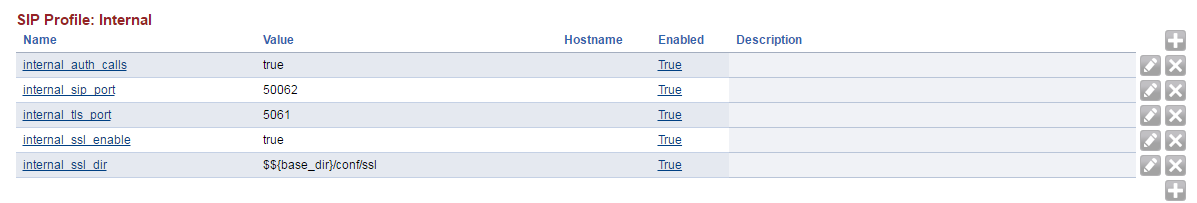
**Chương 5: Bảo mật cho hệ thống tổng đài**

Để tổng đài có thể hoạt động ổn định lâu dài, ta cần cấu hình một số thiết lập bảo mật cho tổng đài. Đầu tiên ta sẽ đổi port mặc định của tổng đài để tránh những người xâm nhập trái phép sử dụng port mặc định để quét password. Ta sẽ vào *Advanced, chọn Variables.* 

Sau đó ta sẽ đổi port 5060 ở dòng sip\_port lại thành port nào mà mình muốn. Chọn một port bất kì nhưng tránh những port quen thuộc để tránh bị tấn công hoặc bị trùng port



Ngoài ra, ta có thể sử dụng ứng dụng Fail2Ban để chặn những người dùng nhập sai password quá nhiều lần. Trước hết, ta bắt đầu cài đặt Fail2Ban bằng lệnh:

*yum install fail2ban*

Sau khi cài đặt hoàn tất, ta bắt đầu cấu hình cho fail2ban. Ta di chuyển tới đường dẫn chứa fail2ban ở trong thư mục /etc. Sau đó, ta tạo tập tin jail.local và chèn đoạn scripts của freeswitch vào

*[freeswitch]*

*enabled = true // dòng này để bật fail2ban*

*port = 5060,5061,5080,5081 // các port mặc định của tổng đài*

*filter = freeswitch // lọc freeswitch*

*logpath = /usr/local/freeswitch/log/freeswitch.log // đường dẫn để chạy fail2ban*

*maxretry = 10 // tối đa là 10 lần*

*action = iptables-allports[name=freeswitch, protocol=all]*

*sendmail-whois[name=FreeSwitch, dest=root,* [*sender=fail2ban@example.org*](mailto:sender=fail2ban@example.org)*] // thực thi*

Tiếp theo ta vào tập tin jail.conf để thiết lập cho fail2ban. Ta chỉnh sửa lại bantime và maxretry. Bantime là thời gian chặn khi người dùng nhập sai pass quá nhiều lần. Maxretry là số lần cho phép người dùng nhập sai. Nếu nhập sai quá số maxretry thì người dùng sẽ bị chặn truy cập trong thời gian bantime. Sau khi hoàn tất phần thiết lập. Ta gõ lệnh restart để chạy lại fail2ban

*/etc/init.d/fail2ban restart*