Test de solutions VPN

**Table des matières**

***ALGO***

[***1.*** ***Installation*** 2](#_Toc173325520)

[***2.*** ***Configuration*** 5](#_Toc173325521)

***Open VPN***

[***3.*** ***Installation*** 8](#_Toc173325523)

[***4.*** ***Configuration*** 8](#_Toc173325524)

**ALGO VPN**

# ***Installation***

1. **Passer en root**

“sudo su”

1. **Mettre à jour le système**

“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**

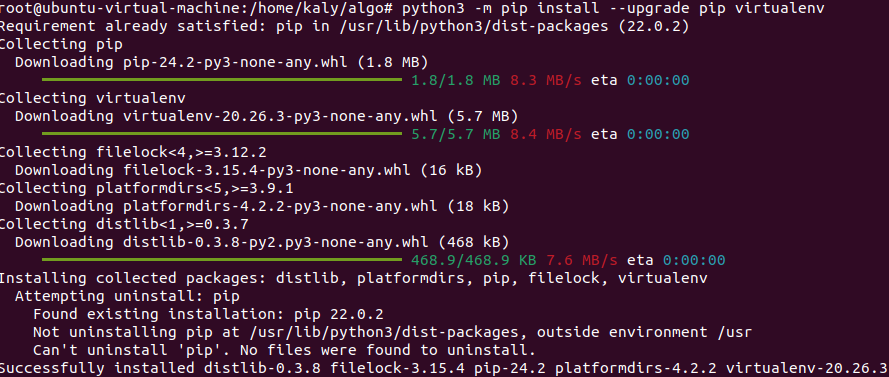
“git clone <https://github.com/trailofbits/algo>”

1. **Accéder au répertoire Algo**

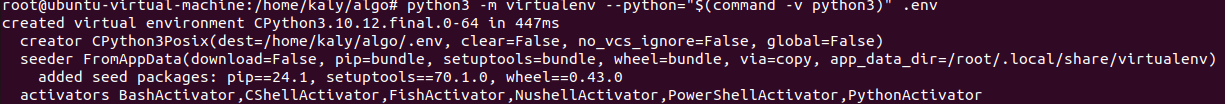
“cd algo”

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

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



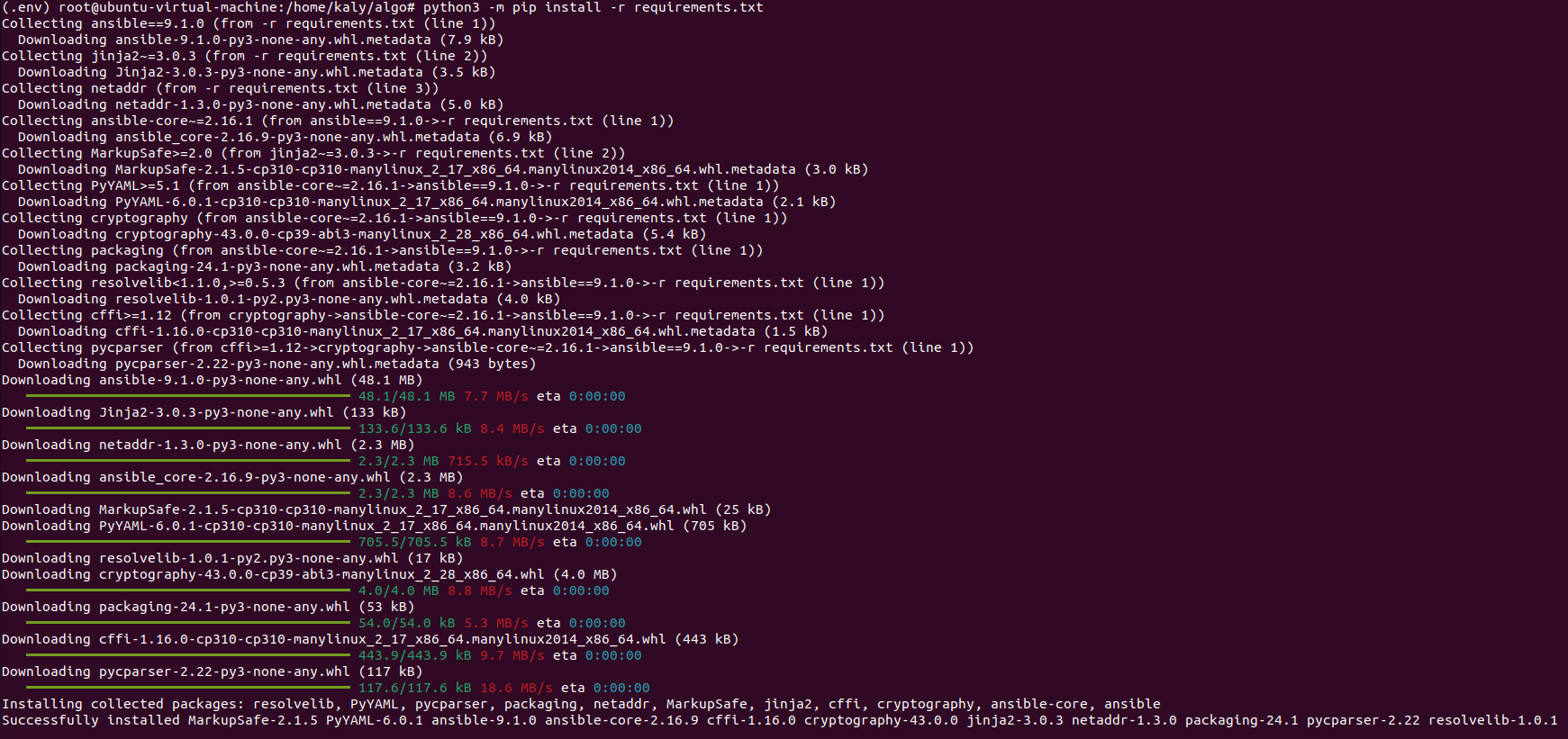
“python3 -m virtualenv --python="$(command -v python3)" .env”



“source .env/bin/activate”

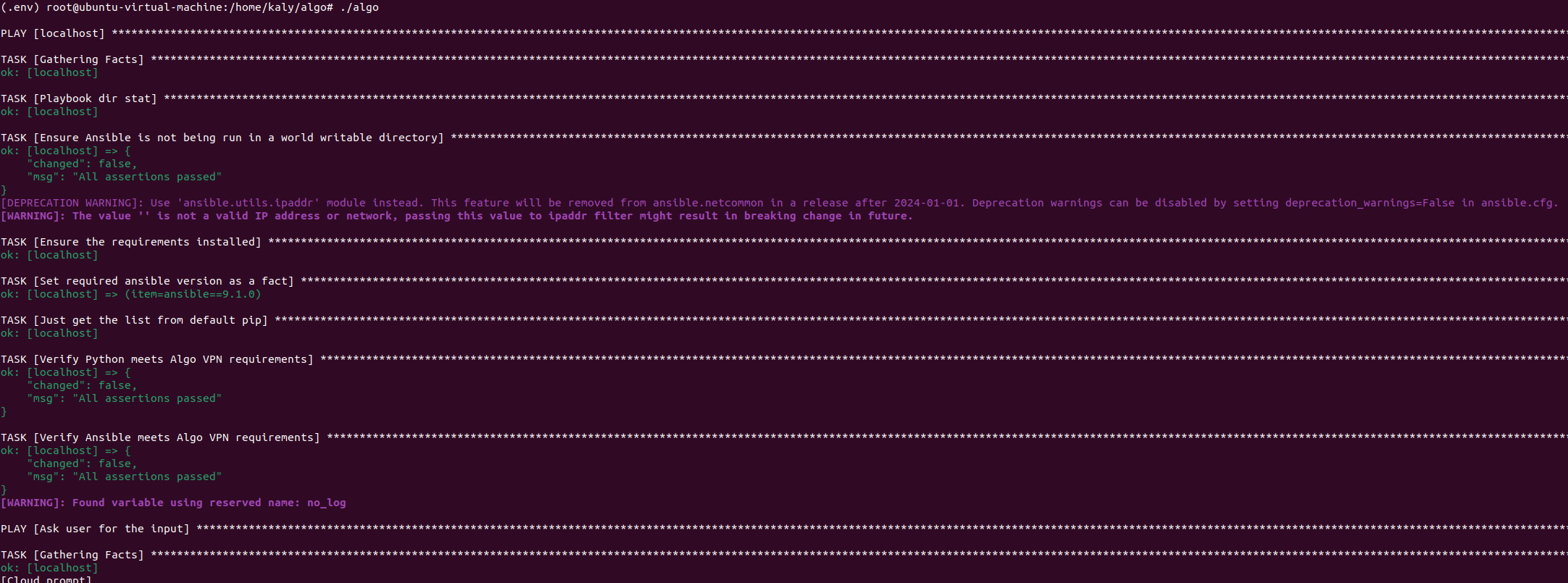
1. **Installé les dépendances**

“python3 -m pip install -r requirements.txt”



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

“./algo”



1. **Vérifiez si Open-SSH est installé sur votre système**

‘’dpkg -s openssh-server’’

1. **Si SSH n’est pas installé, installez-le**

‘’ apt update

apt install openssh-server’’

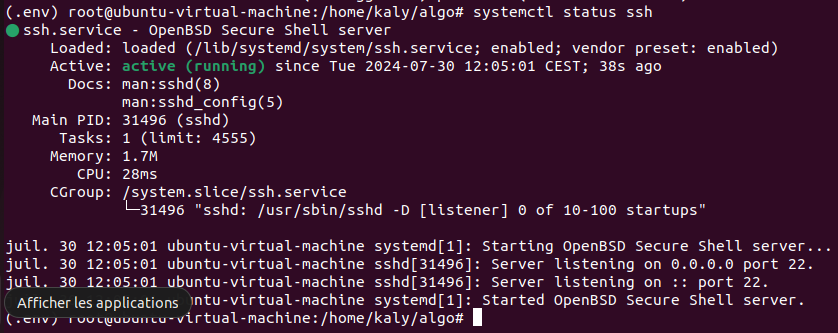
1. **Configurer les ports & les autorisation**

‘’sudo nano /etc/ssh/sshd\_config’’

* Port 22
* Port 2222
* PermitRootLogin yes
* PubkeyAuthentication yes
* PasswordAuthentication no

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

‘’systemctl status ssh’’



1. **Restart SHH**

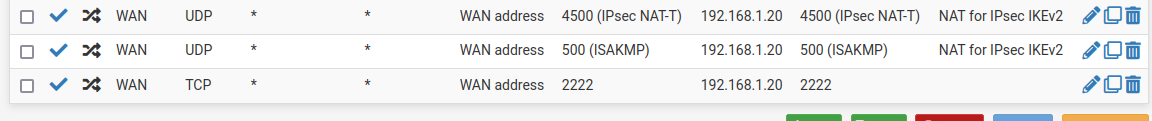
‘’ sudo systemctl restart ssh’’

1. **Installer Ansible**

‘’ sudo apt install ansible’’

1. **Installer Curl & Noter l’IP**  
   ‘’sudo apt install curl’’
2. **Pour configurer Algo VPN**

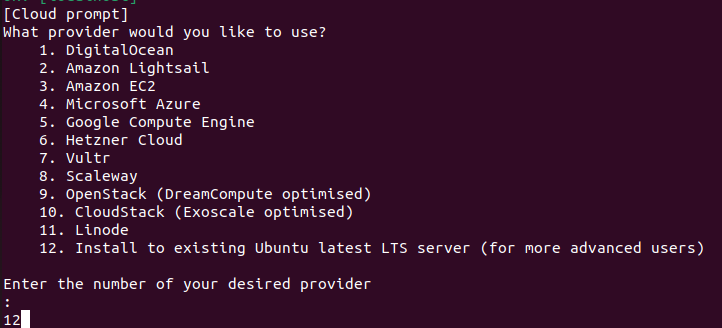
Derrière un routeur PfSense, vous devez vous assurer que les ports 500 et 4500 sont ouverts et redirigés vers votre serveur VPN.



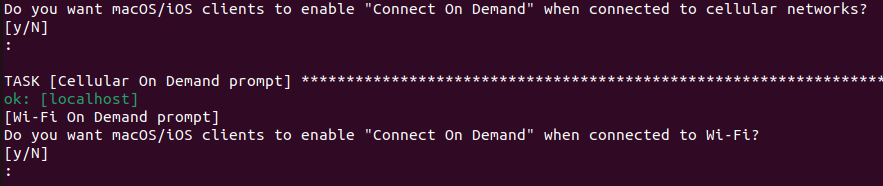
# ***Configuration***

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

“12’’

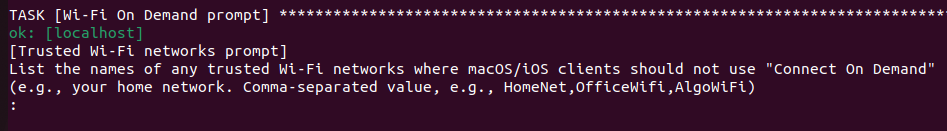


1. **Sélectionnez-‘Y’ pour les 2 prochaines questions**



1. **Sélectionnez**

‘’HomeNet’’



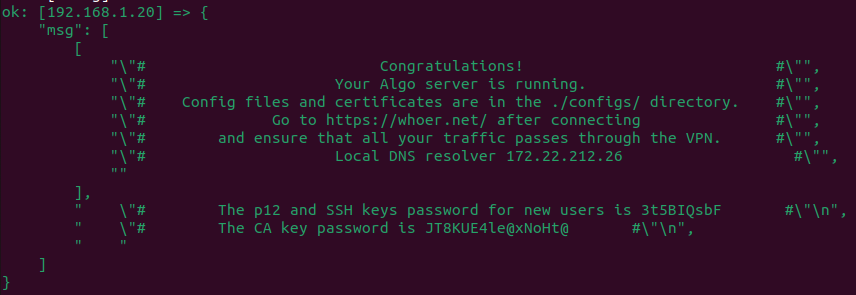
1. **Sélectionnez-‘Y’ pour les 3 prochaines questions**



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



1. **Fin**

****

# **Rappel**

**Arrêter le Service WireGuard**

‘’sudo systemctl stop wg-quick@wg0’’

**Vérification de l'État.**

‘’sudo systemctl status wg-quick@wg0’’

**Démarrer le Service WireGuard :**

‘’sudo systemctl start wg-quick@wg0’’

**OPEN VPN**

# ***Installation***

1. **Mettre à jour le système**

‘’sudo apt update

sudo apt upgrade’’

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**

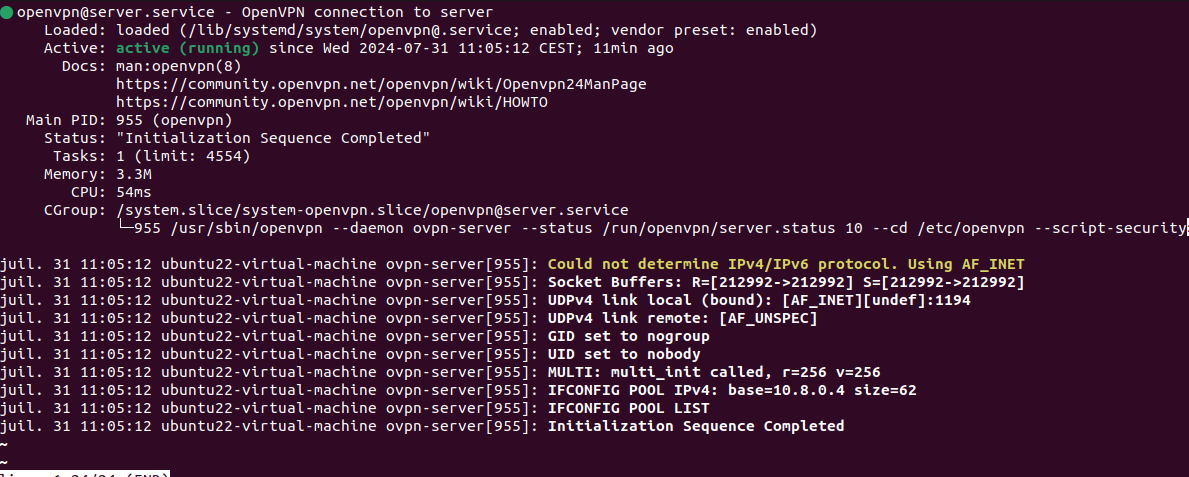
‘’sudo systemctl status openvpn@server’’

1. **Vérifier le statut d'OpenSSH**

‘’sudo systemctl status ssh’’

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

‘’sudo ./openvpn-install.sh’’



***Bonus***

**Stop the service**

‘’sudo systemctl stop openvpn@server’’

**Start the service**

‘’sudo systemctl start openvpn@server’’

**Restart the service**

‘’sudo systemctl restart openvpn@server’’

**Get the service status**

‘’sudo systemctl status openvpn@server’’

**Enable automatic startup of the OpenVPN service**

‘’sudo systemctl enable openvpn@server’’