Mise en place d'un VPN pour Kompta Plus Bien (KPB)

1. Contexte et Objectif

Avec la generalisation du teletravail, KPB souhaite permettre a ses 30 salaries d'acceder a distance, de facon securisee, aux ressources internes de l'entreprise (documents de comptabilite, factures, dossiers partages). L'environnement technique est base sur Debian Linux, ce qui rend OpenVPN particulierement adapte pour repondre a ces besoins grace a sa robustesse et sa flexibilite.

2. Presentation de la solution retenue

Serveur OpenVPN : installe sur une VM Debian dediee, avec une adresse IP fixe et des regles de pare-feu adaptees.

Clients OpenVPN : chaque salarie disposera d'un profil personnalise pour se connecter depuis un poste Debian.

Chiffrement fort : utilisation de l'algorithme AES-256-GCM, reconnu pour sa securite et ses performances.

Haute disponibilite : un plan de secours est prevu pour garantir la continuite de service en cas de panne serveur.

3. Environnement de test (maquette)

Avant la mise en production, une maquette sera realisee :

VM1 : serveur OpenVPN sous Debian (CLI).

VM2 : client OpenVPN sous Debian (GUI ou CLI selon les besoins).

Cela permet de valider la configuration, la securite et la connectivite.

4. Installation et configuration d'OpenVPN

a. Mise a jour du systeme

```
sudo apt update && sudo apt upgrade -y
```

b. Installation d'OpenVPN et Easy-RSA

```
sudo apt install openvpn easy-rsa -y
```

c. Mise en place de la PKI

```
make-cadir ~/openvpn-ca
cd ~/openvpn-ca
source vars
./clean-all
./build-ca
./build-key-server server
./build-dh
./build-key client1
```

Remarque : Generer un certificat et une cle pour chaque utilisateur.

d. Configuration du serveur OpenVPN

Copier les fichiers necessaires dans /etc/openvpn/ : ca.crt, server.crt, server.key, dh.pem

Creer le fichier /etc/openvpn/server.conf :

```
port 1194
proto udp
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh.pem
cipher AES-256-GCM
auth SHA256
user nobody
group nogroup
persist-key
persist-tun
status openvpn-status.log
verb 3
```

Securite supplementaire : ajouter tls-crypt ta.key.

e. Demarrage et activation du service

```
sudo systemctl start openvpn@server
sudo systemctl enable openvpn@server
```

f. Configuration des clients

Generer un certificat et une cle pour chaque client.

Creer un fichier de configuration client (ex : client1.ovpn) :

```
client
dev tun
proto udp
remote [IP_PUBLIQUE_SERVEUR] 1194
resolv-retry infinite
nobind
persist-key
persist-tun
cipher AES-256-GCM
auth SHA256
remote-cert-tls server
verb 3
<ca>...contenu ca.crt...</ca>
<cert>...contenu client1.crt...</cert>
<key>...contenu client1.key...</key>
```

Transferer le fichier .ovpn au client via SFTP ou cle USB.

5. Resilience et plan de secours

Serveur de secours : preparer une deuxieme VM Debian avec la meme configuration et les memes certificats.

Basculement automatique : configurer les clients pour tenter plusieurs serveurs dans leur fichier .ovpn :

```
remote serveur1.kpb.fr 1194
remote serveur2.kpb.fr 1194
```

Sauvegarde reguliere : scripts automatises pour sauvegarder la configuration et les certificats.

Surveillance : mettre en place une supervision du service OpenVPN (ex : avec Nagios, Zabbix ou scripts maison).

6. Bonus : Authentification a deux facteurs (2FA)

Google Authenticator ou Duo peuvent etre integres pour renforcer la securite.

Installer le module PAM approprie sur le serveur.

Configurer OpenVPN pour utiliser PAM en plus des certificats.

Chaque utilisateur associe son smartphone a son compte (QR code).

A la connexion, le client devra fournir un code temporaire genere par l'application mobile.

7. Recommandations et bonnes pratiques

Tests approfondis sur la maquette avant mise en production.

Formation et sensibilisation des utilisateurs a l'usage du VPN et aux bonnes pratiques de securite

(choix des mots de passe, gestion des fichiers de configuration).

Documentation interne detaillee pour l'administration et la maintenance du VPN.

Mises a jour regulieres du serveur et des clients pour garantir la securite.

8. Conclusion

La solution OpenVPN sur Debian, avec chiffrement AES-256-GCM et authentification forte, permet a KPB d'assurer la securite des acces distants pour le teletravail. Le plan de secours et l'option 2FA garantissent la continuite et la robustesse de l'infrastructure VPN.