Refonte et sécurisation d'une architecture Jellyfin exposée sur Internet avec Cloudflare Zero Trust et inspection avancée

PROJET

Sommaire

1. Contexte initial et problématique

À l'origine, l'accès distant à mon serveur multimédia reposait sur un NAS Synology DS216play avec OpenVPN activé. Cette solution permettait de sécuriser l'accès sans exposition directe sur Internet.

Cependant, le processeur du DS216play ne disposant pas d'accélération matérielle pour le chiffrement, le débit VPN était limité à environ 10 Mbps. Cette contrainte était particulièrement pénalisante alors que l'infrastructure réseau repose sur une connexion fibre 2.5 Gbps.

Le VPN constituait donc un goulet d'étranglement important, limitant fortement les performances de streaming et empêchant d'exploiter pleinement la capacité du lien WAN.

Il était nécessaire de repenser entièrement l'architecture afin d'améliorer les performances tout en maintenant un niveau de sécurité élevé.

2. Nouvelle architecture matérielle

Deux serveurs Jellyfin ont été déployés.

Le premier sur un serveur HPE ProLiant ML350 équipé de quatre cartes Nvidia P4, permettant un transcodage matériel performant et la gestion simultanée de plusieurs flux vidéo.

Le second sur un NAS Ugreen DXP 2800 configuré avec :

- deux disques Western Digital Red 6 To en RAID 1 pour la résilience des données,
- deux SSD de 250 Go en RAID 1 utilisés comme cache afin d'améliorer les performances d'accès.

Jellyfin a été déployé via Docker sur le NAS, garantissant isolation et facilité de maintenance.

3. Exposition contrôlée via reverse proxy

Un reverse proxy Nginx a été configuré sur le NAS Ugreen pour centraliser les requêtes entrantes.

Un certificat auto-signé a été utilisé pour sécuriser les communications internes entre Nginx et les instances Jellyfin.

Une redirection NAT/PAT a été configurée sur la box fibre afin de rediriger le trafic WAN vers le reverse proxy.

Cette configuration a permis de supprimer la dépendance au VPN et d'exploiter pleinement la bande passante disponible.

4. Intégration DNS et proxy Cloudflare

Le domaine polishmen.fr, enregistré chez OVH, a été configuré avec plusieurs enregistrements DNS :

- enregistrements A pointant vers l'adresse publique,
- activation du proxy Cloudflare (mode orange) pour masquer l'IP réelle,
- configuration Anycast permettant une meilleure distribution des requêtes.

Les certificats SSL universels Cloudflare ont été activés, incluant :

- certificat Edge actif,
- certificat de secours (backup),
- activation des options HTTPS automatiques.

Les fonctionnalités suivantes ont été activées :

- Automatic HTTPS Rewrites,
- Opportunistic Encryption,
- gestion SSL/TLS en mode sécurisé.

Cela garantit un chiffrement complet entre les visiteurs et l'infrastructure Cloudflare.

5. Sécurisation avancée avec Cloudflare Zero Trust

Pour remplacer la protection VPN initiale, une politique Zero Trust a été mise en place.

L'accès aux applications Jellyfin est désormais soumis à :

- une restriction géographique limitée aux adresses IP françaises ;
- une authentification préalable basée sur une liste blanche d'adresses e-mail ;
- un envoi de code de validation uniquement si l'adresse est autorisée ;
- un blocage total pour les e-mails non déclarés.

Cette configuration permet de bloquer automatiquement toute tentative d'accès non autorisée avant même que la requête n'atteigne le serveur.

6. Secure Web Gateway et inspection HTTPS

Les captures montrent l'activation de fonctionnalités avancées de Cloudflare Secure Web Gateway :

- inspection HTTPS avec déchiffrement TLS activé,
- analyse antivirus des fichiers en upload et download,
- blocage automatique des fichiers non scannables,
- détection renforcée des fichiers via inspection du corps HTTP,
- journalisation complète des flux DNS, HTTP et réseau,
- capture des événements bloqués.

Ces options permettent une analyse approfondie du trafic et renforcent la sécurité applicative.

7. Protection contre les menaces

Plusieurs modules de protection sont actifs :

- protection contre les attaques DDoS,
- détection des exploits web,
- protection contre les abus API,
- analyse du trafic bot,
- mécanismes anti-brute force.

Les tableaux de bord Cloudflare permettent de visualiser :

- les tentatives bloquées,
- les événements bot,
- les requêtes suspectes,
- l'origine géographique du trafic.

Cette supervision apporte une visibilité complète sur l'exposition Internet.

8. Tests réalisés

Des tests ont été effectués dans plusieurs scénarios :

- accès depuis IP française autorisée : accès validé ;
- accès depuis IP étrangère : blocage automatique ;
- tentative avec e-mail non whitelisté : aucune réponse ;
- tentative répétée de connexion : limitation automatique ;
- vérification du masquage IP via proxy Cloudflare.

Les performances de streaming ont été testées avec transcodage GPU actif sur le serveur HPE. Les débits constatés exploitent désormais pleinement la capacité de la connexion fibre.

9. Bilan

Cette refonte complète m'a permis de passer d'un modèle basé sur VPN limité par le matériel à une architecture exposée sur Internet mais sécurisée par plusieurs couches successives :

- reverse proxy local,
- NAT contrôlé,
- proxy Cloudflare,
- certificats SSL Edge,
- politique Zero Trust,
- inspection HTTPS,
- anti-brute force,
- monitoring avancé.

Cette situation démontre ma capacité à concevoir une architecture sécurisée exposée sur Internet, intégrant haute performance, segmentation et défense en profondeur.

Au-delà du projet multimédia, les principes appliqués sont directement transposables à l'exposition sécurisée d'applications professionnelles.