République du Sénégal

Un peuple-Un but -Une Foi

Ministère de l'Enseignement Supérieur de la Recherche et de l'Innovation

GROUPE ISM

SÉCURITÉ INFORMATIQUE

L3 GLRS

OPENVPN

MODÉRATEURS :

Nora BENZERGA

Sephora Uthai TATY MAKANGA

Kokou Godwin TCHAKPANA

PROFESSEUR :

M. **Ahmed KHALIFA**

INTRODUCTION

Habituellement lorsque vous surfez sur internet, votre connexion fonctionne de cette manière : vous partez d'abord de la carte réseau de l'ordinateur et passez par le modem routeur pour accéder à Internet. Avec un VPN, une "couche" supplémentaire est ajouté. Entre votre modem et Internet, se trouve le VPN. Cette couche va prendre le relais et c'est par elle que transitera d'abord les données lorsque vous surfez sur Internet. En effet, Les réseaux privés virtuels communément abrégé en VPN (Virtual Private Network) jouent un rôle essentiel dans le monde actuel de la connectivité en permettant aux utilisateurs de sécuriser leurs communications et d'accéder à des ressources distantes en toute confidentialité. En informatique, un VPN est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics. Avec sa réputation bien établie et son engagement envers la sécurité, OpenVPN en tant que VPN, offre une solution plus qu'intéressante pour garantir la confidentialité et l'intégrité des communications en ligne. Il offre un service qui permet de créer une connexion sécurisée et privée entre un appareil et un réseau Internet. Il agit comme un tunnel chiffré qui protège vos données et votre identité en ligne en masquant votre adresse IP réelle et en cryptant vos informations. Dans certains pays où la censure est présente, un VPN peut vous aider à accéder à des sites Web bloqués en vous connectant à des serveurs situés dans différents pays, contournant ainsi les restrictions imposées par le gouvernement. OpenVPN est une solution VPN open-source largement utilisée, offrant des fonctionnalités avancées de sécurité et de confidentialité. Dans les prochaines lignes, nous allons explorer le fonctionnement d'OpenVPN, son installation et sa configuration, ainsi que ses utilisations courantes et ses avantages par rapport à d'autres solutions VPN.

I. PRÉSENTATION D'OPENVPN

1. Qu'est-ce qu'OpenVPN ?

Conçu par OpenVPN Inc., OpenVPN est un VPN open source. Sous licence GPL, il est conçu pour créer des réseaux privés virtuels au-dessus d'internet en vue d'assurer la sécurité d'une connexion, et ainsi empêcher la fuite ou la captation des données échangées entre le navigateur et une application ou un serveur distant. OpenVPN a été lancé pour la première fois en 2001 par James Yonan et est depuis devenu l'un des protocoles VPN les plus utilisés au monde. Il a été conçu pour être rapide, sécurisé et facile à utiliser, et dispose d'une communauté importante et active d'utilisateurs et de développeurs qui contribuent à son développement continu. OpenVPN a également été audité pour les vulnérabilités de sécurité, ce qui en fait un choix de confiance pour les particuliers et les organisations à la recherche d'une solution VPN fiable.

En outre, c'est un logiciel open source qui permet de créer des connexions sécurisées et chiffrées entre des ordinateurs distants. Il utilise des certificats numériques et des clés de chiffrement pour authentifier les utilisateurs et chiffrer les données. Il peut être utilisé pour établir des connexions VPN site à site, où plusieurs réseaux locaux sont connectés de manière sécurisée, ou pour permettre aux utilisateurs distants de se connecter à un réseau privé de manière sécurisée à partir de n'importe quel endroit. Également disponible en open source, sous licence GNU GPL, il prend en charge un cryptage en 256 bits via OpenSSL. OpenVPN est compatible avec de nombreux systèmes d'exploitation, y compris Windows, macOS, Linux, Android et iOS. Il offre également une grande flexibilité et peut être configuré pour répondre aux besoins spécifiques de chaque utilisateur ou organisation.

2. Son Fonctionnement

OpenVPN est un protocole VPN populaire qui fournit des connexions réseau privées rapides et sécurisées sur Internet. Il utilise le protocole SSL/TLS (Secure Sockets Layer/Transport Layer Security) pour établir une connexion sécurisée entre un client et un serveur VPN. Il utilise un système de clés et de certificats pour authentifier les parties et chiffrer les données échangées. OpenVPN peut fonctionner dans différents modes, tels que le mode client-serveur, où un serveur central gère les connexions des clients, ou le mode peer-to-peer, où les clients se connectent directement les uns aux autres. OpenVPN est compatible avec une large gamme de plateformes, y compris Windows, macOS, Linux et les appareils mobiles.

- **Architecture :**

OpenVPN utilise une architecture client-serveur pour établir une connexion sécurisée entre deux terminaux. Le client OpenVPN initie une demande de connexion au serveur, qui authentifie et autorise ensuite le client à établir un tunnel sécurisé. Le tunnel est créé à l'aide du protocole ***Transport Layer Security*** (TLS), qui fournit un chiffrement de bout en bout de toutes les données transmises entre le client et le serveur.
OpenVPN peut être configuré pour utiliser le protocole de datagramme utilisateur (UDP) ou le protocole de contrôle de transmission (TCP) pour transmettre des données entre le client et le serveur. UDP est plus rapide et plus efficace, tandis que TCP est plus fiable et peut contourner plus facilement les pares-feux. Il fonctionne mieux sur UDP (selon OpenVPN.net), c'est

pourquoi le serveur d'OpenVPN essaie d'abord d'établir des connexions UDP ; si ces connexions échouent, ce n'est qu'alors que le serveur essaie d'établir des connexions TCP. La plupart des fournisseurs VPN offrent également par défaut OpenVPN sur UDP.

- **Chiffrement :**

OpenVPN utilise la bibliothèque OpenSSL pour fournir un cryptage fort de toutes les données transmises sur le réseau. Il prend en charge une large gamme de chiffrements, y compris AES-256, qui est considéré comme l'un des algorithmes de chiffrement les plus sécurisés disponibles aujourd'hui. OpenVPN prend également en charge ***Perfect Forward Secrecy*** (PFS), qui génère une clé de session unique pour chaque connexion. Cela garantit que même si un attaquant accède à une clé de session, il ne peut pas l'utiliser pour déchiffrer d'autres sessions.

- **Authentification :**

OpenVPN utilise une variété de mécanismes d'authentification pour s'assurer que seuls les utilisateurs autorisés peuvent accéder au réseau. Il prend en charge les méthodes de chiffrement conventionnelles, telles que les clés pré-partagées, et le chiffrement à clé publique à l'aide de certificats RSA. OpenVPN fournit également un mécanisme de ***kill switch***, qui met automatiquement fin à la connexion si la connexion VPN est perdue. Cela empêche toute transmission de données non chiffrées sur le réseau, garantissant ainsi la sécurité de vos données. Il prend en charge diverses méthodes d'authentification, notamment les certificats X.509, les clés pré-partagées et les noms d'utilisateur/mots de passe.

En somme, OpenVPN est un protocole VPN rapide, sécurisé et abordable qui fournit une connectivité de réseau privé sur Internet. Son cryptage fort, son architecture flexible et ses mécanismes d'authentification robustes en font un excellent choix pour une utilisation personnelle et professionnelle.

3. Les Services Offerts Par OpenVPN

OpenVPN est une solution VPN open source reconnue mondialement, qui offre une multitude de fonctionnalités avancées pour sécuriser vos communications en ligne. Avec OpenVPN, vous pouvez bénéficier d'une protection de pointe tout en maintenant la confidentialité de vos données et en évitant les risques de piratage. Voici quelques-unes des principales fonctionnalités d'OpenVPN :

- La première fonctionnalité phare d'OpenVPN est **son protocole OpenVPN**, qui garantit un cryptage puissant et fiable de vos données. Grâce à ce protocole de sécurité, vos informations sensibles sont encapsulées dans un tunnel sécurisé, rendant pratiquement impossible leur interception ou leur déchiffrement par des tiers malveillants.

- OpenVPN offre également une **flexibilité optimale en termes d'options de configuration**. Vous pouvez choisir entre plusieurs modes d'authentification, notamment l'authentification par nom d'utilisateur/mot de passe, l'authentification à double facteur, l'intégration avec des services d'annuaire tels que LDAP, et même la possibilité de mettre en place votre

propre système d'authentification personnalisé. Cette polyvalence vous permet de **personnaliser votre infrastructure VPN en fonction des besoins spécifiques de votre entreprise**. OpenVPN prend en charge différents types de connexions, y compris les connexions point à point, les connexions site à site et les connexions client-serveur.

- Une autre fonctionnalité clé d'OpenVPN est **sa capacité à établir des connexions sûres** même à travers des réseaux non fiables ou publics. Grâce à l'utilisation de tunnels chiffrés, vous pouvez accéder à votre réseau privé en toute sécurité, que vous soyez connecté depuis votre domicile, un café ou tout autre lieu disposant d'une connexion Internet. Cela vous permet de travailler en toute tranquillité d'esprit, en sachant que vos données sont protégées, quel que soit l'endroit où vous vous trouvez. OpenVPN utilise des protocoles de cryptage avancés tels que AES (*Advanced Encryption Standard*) pour assurer la confidentialité des données échangées.

- Et pour finir, OpenVPN propose une **gestion avancée des certificats et des clés**, vous permettant de contrôler l'accès à votre réseau VPN de manière précise et sécurisée. Vous pouvez créer et révoquer des certificats, définir des autorisations granulaires pour les utilisateurs et les groupes, et mettre en place des mécanismes de rotation automatique des clés pour renforcer encore davantage la sécurité de votre infrastructure.

4. Comparaison d'OpenVPN avec d'Autres Solutions VPN Populaires

Programmé par James Yonan et sorti en 2001, OpenVPN est l'un des seuls protocoles VPN open-source qui possède également sa propre application open-source. Actuellement, OpenVPN tend à surpasser tous les autres protocoles VPN.

❖ OpenVPN contre SSTP

SSTP et OpenVPN sont assez similaires puisqu'ils utilisent tous deux SSL 3.0, et les deux protocoles VPN peuvent utiliser le port 443. Ils offrent également un niveau de sécurité similaire, car les deux protocoles peuvent utiliser le cryptage 256 bits et le chiffrement AES hautement sécurisé. Cependant, OpenVPN est open-source, ce qui signifie qu'il est beaucoup plus fiable que SSTP, qui est la propriété exclusive de Microsoft – une société qui est connue pour collaborer avec la NSA et le FBI. Aussi, quand il s'agit de pare-feu, OpenVPN semble un peu plus efficace que SSTP. Comment ça se fait ? Eh bien, voici un fait moins connu à propos du SSTP – selon les dires de Microsoft, le protocole ne supporte pas vraiment les proxy Web authentifiés. Cela signifie que l'administrateur réseau pourrait théoriquement détecter les en-têtes SSTP et supprimer la connexion si un proxy de non-authentification est utilisé.

En termes de vitesse, on dit que le SSTP est plus rapide que l'OpenVPN, mais il n'y a pas beaucoup de preuves concluantes. Il est vrai qu'OpenVPN peut être assez gourmand en ressources, mais c'est généralement quand il utilise le port TCP (le même que celui utilisé par SSTP). Cependant, OpenVPN peut également utiliser le port UDP, qui offre des vitesses bien supérieures. En ce qui concerne la compatibilité multi-plateforme, OpenVPN a l'avantage puisqu'il fonctionne sur beaucoup plus de plates-formes que SSTP, qui n'est disponible que sous Windows, Linux, Android et les routeurs. Néanmoins, il est à noter que le SSTP est intégré

nativement dans les plates-formes Windows, il est donc plus facile à configurer qu'OpenVPN. Dans l'ensemble, OpenVPN et SSTP sont un choix décent, mais OpenVPN est simplement plus efficace.

❖ OpenVPN contre PPTP

Pour commencer, le PPTP est nettement plus faible que l'OpenVPN en termes de sécurité. Alors que OpenVPN peut gérer des clés de chiffrement et des cryptages 256 bits comme AES, PPTP ne peut utiliser que des clés 128 bits via le cryptage MPPE. Malheureusement, le cryptage MPPE est très facile à exploiter, voici juste quelques problèmes : -MPPE est vulnérable aux attaques à bascule de bits ; - MPPE ne peut pas crypter les paquets NCP (Network Control Protocol) PPP (Point-to-Point Protocol) ; - Le cryptage ne vérifie généralement pas si le serveur est authentique ; - Le MPPE est vulnérable à l'attaque Reset-Request (une forme d'attaque de l'homme au milieu). De plus, PPTP peut utiliser MS-CHAP-v1 (qui n'est pas sécurisé) ou MS-CHAP-v2 (encore, pas sécurisé du tout). OpenVPN est beaucoup plus sûr puisqu'il peut utiliser un meilleur cryptage pour l'authentification, tel que ***SHA-256***, ***SHA-384*** ou ***SHA-512***.

De plus, PPTP est assez facile à bloquer avec un pare-feu. OpenVPN ne peut pas vraiment être bloqué par l'administrateur réseau puisqu'il utilise le port HTTPS. Oh, et n'oublions pas que la NSA peut apparemment cracker le trafic PPTP. Le seul critère qui permet à PPTP d'être meilleur qu'OpenVPN est sa vitesse en ligne et sa disponibilité native sur plusieurs plates-formes. En raison de son faible cryptage, PPTP est très rapide. Et bien qu'OpenVPN soit hautement compatible multiplateforme, il ne s'intègre pas nativement sur autant de plates-formes que PPTP. Cependant, il convient de mentionner que le PPTP pourrait ne plus être disponible en natif dans les futurs systèmes d'exploitation et appareils.

❖ OpenVPN contre IPSec

IPSec est souvent associé à L2TP et IKEv2, mais vous pouvez trouver des fournisseurs VPN qui offrent l'accès à ce protocole par eux-mêmes. Alors, qu'en est-il du protocole OpenVPN ? Eh bien, les deux offrent un niveau de sécurité tout aussi décent. Cependant, vous devez être plus prudent avec IPSec lors de sa configuration, car une petite erreur peut ruiner la protection qu'il offre. De plus, comme IPSec occupe l'espace du noyau (l'espace sur le périphérique réservé au système d'exploitation), sa sécurité peut être limitée par la façon dont il est configuré par le fournisseur. Cela rend également IPSec moins portable que OpenVPN, qui utilise l'espace utilisateur (mémoire système allouée aux applications).

IPSec est généralement disponible en natif sur de nombreuses plates-formes, alors que OpenVPN doit être configuré manuellement sur celles-ci. Naturellement, ce n'est pas un problème si vous utilisez un service VPN. Une autre chose à noter est que le trafic IPSec peut parfois être bloqué par certains pares-feux, alors que les paquets OpenVPN UDP ou TCP n'ont pas de tels problèmes. Quant à la vitesse et la stabilité, les deux sont assez décents si vous avez assez de bande passante et un appareil relativement puissant. Cependant, vous devez savoir que IPSec peut prendre plus de temps à négocier le tunnel que OpenVPN.

II. INSTALLATION ET CONFIGURATION D'OPENVPN

L'installation d'OpenVPN implique la configuration d'un serveur VPN et des clients qui se connectent à ce serveur. Pour installer OpenVPN, il est nécessaire de télécharger et d'installer les packages appropriés en premier lieu l'application depuis son site officiel. Les étapes de la configuration varient selon le système d'exploitation, mais généralement, elles incluent l'installation des certificats, des clés, et la configuration des fichiers. Ces fichiers contiennent des informations telles que les adresses IP, les ports, les clés et les certificats nécessaires à la connexion VPN. La configuration dépend de l'objectif spécifique, que ce soit en tant que **client pour se connecter à un serveur VPN** ou en tant que **serveur VPN** pour créer un réseau privé. Des outils et des interfaces graphiques sont disponibles pour faciliter l'installation et la configuration d'OpenVPN, même pour les utilisateurs moins expérimentés. Ci-dessous un exemple d'installation et de configuration d'OpenVPN sur Windows. Dans cet exemple, nous allons faire une installation server-client sur une machine-server debian et une machine-client Windows :

1. Installation du serveur

Nous partons du principe que vous êtes connectés en mode console et en tant que root. Si ce n'est pas le cas, assurez-vous que l'utilisateur à les droits adéquates et utilisez "**sudo**" avant chacune des commandes que je vais donner. Nous sommes donc connectés et nous pouvons commencer par lancer l'installation d'Open VPN.

Commencez par installer les paquets suivants (inclut bridge-utils) :

```
aptitude install openvpn openssl
```

Laissez l'installation se dérouler en répondant Y pour Yes quand on vous le demande. Une fois cela effectué, nous allons préparer les dossiers et fichiers nécessaire à la configuration d'OpenVPN.

Créez un nouveau dossier pour OpenVPN :

```
mkdir /etc/openvpn/easy-rsa/
```

Copiez les fichiers de configuration dans ce nouveau répertoire :

```
cp -r /usr/share/doc/openvpn/examples/easy-rsa/2.0/* /etc/openvpn/easy-rsa/
```

Modifiez les droits sur le répertoire :

```
chown -R $USER /etc/openvpn/easy-rsa/
```

2. Configuration d'OpenVPN

2.1. Initialisation

Maintenant que tout est prêt, passons à l'étape de configuration. Rendez-vous tout en bas du fichier **vars** qui contient vos informations puis éditez-les. Initialisez les variables par défaut situées dans le fichier vars :

```
aptitude install openvpn openssl
```

En modifiant les informations suivantes à votre convenance (Vous n'êtes pas obligés d'éditer ces informations, cela ne vous empêchera pas d'utiliser le VPN) :

```
export KEY_COUNTRY="FR"
export KEY_PROVINCE="00"
export KEY_CITY="ville"
export KEY_ORG="organisation"
export KEY_EMAIL="mail.domaine.com"
```

Initialisez ensuite les variables des scripts grâce à la commande source :

```
cd /etc/openvpn/easy-rsa/
source vars
```

Réinitialisez le sous-dossier keys :

```
./clean-all
```

2.2. Génération des Clefs et Certificats

Générez le certificat racine «**ca.cert**» ainsi que la clef d'autorité de certification racine «**ca.key**» :

```
./build-ca
```

Générez le certificat «**nom_srv_vpn.crt**» ainsi que la clef «**nom_srv_vpn.key**» :

```
./pkitool --initca
./pkitool --server nom_srv_vpn
```

Il se peut que vous rencontriez une erreur lorsque vous tapez la commande «*./pkitool --initca* ». Cela est dû à un bug sur certains OS et versions d'OpenSSL. Si c'est le cas, tapez cette commande puis recommencez : ***cp openssl-1.0.0.cnf openssl.cnf.***

Générez le fichier « **dh1024.pem** » contenant les paramètres ***Diffie Hellman*** :

```
./build-dh
```

Cette commande crée une clef statique permettant d'éviter les attaques de type « *Man in the middle* » :

```
openvpn --genkey --secret keys/ta.key
```

2.3. Copie des Clefs et Certificats

A ce stade, vous devez disposer des fichiers suivants dans **/etc/openvpn/easy-rsa/keys** :

- Certificat du serveur de certification (CA) : **ca.crt**
- Clef du serveur de certification (CA) : **ca.ke**y
- Certificat du serveur OpenVPN : **nom_srv_vpn.crt**
- Clef du serveur OpenVPN : **nom_srv_vpn.key**
- Paramètre *Diffie Hellman* : **dh1024.pem**
- Clef d'autorisation pour accès au démon : **ta.key**

Copiez les fichiers du point précédent dans le répertoire ci-indiqué :

```
cd /etc/openvpn/easy-rsa/keys
cp ca.crt /etc/openvpn/
cp ca.key /etc/openvpn/
cp nom_srv_vpn.crt /etc/openvpn/
cp nom_srv_vpn.key /etc/openvpn/
cp dh1024.pem /etc/openvpn/
cp ta.key /etc/openvpn
```

2.4. Fichier de configuration serveur

Vous pouvez récupérer un modèle de configuration dans le dossier ci-dessous :

```
cd /usr/share/doc/openvpn/examples/sample-config-files/
gunzip server.conf.gz
cp server.conf /etc/openvpn/
```

Une fois le fichier ''**server.conf''** créé, adaptez-le à votre besoin à l'aide de la configuration suivante :

################ CONFIG SERVEUR ################
mode server
port 443
proto tcp-server
dev tun
################ CLEFS ET CERTIFICATS ################
ca /etc/openvpn/ca.crt
cert /etc/openvpn/**nom_srv_vpn.**crt
key /etc/openvpn/**nom_srv_vpn.**key
dh /etc/openvpn/dh1024.pem
tls-auth /etc/openvpn/ta.key 0
cipher AES-128-CBC

################ PARAMETRES RESEAU ################
 # Pool d'IP des clients VPN
server **172.16.0.0 255.255.255.0**
#Paramètre DNS
push "dhcp-option DNS 8.8.8.8"
 # Routage intégral du trafic via le tunnel VPN
push "redirect-gateway def1 bypass-dhcp"
################ LOGS ################
 # Niveau log
verb 4
 # Type de log
log openvpn.log
 # Etat du serveur
status openvpn-status.log
################ AUTRES ################
 # Ping toute les 10s et arrêt au bout de 2min
keepalive 10 120
 # Activation compression (à activer également coté client)
comp-lzo
 # Limites l'accès à certaines ressources lors du redémarrage
persist-key
persist-tun

Une fois votre fichier de configuration terminé, exécutez la commande suivante pour vérifier sa configuration :

```
cd /etc/openvpn
openvpn server.conf
```

S'il a bien été configuré, la ligne suivante doit apparaitre en bas du *shell* :

```
Wed Nov 08 23:36:10 2023 us=478984 Initialization Sequence Completed
```

Attention ! Exécutez cette commande qu'après avoir copié votre fichier de configuration. Dans le cas contraire l'erreur du point.

2.5. Génération des Clefs et Certificats

Pour terminer, générez le certificat et la clef pour l'utilisateur « pierre » :

```
cd /etc/openvpn/easy-rsa/
./build-key pierre
```

2.6. Transfert des Fichiers

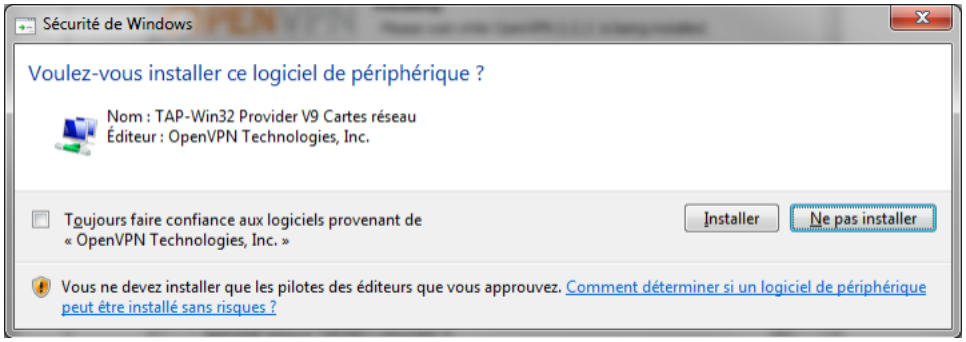
A l'aide de la commande ***SCP*** ou de **WinSCP**, transférez ces fichiers sur votre client Windows :

- Certificat: **ca.crt**
- Certificat: **user.crt**
- Clef: **user.key**
- Clef: **ta.key**

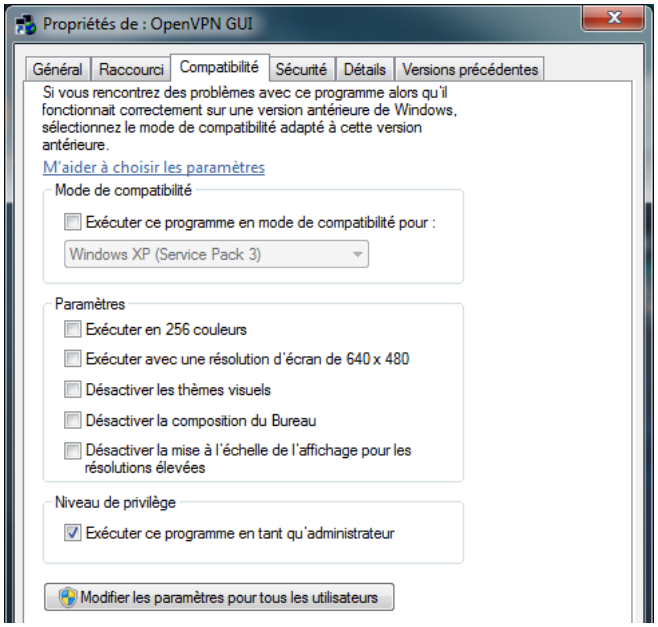
3. Installation du Client

Le client (**OpenVPN GUI**) sera installé sur un *Windows 7 x64*. Pour cela :

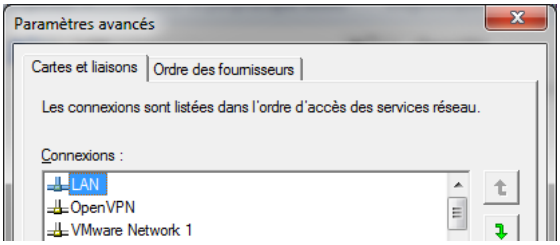
- Télécharger et installez le client *OpenVPN* **ici**
- Acceptez l'ajout d'une carte réseau de type « *TAP-Win32* »



Modifiez le raccourci du programme afin de l'exécuter en tant qu'administrateur (*Vista, Seven* ou supérieur uniquement).



Modifiez l'ordre des adaptateurs réseaux de façon à placer votre carte réseau (WIFI et/ou Ethernet) avant l'adaptateur « Tap » créé par *OpenVPN*. Pour cela, allez dans :
Centre de réseau et partage > touche *« Alt »* **> Avancé > Paramètres avancés**



4. Configuration du Client

4.1. Fichier de configuration client

Créez un fichier nommé **config.ovpn** et copiez les paramètres suivants en les adaptant à votre besoin :

################ CLEFS ET CERTIFICATS ################
cert **user.**crt
key **user.**key
ca ca.crt
tls-auth ta.key 1
tls-client
cipher AES-128-CBC
persist-key
persist-tun
;tls-remote <X509>
################ RESEAU ################
remote **nom de domaine** 443
redirect-gateway def1
dev tun
resolv-retry 1
proto tcp-client
################ AUTRES ################
verb 3
comp-lzo
Pull
nobind

4.2. Proxy

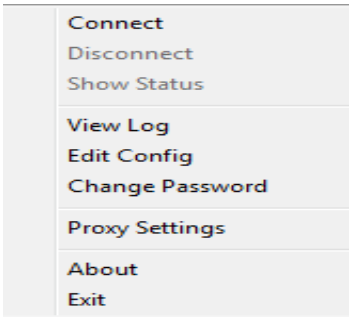
Si vous passez par un serveur proxy, vous devrez ajouter les lignes ci-dessous dans votre fichier de configuration client. Quant au fichier « **authfile.txt** », il devra contenir sur deux lignes votre login et votre mot de passe. Enfin, n'oubliez pas de **NE PAS renseigner de proxy** dans votre navigateur.

################ **PROXY** ################
;http-proxy **<IP proxy>** **<port>** authfile.txt basic OU ;http-proxy **<IP proxy>** **<port>** stdin basic
;http-proxy-retry
;http-proxy-option AGENT "Mozilla/5.0 (Windows; U; Windows NT 6.1; fr; rv:1.9.2.13) Gecko/20101203 Firefox/3.6.13 GTB7.1"

4.3. Client Windows "OpenVPN GUI"

Copiez les fichiers du point **2.6** dans le répertoire **C:\Program Files (x86)\OpenVPN\config**

Et enfin lancez le OpenVpn GUI et se connecter :



5. Routage

5.1. Routage Interne :

- **Activation du « forwarding »**

Nous allons maintenant configurer notre serveur pour que les utilisateurs puissent se connecter et obtenir une adresse IP local à la machine. Activez le routage de façon permanente :

```
nano /etc/sysctl.conf
```

Et décommentez la ligne ci-dessous :

```
net.ipv4.ip_forward=1
```

Vérification de l'état du routage (0 : désactivé, 1 : activé) :

```
cat /proc/sys/net/ipv4/ip_forward
```

ou

```
sysctl net.ipv4.ip_forward
```

- **Activation du NAT**

L'ensemble du trafic de vos clients est dorénavant routé vers votre VPN. Toutefois, le réseau indiqué dans le fichier de configuration du serveur (option « **server 172.16.0.0 255.255.255.0**») n'est pas connu par votre interface physique **eth0**. Il sera donc nécessaire de configurer le « routage » et le « NATage » des clients VPN vers cette interface. Pour cela exécutez la commande suivante :

```
iptables -t nat -A POSTROUTING -s 172.16.0.0/24 -o eth0 -j MASQUERADE
```

Notez toutefois que cette règle sera effacée au redémarrage du serveur. Vous devrez donc le rendre persistante dans votre fichier *iptables*.

5.2. Routage extérieur

Pour que votre VPN soit accessible depuis l'extérieur, il est nécessaire d'ouvrir le port 443 sur votre Box et de le rediriger vers l'IP de votre serveur VPN.

6. Sécurisation du Serveur : Révocation des Certificats

Si vous souhaitez révoquer un certificat utilisateur, exécutez la commande suivante et redémarrez le service *OpenVPN* :
Dans **server.conf**, ajouter la ligne suivante :

```
crl-verify easy-rsa/keys/crl.pem
```

Initialiser la variable *easy-rsa* :

```
source /etc/openvpn/easy-rsa/rsa
```

Révoquer le certificat du client :

```
./revoke-full user.crt
service openvpn restart
```

7. Logs et débogage

Pour redémarrer le service OpenVPN :

```
/etc/init.d/openvpn restart
```

Pour vérifier que le service OpenVPN est bien lancé :

```
ps aux | grep openvpn
```

Pour afficher les processus utilisant le port 443 :

```
cat /etc/services|grep 443
```

Pour afficher les logs :

```
tail -f /etc/openvpn/openvpn.log
```

Pour afficher les interfaces réseau (dont **tun0**) :

```
ifconfig
```

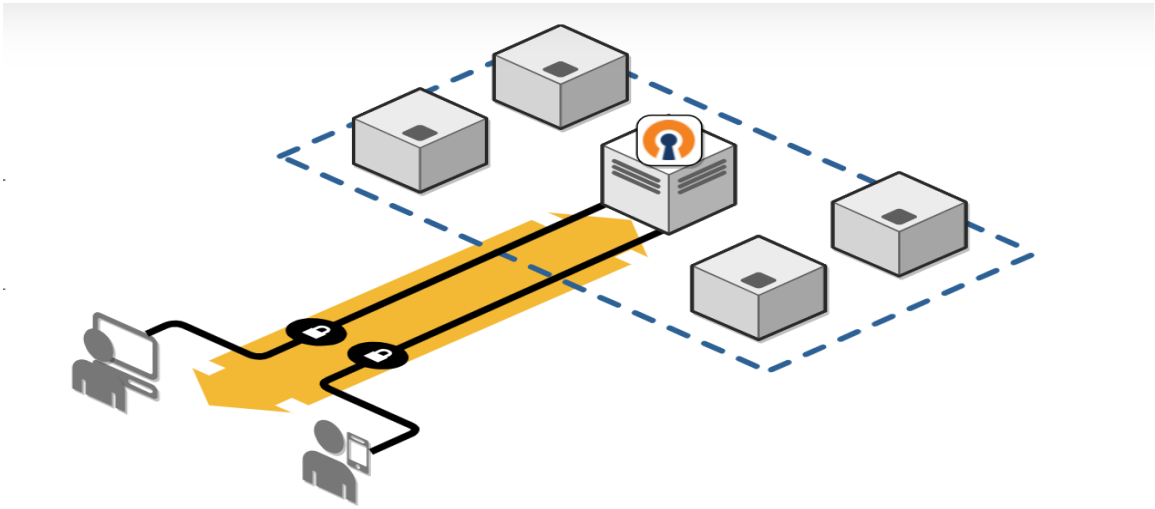
```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet adr:172.16.1.1  P-t-P:172.16.1.2  Masque:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

III. UTILISATION D'OPENVPN

OpenVPN est couramment utilisé pour permettre aux employés d'accéder de manière sécurisée au réseau de l'entreprise depuis des emplacements distants. Grâce à OpenVPN, les employés peuvent se connecter au serveur VPN de l'entreprise et accéder aux ressources internes, telles que les fichiers, les applications et les imprimantes, comme s'ils étaient physiquement présents dans les locaux de l'entreprise. OpenVPN garantit la confidentialité des données échangées en les chiffrant à l'aide de protocoles de cryptage robustes. De plus, il permet de contourner les restrictions de pare-feu et de filtrage Internet, offrant ainsi une connectivité fiable et sécurisée, même à partir de réseaux publics non sécurisés.

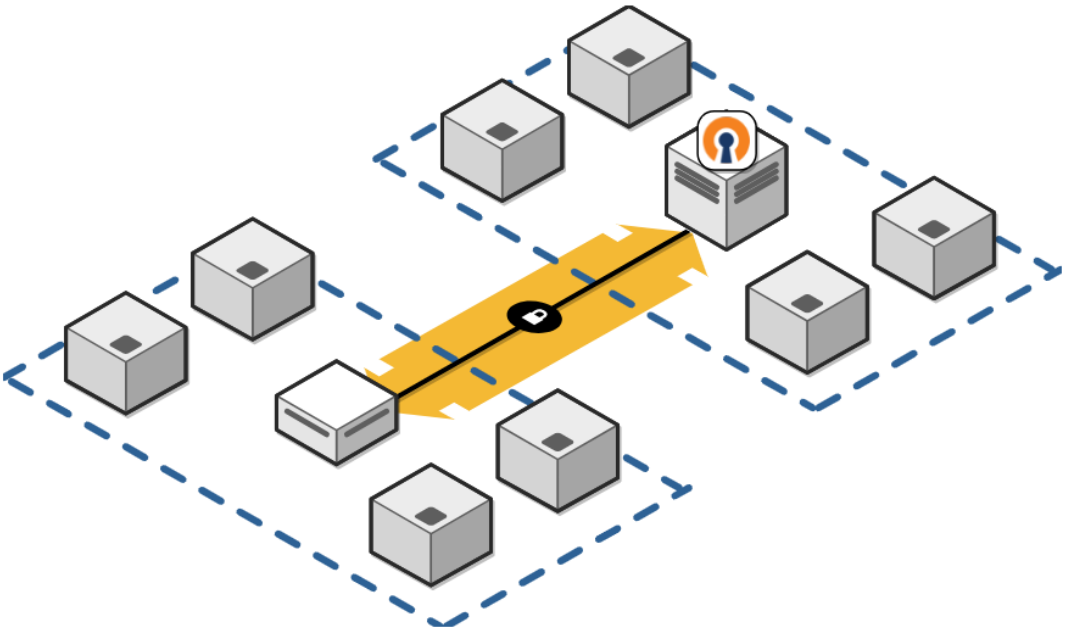
1. Accès à distance sécurisé

Que vous ayez des serveurs dans votre bureau, un centre de données hors site ou un système basé sur le cloud contenant toutes vos données, OpenVPN Access Server peut fournir un accès sécurisé. Dans le diagramme de droite, les utilisateurs de leurs ordinateurs de bureau et appareils mobiles utilisent le programme client OpenVPN pour établir une connexion sécurisée via Internet au serveur d'accès OpenVPN. Selon la façon dont vous configurez les règles de contrôle d'accès dans le serveur d'accès, les utilisateurs peuvent alors accéder de manière transparente à toutes les ressources ou uniquement à des systèmes ou services spécifiques.



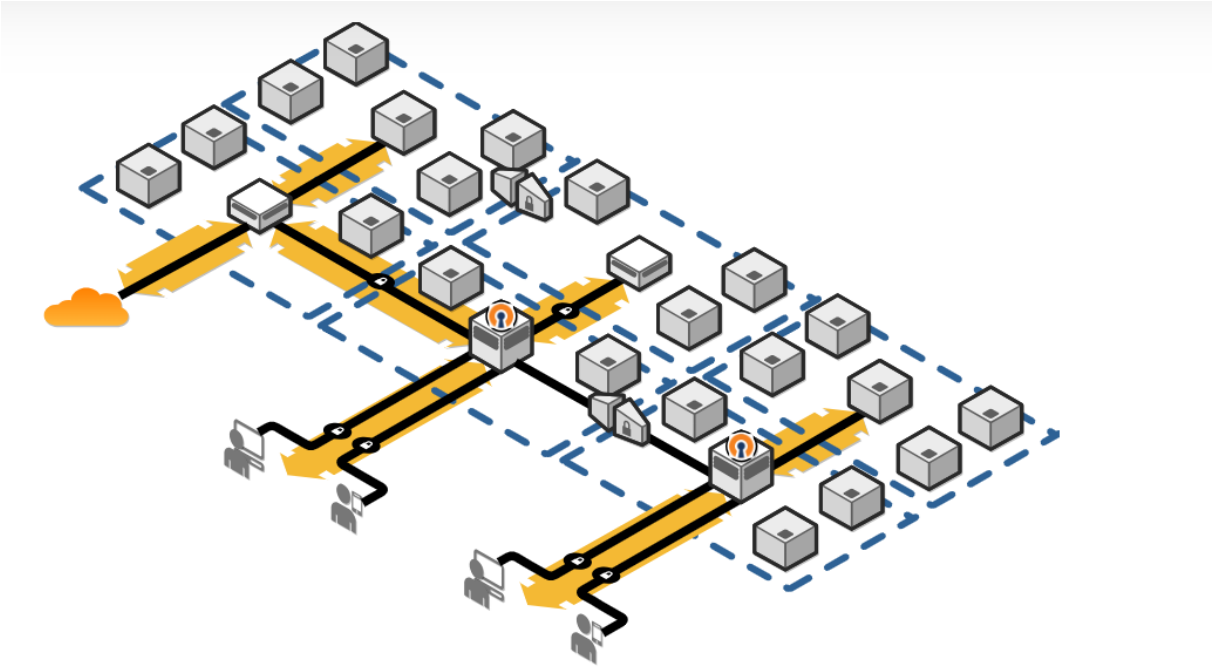
2. Des connexions de site à site pour rassembler les réseaux

En utilisant le modèle client-serveur dans le serveur d'accès OpenVPN, il est possible de connecter un système client Linux dans un réseau à un serveur d'accès OpenVPN dans un autre réseau et d'utiliser ce client connecté comme concentrateur VPN ou système de passerelle client VPN. Les deux termes signifient que le trafic provenant d'un réseau entier peut passer par le tunnel VPN déjà établi entre le client et le serveur et atteindre l'autre réseau. Le trafic peut circuler dans les deux sens, ce qui permet de connecter deux réseaux ensemble et rend l'accès aux ressources d'un réseau sur l'autre réseau transparent et facile.



3. Plusieurs réseaux, sous-réseaux, passerelles et serveurs

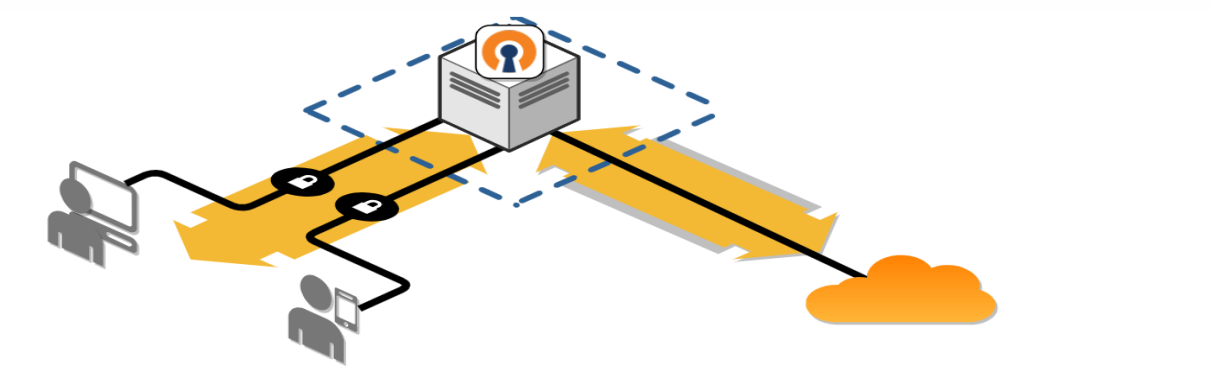
Quelle que soit la complexité de votre configuration existante, le serveur d'accès OpenVPN doit bien s'intégrer. Il est capable d'envoyer des adresses IP et des plages de trafic spécifiques depuis un client VPN via le serveur. Il peut également envoyer le trafic Internet client via le tunnel VPN en fonction de ce que vous configurez. Il peut transférer le trafic entrant via le tunnel VPN destiné à un autre sous-réseau via le serveur de passerelle spécifié (géré dans la table de routage du système d'exploitation). Il peut être utilisé pour connecter plusieurs réseaux différents dans une configuration site à site. Les serveurs d'accès peuvent être connectés les uns aux autres pour donner accès aux ressources ou aux clients VPN.



4. Sécurisez le trafic Internet ou contactez les systèmes à accès limité

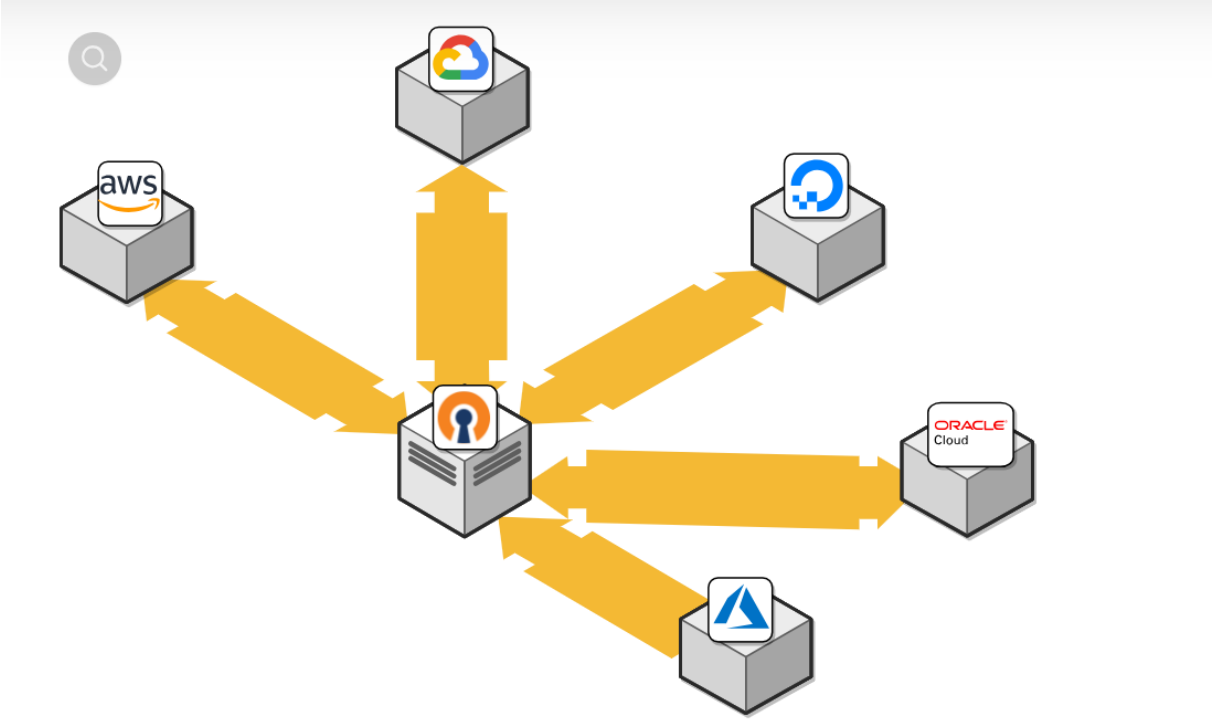
Si OpenVPN Access Server est installé dans un centre de données ou un système cloud, il peut être utilisé pour sécuriser la connexion Internet de vos appareils clients. Si, par exemple, vous êtes sur un réseau public, vous souhaiterez peut-être vous assurer que tout votre trafic Internet passe par un tunnel VPN crypté sécurisé et vers votre propre serveur d'accès. De là, le trafic peut continuer vers sa destination et les réponses sont renvoyées via le même chemin. De cette façon, les programmes et les personnes qui surveillent le réseau sur lequel vous vous trouvez ne peuvent voir que les paquets de données cryptés qui leur sont inutiles.

Un autre cas d'utilisation du type de configuration présenté dans le diagramme est la possibilité de faire en sorte que le trafic des clients VPN connectés semble provenir de l'adresse publique du serveur d'accès OpenVPN lui-même. Ceci est utile si vous disposez d'un serveur sur Internet ou dans un centre de données qui bloque tout accès, à l'exception d'une liste blanche d'adresses IP spécifiques ayant accès. Vous pouvez demander aux clients VPN de se connecter au serveur d'accès et de lui faire gérer le trafic uniquement pour ce système à accès limité. Ce trafic semblera alors provenir du serveur d'accès, que vous pourrez ajouter à votre liste blanche. Tout client VPN connecté aura alors accès à ce serveur de manière sécurisée.



5. Accès sécurisé aux systèmes basés sur le cloud

Le travail à distance n’est plus seulement un concept futuriste. Le télétravail est là, il est populaire et le nombre de travailleurs à distance augmente considérablement chaque année. Très bientôt, les candidats à un emploi s'attendront à ce que les options à distance soient standard – et non seulement à les espérer comme un bonus. Il ne faudra pas longtemps avant que le télétravail soit considéré comme un avantage standard de base, aux côtés des vacances et de l'assurance maladie. Les entreprises qui n’offrent pas ces avantages essentiels ne seront pas aussi compétitives pour attirer les demandeurs d’emploi. Certains employés de l’entreprise travaillent au bureau, mais les autres travaillent exclusivement à distance depuis différents endroits. L'entreprise doit alors fournir un accès à distance aux services cloud afin que les employés puissent accéder à tout ce dont ils ont besoin pour faire leur travail, qu'ils soient au bureau ou à l'autre bout du pays.



IV. ERREURS COURANTES ET DÉPANNAGES

1. Erreur TLS : la négociation de clé TLS n'a pas pu avoir lieu dans les 60 secondes

Cette erreur particulière peut avoir plusieurs causes différentes car il s'agit d'un message d'erreur assez générique. Une explication possible est que le programme client est ancien et ne prend en charge que TLS 1.0, mais que le serveur attend le niveau TLS 1.1 ou supérieur. Pour voir si tel

est le cas, connectez-vous au serveur et vérifiez le fichier journal côté serveur. Il y a de fortes chances que votre programme client soit une version plus ancienne, comme la version 2.2 ou une version antérieure, et qu'il ne sache pas comment gérer une exigence de niveau minimum TLS moderne, lorsque vous voyez des messages qui ressemblent à ceci côté serveur :

```
OpenSSL : erreur : 140760FC : routines SSL : SSL23_GET_CLIENT_HELLO : protocole inconnu'
TLS_ERROR : erreur de lecture BIO tls_read_plaintext'
Erreur TLS : objet TLS -> erreur de lecture de texte en clair entrant »
Erreur TLS : échec de la négociation TLS »
SIGUSR1[soft,tls-error] reçu, redémarrage de l'instance client'
```

La solution à ce problème particulier consiste à mettre à niveau le logiciel client vers la dernière version.

Une autre explication possible est que les paramètres concernant le niveau d'exigence minimum TLS ont été modifiés mais que le client OpenVPN utilise une ancienne copie du profil de connexion qui contient des instructions incorrectes. Les paramètres du client et du serveur doivent correspondre pour que la connexion réussisse. Dans cette situation, l'installation d'une nouvelle copie du profil de configuration résoudra le problème. Une désinstallation complète, un nouveau téléchargement et une réinstallation du client OpenVPN Connect devraient s'en occuper pour vous.

Une autre explication possible est qu'il existe un blocage dans un pare-feu ou chez le fournisseur de services Internet qui bloque ou interfère d'une manière ou d'une autre avec la prise de contact TLS.

2. Erreur TLS : les clés TLS locales/distantes sont désynchronisées

Pour une raison quelconque, la clé TLS négociée à utiliser côté client pour le cryptage/déchiffrement TLS est différente de celle utilisée côté serveur. Cela ne devrait jamais arriver. Lorsque le client et le serveur se parlent, ils conviennent d'une clé TLS à utiliser pour chiffrer et déchiffrer le trafic. Par défaut, dans Access Server, une telle clé est valide pendant 6 heures, et après ces 6 heures, l'actualisation TLS démarre automatiquement et ils se mettront d'accord sur une nouvelle clé. Il existe un court chevauchement au cours duquel l'ancienne et la nouvelle clé sont acceptées, jusqu'à ce que l'ancienne clé soit expirée et que la nouvelle clé doive être utilisée. Si, pour une raison quelconque, l'un des côtés ne le fait pas, ce message d'erreur s'affiche.

Une cause possible est un bug dans le protocole OpenVPN avec la version utilisée dans OpenVPN Connect Client qui a été résolu, où l'actualisation automatique de la clé TLS échouerait parce que le client et le serveur ne pouvaient pas s'entendre correctement sur le chiffrement à utiliser. Donc, si vous rencontrez ce problème particulier et que vous utilisez un client basé sur OpenVPN3 comme OpenVPN Connect Client 2.*, envisagez de mettre à jour vers la dernière version. Vous pouvez le faire par exemple par ordinateur en téléchargeant OpenVPN Connect Client pour Windows ou OpenVPN Connect Client pour macOS depuis le site Web officiel de OpenVPN et en l'installant. Cependant, une meilleure solution serait de

mettre à jour votre serveur d'accès vers la dernière version afin que le client Connect mis à jour y soit intégré, puis de télécharger et d'installer la dernière version d'OpenVPN Connect Client à partir de votre serveur d'accès. Si vous utilisez un autre logiciel client et qu'il présente des problèmes, essayez de trouver une version plus récente. Dans le pire des cas, vous pouvez également envisager de modifier l'actualisation de la clé TLS par quelque chose de plus grand dans la page VPN avancé de l'interface utilisateur d'administration, pour éviter de déclencher le problème. Bien entendu, cela réduit quelque peu la sécurité.

3. Impossible d'obtenir l'ID de session de vpn.yourserver.com, ports=443

Ce message d'erreur se trouve dans le fichier capi.log et également affiché dans le message contextuel sous Windows ou macOS lorsque vous utilisez OpenVPN Connect Client pour Windows ou macOS. Ce message d'erreur indique qu'un profil de connexion verrouillé par le serveur est utilisé, ce qui est le profil par défaut sur le serveur d'accès OpenVPN lorsque vous téléchargez et installez le client OpenVPN Connect. Un profil de connexion verrouillé par le serveur est conçu pour être indépendant de l'utilisateur, ce qui signifie qu'il ne contient aucune information permettant d'identifier l'utilisateur et constitue une sorte de profil universel. Cela permet à tous les comptes d'utilisateurs valides de démarrer une connexion avec ce client OpenVPN Connect. Les informations d'identification sont transmises via un canal HTTPS sécurisé aux services XML-RPC du serveur d'accès pour vérification et, si elles sont approuvées, le client recevra une copie du profil verrouillé par l'utilisateur pour cet utilisateur, ainsi qu'un jeton de session. Ceux-ci serviront à démarrer le tunnel OpenVPN. Une fois le tunnel déconnecté, le profil verrouillé par l'utilisateur et le jeton de session sont supprimés. Mais pour que cela fonctionne, il doit exister une connexion HTTPS fonctionnelle aux services Web du serveur d'accès.

4. Numéro de série introuvable dans la base de données

Le serveur d'accès OpenVPN est livré par défaut avec une structure PKI interne, ce qui signifie un certificat racine auto-signé avec des certificats uniques générés pour chaque client OpenVPN pour ce serveur. Tout cela est unique et lié ensemble. Cela fait partie de la force d'OpenVPN, l'identité d'un client VPN et d'un serveur VPN est vérifiée dans les deux sens lorsqu'une connexion est établie. Le client vérifie le serveur et le serveur vérifie le client. Ainsi, pour chaque compte utilisateur que vous ajoutez au serveur d'accès, un certificat unique est généré. Le certificat est lié au nom du compte utilisateur, vous ne pouvez donc pas vous connecter avec les informations d'identification de l'utilisateur Bob avec les certificats de l'utilisateur Billy. Chaque certificat possède également un numéro de série, un numéro unique identifiant le certificat. Si vous voyez l'erreur indiquant que le numéro de série est introuvable dans la base de données, cela signifie que ce certificat n'est pas connu de ce serveur. Même si vous révoquez un certificat, il est toujours connu du serveur et ne produira pas cette erreur particulière. Vous utilisez peut-être par erreur un certificat d'un serveur d'accès complètement différent, ou peut-être avez-vous commencé avec une nouvelle configuration du serveur d'accès sur votre serveur et les certificats sont effacés et de nouveaux générés pour la nouvelle configuration, alors que vous utilisez toujours anciens certificats de l'installation précédente. Pour résoudre ce problème, veillez à supprimer le mauvais profil de connexion de votre ordinateur client, à en obtenir un

nouveau à partir de votre installation actuelle du serveur d'accès et à l'utiliser pour vous connecter.

V. ALTERNATIVES ET EXTENSIONS D'OPENVPN

1. Quelques Alternatives de OpenVPN

Bien qu'OpenVPN soit une solution populaire, il existe d'autres alternatives open-source, telles que **WireGuard** et **SoftEther VPN**, qui offrent des fonctionnalités similaires. Ces alternatives seront brièvement présentées, mettant en évidence leurs différences par rapport à OpenVPN.

a. SoftEther VPN

Il est sûr de dire que OpenVPN et SoftEther sont tous deux des protocoles vraiment sécurisés. Ils sont open-source, utilisent des algorithmes de chiffrement de niveau militaire comme AES, utilisent un cryptage de 256 bits, et utilisent également SSL 3.0. La principale différence entre eux est l'âge – SoftEther est beaucoup plus récent que OpenVPN. Pour cette raison, certaines personnes pensent qu'OpenVPN est beaucoup plus fiable.

En termes de vitesse, SoftEther est plus rapide que OpenVPN. En fait, selon les recherches de l'Université de Tsukuba, le protocole SoftEther est censé être 13 fois plus rapide que le protocole OpenVPN. Les deux protocoles fonctionnent sur un nombre décent de plates-formes, mais SoftEther semble être un peu plus facile à configurer que OpenVPN. Cependant, vous devez savoir que même si vous utilisez un fournisseur VPN qui offre la connexion SoftEther, vous devrez quand même télécharger un logiciel supplémentaire pour qu'il fonctionne. SoftEther peut également exécuter son propre serveur, mais le serveur SoftEther peut aussi exécuter le protocole OpenVPN, avec d'autres protocoles comme IPSec, L2TP/IPSec, SSTP et SoftEther.

Au final, SoftEther est une solide alternative OpenVPN. Si pour une raison quelconque vous ne pouvez pas utiliser OpenVPN, vous devriez essayer SoftEther. Si vous souhaitez en savoir plus, suivez ce lien.

b. WireGuard VPN

WireGuard est un protocole de communication et un **logiciel libre** et **open source** permettant de créer un réseau privé virtuel. Il est conçu avec des objectifs de facilité d'utilisation, de performances et de surface d'attaque basse. Il utilise des algorithmes modernes et fixes (vous ne pouvez pas les modifier) pour éviter les erreurs de configuration qui entraînent des failles de sécurité. Dans l'ensemble, ils offrent une excellente sécurité au même titre que OpenVPN.

WireGuard est sans aucun doute plus rapide qu'OpenVPN. Sa base de code est beaucoup plus légère (environ 4 000 lignes contre 70 000 à 600 000 lignes) et utilise plus efficacement les

cœurs de processeur. WireGuard est donc la nouvelle coqueluche des enthousiastes du VPN. Ce protocole tout récent a pris le monde du VPN par surprise. On relève notamment un développement éclair, des performances surprenantes, sans oublier son intégration au très select ***Kernel Linux***. Avec autant d'arguments en sa faveur, il a vite trouvé preneur chez de nombreux éditeurs de VPN qui n'ont pas manqué d'intégrer le protocole dans leurs services.

2. Quelques Plugins Utiles

De plus, OpenVPN peut être étendu via des extensions pour ajouter des fonctionnalités supplémentaires, telles que la gestion centralisée des utilisateurs et la prise en charge de protocoles de cryptage spécifiques. Voici quelques plugins et leur rôle :

- **Auth-pam** : Le module *openvpn-auth-pam* permet d'implémenter l'authentification par « nom d'utilisateur/mot de passe » via PAM (''*Pluggable Authentication Modules*'' en français ''*modules d'authentification enfichables*''), et permet essentiellement à toute méthode d'authentification supportée par PAM (comme LDAP, RADIUS) d'être utilisée avec OpenVPN. PAM prend en charge l'authentification par « nom d'utilisateur/mot de passe », mais il peut être combiné avec des certificats X509 pour fournir deux niveaux d'authentification indépendants. Ce module utilise un modèle d'exécution à privilèges partagés qui fonctionnera même si vous supprimez les privilèges du démon OpenVPN à l'aide des directives user, group ou chroot.

- **Down-root** : Le module *down-root* permet à une configuration OpenVPN d'appeler un script down (script de nettoyage) avec les privilèges root, même lorsque les privilèges ont été supprimés en utilisant --user/--group/--chroot. Ce module utilise un modèle d'exécution à privilèges partagés qui doit s'arrêter avant qu'OpenVPN n'abandonne les privilèges root, à l'endroit où le script « up » est habituellement appelé. Le module restera alors dans un état d'attente jusqu'à ce qu'il reçoive un message d'OpenVPN via un tuyau pour exécuter le script « down ». Ainsi, le script « down » sera exécuté dans le même environnement d'exécution que le script up.

- **Deferred Client-Connect** : C'est un plugin qui permet de retarder l'exécution de scripts client-connect jusqu'à ce que la connexion VPN soit établie. Cela permet de s'assurer que les scripts ne s'exécutent pas avant que la connexion soit prête

- **Keying-material-exporter** : est un outil open-source pour OpenVPN qui permet d'exporter les clés de chiffrement et de déchiffrement utilisées par le protocole. Cela peut être utile pour auditer la sécurité du système ou pour effectuer des analyses de trafic.

CONCLUSION

Au terme de notre travail, ce sujet nous a permis de savoir ce qu'est un VPN et à quoi il sert. L'usage des VPN renferme de nombreux avantages tels que la sécurité dans la transmission de nos données à travers un canal sécurisé, l'accès sécurisé à distance à site distant, etc. Particulièrement OpenVPN présente de nombreux autres avantages tel que la gratuité du logiciel, sa fiabilité, sa grande communauté interactive ; elle est "*facile*" à implémenter, et existe en plusieurs versions, et pour plusieurs systèmes d'exploitation. Comme tous les autres VPN, son implémentation rencontre le souci majeur de l'accès aux paramètres du routeur pour la redirection des ports. Son installation et sa configuration ont été nécessaire pour mieux comprendre son mode de fonctionnement.

En un mot, OpenVPN est une solution VPN sécurisée et open-source qui offre une connectivité fiable, sécurisée et privée. Son fonctionnement, son installation et sa configuration ont été expliqués, ainsi que ses utilisations courantes pour l'accès à distance et ses avantages en termes de sécurité et de confidentialité. Pour approfondir ses connaissances sur OpenVPN, il est recommandé de consulter la documentation officielle, les forums de la communauté et les tutoriels en ligne.