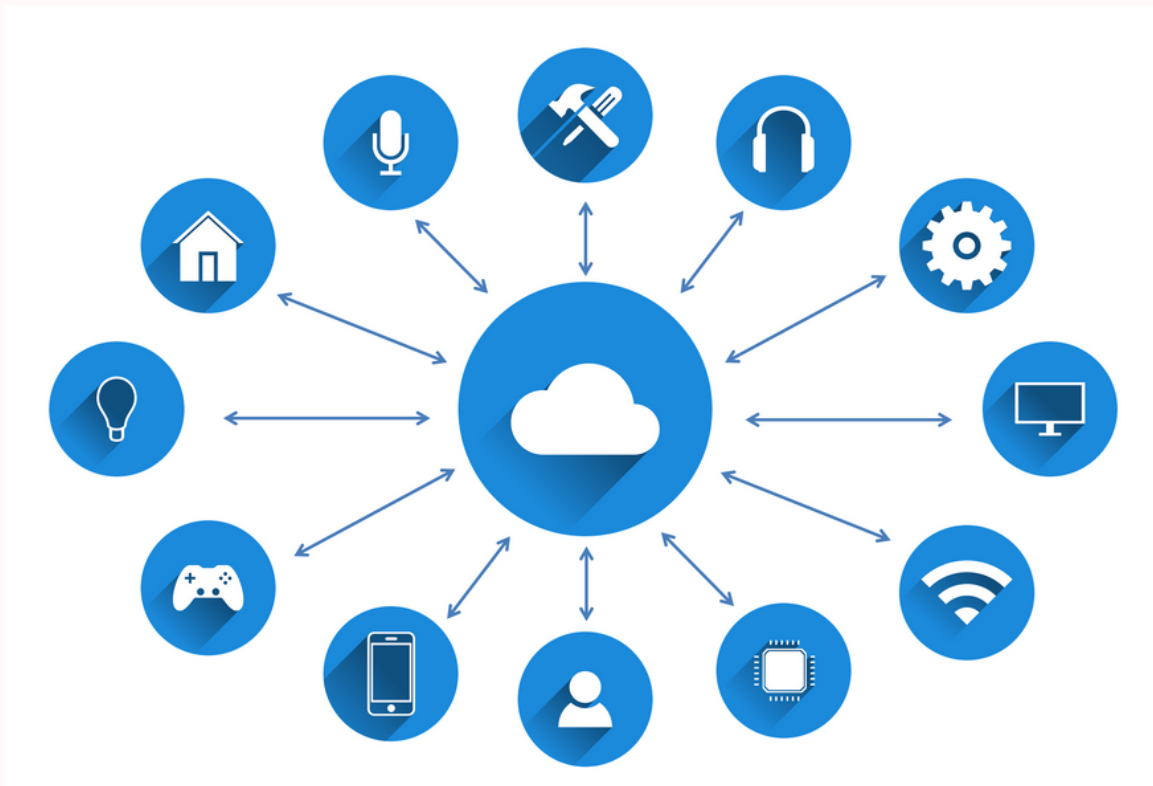
TOULOUSE ynov CAMPUS

PROJET VPN

DOCUMENTATION UTILISATEUR



Nolan Cano
Axelle Refeyton

SOMMAIRE

TOULOUSE
ynov
CAMPUS

PRÉAMBULE

Les VPN (Virtual Private Network) offrent une multitude d'avantages et d'utilisations essentiels : contournement des restrictions géographiques, anonymat en ligne, confidentialité et sécurité des données, sécurité sur les réseaux Wi-Fi publics...
Les aspects qui vont en particulier nous intéresser sont la préservation de l'anonymat des utilisateurs ainsi que l'accès à distance aux réseaux privés.

Dans ce document seront expliqué les étapes à suivre afin de créer un profil client, de se connecter au service OpenVPN et de révoquer un profil déjà existant.

Il ne sera pas expliqué les étapes d'installation et de configuration d'un serveur d'accès OpenVPN.

Afin de pouvoir suivre cette documentation dans les meilleurs conditions, il vous faudra :

- Un serveur d'accès OpenVPN opérationnel avec un profil super user
- Une machine client utilisant un système d'exploitation parmi Windows, Ubuntu, Debian, MacOS, iOS et Android

TOULOUSE ynov CAMPUS

CRÉATION DU PROFIL CLIENT

CRÉATION DE LA REQUÊTE CERTIFICAT

Le VPN utilisé fonctionne de pair avec un serveur de certificat. Ce type de serveur (appelé server AC) permet de sécuriser les accès au serveur VPN en générant des clés pour les utilisateurs.

Pour créer une clé publique, connectez-vous au serveur d'accès VPN et rendez-vous dans le dossier ~/**easy-rsa**. Tapez la commande suivante pour lancer le script de génération de profil client. La suite de cette documentation partira du principe que le profil client créé a été nommé "client1. Si vous souhaitez utiliser un autre nom, il faudra modifier les dossiers et commandes en remplaçant "clietn1" par le nom que vous avez choisi :

```
$ ./easyrsa gen-req client1 nopass
```

Appuyez directement sur entrée pour la création de votre profil, ou entrez un nouveau nom si vous souhaitez le modifier. Copiez ensuite le la clé ainsi générée dans le dossier ~/client-configs/keys/ :

```
$ cp pki/private/client1.key ~/client-configs/keys/
```

Pour recevoir la clé publique, il vous faudra transférer ce fichier au serveur de certificat. Une des manières possibles est de se connecter directement en shell via cette commande shell en changeant les données entrées par celles de votre serveur AC :

```
scp pki/reqs/client1.req user_name@your_ca_server_ip:/tmp
```

TOULOUSE ynov CAMPUS

CRÉATION DU PROFIL CLIENT

Une fois sur le serveur AC, rendez-vous dans le dossier ~/easy-rsa et importez la requête de certificat précédemment générée :

```
$ ./easyrsa import-req /tmp/client1.req client1
```

Pour faire valider la requête, tapez la commande suivante :

```
$ ./easyrsa sign-req client client1
```

Confirmez comme demandé la signature de la requpete en tapant "yes" et entrez votre mot de passe.

Cette commande va créer un fichier de certification client nommé "**client1.crt**". Transférez ce fichier à votre serveur d'accès VPN afin de pouvoir générer un accès, et enregistrez-le dans le dossier **~/client-configs/keys/** .

Une fois reconnecté à votre serveur d'accès VPN, déplacez les fichiers "ca.crt" et "ta.keys" dans le dossier précédents. Ces fichiers sont trouvables respectivement dans les dossiers **~/easy-rsa/** et **/etc/openvpn/server/** . Veillez à ce que ces fichiers aient le bon niveau de sécurité (chown 700).

TOULOUSE ynov CAMPUS

CRÉATION DU PROFIL CLIENT

CONFIGURATION CLIENT

Maintenant que notre client est reconnu par le serveur de certificat, il faut lui générer un fichier de configuration, qui va lui permettre de se connecter au VPN.
Sur le serveur d'accès VPN, rendez-vous dans le dossier **~/client-configs** et lancez le script suivant :

```
$ ./make_config.sh client1
```

Cela va avoir pour effet de créer le fichier "client1.ovpn", contenant la clé publique précédemment générée, dans le dossier **~/client-configs/** .

Transférez ce fichier sur l'appareil depuis lequel vous souhaitez vous connecter au VPN.

TOULOUSE ynov CAMPUS

SE CONNECTER

DEPUIS WINDOWS

Pour vous connecter au VPN depuis un appareil Windows, téléchargez l'application client OpenVPN en vous rendant sur ce lien : https://openvpn.net/community-downloads/ .

Copiez ensuite le fichier .ovpn précédemment généré dans le dossier **C:\Program Files\OpenVPN\config** et lancez l'application en tant qu'administrateur.

Faites un clic-droit sur l'icône OpenVPN dans la barre des tâches, sélctionnez votre profil client et cliquez sur "**Connecter**". Si la connexion s'est bien exécutée, une fenêtre d'état s'ouvrira, montrant la sortie du journal de logs pendant que la connexion est établie, et un message de connexion s'affichera.

Pour se déconnecter, faites un clic-droit sur l'icône OpenVPN dans la barre des tâches, sélctionnez votre profil client et cliquez sur "Déconnecter".

DEPUIS DEBIAN/UBUNTU

Pour vous connecter au VPN depuis un appareil Debian ou Ubuntu, installez le paquet OpenVPN en tapant la commande suivante dans un invité de commande :

```
client$ sudo apt install openvpn
```

TOULOUSE ynov CAMPUS

SE CONNECTER

Configuration client utilisant "system-resolved" :

Installez le paquet correspondant en tapant la commande suivante :

```
sudo apt install openvpn-systemd-resolved
```

Ouvrez ensuite votre fichier .ovpn et décommentez les lignes suivantes en enlevant le symbole ";" en début de ligne, puis sauvegardez le fichier :

```
script-security 2
up /etc/openvpn/update-systemd-resolved
down /etc/openvpn/update-systemd-resolved
down-pre
dhcp-option DOMAIN-ROUTE .
```

Configuration client utilisant "update-resolv-conf" :

Ouvrez simplement votre fichier .ovpn et décommentez les lignes suivantes en enlevant le symbole ";" en début de ligne, puis sauvegardez le fichier :

```
script-security 2
up /etc/openvpn/update-resolv-conf
down /etc/openvpn/update-resolv-conf
```

TOULOUSE ynov CAMPUS

SE CONNECTER

Connexion au service VPN :

Dans les deux cas, il vous suffit d'entrer la commande suivante dans un invité de commande pour bénéficier du service OpenVPN :

```
sudo openvpn --config client1.ovpn
```

DEPUIS MACOS

Téléchargez la dernière image disque en allant sur le lien suivant : https://tunnelblick.net/downloads.html
Double-cliquez sur le fichier .dmg téléchargez et suivez les instructions d'installations.

A la fin de l'installation, Tunnelblick vous proposera de renseigner vos fichiers de configurations en cliquant sur "**I have configuration files**". Une fois l'installation finie, ouvrez une fenêtre d'exploration fichier et double cliquez sur votre fichier .ovpn. Cela va permettre à Tunnelblick d'installer votre profil client.

Pour vous connecter, lancez l'application Tunnelblick et cliquez sur l'icone Tunnelblick en haut à droite de 'lécran, dans le menu de contrôle des connexions, puis cliquez sur "Connecter client1".

TOULOUSE ynov CAMPUS

SE CONNECTER

DEPUIS IOS

Installez l'application OpenVPN Connect depuis l'iTunes AppStore puis connectez votre appareil à un ordinateur.

Depuis votre ordinateur, ouvrez iTunes, puis cliquez sur "iPhones > apps" et sélectionnez "OpenVPN app". Faites glisser votre fichier .ovpn dans la fenêtre vide dédiée au partage de fichiers.

Depuis votre iPhone, lancez l'application OpenVPN et cliquez sur le signe "+" vert pour importer votre profil. Pour vous connecter au VPN, faites glisser le bouton "Connection" sur la position On .

DEPUIS ANDROID

Installez et démarrez l'application OpenVPN Connect depuis le GooglePlay Store.

Cliquez sur le menu "FiLE" , sélectionnez votre fichier .ovpn et appuyez sur le bouton "IMPORT". Tapez le bouton près du profil importé pour vous connecter.

TOULOUSE ynov CAMPUS

RÉVOQUER LE CERTIFICAT CLIENT

Si vous souhaitez retirer les accès d'un certain profil au VPN, il vous faudra révoquer le certificat d'authentification.

Pour ce faire, rendez vous sur le serveur AC et tapez les commandes suivantes :

```
./easyrsa revoke client_name
```

```
./easyrsa gen-crl
```

Transférez le nouveau fichier "**crl.pem**" au serveur d'accès VPN dans le dossier **/etc/openvpn/server** .

Ouvrez ensuite le fichier de configuration server.conf situé dans le dossier **/etc/openvpn/server/** et ajoutez la ligne "crl-verify crl.pem" à la fin du fichier.

Afin que ces modifications soient prises en compte, veillez à redémarrer OpenVPN et le serveur AC.

TOULOUSE ynov CAMPUS