

5.2 - Cloudflare, DNS et accès distant

Cloudflare peut fournir le DNS, un proxy public et des certificats entre le client et son réseau. La configuration doit rester cohérente avec Caddy et Immich.

DNS

Créer un enregistrement pour :

immich.dreamsaphir.net

Deux modes sont possibles :

Mode	Effet
DNS only	le client rejoint directement l'adresse publiée
Proxied	le trafic passe par le proxy Cloudflare

Le mode proxied ajoute une couche de protection mais aussi des limites de taille, de délai et de comportement selon l'offre. Tester les vidéos les plus volumineuses. Si les envois échouent uniquement à travers Cloudflare, comparer avec un accès local et examiner les limites du compte.

TLS

Avec un certificat valide sur Caddy, utiliser un mode de chiffrement strict entre Cloudflare et l'origine. Éviter les modes qui acceptent un certificat invalide.

Ports et pare-feu

- exposer uniquement 80 et 443 vers Caddy si nécessaire ;
- ne pas publier directement 30041 sur Internet ;

- filtrer l'administration TrueNAS ;
- conserver WireGuard pour les accès d'administration ;
- limiter les règles NAT à la cible exacte.

En-têtes et adresse client

Le proxy Caddy doit transmettre l'adresse client et le protocole d'origine. Si plusieurs proxies se suivent, configurer les plages de confiance avec prudence afin d'éviter qu'un client forge `X-Forwarded-For`.

Diagnostic

```
dig +short immich.dreamsaphir.net
curl -vI https://immich.dreamsaphir.net
curl -I http://ADRESSE_TRUENAS:30041
```

Comparer :

1. accès local direct ;
2. accès local par le domaine ;
3. accès extérieur par le domaine ;
4. upload d'une petite photo ;
5. upload d'une grande vidéo.

Erreurs courantes

Symptôme	Piste
525	certificat ou TLS entre Cloudflare et Caddy
403	règle Cloudflare, authentification ou pare-feu
upload interrompu	taille ou délai du proxy
boucle OAuth	domaine ou URI de redirection incorrecte
mauvaise adresse client	chaîne d'en-têtes proxy incorrecte

La protection d'accès Cloudflare placée devant tout Immich peut interférer avec l'application mobile et OAuth. Tester avant de l'imposer.

Référence Immich : <https://docs.immich.app/administration/reverse-proxy/>

Revision #1

Created 2026-08-08 02:04:16 CEST by Admin

Updated 2026-08-08 02:04:16 CEST by Admin