Mise en Place d’un VPN – Société SMH.JBT (Annecy)

Semih DAG

BTS SIO 2024-2025

Table des matières

1. Objectifs du VPN pour SMH.JBT

La société SMH.JBT souhaite mettre en place une solution VPN afin de permettre à ses collaborateurs de se connecter de manière sécurisée au réseau interne de l'entreprise, notamment pour :

- Le télétravail
- L'accès distant aux serveurs internes (ERP, fichiers partagés)
- L'administration des équipements informatiques

2. Qu'est-ce qu'un VPN ?

Un VPN (réseau privé virtuel) permet de créer un tunnel chiffré entre un poste distant (PC, smartphone) et le réseau de l'entreprise. Les données sont transmises en toute sécurité via Internet comme si l'utilisateur était physiquement dans les locaux.

Avantages :

- Sécurité renforcée grâce au chiffrement
- Confidentialité des données
- Accès aux ressources internes (partages SMB, imprimantes, intranet, etc.)

3. Technologies VPN possibles

Solution	Protocole	Avantages	Remarques
OpenVPN	TLS/SSL	Open-source, très sécurisé	Nécessite un client installé
IPsec (avec L2TP)	IPsec	Intégré aux OS, hautement fiable	Plus complexe à

configurer
WireGuard | WireGuard | Moderne, rapide et léger | Moins de support sur vieux OS
VPN SSL (Forti) | HTTPS | Accès via navigateur ou client | Dépend du firewall utilisé

Recommandation pour SMH.JBT : OpenVPN ou VPN SSL via firewall professionnel (type Fortinet ou Sophos).

4. Étapes de Mise en Place

A. Côté Serveur (Entreprise)

1. Choix de l'infrastructure VPN (OpenVPN, Fortinet...)
2. Configuration réseau : ouverture du port VPN (ex. UDP 1194), plage IP dédiée (ex : 10.8.0.0/24)
3. Génération des certificats/identifiants utilisateurs
4. Sécurité : authentification forte, journalisation

B. Côté Client (Collaborateurs)

1. Installation du client VPN (OpenVPN Connect, FortiClient...)
2. Importation du fichier de configuration (.ovpn)
3. Connexion avec les identifiants fournis
4. Vérification de l'accès aux ressources internes

5. Sécurité et Bonnes Pratiques

- Utilisation de certificats pour l'authentification
- Implémentation d'une MFA (authentification à deux facteurs)
- Surveillance des connexions VPN actives
- Limitation des droits selon les profils
- Chiffrement robuste (AES-256)

6. Schéma Réseau VPN (optionnel)

Un schéma visuel peut être fourni pour illustrer l'architecture :
- Poste distant -> Internet -> Firewall/VPN Server -> Réseau interne
- Interaction avec le pare-feu, l'Active Directory et les serveurs applicatifs