Création d'un VPN (OPENVPN)

Introduction

I – Contexte

Motivations : Afin de renforcer ma confidentialité, ma sécurité et mon anonymat quand je navigue sur le web, j’ai décidé de mettre mes compétences à profit pour me faire mon propre serveur VPN.

C’est quoi un VPN : Un VPN, ou réseau privé virtuel, est un service qui permet de créer une connexion sécurisée et chiffrée entre votre appareil (comme un ordinateur, un smartphone ou une tablette) et un serveur distant. En utilisant un VPN, votre trafic internet est acheminé à travers ce tunnel sécurisé, masquant ainsi votre adresse IP réelle et cryptant les données échangées entre votre appareil et le serveur. Cela offre plusieurs avantages, notamment la protection de votre vie privée en ligne, la sécurisation des communications sur les réseaux Wi-Fi publics, et la possibilité d'accéder à des contenus géo-restreints en apparaissant comme si vous vous trouviez dans une autre région du monde.

II – Prérequis

Le serveur que nous allons mettre en place ne demande pas beaucoup de ressources. Dans mon cas voici ma configura/on :

- 1vCPU
- 1Go de RAM
- Debian 12 (stable)

Pour les autres prérequis, il vous faut si possible un VPS chez l’hébergeur de votre choix, j’ai choisi les 3 mois gratuit sur AWS, et mon VPS est situé en virginie. Si vous souhaitez le faire à domicile, il vous faut un vieux PC ou Raspberry. Et évidemment quelques connaissances même si ce n’est pas très compliqué. Je ne vais pas détailler l’installation de Debian dans cette procédure.

Installation et configuration

III – Installation et configuration

Pour installer OpenVPN, je vais utiliser le script que vous pouvez télécharger grâce a cette commande :

```
curl -O https://github.com/antoninpomies/Procedures/blob/main/Cr%C3%A9er%20son%20VPN/openvpn-install.sh
```

Ou le télécharger directement dans le fichier ou se trouver la procédure suivante. Nous allons ensuite donner les droits d'exécution sur le script téléchargé avec la commande suivante.

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

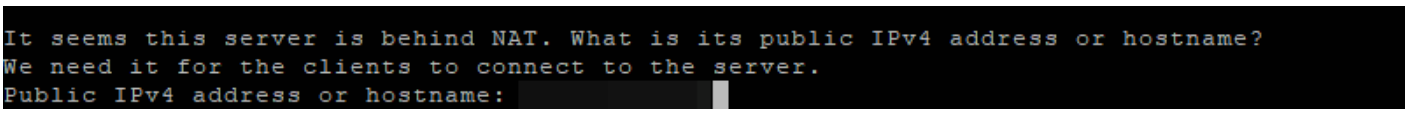
On va ensuite exécuter le script grâce à la commande suivante

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

Il va ensuite y avoir un genre de QCM. Il doit être fait en fonction de vous et de votre configuration.

1. Il faut spécifier une adresse IP. Mais normalement elle est mise par défaut. Changer cette adresse uniquement si besoin et faite « Entrer »

2. Il faut laisser la seconde étape par défaut



3. Ensuite au niveau du port, soit vous le laisser par défaut (1194) soit vous décider de mettre un port comme le 80 ou le 443 qui sont des ports utiliser par le http / https qui permette de masquer votre VPN.

4. Pour le choix du protocole, le mieux est de rester en UDP car il a une meilleure vitesse, mais si vous souhaiter passer en TCP c'est un peu mieux pour passer au travers des pare-feu surtout couplé au port 443.

5. Pour le choix du DNS, j'ai choisi le choix 13 et entré le DNS : 1.1.1.1 mais libre a vous de choisir celui qui vous convient le mieux.

6. Pour le choix de la compression, laisser par défaut c'est-à-dire mettre le choix 'n'

7. Ensuite je vous conseille de laisser le chiffrement par défaut sauf si vous souhaiter que ce soit un chiffrement particulier auquel cas il vous suffit de préciser 'y'

8. Je vous mets ci-dessous un exemple de configuration du 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
```

9. Un texte va ensuite vous expliquer que le QCM est terminé. Appuyez donc sur une touche pour continuer et passer a la suite.

10. Création du premier client. Pour ce faire entrer le nom du client concerné.

11. Ensuite appuyer sur 2 pour configurer un mot de passe de connexion pour le VPN

12. Une fois cela fait, un fichier <nomduclient>.ovpn va être générer dans le répertoire home de la session en cours. Dans mon cas, j'étais connecter avec la session admin. Le fichier se trouver donc dans /home/admin/<nomduclient>.ovpn

13. On va ensuite s'occuper de télécharger le fichier qui vient d'être crée. Pour ce faire nous allons faire une copie via le SSH grâce à la commande suivante. Il sera peut-être nécessaire d'y apporter des modification en fonction de votre configuration.

```
scp -i proxy.pem admin@172.31.31.141:/home/admin/MAC-Antonin.ovpn MAC-Antonin.ovpn
```

Explications :

scp : 'Secure Copy' permet de copier des fichiers via SSH

-i proxy.pem : c'est un argument qui me permet de me connecter avec une clé ssh. Ce paramètre n'est pas obligatoire, il peut être supprimer dans votre cas.

admin@172.31.31.141 : mon nom d'utilisateur@ip de ma machine, il est nécessaire de spécifier l'IP publique dans le cas d'un VPS.

/home/admin/MAC-Antonin.ovpn : localisation du fichier cible dans la machine

MAC-Antonin.ovpn : Localisation du téléchargement du fichier. Si uniquement le nom du fichier est précisé alors il sera téléchargé dans le répertoire actuel si vous souhaite un endroit précis spécifié le chemin complet de celui-ci.

IV – Ouverture des ports

Pour l'ouverture des ports sur la machine, je vous conseille d'aller voir ma documentation sur le Proxy qui détaille la marche a suivre. Elle est disponible ici :

https://docs.antoninpomies.fr/books/mise-en-place-dun-proxy-socks

V - Configuration du Client

1. Pour la configuration du / des clients, il vous suffit de télécharger OpenVPN Connect sur le site officiel a ce lien : https://openvpn.net/client/

2. Une fois télécharger installer le logiciel, et importer le fichier .ovpn dans le logiciel.

3. Saisissez le mot de passe et appuyer sur connect et la connexion devrais se lancer.

Annexes

Annexes

Pour ajouter d’autre client, il vous suffit de réexécuter le script lancer au tout début et de faire le choix qui convient. Si vous avez des soucis de configuration je vous invite à aller consulté les sources ci-dessous.

Sources

IT-Connect : https://www.it-connect.fr/debian-11-et-openvpn-comment-creer-son-propre-serveur-vpn/

Github : https://github.com/antoninpomies/Procedures/blob/main/Cr%C3%A9e%20son%20Proxy.pdf