If you are running a **predictive dialer** (or any kind of Asterisk server) or a web hosting server, you have probably experienced often hacker/lamer **brute force** attempts. These attacks can be easily blocked by implementing optimal server configuration, using a good Firewall (i.e. SonicWall, PfSense, Tomato) etc. A very useful method of blocking brute force attacks is installing **Fail2Ban**, which will block the attacker from accessing your server through SSH, Asterisk... for a specified period of time after a number of unsuccessful login attempts.

The following guide explains installation of **Fail2Ban** service on a **CentOS** server.

1. Install

If you haven't done it already, download the EPEL repository:

```
# rpm -Uvh http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
```

When the repository has been downloaded, install fail2ban:

```
# yum install fail2ban
```

2. Configure

Editing the main config file (jail.conf) is not something you should do. Create a local copy of the jail file:

```
# cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

Setup your preferences by editing the jail.local file:

```
# nano /etc/fail2ban/jail.local
```

You will find the Asterisk section around the middle. Make sure that you whitelist your own external IP address and to keep the 127.0.0.1 in place. We strongly suggest setting the bantime to a much higher value (i.e. one week - 604800 seconds)

3. Restart Fail2Ban

Restart Fail2Ban:

sudo service fail2ban restart

Voila!

4. Adding a lamer IP address to IPTABLES

iptables -A INPUT -s 123.456.789.012 -j DROP & iptables-save