Infrastructure Hybride (VPS / On-Premise)

Documentation rédigée par : GADONNAUD Ewen

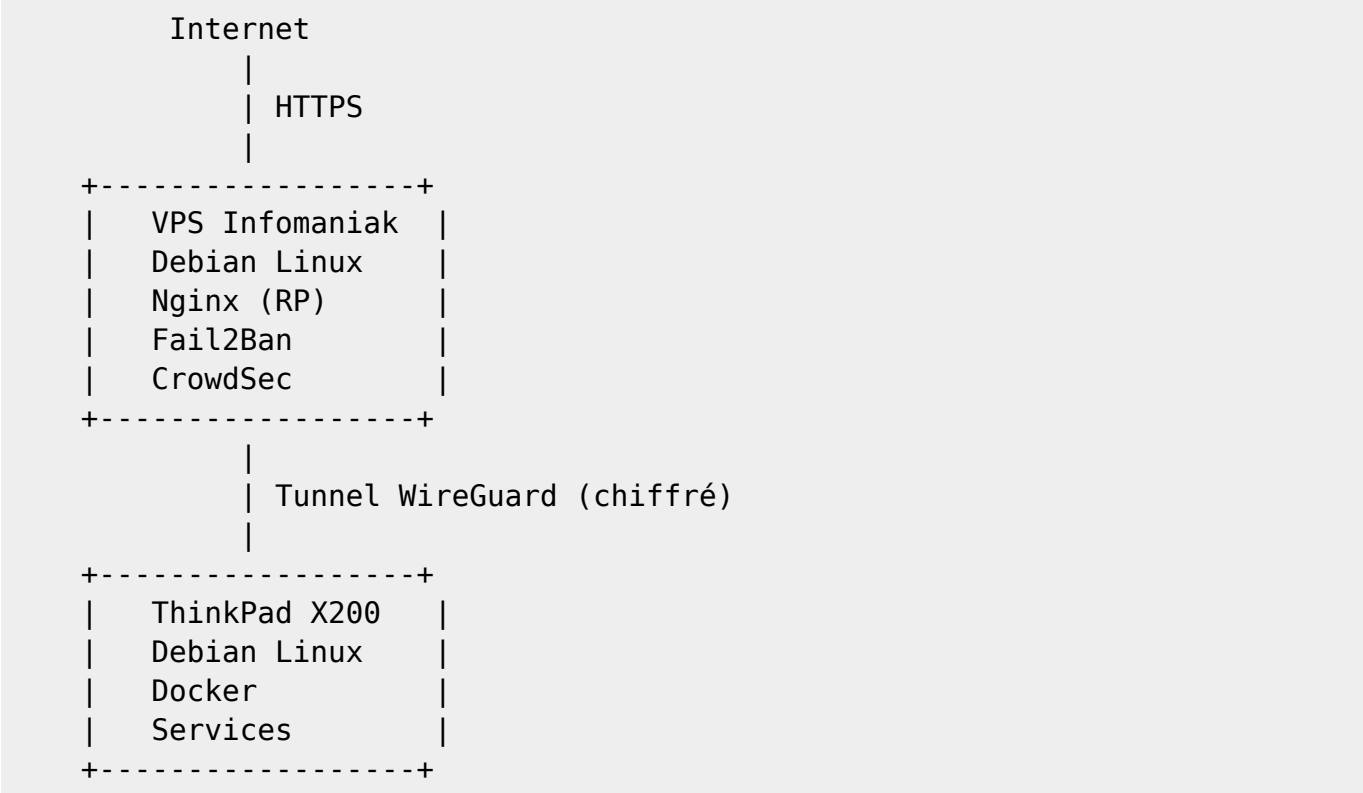
Formation : BTS SIO 1ère année - Option SISR

Établissement : Lycée Paul-Louis Courier, Tours

Date : Mars 2026

1. Architecture générale

L'infrastructure repose sur un modèle **hybride** combinant un point d'entrée public (VPS) et un serveur privé local, interconnectés via un tunnel VPN chiffré.



Principe clé : Le X200 n'expose aucun port directement sur Internet. Tout le trafic entrant transite par le VPS, qui le relaie via le tunnel WireGuard vers les services internes. Le X200 est ainsi invisible depuis l'extérieur.

Composant	Rôle
VPS Infomaniak	Point d'entrée public, reverse proxy, pare-feu périmétrique
ThinkPad X200	Hébergement de l'ensemble des services conteneurisés
Tunnel WireGuard	Lien chiffré entre le VPS et le X200

Choix du provider VPS : Infomaniak

Le VPS est hébergé chez **Infomaniak**, hébergeur suisse souverain. Ce choix repose sur trois critères :

- **Souveraineté des données** — l'infrastructure est soumise à la législation suisse (LPD), reconnue comme l'une des plus protectrices en matière de données personnelles, indépendante du RGPD européen et hors de portée du Cloud Act américain
- **Cohérence avec la démarche** — héberger une infrastructure orientée vie privée (SearXNG, Nextcloud …) chez un acteur dont le modèle économique ne repose pas sur l'exploitation des données est un choix délibéré
- **Accessibilité financière** — tarif à 3,60€/mois, adapté à un budget étudiant

2. Services déployés

L'intégralité des services tourne sur le X200 via Docker Compose, offrant isolation et portabilité.

Service	Technologie	Rôle
Moteur de recherche	SearXNG	Méta-moteur orienté vie privée
Base de connaissances	DokuWiki	Documentation technique (ce wiki)
Forge Git	Forgejo	Hébergement de dépôts Git auto-hébergé
Stockage cloud	Nextcloud	Synchronisation de fichiers privée
Synchronisation notes	CouchDB	Backend Obsidian LiveSync (non exposé Internet)
Filtrage DNS	Pi-hole	Blocage publicités et domaines malveillants
Tableau de bord	Homer	Accès centralisé aux services
Outils dev	IT-Tools	Utilitaires exécutés côté client
Blog	Nginx	Diffusion d'articles statiques

3. Sécurité

La sécurité est organisée en couches successives, du périmètre réseau jusqu'à l'authentification applicative.

Sécurité périmétrique (VPS)

- **Fail2Ban** — protection SSH avec prison `recidive` pour bannissement long terme des attaquants persistants
- **CrowdSec** — analyse comportementale du trafic web, bouncers iptables et Nginx, abonnements aux blocklists communautaires (FireHOL, proxies ouverts, botnets, AI crawlers), agis également en tant que “videur” SSH en complément avec Fail2Ban

Sécurité applicative

- Chiffrement HTTPS sur tous les services exposés (Let's Encrypt / Certbot)
- Authentification 2FA (TOTP) sur les services critiques (Vaultwarden)
- CouchDB isolé sur le réseau interne, non exposé sur Internet

4. Monitoring

- **Beszel** — surveillance en temps réel du X200 (CPU, RAM, I/O disque)
- **GoAccess** — analyse des logs Nginx du VPS (trafic, 404, bots…)
- **Audit manuel** — consultation régulière des décisions CrowdSec et Fail2Ban via CLI et WebApp CrowdSec

5. Automatisation

Plusieurs tâches récurrentes sont automatisées via cron :

- **Sauvegardes** — scripts de sauvegarde des volumes Docker avec rotation et compression
- **Notifications** — bot Telegram pour les alertes en temps réel (statut des backups, alertes système) et récapitulatif hebdomadaire des mises à jour effectuées sur le X200
- **Mises à jour système** — automatisation des mises à jour de paquets pour application rapide des correctifs de sécurité

6. Principes de conception

- **Moindre privilège** — chaque service tourne avec les droits strictement nécessaires
- **Isolation** — conteneurisation Docker, CouchDB non exposé, X200 invisible depuis Internet
- **Résilience** — sauvegardes automatisées, monitoring continu, rotation des logs