Documentation technique première version échouée : VPN

Ce document explique en détail comment mettre en place un serveur OpenVPN, sous une machine kali. Nous avons crée une infrastructure PKI, nous géront grâce à des certificats la communication de manière sécurisé.

Prérequis :

- Une machine kali.

- Un accès root.

Définition du réseau :

|  |  |
| --- | --- |
| Eléments | Rôle |
| Client VPN | Ordinateur de l’utilisateur, connecté avec un fichier .ovpn. |
| Serveur OpenVPN | Serveur OpenVPN sur une machine Kali. |
| Interface VPN | Interface crée par OpenVPN. |
| Interface réseau | Accès réseau vers Internet. |
| Intranet | Réseau privé contenant fichier, serveur interne. |

Bonnes pratiques :

PKI (Public Key Infrastructure) : Clés publics et privés qui permettent l’authentification des clients et des serveurs.

TLS (Transport Layer Security) : protocole de sécurité pour vérifier l’intégrité et l’authenticité d’un message.

DH (diffie-hellman) : Le client et le serveur disposent chacun de leur clé privée, qu'ils utilisent avec la clé publique pour créer une clé commune. La clé privée est également appelée clé secrète.

HMAC (hash-based Message Authentification Code) : clé statique utilisée pour protéger le serveur d’attaque par force brut ou Dos.

UFW (Uncomplicated Firewall) : Génère un pare-feu.

NAT (Network Address Translation) : permet à des serveurs, des hôtes et des consoles se trouvant sur différents réseaux de communiquer entre eux via un réseau interne commun.

I - Mise à jour du système et Installation des logiciels nécessaires.

Pour commence nous vérifions que notre système est à jour et nous installons les logiciels nécessaires :

sudo apt update

sudo apt install openvpn easy-rsa ufw

La première commande, permet de vérifier si notre système est à jour et de le mettre à jour si tel n’est pas le cas. La deuxième commande, install openvpn, mais aussi l’outil easy-rsa qui va nous permettre de gérer les certificas et la pki. Enfin, nous installons uwf, qui permet une sécurité simplifié.

II - Création de l’infrastructure PKI :

Nous allons maintenant créer un dossier pour Easy-rsa qui contiendra les scripts nécessaires pour pouvoir stocker les clés et les certificats :

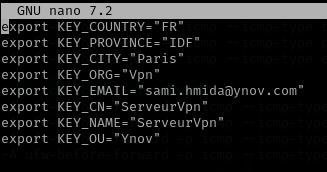
IMG_256

IMG_256

III - Configuration des valeurs par défaut des PKI :

nano vars

On édite le fichier «vars» pour configurer les valeurs par défaut qui seront présentes dans chaque certificats :



IV - Initialisation de la PKI :

IMG_256

Dans cette étape, nous éxécutons un script qui initialise easy-rsa, et ensuite nous initialisons la PKI avec «init-pki» qui crée un sous-dossier qui contiendra les certificats, les clés etc.

V - Création de la CA :

Maintenant nous créons une autorité de certifications qui s’occupera dans le futur pour certifier les certificats et les clients du VPN.

IMG_256

Cette commande, construit l’autorité de certification et génère une paire de clé :

- une clé secrète

- une clé public.

VI - Requête et clé du serveur :

Maintenant que nous avons crée notre CA, nous créons la clé privée du serveur et le certificat.

IMG_256

Cette commande génère une clé privée pour le serveur mais aussi une requête de certificat pour le serveur. La requête de certificat devra donc être validé par le CA.

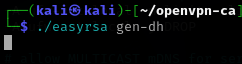
VII - Validation du certificat du serveur :

IMG_256

Cette commande, permet de valider la requête du serveur fait dans l’étape d’avant avec le CA. La commande indique qu’il y a un certificat à valider, on lui indique le type et le nom, ici «server».

VIII - Génération de la clé DH :

Dans cette étape, nous créons la clé DH qui est un protocole de sécurité indispensable pour OpenVpn. En effet, elle permet d’établir des connexions sécurisés entre le serveur et le client.



IX - Génération de la clé TLS HMAC :

IMG_256

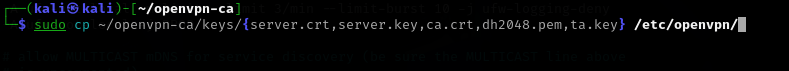
Cette commande, rajoute une protection supplémentaire de sécurité à la clé DH. Elle permet de protéger le serveur des attaques de brut-force ou de Dos. Elle génère une clé statique que l’on stocke dans le fichier ta.key. Ce fichier devra être partagé entre le client et le serveur pour chiffrer et permettre l’authentification.

X - Requête et clé client :



Comme pour l’étape 6, nous générons une clé et une requête de certificat pour un client. Puis cette requête est validé par la CA, nous indiquons que c’est un client et son nom «client1».

XI - Copie des certificats pour OpenVpn :

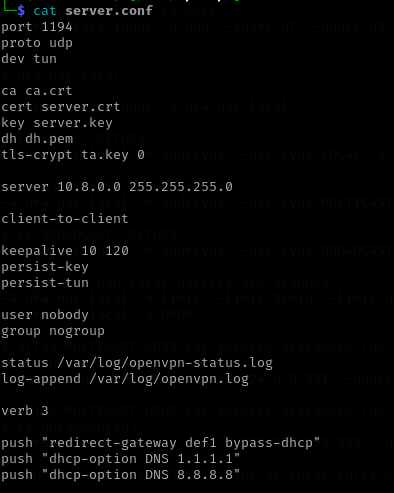


Cette commande copie les certificats crée depuis le début de la configuration dans le fichier d’openvpn pour qu’il puisse y avoir accès et démarrer correctement.

XII - Création du fichier de configuration serveur :

Dans cette étape, nous configurons les paramètres de fonctionnement du serveur VPN. Pour cela nous créons un fichier appelé «server.conf», on y retrouve les port d’écoute, les protocoles, les plages ip etc. C’est ce fichier qui sera lu au démarrage d’openvpn.

XIII - Modification de server.conf :



Dans le fichier server.conf on retrouve donc les ports, les plages d’ip, les certificats et clés, la sécurité et les logs.

XIV - Démarrage du service OpenVpn :

IMG_256

Cette commande lance donc OpenVpn, une fois la configuration en place.

IMG_256

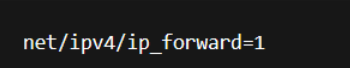
Cette commande nous permet de laisser actif le VPN même après un redémarrage système.

XV - Activation du routage IP :

Maintenant que nous avons un VPN actif et en marche, nous devons nous assurer que les clients qui se connecte au VPN puisse accéder à internet. Pour cela nous faisons cette commande pour activer le routage IP :

IMG_256

Et nous décommentons cette ligne :

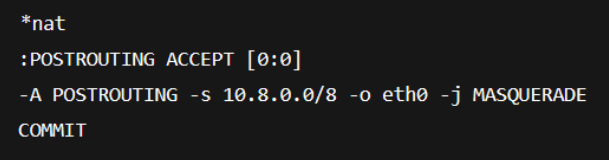


Cette ligne, permet d’autoriser le transfert de paquets IP d’une interface à une autre. Le serveur sert de pont entre les deux réseaux.

XVI - Ajout d’une règle dans UFW :

Dans cette étape, nous modifions les règles du prae-feu ufw pour ajouter une règle NAT, pour protéger les clients en masquant leur ip.

IMG_256



Cette règle, applique à tous les paquets sortants depuis le réseau VPN un masque de leur adresse avec l’adresse source du serveur.

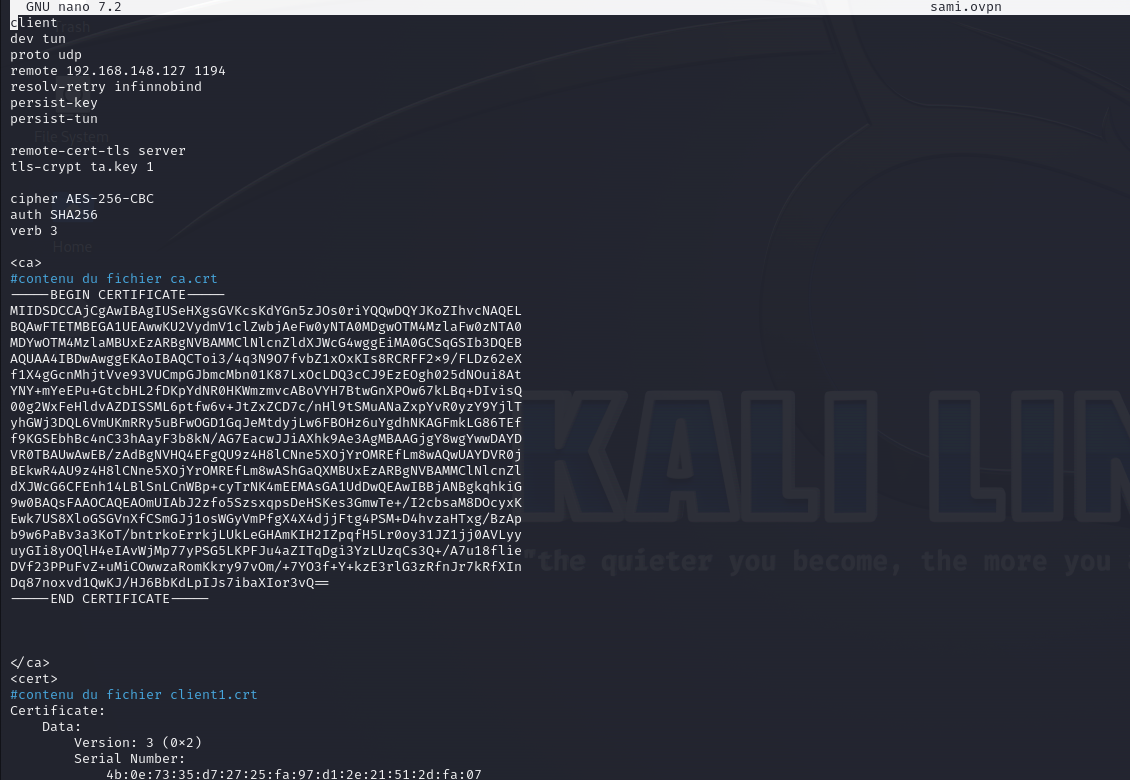
IMG_256

Comme on a modifié les règles du pare-feu, nous rechargeons la configuration pour appliquer les nouvelles règles.

XVII - Création du fichier client :

Maintenant que le serveur est en place, nous créons le fichier de configuration pour le client. Ce fichier permettra à un client de se connecter facilement.

IMG_256



Ce fichier contient tous les éléments pour se connecter au serveur, on y retrouve les certificats, les clés etc.

XVIII - Lancement du client pour se connecter au VPN :

Maintenant que nous avons un fichier .ovpn, nous réalisons cette commande pour se connecter au VPN :

IMG_256

