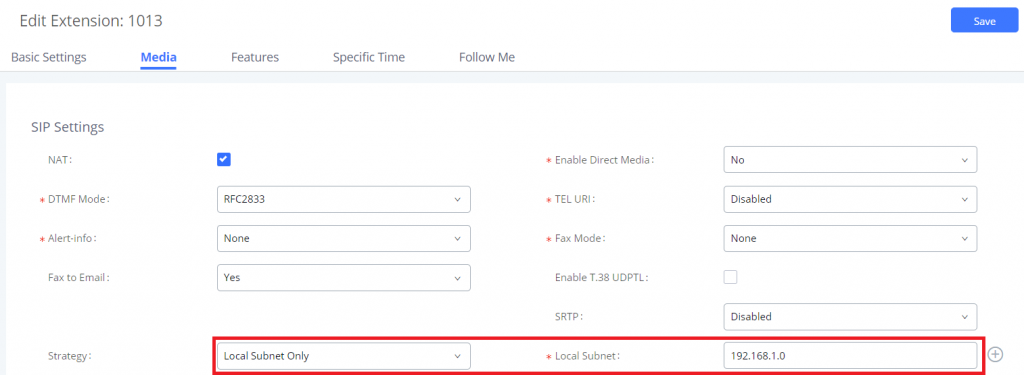
**HƯỚNG DẪN BẢO MẬT HỆ THỐNG TỔNG ĐÀI IP GRANDSTREAM**

Video hướng dẫn bảo mật tổng đài IP Grandstream  
- Với khách hàng sử dụng tổng đài IP Grandstream và kết nôi SIPtrunk theo đường internet, hay kết nối điện thoại IP/Softphone từ xa qua internet thì cần thiết lâp các bước cài đặt bảo mật cho tổng đài, tránh bị hack và xâm nhập trái phép...

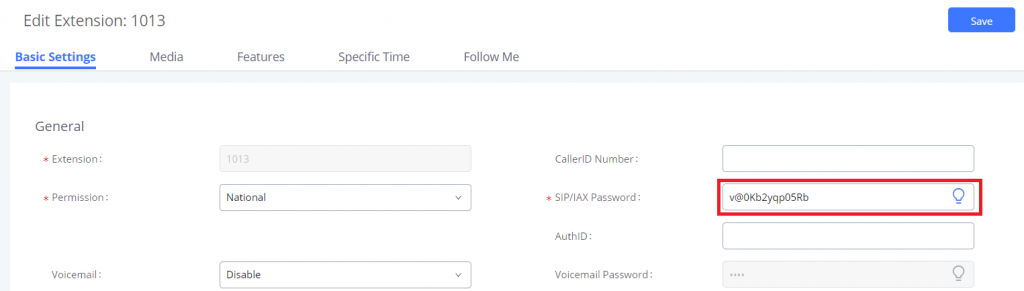
**Bước 1**:  Giới hạn địa chỉ IP kết nối đến máy nhánh và đặt password cho máy nhánh khó nhớ.

* Vào **Extension/Trunk --> Extension** --> edit máy nhánh nào đó rồi vào tab Media tìm đến mục **Strategy**

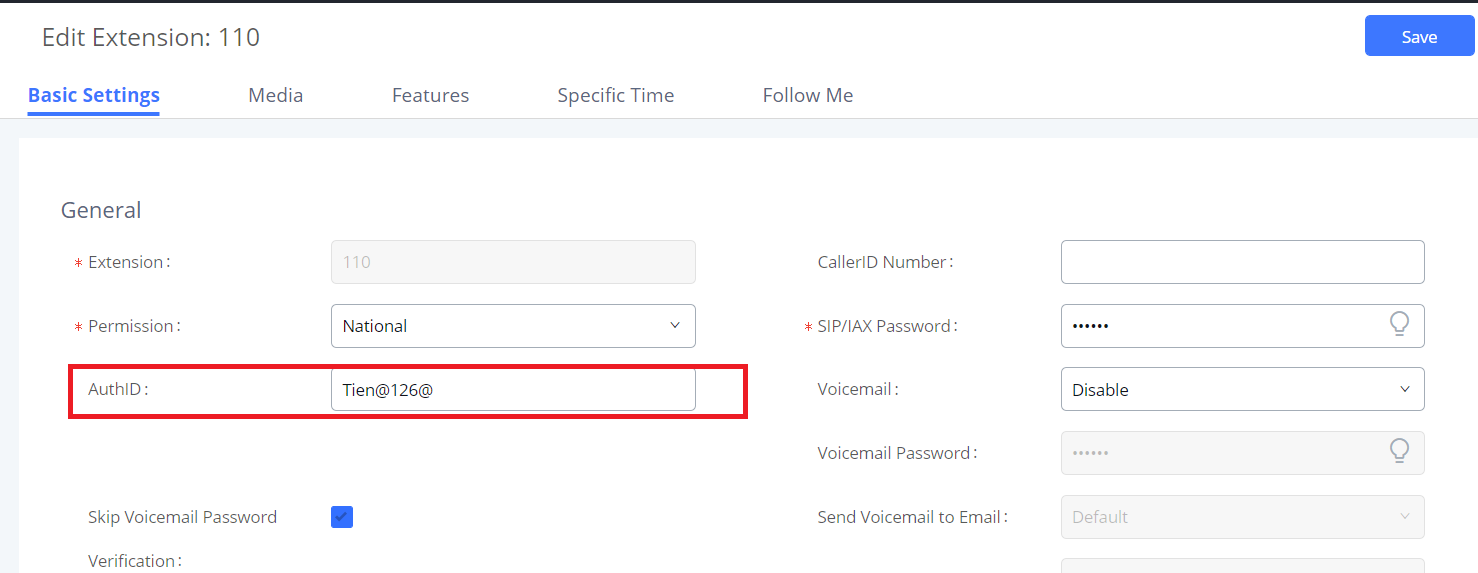
Các bạn đặt giới hạn dải IP được phép kết nối theo hình.



* Đặt Password khó nhớ cho máy nhánh hoặc các bạn để chế độ password mặc định là Ranrom



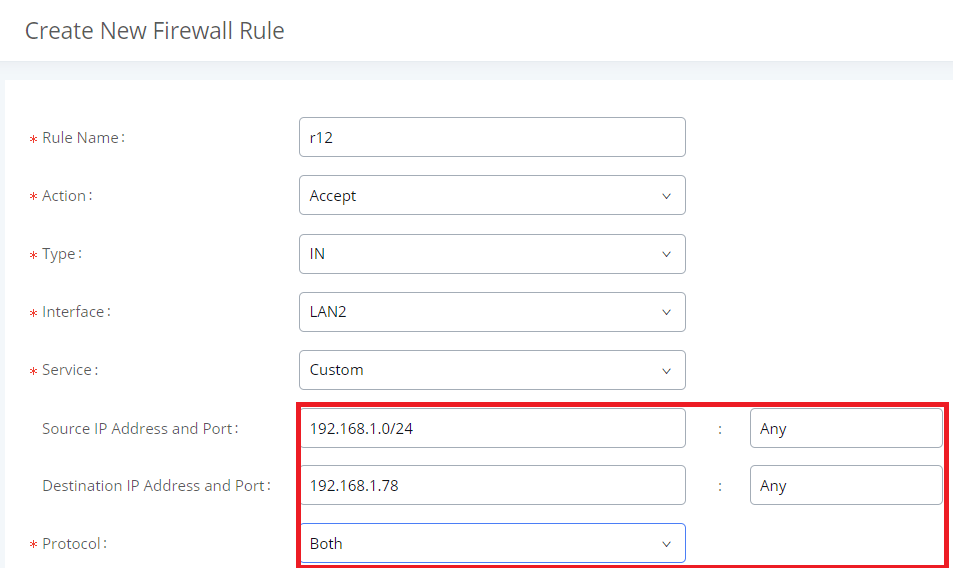
Để bảo mật hơn nữa các bạn cần đặt**AuthID** là tên có chữ và số khi đó trên điện thoại cũng cần điền **AuthID** này:



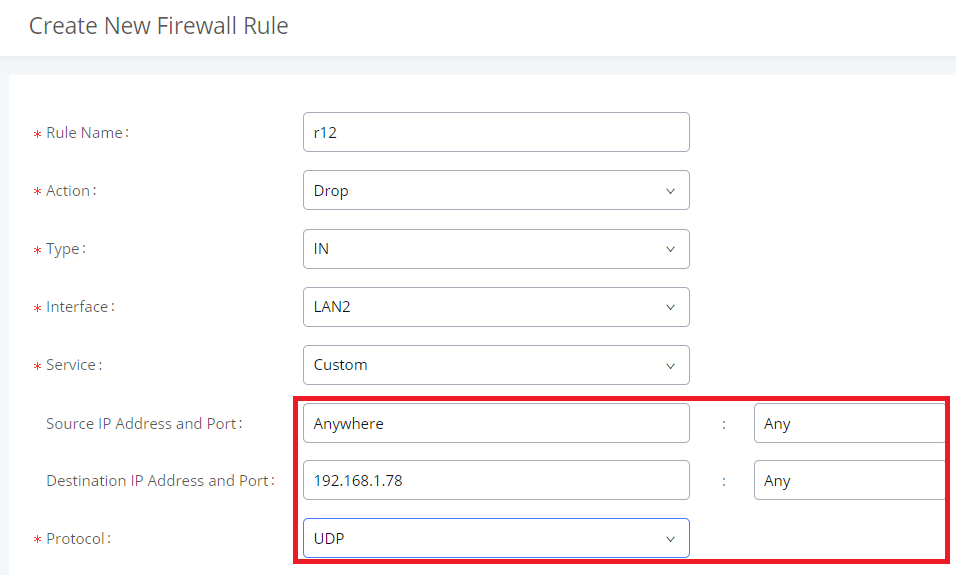
**Bước 2: Tạo Firewall Rule**

Vào**System Settings --> Security Settings ->Static Defense ->  trong Custom Firewall Settings --> Create new rule**

* Đầu tiên tạo các rule cho chép kết nối **Accerpt**( Lưu ý: các bạn cần tạo toàn bộ rule IN và OUT cho phép kết nối trước sau đó mới tạo rule chặn )
* Bao gồm các rule cho phép dải ip kết nối, dải ip siptrunk kết nối...

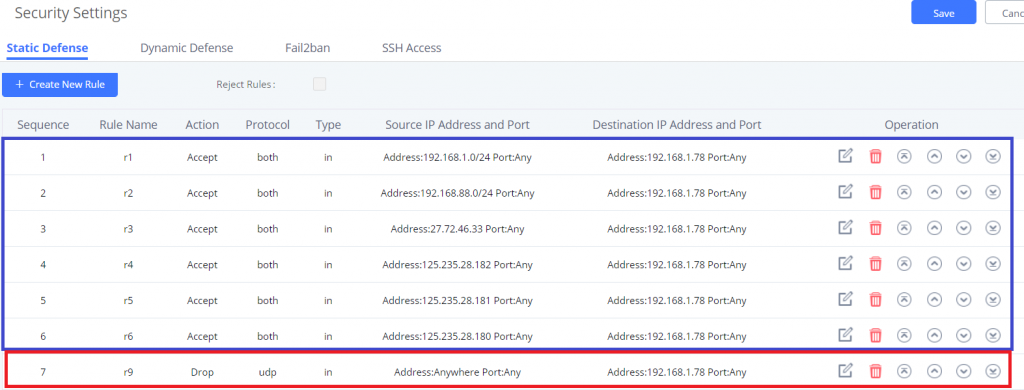


* Tiếp đến tạo rule chặn toàn bộ Drop. ( Ở rule này ta chặn toàn bộ Anywhere: Any tức là toàn bộ địa chỉ ip và port bên ngoài kết nối đến địa chỉ ip tổng đài )



Như vậy ta có bảng firewall như sau bao gồm nhưng ip được phép kết nối và chặn toàn bộ các ip khác.

Màu xanh là rule được phép còn màu đỏ là chặn.



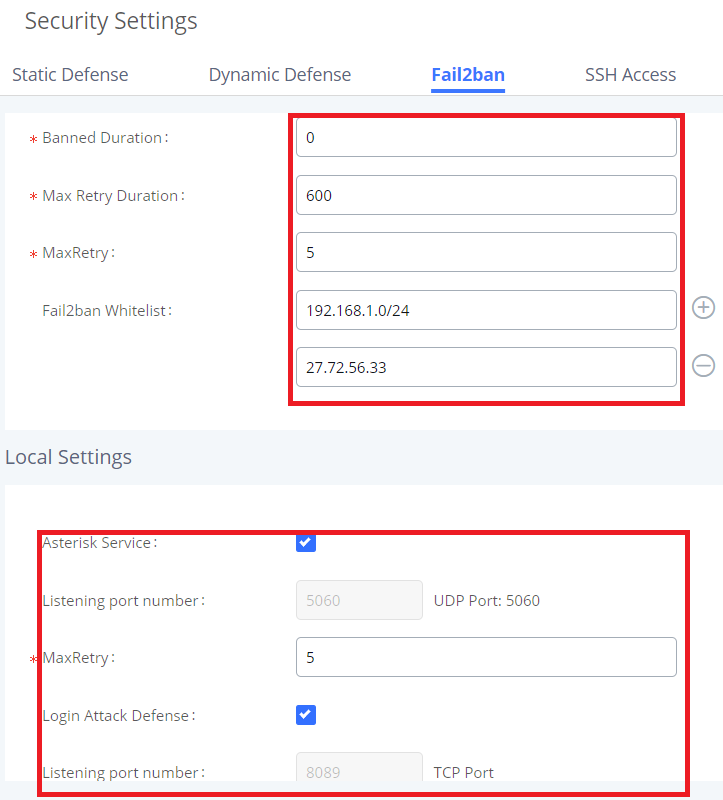
**Bước 3**: Bật **Fail2ban** trên tổng đài.

Vào**System Settings --> Security Settings ->Fail2ban và Enable Fail2Ban**

* Banned Duration: thời gian chăn ( nếu đặt là 0 sẽ chặn vĩnh viễn )
* Max Retry Duration: Thời gian cho phép đăng nhập sai
* MaxRetry: cho phép đăng nhập tối thiểu bao nhiêu lần

**Local settings**

* Asterisk Service : cần được kích hoạt nếu bên ngoài đăng ký đến port 5060 theo điều kiện ở trên sẽ bị chặn
* Login Attack Defense : Đăng nhập sai với port web mặc định cũng sẽ bị chặn theo điều kiện như trên



**Có thể giới hạn IP kết nối tới web tổng đài**

- Để giới hạn các bạn vào System Settings --> HTTP Server và làm theo hình sau.

Chỉ cho phép một số ip local truy cập web tổng đài, nếu có mở port web ra internet thì cũng chỉ cho phép ip nào được kết nối

