

Nextcloud & WireGuard

Sur un serveur Ubuntu domestique

Conception d’un NAS auto-hébergé avec accès distant chiffré de bout en bout, pensé comme une étude de cas d'architecture système à petite échelle.

Contexte & motivation

- Souveraineté des données personnelles
- Coût marginal nul (matériel existant)
- Terrain d'apprentissage réseau / Linux
- Accès distant sans ports non essentiels

Empilement technique

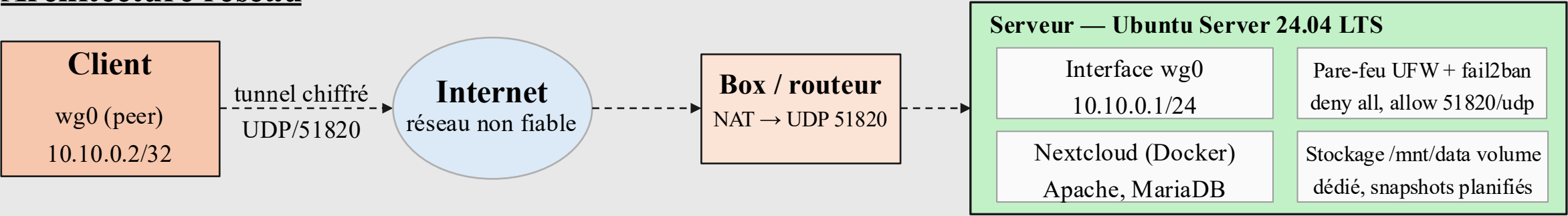
Ubuntu 24.04 LTS, Docker, Nextcloud, WireGuard, MariaDB, UFW, fail2ban, ZFS/RAID

Résumé

Ce projet documente la mise en place d'un serveur personnel hébergeant Nextcloud comme NAS logiciel (fichiers, calendrier, contacts, photos), couplé à un tunnel WireGuard pour un accès distant sécurisé, sans exposer directement le serveur sur Internet.

Métrique	Valeur observée	Cible
Latence tunnel (LAN → serveur)	≈ 3–5 ms	< 10 ms
Débit synchronisation Nextcloud	à mesurer	≥ 50 Mo/s
Temps de handshake WireGuard	< 1 s	–
Ports exposés publiquement	1 (UDP)	1

Architecture réseau



Le client n'atteint jamais directement les services applicatifs : tout le trafic distant transite par le tunnel WireGuard avant d'être traité par le pare-feu, puis relayé vers Nextcloud.