Reverse proxy (Nginx Proxy Manager)

Reverse proxy (Nginx Proxy Manager)

> *Dernière mise à jour : 2026-05-10*

URL prod

- **Public** : https://rules.thymon.fr
- **LAN direct** : `http://192.168.10.100:3000` (utile pour debug si NPM tombe — dans la limite du `CORS_ORIGIN` configuré)

Config NPM

Côté UI NPM (pas dans le repo) :

- **Domain** : `rules.thymon.fr`
- **Forward Hostname / IP** : `boardgame-referee` (nom du container)
- **Forward Port** : `3000`
- **SSL** : Let's Encrypt (renew auto)
- **Force SSL** : oui (HTTP redirige vers HTTPS)
- **HSTS** : oui (dans Advanced)

NPM est sur le même réseau Docker `proxy` que le container app, donc il joint le container par son nom DNS interne.

`TRUST_PROXY=true`

Variable d'env importante : `TRUST_PROXY=true` dans `.env` prod. Hono fait alors confiance aux headers `X-Forwarded-*` de NPM :

- `X-Forwarded-For` → IP réelle du client (utilisé par le rate-limiter login)
- `X-Forwarded-Proto` → `https` (utilisé pour `Set-Cookie Secure`)
- `X-Forwarded-Host` → host original (`rules.thymon.fr`)

Heartbeats SSE 8s

⚠ Critique : les endpoints streamSSE (`/api/ask/stream`, `/api/admin/games/:id/sync-cards`, `/api/games/ingest` SSE) émettent un event `{ type: 'heartbeat' }` toutes les 8s.

Sans ça, le `proxy_read_timeout 60s` par défaut de Nginx fermerait la connexion alors que le backend travaille encore (Claude streamant lentement, par exemple). L'utilisateur verrait une fausse "network error" alors que la réponse arrive bien en base.

Côté frontend, `useEventStream` filtre déjà ces events via `skipHeartbeat`.

Si tu changes le `proxy_read_timeout` côté NPM (par ex. à 5min), tu peux espacer les heartbeats — mais 8s est un bon défaut robuste.

Pas de Helmet Hono

Tous les headers sécurité (HSTS, CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy) sont gérés par NPM en amont via Advanced → Custom Nginx Configuration. Évite la duplication / contradiction.

Si tu veux les voir / vérifier : `curl -I https://rules.thymon.fr` doit montrer :

```
Strict-Transport-Security: max-age=...
Content-Security-Policy: ...
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
```

```
Referrer-Policy: strict-origin-when-cross-origin
```

Backup config NPM

NPM stocke sa config dans `/mnt/user/appdata/nginx-proxy-manager/data/nginx/proxy_host/`. Backup régulier ces fichiers + `database.sqlite` au cas où le container NPM se corrompt.

Si NPM tombe

Le container `app` reste up et écoute sur `:3000` interne. Tu peux y accéder direct via LAN avec :

```
curl http://192.168.10.100:3000/api/health
```

Pour que le frontend fonctionne sans NPM en accès LAN, il faut que `CORS_ORIGIN` autorise l'IP/CIDR LAN (`192.168.10.0/24`).

Revision #1
Created 2026-05-10 15:20:00 UTC by thymon
Updated 2026-05-10 15:20:00 UTC by thymon