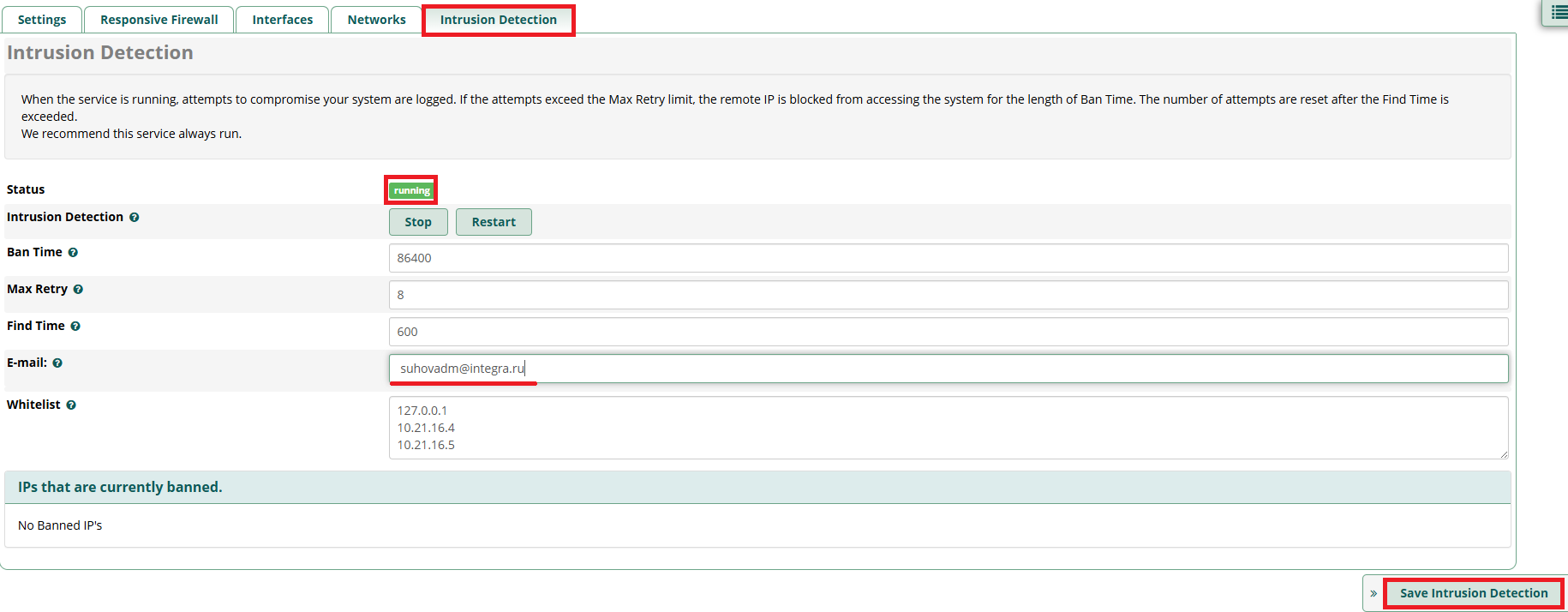
E-mail:

*сюда пишем свой e-mail. Если в бан будет добавлен какой-то подозрительный адрес, на e-mail сразу же придёт уведомление.*

Whitelist:

*Сюда полезно заранее занести шлюзы, подсети, отдельные IP адреса, proxy-сервера, контроллеры доменов, локальные DNS—ы и прочие IP адреса, которым мы доверяем.*

Пример.



***Как настроить БАН-ТАЙМ и ПОПЫТКИ ПОДКЛЮЧЕНИЯ К СЕРВЕРУ ЧУТЬ БОЛЕЕ ПОДРОБНО ?***

***Ban Time****: 259200 – бан на неделю****.***

***Max Retry:*** *5 – количество попыток подключения к серверу и веб-морде****.***

***Find Time:*** *300 – в течение какого времени можно осуществлять попытки подключения. 300 сек. = 5 мин****.***

***E-Mail:*** *указываем e-mail, на который будут приходить уведомления о том, что что-то происходит****.***