

Projet: Déploiement d'un VPN WireGuard personnel

Contexte et objectif

J'ai déployé un serveur VPN basé sur **WireGuard** sur un Raspberry Pi 5. L'objectif est double :

- Sécuriser mes connexions lors de l'utilisation de Wi-Fi publics.
- Accéder à distance à mes ressources locales (NAS, services internes).

Réalisation

- Mise en place du serveur avec **PiVPN** et routage NAT.
- Configuration de plusieurs clients (PC portable, smartphone) avec import via QR code.
- Application d'un pare-feu UFW pour protéger la machine.

Problème rencontré

Après activation d'UFW, le trafic VPN ne passait plus.

Analyse: le firewall bloquait le forwarding et les flux WireGuard.

Solution : autorisation du port UDP 51820 et ajout d'une règle « ufw route allow » pour rétablir le routage.

Résultat

- VPN fonctionnel, utilisable en mobilité.
- Machine protégée par un firewall configuré de façon restrictive.
- Accès sécurisé et chiffré à Internet et au réseau local.

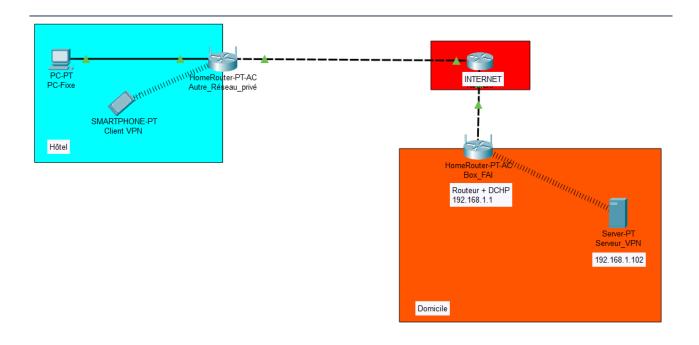
Compétences démontrées

- Déploiement d'un VPN sécurisé avec WireGuard.
- Résolution de problème lié à la configuration réseau et au firewall.
- Compréhension du **NAT**, forwarding **IP** et filtrage.
- Mise en place d'une solution utilisée en **conditions réelles**.

Nexus Secure 1



Topologie Réseau



Nexus Secure 2