Test de solutions VPN

**Table des matières**

***Algo VPN***

[***1.*** ***Installation*** 2](#_Toc173512527)

[**Algo VPN** 2](#_Toc173512528)

[**SSH** 5](#_Toc173512529)

[**Ansible** 6](#_Toc173512530)

[**Curl** 6](#_Toc173512531)

[**WireGuard** 6](#_Toc173512532)

[**2.** **Conclusion** 9](#_Toc173512533)

**Open VPN**

[***1.*** ***Installation*** 11](#_Toc173512534)

[***2.*** ***Configuration*** 11](#_Toc173512535)

[**3.** **Conclusion** 13](#_Toc173512536)

**Final**

[**1.** **Comparatif Final** 15](#_Toc173512537)

**ALGO VPN**

# ***Installation***

## **Algo VPN**

1. **Passer en root & upgrade**

sudo su

apt update && apt upgrade -y

1. **Installer les dépendances nécessaires**

apt install python3 python3-pip git -y

1. **Installer git si besoin**

apt install git”

1. **Cloner le dépôt**

git clone <https://github.com/trailofbits/algo>

1. **Accéder au répertoire Algo**

cd algo

1. **Installé et configurer l’environnement virtuel**

“python3 -m pip install --upgrade pip virtualenv”

“python3 -m virtualenv --python="$(command -v python3)" .env”“source .env/bin/activate”

1. **Installé les dépendances**

python3 -m pip install -r requirements.txt

1. **Lancé le script d’installation Algo**

“./algo”

1. **Installer sur un serveur Ubuntu existant**

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

1. **Sélectionnez-‘Y’ pour les 2 prochaines questions**

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

1. **Sélectionnez**

‘’HomeNet’’

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

1. **Sélectionnez ‘Y’ pour les 3 prochaines questions**

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

1. **Entrez l’IP récupérer avec Curl**



1. **Message final Algo**

**Une image contenant texte, capture d’écran, Police

Description générée automatiquement**

## **SSH**

1. **Installé Open-SSH**

dpkg -s openssh-server

apt install openssh-server

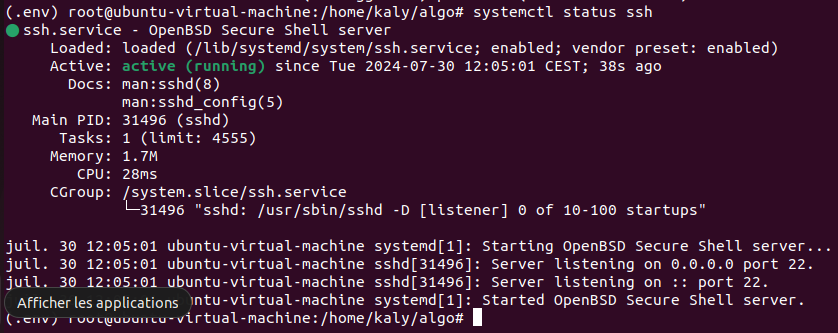
1. **Configurer les ports & les autorisation**

‘’sudo nano /etc/ssh/sshd\_config’’

* Port 22
* PermitRootLogin yes
* PubkeyAuthentication yes
* PasswordAuthentication no

1. **Assurez-vous que le service est en cours**

‘’systemctl status ssh’’



1. **Restart SHH**

‘sudo systemctl restart ssh

1. **Surveillance de port**

sudo tcpdump -i ens33 port 22

1. **Forcer le mode promiscuous**

sudo ip link set ens33 promisc on

## **Ansible**

1. **Installer Ansible**

sudo apt install ansible

1. **Configurer le fichier Ansible** config.cfg

sudo nano config.cfg

« ansible\_ssh\_port: 22 »

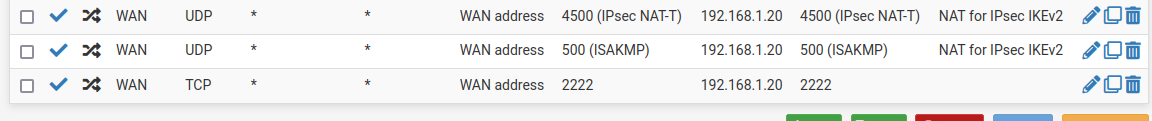
## **Curl**

1. **Installer Curl**   
   sudo apt install curl
2. **Noté L’IP**

Curl ifconfig.me

1. **Configurer Algo VPN & PfSense**

Derrière un routeur PfSense, vous devez vous assurer que les ports 500 et 4500 sont ouverts et redirigés vers votre serveur VPN.



## **WireGuard**

1. **Installez WireGuard**

sudo apt-get install wireguard

1. **Générez la clé privée du serveur**

wg genkey | sudo tee /etc/wireguard/server\_private.key

1. **Générez la clé publique du serveur**

sudo cat /etc/wireguard/server\_private.key | wg pubkey | sudo tee /etc/wireguard/server\_public.key

1. **Générez la clé privée du client :**

wg genkey | sudo tee /etc/wireguard/client\_private.key

1. **Générez la clé publique du client :**

sudo cat /etc/wireguard/client\_private.key | wg pubkey | sudo tee /etc/wireguard/client\_public.key

1. **Créez le fichier de configuration du serveur :**

sudo nano /etc/wireguard/wg0.conf

1. **Ajoutez le contenu suivant au fichier**wg0.conf

[Interface]

PrivateKey = <contenu de /etc/wireguard/server\_private.key>

Address = 10.49.0.1/24

ListenPort = 51820

[Peer]

PublicKey = <contenu de /etc/wireguard/client\_public.key>

AllowedIPs = 10.49.0.2/32

1. **Créez le fichier de configuration du client**

sudo nano /home/kaly/algo/configs/client\_phone.conf

1. **Ajoutez le contenu suivant au fichier**client\_phone.conf**:**

[Interface]

PrivateKey = <contenu de /etc/wireguard/client\_private.key>

Address = 10.49.0.2/24

DNS = 8.8.8.8

[Peer]

PublicKey = <contenu de /etc/wireguard/server\_public.key>

Endpoint = <adresse IP publique du serveur>:51820

AllowedIPs = 0.0.0.0/0

PersistentKeepalive = 25

1. **Démarrez le service WireGuard :**

sudo systemctl start wg-quick@wg0

1. **Activez le service WireGuard au démarrage**

sudo systemctl enable wg-quick@wg0

1. **Vérifiez l'état de WireGuard**

sudo wg show

1. **Activez le forwarding IP**

echo 1 | sudo tee /proc/sys/net/ipv4/ip\_forward

**Service WireGuard**

sudo systemctl stop wg-quick@wg0

sudo systemctl status wg-quick@wg0

sudo systemctl start wg-quick@wg0

# **Conclusion**

**Algo VPN**, se présente comme une solution de déploiement **VPN** moderne et sécurisée. Cependant, l'expérience utilisateur peut varier considérablement, en particulier lors de l'installation et de la configuration initiale.

**Complexité d'Installation**

L'installation d'**Algo VPN** peut s'avérer complexe et difficile pour de nombreux utilisateurs. Les étapes d'installation nécessitent souvent une compréhension approfondie des systèmes **Linux**, des lignes de commande, et des concepts de réseaux.

**Sécurité et Performance**

Malgré les difficultés d'installation, **Algo VPN** offre des avantages en termes de sécurité. Il utilise des protocoles modernes comme **WireGuard** et **IPsec** avec **IKEv2**, qui sont reconnus pour leur robustesse et leurs performances. La configuration par défaut est orientée vers la sécurité, ce qui est un point positif pour ceux qui parviennent à le mettre en place.

**Flexibilité et Personnalisation**

**Algo VPN** permet une grande flexibilité dans le choix du fournisseur d'hébergement et offre des options de personnalisation. Cependant, cette flexibilité peut aussi contribuer à la complexité de l'installation, car elle nécessite une compréhension des différentes plateformes cloud et de leurs spécificités.

**Support et Documentation**

L'expérience utilisateur pourrait être grandement améliorée par une documentation plus détaillée et accessible, ainsi que par un meilleur support pour les utilisateurs rencontrant des difficultés lors de l'installation.

**Conclusion Générale**

**Algo VPN** est une solution qui promet une sécurité élevée et des performances optimales, mais au prix d'un processus d'installation qui peut être décourageant pour de nombreux utilisateurs. Bien qu'il offre des avantages en termes desécurité et de flexibilité, il n'est peut-être pas la solution la plus adaptée pour ceux qui recherchent une expérience "plug-and-play" ou qui n'ont pas de solides connaissances techniques.

Pour les utilisateurs prêts à investir du temps dans l'apprentissage et la configuration, Algo VPN peut offrir une solution VPN robuste et personnalisable.

**OPEN VPN**

# ***Installation***

1. **Installer OpenVPN & OpenSSH**

‘’sudo apt install openvpn openssh-server’’

# ***Configuration***

***Open VPN***

1. **Télécharger le script d'installation**

‘’wget https://git.io/vpn -O openvpn-install.sh’’

1. **Rendre le script exécutable**

‘’chmod +x openvpn-install.sh’’

1. **Exécuter le script d'installation**

‘’sudo ./openvpn-install.sh’’

***Suivre les instructions à l'écran pour configurer OpenVPN***

**Easy-RSA**

1. **Installer Easy-RSA**

‘’sudo apt install easy-rsa’’

1. **Configuration de Easy-RSA**

‘’mkdir ~/easy-rsa

ln -s /usr/share/easy-rsa/\* ~/easy-rsa/

cd ~/easy-rsa’’

1. **Initialisation de l'infrastructure PKI**

‘’./easyrsa init-pki’’

1. **Création de l'autorité de certification (CA)**

‘’./easyrsa build-ca nopass’’

1. **Génération de la demande de certificat pour le serveur**

‘’./easyrsa gen-req server nopass’’

1. **Signature de la demande de certificat du serveur**

‘’./easyrsa sign-req server server’’

1. **Copie des fichiers générés dans le répertoire OpenVPN**

‘’sudo cp ~/easy-rsa/pki/ca.crt /etc/openvpn/server/

sudo cp ~/easy-rsa/pki/issued/server.crt /etc/openvpn/server/

sudo cp ~/easy-rsa/pki/private/server.key /etc/openvpn/server/

sudo cp ~/easy-rsa/pki/dh.pem /etc/openvpn/server/

sudo cp ~/easy-rsa/ta.key /etc/openvpn/server/’’

1. **Création du fichier de configuration du serveur**

‘’sudo nano /etc/openvpn/server.conf’’

1. **Ajoutez le contenu suivant dans le fichier de configuration**

port 1194

proto udp

dev tun

ca /etc/openvpn/server/ca.crt

cert /etc/openvpn/server/server.crt

key /etc/openvpn/server/server.key

dh /etc/openvpn/server/dh.pem

server 10.8.0.0 255.255.255.0

ifconfig-pool-persist /etc/openvpn/server/ipp.txt

push "redirect-gateway def1 bypass-dhcp"

push "dhcp-option DNS 8.8.8.8"

push "dhcp-option DNS 8.8.4.4"

keepalive 10 120

cipher AES-256-CBC

user nobody

group nogroup

persist-key

persist-tun

status /etc/openvpn/server/openvpn-status.log

verb 3

1. **Vérification des permissions des fichiers**

sudo chown -R root:root /etc/openvpn/server/

sudo chmod 600 /etc/openvpn/server/server.key

***Pare-Feu***

1. **Autoriser le trafic OpenVPN port UDP 1194 & Open**

sudo ufw allow 1194/udp

sudo ufw allow 22/tcp

***Vérification des services***

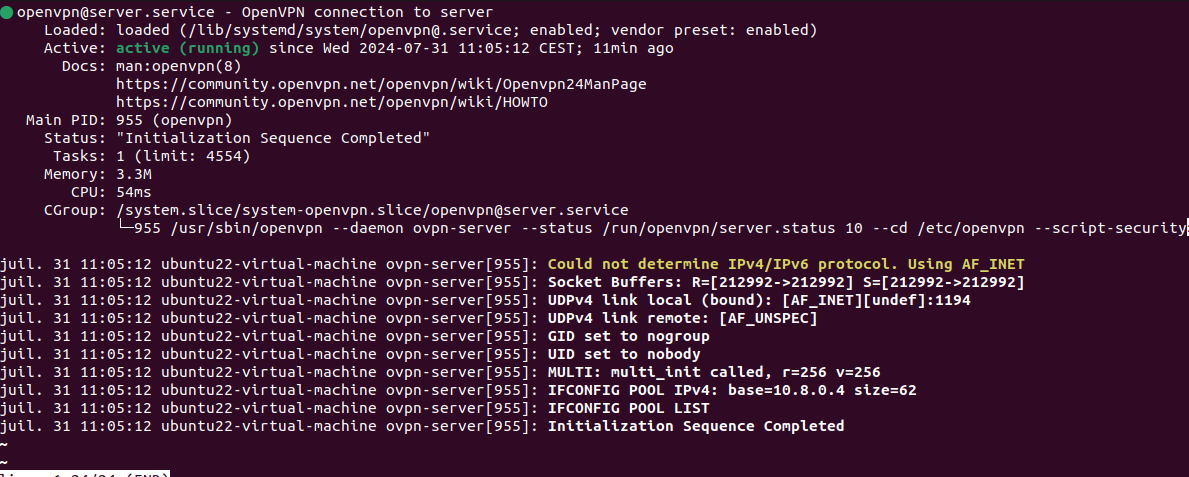
1. **Vérifier le statut d'OpenVPN et OpenSSH**

sudo systemctl status openvpn@server

sudo systemctl status ssh

***Exécuter à nouveau le script pour ajouter un nouveau client***

‘’sudo ./openvpn-install.sh’’



# **Conclusion**

**Open VPN** est l'un des protocoles VPN les plus populaires et les plus utilisés dans le monde. Il a été développé pour offrir une solution VPN flexible, sécurisée et compatible avec une grande variété de plateformes.

**Sécurité**

**OpenVPN** est reconnu pour sa robustesse en matière de sécurité. Il utilise des protocoles de chiffrement de pointe tels que **AES-256**, ainsi que des certificats pour l'authentification. Cette combinaison offre une protection solide contre les interceptions et les attaques.

**Flexibilité**

L'un des principaux avantages **d'OpenVPN** est sa flexibilité. Il peut être configuré pour fonctionner sur presque toutes les plateformes, y compris Windows, macOS, Linux, Android et iOS. **OpenVPN** peut être utilisé en mode **TCP** ou **UDP**, ce qui permet de s'adapter à différents types de réseaux et de besoins.

**Performance**

En termes de performance, OpenVPN est généralement plus lent que les protocoles plus récents comme WireGuard. Cela est dû à sa complexité et à la quantité de traitement nécessaire pour le chiffrement et le déchiffrement des données. Cependant, OpenVPN reste performant et fiable pour la plupart des usages courants.

**Support et compatibilité**

**OpenVPN** bénéficie d'un large support et est compatible avec de nombreux dispositifs et systèmes d'exploitation. Il est également supporté par de nombreux fournisseurs de services VPN commerciaux, ce qui en fait un choix populaire pour les entreprises et les particuliers

**Conclusion Générale**

**OpenVPN** est une solution VPN éprouvée et fiable, offrant une grande flexibilité et une sécurité robuste, il reste une option solide pour ceux qui ont besoin d'une solution VPN flexible et compatible avec une large gamme de dispositifs. Pour les utilisateurs recherchant une performance maximale et une installation simplifiée, des alternatives comme WireGuard peuvent être plus appropriées. Cependant, pour ceux qui privilégient la sécurité et la flexibilité, OpenVPN demeure un choix de premier ordre.

# **Comparatif Final**

**Protocole**

- Algo VPN utilise WireGuard comme protocole VPN principal.

- OpenVPN utilise son propre protocole propriétaire.

**Performance**

- Algo VPN, grâce à l'utilisation de WireGuard, offre généralement de meilleures performances en termes de vitesse et de latence.

- OpenVPN, bien que fiable, est généralement plus lent que WireGuard.

**Facilité d'utilisation**

- Algo VPN vise à simplifier le déploiement de VPN, mais peut être complexe pour les utilisateurs novices.

- OpenVPN dispose d'une documentation extensive et d'un large support communautaire.

**Sécurité**

- Les deux offrent un haut niveau de sécurité.

- Algo VPN bénéficie de la sécurité moderne de WireGuard.

- OpenVPN a une longue histoire de sécurité éprouvée.

**Flexibilité**

- Algo VPN offre une bonne flexibilité pour le déploiement sur différentes plateformes cloud.

- OpenVPN offre plus d'options de configuration et de personnalisation.

**Compatibilité**

- Algo VPN, utilisant WireGuard, a une bonne compatibilité avec les systèmes modernes.

- OpenVPN a une compatibilité plus large, notamment avec des systèmes plus anciens.

**En résumé**

Algo VPN, basé sur WireGuard, offre des performances supérieures pour le déploiement sur le cloud, ce qui le rend attrayant pour les utilisateurs recherchant une solution moderne et rapide. OpenVPN, en revanche, reste un choix solide pour ceux qui ont besoin d'une flexibilité maximale, d'une large compatibilité, et qui apprécient sa longue histoire de fiabilité et de sécurité éprouvée.

Le choix entre Algo VPN et OpenVPN dépendra donc des besoins spécifiques de l'utilisateur : pour une solution rapide et moderne orientée cloud, Algo VPN est préférable, tandis que pour une flexibilité maximale et une compatibilité étendue, OpenVPN reste un excellent choix.

**Fin**

Malgré tous mes efforts pour configurer et installer les solutions VPN, je n'ai pas réussi à établir une connexion fonctionnelle au réseau créé avec Algo VPN. Toutes les étapes de configuration ont été suivies avec soin, mais le résultat final n'a pas permis d'accéder au réseau.

En conséquence, je n'ai pas pu réaliser les tests de vitesse et les comparaisons pratiques initialement prévus.

Les conclusions et les comparaisons dans ce document reposent donc sur des recherches et des données théoriques plutôt que sur des résultats pratiques.