Installation et configuration d’un serveur OpenVPN sur Debian 13

Table des matières / Sommaire

1. Cahier des charges – Expression des besoins

Descriptif de l'existant

L'entreprise dispose d'un réseau interne avec des ressources critiques (serveurs, fichiers, applications internes). Actuellement, l'accès à ces ressources nécessite une présence physique ou une connexion directe au réseau local. Il n'existe pas de solution sécurisée permettant aux techniciens d'intervenir à distance, ce qui limite la réactivité, notamment en situation de mobilité ou de télétravail.

Besoin(s)

L'objectif est de mettre en place un accès à distance sécurisé pour les techniciens du service informatique. La solution doit permettre :

- La connexion au réseau interne depuis n'importe quel accès internet (télétravail, déplacement).
- La garantie de la sécurité des données grâce à un canal de communication chiffré (VPN).
- L'authentification forte des utilisateurs via des certificats numériques.
- Une réduction des risques d'interception de données sur Internet.

Contrainte(s)

Type de contrainte	Description
Technique	Utilisation du logiciel OpenVPN sur un système Debian 13.
Sécurité	Chiffrement obligatoire des flux (Confidentialité et Intégrité).
Organisation	Utilisation d'un script d'automatisation GitHub pour limiter les erreurs humaines lors du déploiement.
Financière	Solution basée sur des outils Open Source (coût de licence nul).

2. Ressources

Ressources mises à disposition

- **Serveur :** Une machine sous Debian 13 configurée et fonctionnelle.
- **Droits :** Un compte avec les privilèges d'administrateur (**root** ou **sudo**) pour l'installation des services.
- **Réseau :** Un accès internet pour les mises à jour et le port **UDP 1194** ouvert sur le pare-feu ou le routeur.

Ressources dont vous avez besoin pour la réalisation

- **Script d'automatisation :** Le script d'installation OpenVPN récupéré sur GitHub pour automatiser la configuration.
- **Outils d'administration :** Un terminal avec accès **SSH** pour la gestion distante du serveur et un éditeur de texte type **Nano**.
- **Logiciel Client :** L'application **OpenVPN Connect** à installer sur les postes Windows ou Linux des techniciens.

Façon dont vous allez gérer ses ressources

Pour optimiser le déploiement, les ressources sont gérées de manière centralisée. L'utilisation du script GitHub permet de générer automatiquement les certificats de sécurité et les profils clients, ce qui réduit les erreurs de configuration manuelle et assure une gestion fluide des accès.

3. Analyse

Descriptifs des solutions

La solution retenue est **OpenVPN**, un logiciel open-source permettant de créer un tunnel sécurisé (VPN SSL/TLS) entre un client distant et le réseau de l'entreprise. Il assure que toutes les données circulant sur Internet sont encapsulées dans un flux chiffré, rendant les informations illisibles pour un tiers.

Comparaison des solutions

Critère	OpenVPN	VPN IPsec
Coût	Gratuit (Open-Source)	Souvent lié à du matériel payant
Mise en œuvre	Simple (via script automatisé)	Complexe à configurer
Flexibilité	Haute (compatible tous OS)	Moyenne (dépend du matériel)

Choix d'une solution

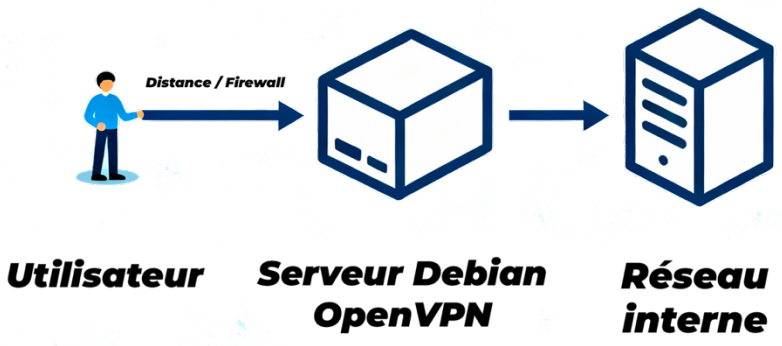
OpenVPN a été choisi car il répond parfaitement aux contraintes de l'entreprise :

- **Sécurité :** Utilisation de protocoles de chiffrement robustes.
- **Coût :** Logiciel gratuit, ce qui respecte le budget zéro.
- **Fiabilité :** L'automatisation par script GitHub garantit une installation propre, sans erreurs de configuration humaine sur les certificats.

Plan d'adressage

Le fonctionnement repose sur la création d'un tunnel entre l'IP publique du serveur et le poste client.

- **IP LAN du serveur :** 172.26.1.40
- **Port utilisé :** 1194 (UDP)
- **Réseau VPN (virtuel) :** 10.8.0.0/24

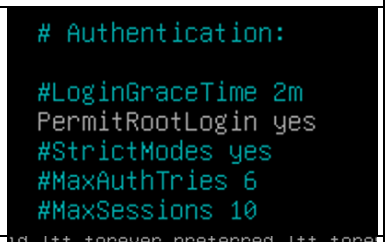
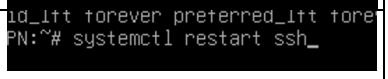
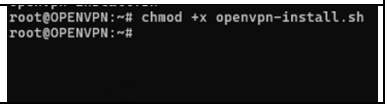


Étude de l'impact sur le SI existant

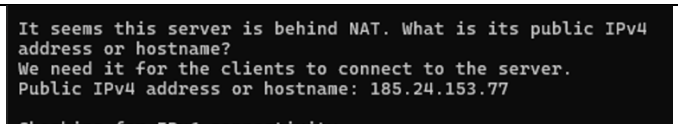
La mise en place de cette solution impacte positivement la sécurité du Système d'Information :

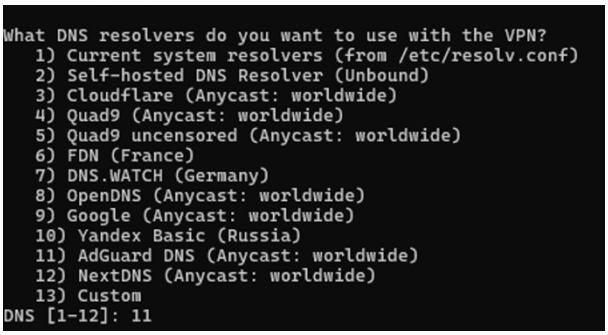
- **Confidentialité** : Seuls les possesseurs du certificat .ovpn peuvent lire les données.
- **Intégrité** : Le tunnel empêche la modification des paquets durant le transport.
- **Disponibilité** : Les techniciens peuvent désormais assurer la maintenance du réseau à tout moment, même à distance.

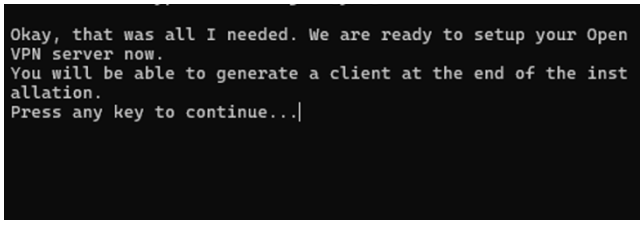
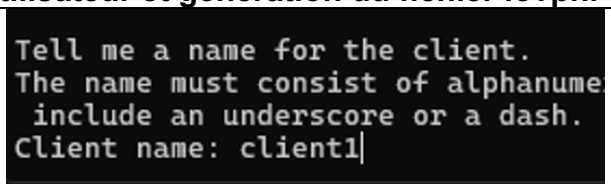
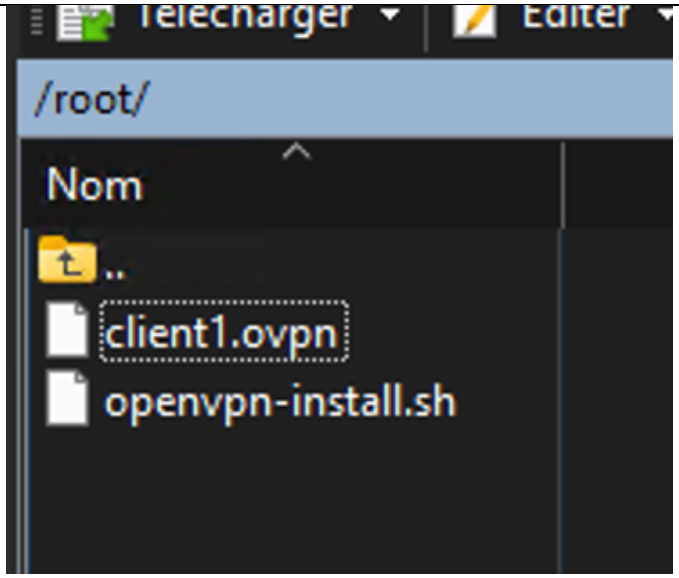
4. Mise en place

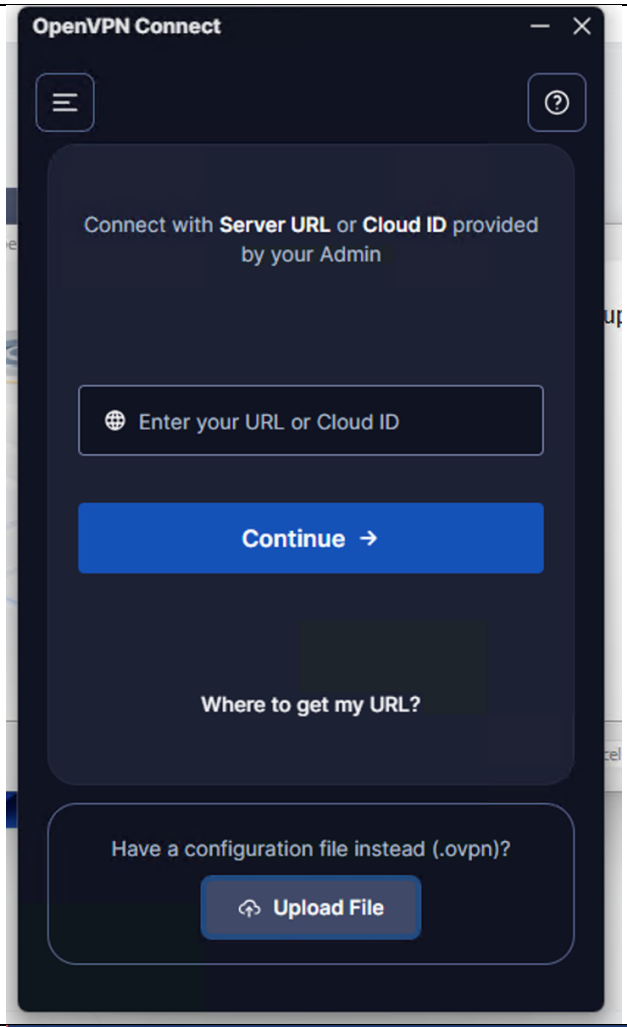
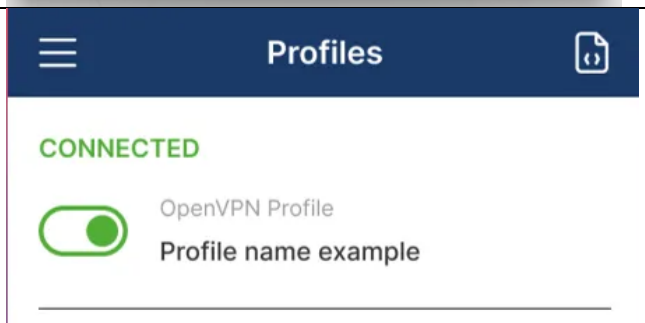
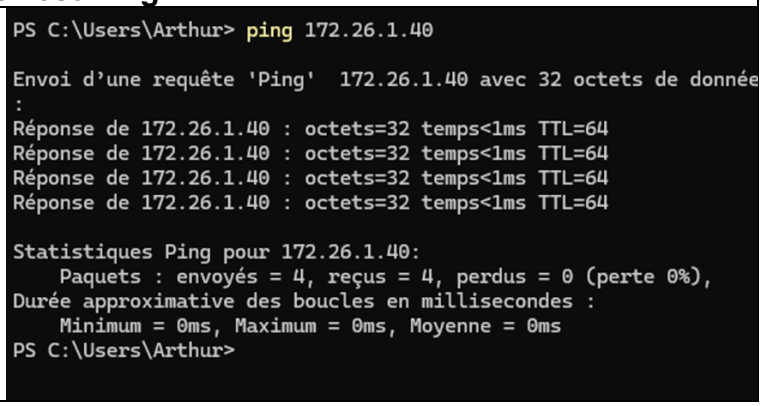
Étapes	Description	Images
Étape 1 à 4 : Configuration du SSH et accès Root.		
1	Éditer le fichier sshd_config (optionnel) sudo nano /etc/ssh/sshd_config Cela va permettre de se connecter en SSH en tant que root.	
2	Dans le fichier il faudra changer : **« PermitRootLogin yes »** Cela permet la connexion SSH directe avec le compte root. Puis sauvegarder le fichier.	
3	Redémarrer le service SSH **« systemctl restart sshd »**	
4	Ensuite connexion au serveur Se connecter en SSH au serveur Debian : ssh root@ip_du_serveur	
Étape 5 : Mise à jour du système (apt update).		
5	Faire une mise à jour du système **« apt update && apt upgrade -y »**	
Étape 6 à 7 : Téléchargement et lancement du script GitHub.		
6	Téléchargement du script GitHub OpenVPN « curl -O https://raw.githubusercontent.com/angristan/openvpn-install/master/openvpn-install.sh » Cette commande va permettre de récupérer le lien de la distribution OpenVPN sur GitHub.	
7	Donner les droits d'exécution au script « chmod +x openvpn-install.sh »	

<table>
<tr><th colspan="3">Étape 8 : Configuration des paramètres (IP, Port 1194, DNS Cloudflare).</th></tr>
<tr><td>8</td><td>Lancer l'installation du serveur OPENVPN.
En faisant : « ./openvpn-install.sh »

Le script posera plusieurs questions :
- Adresse IP publique -> Accepter par défaut (Entrée)
- Protocole (UDP/TCP) → Choisir UDP
- Port → Laisse 1194
- DNS à utiliser → Choisir par exemple 3 : DNS Cloudflare.
L'installation démarre automatiquement.</td><td> 




</td></tr>
<tr><td colspan="3">Étape 9 à 10 : Création de l'utilisateur et génération du fichier .ovpn.</td></tr>
<tr><td>9</td><td>On va choisir le nom du premier client pour le VPN qui sera : Client1
Ensuite appuyer sur la touche (Entrée)</td><td> 
</td></tr>
<tr><td>10</td><td>Ensuite il faut récupérer du profil client dans le répertoire du PC /root/client1.ovpn.</td><td> 
</td></tr>
<tr><td colspan="3">Étape 11 à 12 : Configuration du client OpenVPN</td></tr>
</table>

11	Sur la machine du client il faudra installer OPENVPN Connect depuis : https://openvpn.net/client/ Après avoir installé l'outil sur l'ordinateur il faudra cliquer « Upload file »	
12	Le client est maintenant connecté au VPN. Qu'on a mis en place.	
Étape 13 : Connecté au VPN / Test Ping		
13	Depuis le poste client, effectuer un test de connectivité : Si le ping répond, la connexion VPN est fonctionnelle. Le ping depuis le poste client, le VPN fonctionne.	

Rapport de tests

Vérification	Commande / Méthode	Résultat attendu
Service OpenVPN actif	systemctl status openvpn	Actif (running)
Port 1194 ouvert	‘ss -tulpn	Grep 1194’
Client connecté	Vérification via OpenVPN Connect	Oui
Ping du client vers l’IP du serveur	Ping 10.8.0.1	OK

Rapport de déploiement

Le serveur est pleinement opérationnel. Le fichier de configuration a été importé avec succès dans le client **OpenVPN Connect**. La connexion est stable et le tunnel chiffré permet d'accéder aux ressources du LAN sans erreur.

5. Bilan

Conclusion

La mise en place du serveur **OpenVPN** sur Debian 13 répond parfaitement aux besoins initiaux de l'entreprise. Cette solution permet désormais aux techniciens d'accéder aux ressources internes de manière sécurisée, tout en garantissant la **confidentialité** et l'**intégrité** des données grâce au tunnel chiffré. L'utilisation du script automatisé a permis un déploiement rapide, fiable et conforme aux contraintes de temps et de budget fixées.

Auto évaluation sur la qualité du travail réalisé

Le projet a été mené à bien et le résultat est totalement fonctionnel, comme le prouvent les tests de connectivité réussis. Ce travail m'a permis de mobiliser et de valider plusieurs compétences essentielles du bloc **SISR.**

Compétence SISR mobilisée	Description du travail réalisé
Gérer le patrimoine informatique	Installation et configuration complète d'un service réseau sécurisé sous Debian[7].
Assurer la continuité de service	Mise en place d'un accès distant pour maintenir la disponibilité des ressources[8].
Mettre en œuvre la sécurité du SI	Utilisation d'un tunnel VPN et de certificats pour protéger les flux[9].