SSH

Create an SSH jail by creating the file `/etc/fail2ban/jail.d/ssh.local`. Paste in the following config, adapt it to your needs

```
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 3
findtime = 300
bantime = 3600
ignoreip = 127.0.0.1
```

You can only use the ban action ufw, if you have it installed, configured, and enabled.

Start and reload SSHD, and then add your jail

```
sudo fail2ban-client start
sudo fail2ban-client reload
sudo fail2ban-client add sshd
```

Revision #2
Created 24 November 2024 17:12:51 by Nicolas
Updated 16 December 2024 10:42:28 by Nicolas