26/05/2023

Descriptif du projet

Création d'un VPN
Infrastructure et réseaux SI

Présenté par : CABEE Pauline, VELAY Yohan
Bachelor 2 Informatique, Toulouse Ynov Campus

TOULOUSE ynov CAMPUS

Introduction

En tant qu'étudiants en informatique en cours de sécurité des réseaux et infrastructure, nous avons choisi d'approfondir nos connaissances sur le projet "VPN", en créant un réseau privé virtuel (VPN) à l'aide de la solution open-source OpenVPN. Un VPN est un outil essentiel pour garantir la confidentialité, l'intégrité et la disponibilité des informations échangées sur un réseau, en particulier dans un monde numérique de plus en plus connecté et exposé aux menaces en ligne. Cette étude technique vise à présenter le processus complet de mise en place d'un VPN en utilisant OpenVPN. Tout au long de ce dossier, nous allons expliquer en détail les différents aspects liés à la création d'un VPN, de la configuration du serveur OpenVPN à l'installation des clients, en passant par la gestion des certificats et les mesures de sécurité appropriées.

La première partie de ce dossier portera sur les notions de base des réseaux privés virtuels et leur utilité dans le contexte actuel. Nous aborderons également les principes de cryptographie et de chiffrement qui sous-tendent le fonctionnement d'OpenVPN. Comprendre ces concepts fondamentaux est essentiel pour une mise en œuvre réussie et sécurisée d'un VPN.

Dans la deuxième partie, nous explorerons les différentes options d'architecture pour la mise en place d'un serveur OpenVPN. Nous détaillerons les exigences matérielles et logicielles, ainsi que les meilleures pratiques pour configurer le serveur en fonction des besoins spécifiques du réseau. De plus, nous présenterons les différentes options de déploiement, y compris la mise en place d'un serveur sur site ou l'utilisation d'un service de fournisseur de VPN.

La troisième partie de ce dossier se concentrera sur la configuration des clients OpenVPN. Nous fournirons des instructions détaillées sur l'installation et la configuration des clients sur différents systèmes d'exploitation, en soulignant les étapes clés pour garantir une connexion sécurisée au VPN.

Enfin, nous aborderons les aspects de sécurité et de gestion des certificats dans la quatrième partie. J'expliquerai les méthodes appropriées pour générer et distribuer les certificats, ainsi que les meilleures pratiques pour sécuriser les échanges entre les clients et le serveur OpenVPN.

En conclusion, ce dossier technique vise à présenter de manière approfondie la création d'un VPN avec OpenVPN. En suivant les étapes et les bonnes pratiques décrites, vous serez en mesure de mettre en place un réseau privé virtuel sécurisé pour protéger vos données et vos communications dans un environnement en ligne potentiellement hostile.

I - Le VPN

La première partie de ce dossier se concentre sur les notions de base des réseaux privés virtuels (VPN) et leur utilité dans le contexte actuel. Dans un monde de plus en plus connecté, où la confidentialité et la sécurité des données sont des préoccupations majeures, les VPN jouent un rôle crucial dans la protection des informations sensibles lorsqu'elles sont transmises sur des réseaux publics tels qu'Internet.
Un VPN est essentiellement un tunnel sécurisé qui permet de créer une connexion privée entre un appareil et un réseau distant. Il utilise des protocoles de chiffrement pour garantir la confidentialité, l'intégrité et l'authenticité des données qui transitent à travers le réseau.

A quoi ça sert ? Cela permet aux utilisateurs d'accéder à des ressources réseau de manière sécurisée, même à partir d'un réseau non fiable ou non sécurisé.

L'une des technologies les plus couramment utilisées pour implémenter des VPN est OpenVPN, qui est une solution open-source populaire qui offre une compatibilité multiplateforme et une configuration flexible. Il repose sur des principes de cryptographie et de chiffrement pour sécuriser les données transmises.

Cryptographie: protéger les informations en les transformant.
Dans le contexte d'OpenVPN, la cryptographie est utilisée pour protéger les paquets de données qui traversent le tunnel VPN, en s'assurant qu'ils ne peuvent pas être interceptés ou modifiés par des tiers non autorisés.

Chiffrement: processus de conversion des données à l'aide d'une clé de chiffrement. Cette clé est nécessaire pour déchiffrer les données chiffrées et les reconvertir en données en clair. OpenVPN prend en charge différents algorithmes de chiffrement, tels que AES (Advanced Encryption Standard), qui est considéré comme sécurisé et largement utilisé.

Comprendre ces concepts fondamentaux de cryptographie et de chiffrement est essentiel pour une mise en œuvre réussie et sécurisée d'un VPN. Il est important de choisir des algorithmes de chiffrement solides et de configurer correctement les paramètres de sécurité pour garantir la confidentialité et l'intégrité des données. De plus, la gestion adéquate des clés de chiffrement est cruciale pour maintenir la sécurité du VPN.

II- Options d'architecture

Tout d'abord, il est important de considérer les exigences matérielles et logicielles pour le serveur OpenVPN. Les exigences peuvent varier en fonction du nombre d'utilisateurs et du volume de trafic attendu. Idéalement, le serveur devrait disposer d'une puissance de calcul adéquate, de suffisamment de mémoire et d'espace de stockage pour traiter efficacement les connexions VPN.

Il est recommandé d'utiliser une distribution Linux, telle que Ubuntu ou CentOS, qui offre une compatibilité et une stabilité élevées avec OpenVPN.

La configuration du serveur OpenVPN dépendra des besoins spécifiques du réseau. Il est essentiel de définir les objectifs du VPN, tels que l'accès distant aux ressources réseau, la sécurisation des connexions Internet publiques ou la connexion de succursales distantes. En fonction de ces objectifs, des paramètres spécifiques devront être configurés, tels que les plages d'adresses IP, les protocoles de chiffrement, les certificats et les méthodes d'authentification.

Lors de la configuration du serveur OpenVPN, il est recommandé de suivre les meilleures pratiques de sécurité. Cela peut inclure l'utilisation de certificats SSL/TLS pour l'authentification des clients, l'activation du chiffrement fort pour les communications VPN, la mise en place de règles de pare-feu pour limiter l'accès au serveur, et la surveillance régulière des journaux pour détecter toute activité suspecte. La mise en œuvre de ces mesures renforce la sécurité et protège les données transmises à travers le VPN.

En ce qui concerne le déploiement du serveur OpenVPN, il existe différentes options à considérer. L'une d'entre elles est la mise en place d'un serveur sur site, où le VPN est géré directement par l'organisation elle-même. Cela offre un contrôle total sur l'infrastructure et les politiques de sécurité, mais nécessite des ressources techniques et une expertise interne pour la gestion et la maintenance du serveur.

Une autre option est d'utiliser un service de fournisseur de VPN. De nombreux fournisseurs proposent des solutions de VPN hébergées dans le cloud, ce qui simplifie la configuration et la gestion du serveur. Cela peut être avantageux pour les petites entreprises ou les organisations qui ne disposent pas des ressources techniques nécessaires pour gérer un serveur VPN en interne. Cependant, il est important de choisir un fournisseur de confiance et de prendre en compte les aspects liés à la confidentialité et à la sécurité des données.

III- Installation client

• Windows

La troisième partie de ce dossier se concentre sur la configuration des clients OpenVPN. Il est essentiel de comprendre comment installer et configurer correctement les clients sur différents systèmes d'exploitation afin de garantir une connexion sécurisée au VPN.

1.Installation du client OpenVPN sur Windows :

- Téléchargez le client OpenVPN compatible avec la version de votre système d'exploitation Windows.
- Exécutez le programme d'installation et suivez les instructions à l'écran pour installer le client.
- Une fois l'installation terminée, vous devez configurer le client en lui fournissant les informations nécessaires, telles que l'adresse du serveur VPN, les certificats et les clés d'authentification.

2.Configuration du client OpenVPN sur Windows :

- Localisez le fichier de configuration fourni par l'administrateur du serveur VPN. Ce fichier a généralement une extension .ovpn.
- Copiez ce fichier dans le répertoire d'installation du client OpenVPN.
- Lancez le client OpenVPN et recherchez l'icône dans la barre des tâches.
- Cliquez avec le bouton droit sur l'icône et sélectionnez "Importer un fichier de configuration". Sélectionnez le fichier .ovpn que vous avez copié précédemment.
- Une fois importé, cliquez avec le bouton droit sur l'icône OpenVPN et sélectionnez "Connecter" pour établir la connexion VPN.

III- Installation client

• Mac OS

1.Installation du client OpenVPN sur macOS :

- Téléchargez le client OpenVPN compatible avec votre version de macOS.
- Ouvrez le fichier d'installation téléchargé et suivez les instructions pour installer le client.
- Après l'installation, vous devez configurer le client en fournissant les informations nécessaires, telles que l'adresse du serveur VPN, les certificats et les clés d'authentification.

2.Configuration du client OpenVPN sur macOS :

- Localisez le fichier de configuration (.ovpn) fourni par l'administrateur du serveur VPN.
- Ouvrez le client OpenVPN et cliquez sur l'icône dans la barre de menus.
- Sélectionnez "Importer le profil" et choisissez le fichier .ovpn.
- Une fois importé, cliquez sur l'icône OpenVPN dans la barre de menus et sélectionnez "Connecter" pour établir la connexion VPN.

III- Installation client

• Linux

1.Installation du client OpenVPN sur Linux :

- Consultez la documentation de votre distribution Linux pour connaître la méthode d'installation du client OpenVPN spécifique.
- Installez le client OpenVPN à l'aide de la commande appropriée.
- Après l'installation, vous devrez configurer le client en fournissant les informations nécessaires, comme l'adresse du serveur VPN, les certificats et les clés d'authentification.

2.Configuration du client OpenVPN sur Linux :

- Localisez le fichier de configuration (.ovpn) fourni par l'administrateur du serveur VPN.
- Copiez ce fichier dans le répertoire /etc/openvpn/.
- Lancez le client OpenVPN en utilisant la commande "sudo openvpn --config /etc/openvpn/nom_du_fichier.ovpn".
- Le client OpenVPN se connectera au serveur VPN et vous pourrez voir les journaux de connexion dans la console.

Il est important de noter que les étapes ci-dessus sont des indications générales et peuvent varier en fonction des versions spécifiques du client OpenVPN et du système d'exploitation. Il est toujours recommandé de se référer à la documentation officielle du client OpenVPN et aux instructions fournies par l'administrateur du serveur VPN pour une configuration précise.

En résumé, cette partie du dossier a fourni des instructions détaillées sur l'installation et la configuration des clients OpenVPN sur différents systèmes d'exploitation. En suivant ces étapes, vous serez en mesure d'établir une connexion sécurisée au VPN et de profiter des avantages de la protection des données lors de l'accès à des ressources réseau à distance.

III- Installation client

• Création et suppression d'un certificat client

• GÉNÉRATION DE LA REQUÊTE DES CERTIFICATS DU CLIENT

```
srv-vpn@SRV-VPN:~/easy-rsa$ ./easyrsa gen-req Yohan
Using SSL: openssl OpenSSL 3.0.2 15 Mar 2022 (Library: OpenSSL 3.0.2 15 Mar 2022)
.....+ ... ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++* ... +.......+ .. ++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++*.+.....+ ... +.......+ .. +............+ ... +.........+.....+ ... + ... ++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
.. + ... +.........+......+.+ .. +.+.....+.+......+.........+ ... + .. +.+.........+.........+.....................+.........+
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*....+ ... +.......+ .. +.+......++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++*....+.+.........+......+ .. +..........+ ... + ... +...........+ ... +.........
............+.+ ... + ... + .. +.......+..............+......+ .. + ... +.......+...........+....++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [Yohan]:

Keypair and certificate request completed. Your files are:
req: /home/srv-vpn/easy-rsa/pki/reqs/Yohan.req
key: /home/srv-vpn/easy-rsa/pki/private/Yohan.key
```

• COPIE DE LA CLÉ + SÉCURITÉ

```
srv-vpn@SRV-VPN:~/easy-rsa$ cp pki/private/Yohan.key ~/client-configs/keys/
srv-vpn@SRV-VPN:~/easy-rsa$ scp pki/reqs/Yohan.req srv-ca@192.168.1.48:/tmp
srv-ca@192.168.1.48's password:
Yohan.req                                     100%  887   331.3KB/s   00:00
srv-vpn@SRV-VPN:~/easy-rsa$
```

• IMPORTATION DE LA REQUÊTE + CREATION DU CLIENT

```
srv-ca@SRV-CA:~/easy-rsa$ ./easyrsa import-req /tmp/Yohan.req Yohan
Using SSL: openssl OpenSSL 3.0.2 15 Mar 2022 (Library: OpenSSL 3.0.2 15 Mar 2022)

The request has been successfully imported with a short name of: Yohan
You may now use this name to perform signing operations on this request.

srv-ca@SRV-CA:~/easy-rsa$ ./easyrsa sign-req client Yohan
Using SSL: openssl OpenSSL 3.0.2 15 Mar 2022 (Library: OpenSSL 3.0.2 15 Mar 2022)


You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a client certificate for 825 days:

subject=
    commonName                = Yohan


Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
Using configuration from /home/srv-ca/easy-rsa/pki/easy-rsa-2616.EMGhbD/tmp.FZCnTa
Enter pass phrase for /home/srv-ca/easy-rsa/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'Yohan'
Certificate is to be certified until Aug 27 09:43:27 2025 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /home/srv-ca/easy-rsa/pki/issued/Yohan.crt


srv-ca@SRV-CA:~/easy-rsa$ scp pki/issued/Yohan.crt srv-vpn@192.168.1.220:/tmp
The authenticity of host '192.168.1.220 (192.168.1.220)' can't be established.
ED25519 key fingerprint is SHA256:O6NgYmgtvw1ZZZ8jrYZAMlbzoPLJKgRYN+rouHPjYqk.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
    ~/.ssh/known_hosts:4: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.220' (ED25519) to the list of known hosts.
srv-vpn@192.168.1.220's password:
Yohan.crt
```

III- Installation client

• Création et suppression d'un certificat client

• CONFIGURATION DU CLIENT

```
srv-vpn@SRV-VPN:~/easy-rsa$ mv /tmp/Yohan.crt ~/client-configs/keys/
```

```
srv-vpn@SRV-VPN:~/client-configs$ cd ~/client-configs/
srv-vpn@SRV-VPN:~/client-configs$ ./make_config.sh Yohan
srv-vpn@SRV-VPN:~/client-configs$ ls ~/client-configs/files/
client1.ovpn  Nybtech.ovpn  Yohan.ovpn
```

• REVOCATION DU CONTRAT

```
$ cd ~/easy-rsa
$ ./easyrsa revoke server-server
```

• COMMENT SUPPRIMER UN CLIENT (PAR ÉTAPES)

Accédez au serveur OpenVPN : Connectez-vous au serveur OpenVPN où le client que vous souhaitez supprimer est enregistré.

Localisez le fichier de configuration du client : Recherchez le fichier de configuration spécifique au client que vous souhaitez supprimer.

Ouvrez le fichier de configuration : recherchez les sections spécifiques au client que vous souhaitez supprimer. Ces sections commencent généralement par "client" suivi du nom ou de l'identifiant du client.

Supprimez les sections du client

Enregistrez les modifications

Redémarrez le service OpenVPN pour que les changements prennent effet.

Utilisez la commande appropriée pour redémarrer le service en fonction de votre système d'exploitation.

IV- La sécurité

1.Génération des certificats : Pour établir une connexion sécurisée entre les clients et le serveur OpenVPN, des certificats doivent être générés. Cela implique la création d'une autorité de certification (AC) pour émettre les certificats. Voici les étapes générales pour générer les certificats :

- Créez une clé privée pour l'autorité de certification (AC).
- Générez un certificat d'autorité de certification (AC) à l'aide de la clé privée.
- Générez une paire de clés privée/publique pour le serveur OpenVPN.
- Signez le certificat du serveur avec la clé privée de l'autorité de certification.
- Générez une paire de clés privée/publique pour chaque client.
- Signez les certificats des clients avec la clé privée de l'autorité de certification.

2.Distribution des certificats : Une fois les certificats générés, il est essentiel de les distribuer aux clients de manière sécurisée. Voici quelques méthodes courantes pour distribuer les certificats :

- Distribuez les certificats manuellement à chaque client en utilisant des supports de stockage sécurisés (par exemple, clés USB) ou des canaux sécurisés tels que le courrier électronique crypté.
- Utilisez une plateforme de gestion des certificats pour automatiser la distribution et la révocation des certificats. Cela peut être particulièrement utile pour les environnements avec un grand nombre de clients.

3.Meilleures pratiques pour sécuriser les échanges : Il est important de mettre en place des mesures de sécurité pour protéger les échanges entre les clients et le serveur OpenVPN. Voici quelques meilleures pratiques :

- Utilisez des protocoles de chiffrement forts, tels que AES-256, pour sécuriser les communications.
- Activez l'authentification mutuelle, qui nécessite que les clients présentent également un certificat valide pour établir une connexion.
- Mettez en place des politiques de gestion des certificats pour gérer leur expiration, leur révocation et leur renouvellement de manière appropriée.
- Utilisez des mots de passe forts pour protéger les clés privées et les certificats.
- Surveillez régulièrement les journaux de connexion pour détecter toute activité suspecte ou non autorisée.

Problèmes potentiels Et solution adaptée !

1.Configuration incorrecte : Une configuration incorrecte peut entraîner des problèmes de connectivité et de sécurité. Assurez-vous de suivre les étapes de configuration correctement et de vérifier les paramètres tels que les adresses IP, les ports, les certificats et les clés d'authentification.

Solution : Vérifiez attentivement les instructions de configuration, référez-vous à la documentation officielle et assurez-vous que tous les paramètres sont correctement définis. Effectuez des tests de connectivité pour vous assurer que le VPN fonctionne comme prévu.

2.Problèmes de pare-feu : Les pare-feu peuvent bloquer les connexions VPN, ce qui entraîne des échecs de connexion ou des performances médiocres. Les règles de pare-feu doivent être configurées pour autoriser le trafic VPN entrant et sortant.

Solution : Ajoutez les règles de pare-feu appropriées pour permettre le trafic VPN. Vérifiez également les pare-feu des clients et assurez-vous qu'ils autorisent le trafic VPN sortant.

3.Problèmes de compatibilité des systèmes d'exploitation : Différents systèmes d'exploitation peuvent nécessiter des configurations spécifiques pour se connecter au VPN. Des incompatibilités peuvent entraîner des erreurs de connexion ou des fonctionnalités limitées.

Solution : Assurez-vous de suivre les instructions de configuration spécifiques à chaque système d'exploitation. Consultez la documentation d'OpenVPN pour obtenir des conseils sur la compatibilité des différents systèmes d'exploitation.

Problèmes potentiels Et solution adaptée !

4.Problèmes de performances : Un VPN mal configuré ou surchargé peut entraîner des problèmes de performances, tels que des déconnexions fréquentes, des vitesses de connexion lentes ou une latence élevée.

Solution : Optimisez les paramètres de configuration du VPN, tels que la compression des données, le choix des protocoles de chiffrement et les paramètres de tunnel. Assurez-vous également que les ressources matérielles du serveur VPN sont adéquates pour gérer la charge de trafic.

5.Problèmes de sécurité : Une mauvaise configuration de la sécurité peut exposer votre réseau à des vulnérabilités, telles que des attaques par force brute, des fuites DNS ou des atteintes à la confidentialité des données.

Solution : Mettez en œuvre les meilleures pratiques de sécurité recommandées, telles que l'utilisation de certificats et de clés d'authentification robustes, l'activation de l'authentification mutuelle, l'utilisation de protocoles de chiffrement forts et la gestion appropriée des certificats.

6.Problèmes de gestion des certificats : La gestion des certificats peut être complexe, notamment en ce qui concerne leur expiration, leur renouvellement et leur révocation. Une mauvaise gestion peut entraîner des problèmes de connexion ou des risques de sécurité.

Solution : Établissez des politiques de gestion des certificats claires et suivez-les attentivement. Utilisez des outils de gestion des certificats pour automatiser les tâches de renouvellement et de révocation des certificats.

Portée du Travail

ETAPE 1:

- INSTALLATION OPENVPN + EASY RSA
- CREATION D'UNE ICP POUR OPENVPN
- CREATION DEMANDE CERTIFICAT OPENVPN + CLÉ SECURITE
- FINALISATION DU CERTIFICAT

ETAPE 2:

- CONFIGURATION MATERIEL OPENVPN
- GÉNÉRATION CERTIFICAT CLIENT+ PAIRE DE CLÉ
- CONFIGURER OPENVPN
- REDIRECT GATEWAY
- PORT ET PROTOCOLE
- CONFIGURATION RESEAU OPENVPN

ETAPE 3:

- CONFIGURATION PARE FEU
- DEMARRER OPENVPN
- CRÉER INFRASTRUCTURE CLIENT
- GÉNÉRER CONFIGURATIONS CLIENT
- INSTALLATION

En images maintenant

DESCRIPTION DU TRAVAIL	DATE DE DÉBUT	DATE DE FIN
PHASE 1 Recherche et formation du groupe	28 Avril 2023	5 Mai 2023
PHASE 2 Mise en place de la répartition des tâches	5 Mai 2023	12 Mai 2023
PHASE 3 Travail d'équipe et création	12 Mai 2023	26 Mai 2023

En images maintenant

• Etape 1:

- INSTALLATION OPENVPN + EASY RSA

```
$ sudo apt update
$ sudo apt install openvpn easy-rsa
$ mkdir ~/easy-rsa
$ ln -s /usr/share/easy-rsa/* ~/easy-rsa/
$ sudo chown serveur ~/easy-rsa
$ chmod 700 ~/easy-rsa
$ cd ~/easy-rsa
$ nano vars
```

- CREATION D'UNE ICP POUR OPENVPN
- CREATION DEMANDE CERTIFICAT OPENVPN + CLÉ SECURITE

```
(Modification de vars avec :

set_var EASYRSA_ALGO "ec"
set_var EASYRSA_DIGEST "sha512")

$ ./easyrsa init-pki
$ cd ~/easy-rsa
$ ./easyrsa gen-req server nopass
$ sudo cp /home/serveur/easy-rsa/pki/private/server.key /etc/openvpn/server/
```

- FINALISATION DU CERTIFICAT

```
$ scp /home/serveur/easy-rsa/pki/reqs/server.req serveur@your_ca_server_ip:/tmp
(- On passe sur le serveur CA)
$ cd ~/easy-rsa
$ ./easyrsa import-req /tmp/server.req server
$ ./easyrsa sign-req server server
$ scp pki/issued/server.crt serveur@your_vpn_server_ip:/tmp
$ scp pki/ca.crt serveur@your_vpn_server_ip:/tmp
(- On passe sur le serveur openvpn)
$ sudo cp /tmp/{server.crt,ca.crt} /etc/openvpn/server
```

En images maintenant

• Etape 2:

• CONFIGURATION MATERIEL OPENVPN

```
$ cd ~/easy-rsa
$ openvpn --genkey --secret ta.key
$ sudo cp ta.key /etc/openvpn/server
```

• GÉNÉRATION CERTIFICAT CLIENT+ PAIRE DE CLÉ

```
$ mkdir -p ~/client-configs/keys
$ chmod -R 700 ~/client-configs
$ cd ~/easy-rsa
$ ./easyrsa gen-req client1 nopass
$ cp pki/private/client1.key ~/client-configs/keys/
$ scp pki/reqs/client1.req serveur@your_ca_server_ip:/tmp
(- On passe sur le serveur CA)
$ cd ~/easy-rsa
$ ./easyrsa import-req /tmp/client1.req client1
$./easyrsa sign-req client client1
$ scp pki/issued/client1.crt serveur@your_server_ip:/tmp
(- On passe sur le serveur openvpn)
$ cp /tmp/client1.crt ~/client-configs/keys/
$ cp ~/easy-rsa/ta.key ~/client-configs/keys/
$ sudo cp /etc/openvpn/server/ca.crt ~/client-configs/keys/
$ sudo chown serveur.serveur ~/client-configs/keys/*
```

• CONFIGURER OPENVPN

```
$ sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz/etc/openvpn/server/
$ sudo gunzip /etc/openvpn/server/server.conf.gz
$ sudo nano /etc/openvpn/server/server.conf
(Modification des clés de sécurté + auth SHA256 algo cryptage)
(Modification dns pour rediriger tout le trafic par le vpn)
(Ajuster le port et le protocole passage udp à tcp par exemple)
```

```
$ sudo nano /etc/sysctl.conf
$ sudo sysctl -p
```

En images maintenant

• Etape 3:

- CONFIGURATION PARE FEU

```
$ ip route list default
$ sudo nano /etc/ufw/before.rules
(modifier règles UFW)
$ sudo nano /etc/default/ufw
(modifier politique par défaut -drop à -accept)
$ sudo ufw allow 1194/udp
$ sudo ufw allow OpenSSH
$ sudo ufw disable
$ sudo ufw enable
```

- DEMARRER OPENVPN
- CRÉER INFRASTRUCTURE CLIENT

```
$ sudo systemctl -f enable openvpn-server@server.service
$ sudo systemctl start openvpn-server@server.service
$ sudo systemctl status openvpn-server@server.service
$ mkdir -p ~/client-configs/files
$ cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf
$ nano ~/client-configs/base.conf
(modifier fichier base.conf)
$ nano ~/client-configs/make_config.sh
(ajouter un script à ce fichier)
$ chmod 700 ~/client-configs/make_config.sh
```

- GÉNÉRER CONFIGURATIONS CLIENT
- INSTALLATION

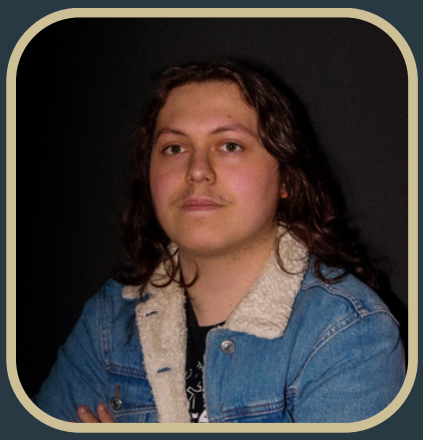
```
$ cd ~/client-configs
$ ./make_config.sh client1
$ ls ~/client-configs/files
(Installation poste client + connexion)
$ sudo openvpn --config client1.ovpn
```

Notre groupe

Qui est dans notre équipe ?

Notre équipe est composée de deux étudiants en deuxième année informatique.

VELAY Yohan
CABEE Pauline



Conclusion

En conclusion, ce dossier technique a couvert de manière approfondie la création d'un VPN avec OpenVPN. En suivant les étapes, les bonnes pratiques et les recommandations présentées, vous pouvez mettre en place un réseau privé virtuel sécurisé pour protéger efficacement vos données et vos communications dans un environnement en ligne potentiellement hostile.

Nous avons exploré les notions de base des réseaux privés virtuels (VPN) et leur utilité dans le contexte actuel, en mettant l'accent sur les principes de cryptographie et de chiffrement qui sous-tendent le fonctionnement d'OpenVPN. Comprendre ces concepts fondamentaux est essentiel pour une mise en œuvre réussie et sécurisée d'un VPN.

Nous avons également examiné les différentes options d'architecture pour la mise en place d'un serveur OpenVPN, en soulignant les exigences matérielles et logicielles, ainsi que les meilleures pratiques pour configurer le serveur en fonction des besoins spécifiques du réseau. Nous avons également présenté les options de déploiement, qu'il s'agisse de la mise en place d'un serveur sur site ou de l'utilisation d'un service de fournisseur de VPN. La troisième partie du dossier s'est concentrée sur la configuration des clients OpenVPN, en fournissant des instructions détaillées pour installer et configurer les clients sur différents systèmes d'exploitation. Nous avons souligné l'importance de suivre les étapes clés pour garantir une connexion sécurisée au VPN.

Enfin, nous avons abordé les aspects de sécurité et de gestion des certificats, en expliquant les méthodes appropriées pour générer et distribuer les certificats, ainsi que les meilleures pratiques pour sécuriser les échanges entre les clients et le serveur OpenVPN. La sécurité des certificats et des communications est cruciale pour maintenir l'intégrité et la confidentialité des données échangées via le VPN.

En mettant en pratique les connaissances acquises dans ce dossier, vous serez en mesure de créer un VPN sécurisé avec OpenVPN, renforçant ainsi la protection de vos données et de vos communications en ligne. N'oubliez pas de mettre régulièrement à jour votre infrastructure et de suivre les évolutions en matière de sécurité pour rester à jour avec les meilleures pratiques.

En résumé, ce dossier vous a fourni une compréhension approfondie de la création d'un VPN avec OpenVPN, vous permettant de mettre en place un réseau privé virtuel sécurisé dans le but de protéger vos données et vos communications dans un environnement en ligne potentiellement hostile.