Author: Jean-Marc LAMBERT
Boulevard de Dixmude, 30 Box 10
1000 BRUSSELS
Email: navis.lambert@gmail.com
Skype account: thegreatmonarch
http://www.specialistes.be

Change the ssh port of your server

Caution ! - This operation is dangerous and you probably will have to ask license of your datacenter in somes cases.

First of all: In some datacenters, it is absolutely asked to stipulate to some firewall taht another port that port 22 will be used to SSH access. Just try it when you are inside in your datacenter, restart your server, and ask to somebody outside to enter in your server and check that it is possible.

Secundly:

If you want to change the SSH port number,

- you will have to change it in **/etc/fail2ban/jail.conf** AND **/etc/ssh/sshd_config**
- you will have to restart ssh and fail2ban with **/etc/init.d/sshd restart** and **/etc/init.d/fail2ban restart**
- use the same port number !!!

By example, I change the ssh port from 22 to 2326 here, but you would choose a port of your choice, between a range from 1000 to 2500.

Do not use port dedicated for specific use, as 5060 (Voip) !!!

```
[ssh-iptables]

enabled  = true
filter   = sshd
action   = iptables[name=SSH, port=2326, protocol=tcp]
logpath  = /var/log/secure
maxretry = 5
bantime = 600
```

In sshd_config

Replace

#Port 22

By

Port 2326 (without “#” wich indicate a comment line)

Now you will have to restart ssh and fail2ban with

/etc/init.d/sshd restart

and

/etc/init.d/fail2ban restart

Advice: Do not close your ssh connection, try first on another computer if you can access with the secondary account.

Technical note written by Jean-Marc LAMBERT www.specialistes.be