Fail2ban is an intrusion prevention framework, which works together with a packet-control system or firewall installed on your server, and is commonly used to block connection attempts after a number of failed tries. It operates by monitoring log files for certain type of entries and runs predetermined actions based on its findings. You can install the software with the following

```
sudo aptitude install fail2ban
```

Once installed, copy the default jail.conf file to make a local configuration with this command

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

Then open the new local configuration file for edit with your favourite text editor, for example

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

Scroll down to go through some of the settings available in the configuration file.

First up are the basic defaults for ignoreip, which allows you to exclude certain IP addresses from being banned, for example if your own computer has a fixed IP you can enter it here. Next set the bantime which determines how long an offending host will remain blocked until automatically unblocked. Lastly check the findtime and maxretry counts, of which the find time sets the time window for the max retry attempts before the host IP attempting to connect is blocked.

```
[DEFAULT]
ignoreip = 127.0.0.1
bantime  = 3600
findtime = 600
maxretry = 3
```

If you have a sendmail service configured on your cloud server, you can enable the email notifications from Fail2ban by entering your email address to the parameter destemail and changing the action = %(action_)s to action = %(action_mw)s.

Once you've done the basic configurations, check the different jails available in the configuration options. Jails are the rules which

fail2ban applies to any given application or log file. SSH jail settings, which you can find at the top of the jails list, are enabled by default.

```
[sshd]
enabled = true
```

You can enable any other jail modules in the same fashion by editing the enabled parameter to true.

When you've enabled all the jails you wish, save the configuration file and exit the editor. Then you'll need to restart the monitor with the following command

```
sudo service fail2ban restart
```

With that done, you should now check your iptable rules for the newly added jail sections on each of the application module you enabled.

```
sudo iptables -L
```

everyone try to ssh to someone machine

Fail2ban supports other protect protocal like smtp, http, wordpress and others. scroll down to this other protocal supports by default

if you want to get emails when someone is banned edit this part and remember to install send mail. put your valid email

```
destemail = root@localhost
sendername = Fail2Ban
mta = sendmail
```

This parameter configures the action that fail2ban takes when it wants to institute a ban. The value action_ is defined in the file shortly before this parameter. The default action is to simply configure the firewall to reject traffic from the offending host until the ban time elapses.

If you would like to configure email alerts, add or uncomment the action item to the jail.local file and change its value from action_

to action_mw. If you want the email to include the relevant log lines, you can change it to action_mwl. Make sure you have the appropriate mail settings configured if you choose to use mail alerts