OpenVPN est un logiciel libre permettant de créer un réseau privé virtuel (VPN). Son développement a commencé le 13 mai 2001 grâce à James Yonan.

SOMMAIRE

Télécharger le script d'installation

Connectez-vous sur votre futur serveur VPN, et commencez par mettre à jour le cache des paquets. On en profite aussi pour installer cURL.

```
sudo apt-get update
sudo apt-get install curl
```

Ensuite, téléchargez le script d'installation avec cURL :

```
curl -O https://raw.githubusercontent.com/Angristan/openvpn-install/master/openvpn-install.sh
```

Dès que le script est téléchargé, vous devez ajouter des droits d'exécution afin de pouvoir l'exécuter par la suite :

```
chmod +x openvpn-install.sh
```

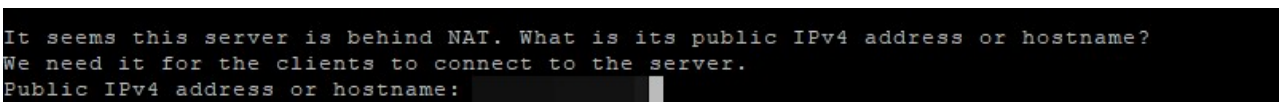
Ensuite, exécutez le script pour commencer la configuration pas à pas d'OpenVPN Server :

```
sudo ./openvpn-install.sh
```

Configurer le VPN

Le message "Welcome ton the OpenVPN installer!" s'affiche et les étapes de configuration vont s'enchaîner. Tout d'abord, il faut **indiquer l'adresse IPv4 du serveur VPN**, mais la bonne nouvelle, c'est qu'elle remonte automatiquement. **S'il s'agit de l'adresse IP locale, cela signifie qu'il y a un NAT et dans ce cas, c'est logique. Sinon, l'adresse IP publique de votre serveur, par exemple de votre serveur VPS, s'affichera ici.** Ici, le script remonte bien "192.168.100.51" Validez.

D'ailleurs, le script détecte la présence du NAT et indique l'adresse IP publique. Il suffit de valider, à moins que vous souhaitiez préciser un nom de domaine spécifique ou corriger l'information remontée par le script (qui s'appuie sur cURL pour récupérer votre IP publique).



Il est demandé si vous souhaitez activer le support IPv6, vous pouvez indiquer "n" pour refuser.

What port do you want OpenVPN to listen to?

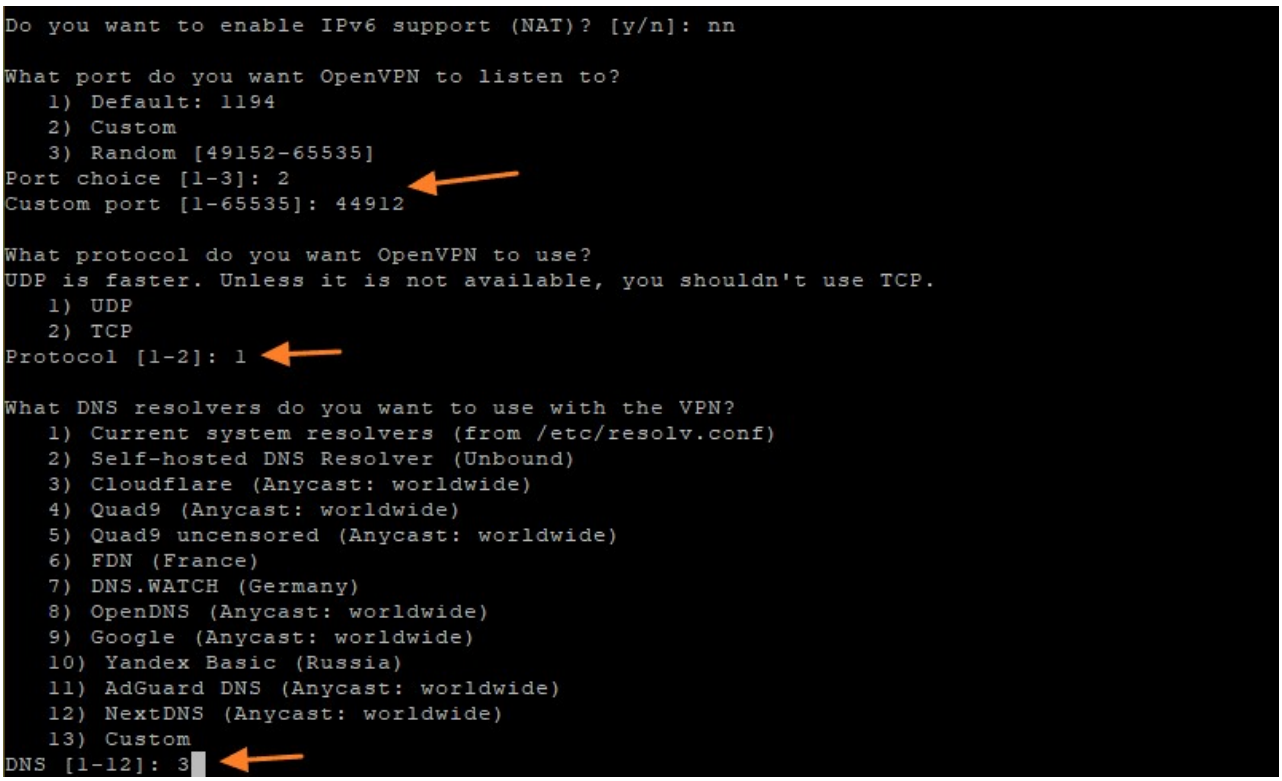
Ensuite, il faut choisir le port sur lequel va écouter le serveur VPN. **Par défaut, c'est le port 1194, mais je vous recommande d'utiliser un port personnalisé pour masquer votre VPN** (vous pouvez utiliser un port utilisé par un autre protocole (exemple : 443/HTTPS) pour passer plus facilement au travers de certains pare-feu).
Pour définir un port personnalisé, indiquez "2" puis indiquez le numéro de port. Par exemple "44912" dans mon exemple.

What protocol do you want OpenVPN to use ?

OpenVPN est plus rapide avec le protocole de transport UDP, et d'ailleurs c'est son mode de fonctionnement par défaut. Je vous encourage à rester sur UDP, sauf si vous chercher à passer au travers d'un pare-feu : si vous utilisez le port 443, il est plus cohérent d'utiliser le TCP pour faire comme le HTTPS !

What DNS resolvers do you want to use with the VPN ?

Une fois connecté au VPN, quel serveur VPN voulez-vous utiliser pour la résolution de noms. Vous pouvez choisir un serveur personnalisé avec le choix 13, ou en choisir un dans la liste en indiquant son numéro.



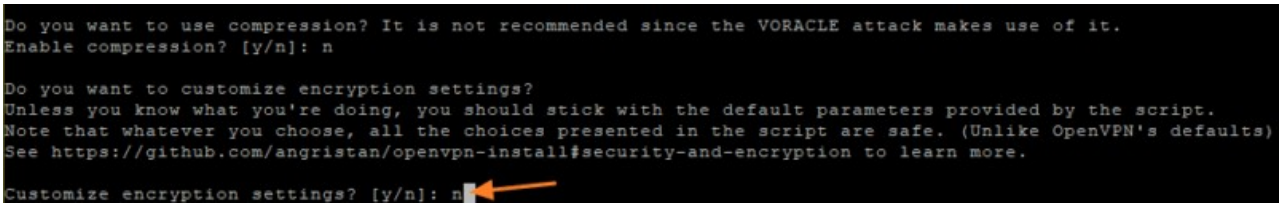
Voilà pour la première série de questions. Passons à la suite.

Do you want to use compression ?

Le script nous recommande de ne pas utiliser la compression, car elle est exploitée par les attaques VORACLE. Indiquez "n" et validez.

Customize encryption settings ?

Le script est déjà préconfiguré pour utiliser certains paramètres pour le chiffrement du tunnel VPN et sa sécurité dans son ensemble. Vous avez la possibilité de définir vos propres paramètres en indiquant "y", sinon il suffit de faire "n".



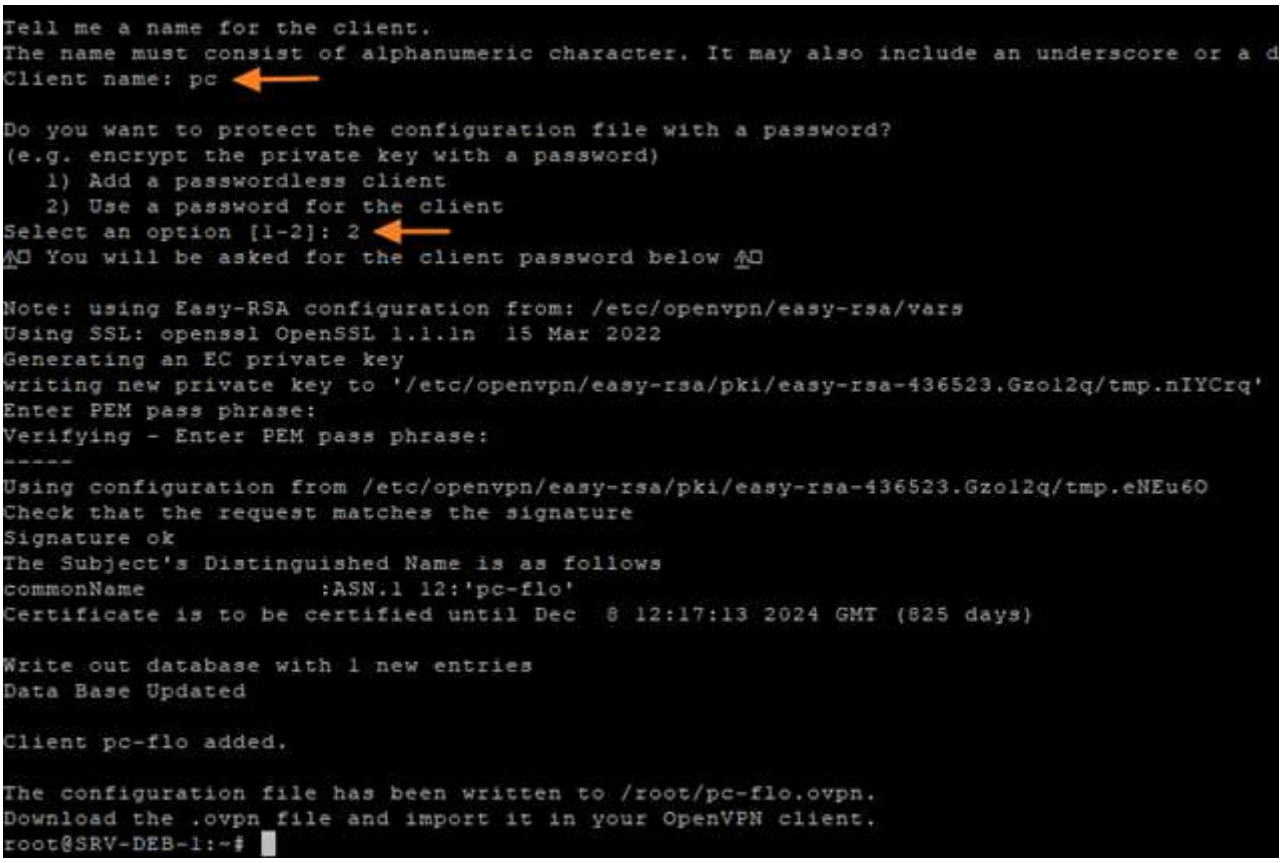
Ci-dessous, voici les différentes options proposées (*ainsi que les choix recommandés et correspondants à la configuration automatique*) pour ceux qui décident de personnaliser les options de chiffrement.

```
Choose which cipher you want to use for the data channel:
   1) AES-128-GCM (recommended)
   2) AES-192-GCM
   3) AES-256-GCM
   4) AES-128-CBC
   5) AES-192-CBC
   6) AES-256-CBC
Cipher [1-6]: 1

Choose what kind of certificate you want to use:
   1) ECDSA (recommended)
   2) RSA
Certificate key type [1-2]: 1

Choose which curve you want to use for the certificate's key:
   1) prime256v1 (recommended)
   2) secp384r1
   3) secp521r1
Curve [1-3]: 1

Choose which cipher you want to use for the control channel:
   1) ECDHE-ECDSA-AES-128-GCM-SHA256 (recommended)
   2) ECDHE-ECDSA-AES-256-GCM-SHA384
Control channel cipher [1-2]: 1

Choose what kind of Diffie-Hellman key you want to use:
   1) ECDH (recommended)
   2) DH
DH key type [1-2]: 1

Choose which curve you want to use for the ECDH key:
   1) prime256v1 (recommended)
   2) secp384r1
   3) secp521r1
Curve [1-3]: 1

The digest algorithm authenticates tls-auth packets from the control channel.
Which digest algorithm do you want to use for HMAC?
   1) SHA-256 (recommended)
   2) SHA-384
   3) SHA-512
Digest algorithm [1-3]: 1

You can add an additional layer of security to the control channel with tls-auth and tls-crypt
tls-auth authenticates the packets, while tls-crypt authenticate and encrypt them.
   1) tls-crypt (recommended)
   2) tls-auth
Control channel additional security mechanism [1-2]: 1
```

La première partie de l'interrogatoire est terminé ! Jusqu'à présent, le script n'a pas encore modifié la machine locale. Cependant, à ce moment précis si vous appuyez sur la touche "Entrée" (ou une autre touche), l'installation du serveur OpenVPN débutera.

Création d'un premier client

À la suite de la configuration du serveur VPN, l'installation via le script se poursuit avec la création d'un premier client VPN. Indiquez le nom du PC qui va utiliser le VPN (histoire de s'y retrouver), par exemple "pc".
Ensuite, la question "Do you want to protect the configuration file with a password?" s'affiche, indiquez "2" pour oui afin de définir un mot de passe qui sera nécessaire pour établir la connexion VPN.



Ceci va générer un fichier de configuration OVPN dans le profil de l'utilisateur en cours d'utilisation. Ici, je suis connecté en tant que root alors la configuration est générée dans "/root/". D'un point de vue du serveur VPN, l'ajout de ce client va générer deux fichiers :

Le certificat du client dans /etc/openvpn/easy-rsa/pki/issued/<nom du client>.crt
La clé privée du client dans /etc/openvpn/easy-rsa/pki/private/<nom du client>.key

Ajouter un nouveau client OpenVPN

À tout moment, vous pouvez ajouter un nouveau client pur que chaque machine qui se connecte dispose de son propre certificat. Que ce soit pour ajouter ou supprimer un nouveau client, il suffit de réexécuter le script et de faire le choix "1".

```
sudo ./openvpn-install.sh
```

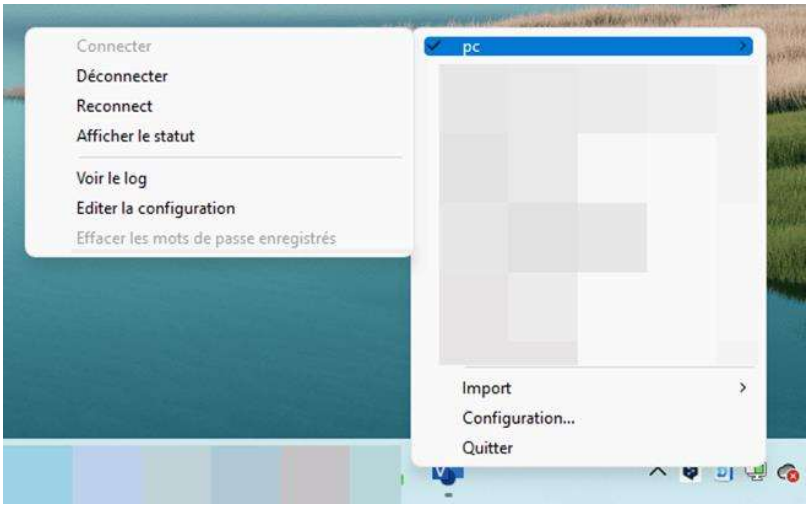
Tester la connexion VPN

Le fichier de configuration généré précédemment (*/root/pc.ovpn*) dans le profil de l'utilisateur doit être transféré sur l'ordinateur qui doit se connecter au VPN. Si vous êtes sur Windows, vous pouvez utiliser WinSCP ou SCP, et sous Linux vous pouvez utiliser SCP.

Sur Windows, il faudra installer OpenVPN GUI ou OpenVPN Connect. Personnellement, j'utilise OpenVPN GUI donc je dois copier-coller le fichier OVPN dans le répertoire suivant :

```
C:\Program Files\OpenVPN\config
```

Ainsi, dans mon client VPN, je vois bien ma nouvelle connexion VPN apparaître qui reprend pour nom celui du fichier OVPN :



En cliquant sur "**Connecter**", je dois **saisir le mot de passe associé au client "PC"** afin de m'authentifier à l'aide de mon certificat.
Une fois connecté, je peux **accéder en SSH à mon serveur Debian 11 grâce à son adresse IP locale**, à savoir "*192.168.100.51*". Je peux également accéder aux autres serveurs de mon infrastructure distante. **Si j'accède à Internet, je passe par mon VPN et j'utilise donc la connexion Internet de mon serveur VPN !**
Côté Windows, en regardant la configuration IP de ma machine, je vois que le tunnel VPN fonctionne sur le réseau "*10.8.0.0/24*" puisque je dispose de l'adresse IP "*10.8.0.2/24*". **Ce sous-réseau est défini dans le fichier "/etc/openvpn/server.conf" du serveur VPN via la ligne "server 10.8.0.0 255.255.255.0"**. Au niveau des serveurs DNS, ce sont bien ceux de Cloudflare qui sont définis (1.0.0.1 et 1.1.1.1) et que j'avais choisis lors de la configuration initiale.

```
Carte inconnue OpenVPN TAP-Windows6 :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : TAP-Windows Adapter V9
   Adresse physique . . . . . . . . . . . : 00-FF-B4-3E-C3-E4
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::49ab:a50:37f3:44e5%20(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 10.8.0.2(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Bail obtenu. . . . . . . . . . . . . . : lundi 5 septembre 2022 16:17:14
   Bail expirant. . . . . . . . . . . . . : mardi 5 septembre 2023 18:15:46
   Passerelle par défaut. . . . . . . . . :
   Serveur DHCP . . . . . . . . . . . . . : 10.8.0.0
   IAID DHCPv6 . . . . . . . . . . . : 318832564
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-29-E9-17-DE-50-EB-F6-2A-1D-95
   Serveurs DNS. . . . . . . . . . . . . : 1.0.0.1
                                   1.1.1.1
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

Les journaux sur le serveur VPN

La connexion du poste client est visible dans les journaux du serveur VPN, en exécutant la commande ci-dessous.

```
journalctl --identifier ovpn-server
```

Par exemple, lors de la connexion depuis mon poste client sous Windows, les journaux suivants sont visibles :

```
SRV-DEB-1 ovpn-server[436393]: MULTI: multi_init called, r=256 v=256
SRV-DEB-1 ovpn-server[436393]: IFCONFIG POOL IPv4: base=10.8.0.2 size=252
SRV-DEB-1 ovpn-server[436393]: IFCONFIG POOL LIST
SRV-DEB-1 ovpn-server[436393]: Initialization Sequence Completed
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 Outgoing Control Channel
Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 Outgoing Control Channel
Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 Incoming Control Channel
Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 Incoming Control Channel
Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 TLS: Initial packet from
[AF_INET]89.87.49.50:53471, sid=eb971c1d a6a6884b
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 VERIFY OK: depth=1,
CN=cn_uIEY50Oeg1zhnla8
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 VERIFY OK: depth=0, CN=pc
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 peer info: IV_VER=2.5.6
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 peer info: IV_PLAT=win
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 peer info: IV_PROTO=6
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 peer info: IV_NCP=2
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 peer info: IV_CIPHERS=AES-256-
GCM:AES-128-GCM
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 peer info: IV_LZ4=1
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 peer info: IV_LZ4v2=1
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 peer info: IV_LZO=1
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 peer info: IV_COMP_STUB=1
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 peer info: IV_COMP_STUBv2=1
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 peer info: IV_TCPNL=1
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 peer info:
IV_GUI_VER=OpenVPN_GUI_11
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 peer info:
IV_SSO=openurl,crtext
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 Control Channel: TLSv1.3,
cipher TLSv1.3 TLS_AES_256_GCM_SHA384, 256 bit EC, curve: prime256v1
SRV-DEB-1 ovpn-server[436393]: <IP du serveur VPN>:53471 [pc] Peer Connection Initiated
with [AF_INET]<IP publique du PC Client>:53471
```