Rapport de Projet : Mise en place d'un VPN WireGuard

1. Présentation du projet

Nom du projet :
Accès à distance sécurisé au serveur de virtualisation via un VPN

Contexte :
Le serveur de virtualisation Proxmox (hyperviseur de niveau 1) est actuellement hébergé sur un réseau local ADSL. Pour garantir un accès sécurisé à distance depuis un réseau externe (notamment le domicile), la mise en place d'un VPN était nécessaire.

Objectif :
Permettre aux membres du pôle numérique d'accéder au serveur de virtualisation en toute sécurité, où qu'ils soient, grâce à un VPN efficace, simple à mettre en place et à maintenir.

---

2. Présentation de WireGuard

Qu'est-ce que WireGuard ?
WireGuard est un protocole VPN moderne, open source et extrêmement léger. Conçu pour être plus rapide, plus simple et plus sécurisé que les solutions traditionnelles (comme OpenVPN ou IPsec), il est désormais intégré directement dans le noyau Linux.

Fonctionnement (inspiré du tutoriel IT-Connect)
WireGuard repose sur des concepts simples et une architecture minimale :

- Chaque pair (client ou serveur) possède une **clé publique** et une **clé privée**.
- L'authentification repose sur un échange de clés asymétriques.
- Une fois les pairs configurés, la communication est **chiffrée de bout en bout** via UDP.
- Contrairement à d'autres VPN, il ne nécessite pas de certificats ou d'infrastructure complexe.

Avantages de WireGuard :

- **Performance élevée** : faible latence et vitesse de transfert optimisée.
- **Sécurité** : cryptographie de pointe (ChaCha20, Curve25519...).
- **Simplicité** : configuration rapide, fichiers de configuration très courts.
- **Léger** : faible consommation de ressources, très stable.

---

3. Mise en œuvre du projet

Étapes réalisées :

1. **Analyse des besoins**
   Étude des usages, contraintes réseau et sécurité pour proposer une solution adaptée.
2. **Choix technologique**
   Même si OpenVPN était mentionné initialement, j'ai opté pour **WireGuard** pour sa légèreté, sa rapidité de déploiement et sa performance.
3. **Installation & Configuration**
   - Installation de WireGuard sur le serveur Proxmox.
   - Génération des paires de clés pour le serveur et les clients.
   - Configuration de l'interface wg0 sur le serveur.
   - Redirection des ports nécessaires sur la Livebox (port UDP 51820).
   - Création des profils client et déploiement sur les postes utilisateurs.
4. **Tests et validation**
   - Connexion depuis différents postes distants (réseau ADSL et 4G).
   - Vérification de la stabilité de la connexion, de l'accès aux services internes et de la sécurité.
5. **Documentation**
   - Rédaction d'un guide utilisateur (fichier de configuration, installation client WireGuard).
   - Sauvegarde des configurations serveur.
6. **Mise en production**
   - Déploiement opérationnel de la solution.
   - Suivi en phase pilote pour affiner les réglages.

---

4. Bénéfices apportés

- Accès distant sécurisé et permanent à l'environnement Proxmox.
- Simplicité de gestion et de maintenance du VPN.
- Amélioration de la productivité en permettant le travail à distance.

- Environnement de test accessible à tout moment pour les expérimentations internes.

---

5. Perspectives

- Ajouter une interface d’administration graphique pour simplifier la gestion des pairs WireGuard.
- Intégrer la supervision du tunnel VPN avec un outil de monitoring (Zabbix, Grafana…).
- Étendre l’usage du VPN à d’autres services internes du SI.