Vérifier le pare-feu

Pourquoi cette étape est indispensable

Une jail «active» côté fail2ban (fail2ban-client status qui répond) ne garantit **pas** que le ban est réellement appliqué au niveau du pare-feu — surtout sur l'infra Rakouns où Docker manipule ses propres règles iptables. C'est l'erreur la plus fréquente : croire qu'une jail fonctionne juste parce qu'elle est listée comme enabled.

Vérification générique : ban classique

Pour une jail standard (ex : sshd), vérifier que la règle de ban apparaît bien dans iptables :

```
sudo iptables -L f2b-sshd -n
```

Résultat attendu après un ban :

```
Chain f2b-sshd (1 references)
target     prot opt source               destination
DROP       all  --  203.0.113.42         0.0.0.0/0
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
```

Vérification Docker : chaîne DOCKER-USER

Pour les jails utilisant l'action iptables-docker (cas Vaultwarden et tous les services conteneurisés), c'est la chaîne DOCKER-USER qu'il faut inspecter, **pas** INPUT :

```
sudo iptables -L DOCKER-USER -n --line-numbers
```

La chaîne dédiée du service doit apparaître en première position (insérée avec -I, donc évaluée avant le reste) :

```
Chain DOCKER-USER (1 references)
num  target          prot opt source               destination
1    f2b-vaultwarden all  --  0.0.0.0/0            0.0.0.0/0
2    RETURN          all  --  0.0.0.0/0            0.0.0.0/0
```

Puis inspecter la sous-chaîne pour voir si une IP y est effectivement droppée :

```
sudo iptables -L f2b-vaultwarden -n

Chain f2b-vaultwarden (1 references)
target     prot opt source               destination
DROP       all  --  203.0.113.42         0.0.0.0/0
RETURN     all  --  0.0.0.0/0            0.0.0.0/0
```

Si la chaîne f2b-vaultwarden n'apparaît pas du tout dans DOCKER-USER, l'action iptables-docker n'a pas pu s'initialiser correctement : vérifier actionstart dans iptables-docker.conf (page 2) et relire les logs fail2ban (section suivante).

Provoquer un ban de test (en sécurité)

Pour valider toute la chaîne sans attendre une vraie attaque, depuis une machine **différente** de celle utilisée pour administrer le service (sinon tu te bannis toi-même de ton accès SSH/admin) :

```
# Déclencher volontairement des échecs d'auth (exemple Vaultwarden via curl)
for i in {1..6}; do
  curl -s -o /dev/null -w "%{http_code}\n" \
    -X POST https://vault.rakouns.bzh/identity/connect/token \
    -d "username=test@test.com&password=wrongpassword&grant_type=password"
done
```

Puis vérifier côté fail2ban :

```
sudo fail2ban-client status rakouns-vaultwarden
```

L'IP de test doit apparaître dans Banned IP list. Pour débannir manuellement après test :

```
sudo fail2ban-client set rakouns-vaultwarden unbanip <IP_DE_TEST>
```

Logs fail2ban : diagnostic en cas de doute

```
sudo tail -f /var/log/fail2ban.log
```

Lignes à surveiller :

- [rakouns-vaultwarden] Found <IP> → un échec a été détecté par le filter (le filter fonctionne).
- [rakouns-vaultwarden] Ban <IP> → le seuil maxretry a été atteint et le ban a été déclenché (la jail fonctionne).
- Absence totale de Found malgré des échecs visibles dans les logs applicatifs → revenir à la Page 3 et retester le filter avec fail2ban-regex.
- Found présent mais jamais de Ban → vérifier maxretry/findtime, ou que ignoreip (jail.local) n'exclut pas l'IP de test par erreur.

Vérification post-reboot / post-recreate

Deux cas fréquents sur Rakouns où le ban peut «disparaître» silencieusement :

1. **Reboot du host** : les règles iptables ne sont pas persistées par défaut. Vérifier que fail2ban redémarre bien après le pare-feu/Docker (systemctl status fail2ban), et que DOCKER-USER est repeuplée par actionstart au démarrage du service.
2. **Recréation d'un conteneur** (mise à jour d'image) : le container_id change, donc le logpath de la jail devient invalide. Penser à relancer le script de détection automatique du chemin de log (mentionné en Page 4) puis fail2ban-client reload <jail>.

Checklist de vérification rapide

```
# 1. La jail est listée et active
sudo fail2ban-client status

# 2. Le filter remonte des "Found" sur le service concerné
sudo fail2ban-client status rakouns-vaultwarden

# 3. La chaîne f2b-<service> existe dans DOCKER-USER (cas Docker)
sudo iptables -L DOCKER-USER -n

# 4. Les logs confirment Found -> Ban en cas d'incident réel
sudo grep "rakouns-vaultwarden" /var/log/fail2ban.log | tail -20
```

Revision #1
Created 2026-06-20 12:15:49 UTC by clement-derouet
Updated 2026-06-20 12:19:00 UTC by clement-derouet