

# PROCÉDURE : Sécurisation avec Fail2Ban (Nginx)

---

## 🔗 Objectif

Protéger les applications web contre :

- Les tentatives de brute-force
- L'exploration de pages inexistantes (404)

## 🔗 Pré-requis

- Fail2Ban installé :

```
sudo apt install fail2ban -y
```

- Nginx doit avoir ses logs activés :

(/var/log/nginx/access.log et /var/log/nginx/error.log)

## 🔗 Étapes de mise en place

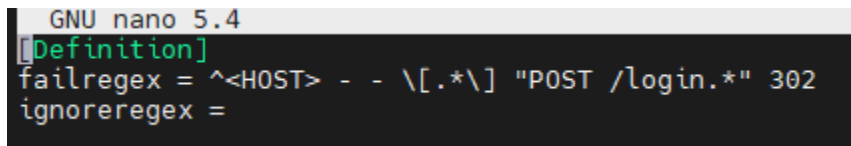
### 1. Créer les filtres personnalisés

🔗 /etc/fail2ban/filter.d/nginx-auth.conf

[Definition]

```
failregex = ^<HOST> - - \[.*\] "POST /login.*" 302
```

```
ignoreregex =
```



```
GNU nano 5.4
[Definition]
failregex = ^<HOST> - - \[.*\] "POST /login.*" 302
ignoreregex =
```

🔗 /etc/fail2ban/filter.d/nginx-badbot.conf

[Definition]

```
failregex = ^<HOST> - - \[.*\] "." 404
```

```
ignoreregex =
```

```
GNU nano 5.4
[Definition]
failregex = ^<HOST> - - \[.*\] ".*" 404
ignoreregex =
```

## 2. Configurer les jails

📄 /etc/fail2ban/jail.d/nginx.local

```
[nginx-auth]
enabled = true
port = http,https
filter = nginx-auth
logpath = /var/log/nginx/access.log
findtime = 300
maxretry = 3
bantime = 30
```

```
[nginx-badbot]
enabled = true
port = http,https
filter = nginx-badbot
logpath = /var/log/nginx/access.log
findtime = 300
maxretry = 3
bantime = 30
```

```
GNU nano 5.4
[nginx-auth]
enabled = true
port = http,https
filter = nginx-auth
logpath = /var/log/nginx/access.log
findtime = 300
maxretry = 3
bantime = 30

[nginx-badbot]
enabled = true
port = http,https
filter = nginx-badbot
logpath = /var/log/nginx/access.log
findtime = 300
maxretry = 3
bantime = 30
```

## 3. Redémarrer Fail2Ban

sudo systemctl restart fail2ban

## 4. Vérifier que les jails sont actives

sudo fail2ban-client status

### 🔗 Tester les protections

🔗 Tester le filtre nginx-auth

- Faites plusieurs connexions échouées à /login
- Vérifiez : sudo fail2ban-client status nginx-auth

```
aftec@debian:/etc/fail2ban/jail.d$ sudo fail2ban-client status nginx-auth
Status for the jail: nginx-auth
|- Filter
| |- Currently failed: 0
| |- Total failed: 19
| '- File list: /var/log/nginx/access.log
- Actions
| - Currently banned: 1
| - Total banned: 6
| - Banned IP list: 78.117.86.165
```

🔗 Tester nginx-badbot

- Appelez une URL inexistante comme <https://site:port/toto>
- Vérifiez : sudo fail2ban-client status nginx-badbot

```
aftec@debian:/etc/fail2ban/jail.d$ sudo fail2ban-client status nginx-badbot
Status for the jail: nginx-badbot
|- Filter
| |- Currently failed: 0
| |- Total failed: 255
| '- File list: /var/log/nginx/access.log
- Actions
| - Currently banned: 1
| - Total banned: 54
| - Banned IP list: 78.117.86.165
```

### 🔗 Commandes utiles

- Voir les IP bannies : sudo fail2ban-client status nginx-badbot
- Débannir une IP : sudo fail2ban-client set nginx-badbot unbanip <IP>

### 🔗 Tests et activation des règles

a) Tester un filtre :

```
sudo fail2ban-regex /var/log/nginx/access.log /etc/fail2ban/filter.d/nginx-auth.conf
```

b) Activer les jails :

```
sudo systemctl restart fail2ban
```

c) Vérifier les jails actives :

```
sudo fail2ban-client status
```

```
sudo fail2ban-client status nginx-auth
```

d) Voir les adresses IP bannies :

```
sudo fail2ban-client status nginx-auth
```

e) Débannir une IP :

```
sudo fail2ban-client set nginx-auth unbanip <IP>
```