ANNEXE - Fail2Ban

ANNEXE : DÉFENSE ACTIVE (UFW & FAIL2BAN)

Concept : Sécuriser SSH, c'est bien. Empêcher les barbares d'atteindre la porte, c'est mieux.

- **UFW (Uncomplicated Firewall) :** Le mur d'enceinte. Il bloque tout ce qui n'est pas invité.
- **Fail2Ban :** Le tireur d'élite. Il surveille ceux qui essaient de forcer la porte et les abat (bannissement IP).

UFW (Uncomplicated FireWall) : Le Mur d'Enceinte

UFW est une interface simplifiée pour nftables ou iptables. C'est "Uncomplicated", donc parfait pour les humains.

Installation et Politique par Défaut

On commence par installer l'outil.

```
sudo apt install ufw
```

Ensuite, on applique la règle de base de toute sécurité informatique : **Tout ce qui n'est pas autorisé est interdit.**

On refuse tout ce qui vient de l'extérieur, on laisse le serveur sortir (mises à jour, curl, etc.)

```
sudo ufw default deny incoming
```

```
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
```

```
sudo ufw default allow outgoing
```

```
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
```

Ouverture du Port SSH (Critique)

C'est ici que vous jouez votre vie. Vous devez ouvrir le port SSH **AVANT** d'activer le pare-feu. Dans cet exemple, nous utilisons le port **50922** (à adapter selon votre sshd_config).

Autorisation du port TCP spécifique

```
sudo ufw allow 50922/tcp
```

```
Rules updated
Rules updated (v6)
```

Activation (Le saut de la foi)

C'est le "moment de prier" comme tu dis. Si vous avez raté l'étape précédente, vous êtes dehors.

Active le pare-feu et l'ajoute au démarrage

```
sudo ufw enable
```

```
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
```

Le système vous avertira que cela peut couper les connexions SSH. Répondez y.

Vérification

On ne fait pas confiance, on vérifie.

```
sudo ufw status verbose
```

```
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
51322/tcp                  ALLOW IN    Anywhere
51322/tcp (v6)             ALLOW IN    Anywhere (v6)
```

Résultat attendu : Status: active, et une ligne indiquant 51322/tcp ALLOW IN Anywhere.

Fail2Ban : Le Gardien Automatisé

Fail2Ban lit les logs en temps réel. Si une IP échoue trop souvent à s'authentifier, elle est bannie via le pare-feu.

Installation

```
sudo apt install fail2ban
```

Configuration (La méthode propre)

Règle d'or : Ne touchez jamais à /etc/fail2ban/jail.conf. Ce fichier est écrasé à chaque mise à jour. Créez un fichier .local qui aura la priorité.

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

```
[DEFAULT]

# Durée du bannissement (1h ici).
# Pour la prod, soyez méchants : 24h ou 1 semaine.
bantime = 1h

# Fenêtre de temps de surveillance
# Si X échecs durant ces 10 minutes -> BAN
findtime = 10m

# Nombre d'essais max avant ban
maxretry = 3

# IMPORTANT : On dit à Fail2Ban d'utiliser UFW pour bannir l’IP (plus propre que iptables direct)
banaction = ufw

# Ignorer ta propre IP (Optionnel : Mets l'IP de ton domicile si elle est fixe pour ne jamais te bannir)
# ignoreip = 127.0.0.1/8 ::1

[sshd]
enabled = true

# TRES IMPORTANT : Ton port personnalisé !
port = 50922

# TRES IMPORTANT : Indispensable pour Debian 12+ (qui n'utilise plus syslog par défaut)
backend = systemd
```

Activation et Surveillance

On démarre le service et on vérifie qu'il surveille bien la prison sshd.

Activation au démarrage et démarrage immédiat

```
sudo systemctl enable fail2ban
```

```
Synchronizing state of fail2ban.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable fail2ban
```

```
sudo systemctl restart fail2ban
```

Vérification du statut de la prison SSH

```
sudo fail2ban-client status sshd
```

```
Status for the jail: sshd
|- Filter
|  |- Currently failed:      0
|  |- Total failed:   0
|  `- Journal matches:_SYSTEMD_UNIT=ssh.service + _COMM=sshd
`- Actions
   |- Currently banned:      0
   |- Total banned:   0
   `- Banned IP list:
backend = systemd
```

Ce qu'il faut regarder :

- Status for the jail: sshd
- Filter: Doit montrer que le backend est actif.
- Total banned: Le nombre de "victimes" actuelles.

Gérer les erreurs (Débannir, juste au cas ou)

Si vous avez banni votre collègue (ou vous-même via une autre connexion), voici la commande d'amnistie :

Remplacez <IP> par l'adresse bannie

```
sudo fail2ban-client set sshd unbanip <IP>
```