OpenVPN sous pfSense

On ajoute un VPN au routeur pfSense. Dans cette configuration, on ajoute l'authentification d'un utilisateur (à créer sur le routeur). OpenVPN, ici, repose sur une PKI complète ; il faudra créer une autorité de certification qui signera le certificat du serveur. A la fin, il faudra générer une bi-clé par client de connexion.

1 Création de la PKI

Il faut successivement créer une autorité de certification puis un certificat de serveur.

1.1 Création de l'autorité de certification

On passe par le choix du menu `System/Certificate`. On accède à l'onglet `Authorities` et on clique sur le bouton `+Add`. Dans la section `Create/Edit CA`, on nomme l'autorité de certification et on choisit dans le menu déroulant de `Method` l'entrée `Create an Internal Certificate Authority`. La section `Internal Certificate Authority` est à remplir en choisissant comme `Common Name` le FQDN du réseau que nous avons créé au TP 3 (`cs.sr`). Les autres champs sont à remplir correctement, comme lors de la création d'un certificat avec OpenSSL.

1.2 Création du certificat de serveur

On sélectionne ensuite l'onglet `Certificates` pour générer le certificat de serveur en cliquant sur le bouton `+Add/Sign`. Dans la section `Add/Sign a New Certificate` choisir la méthode `Create an Internal Certificate` en le nommant (p.e. `OpenVPN-remote-access`). Dans la section suivante `Internal Certificate`, on sélectionne l'autorité de certification créée précédemment en précisant bien le champ `Common Name` avec le nom du serveur (`pfSense.cs.sr`). La section `Certificate Attributes` doit préciser qu'on souhaite un certificat de serveur dans le menu déroulant `Certificate Type`. Après avoir cliqué sur `Save`, le certificat doit apparaitre.

2 Création d'un utilisateur

On crée un utilisateur `alice` par le choix du menu `System/User Manager`. Attention, il faut que l'utilisateur ait le droit de se connecter. Il n'est pas utile de lui accorder des privilèges, son compte ne sert qu'à l'authentifier pour l'accès OpenVPN. On doit créer un certificat à l'utilisateur en cochant la case `Click to create a user certificate`.

3 Configuration d'OpenVPN

Le plus compliqué reste à faire, configurer OpenVPN puis transmettre la configuration au client.

3.1 Configuration

On fait appel au Wizard (accessible depuis le choix `VPN/OpenVPN` onglet `Wizards` qui comporte un certain nombre d'étapes (11). Voici quelques indications dans les choix pour le type de serveur sera `Local user access`. Vous adapterez les adresses données en exemple à votre configuration (adresse WAN et LAN notamment) et assignerez une adresse VPN (appelée plus loin `IPv4 Tunnel Net`). Voici mon plan d'affectation d'adresses (suivi d'un espace vierge pour les votres) :

WAN	172.16.250.133	
LAN	192.168.140.13	
IPv4 Tunnel Net	192.168.100.0/243	

La suite décrit les choix à faire aux différentes étapes de la configuration par le Wizard :

```
Type of server : Local User Access
(5) CA : OK
(7) Server cert : OK
(9) Section Tunnel Settings
    Tunnel Network : 192.168.100.0/24
    Local Network : 192.168.140.0/24
    Section Client Settings
    DNS Default Domain : cs.sr
    DNS Server 1: LAN IP 192.168.140.1
(10) Section Traffic from clients to server
     Add a firewall Rule
     Add an OpenVPN rule
```

Le wizard ne fait hélas pas tout le travail et il faut ensuite éditer la configuration (avec le bouton crayon) créée pour modifier les sections pointées conformément à ce qui suit :

```
Advanced Configuration
    push "route 192.168.140.0 255.255.255.0"
Gateway creation
    IPv4 only
Verbosity level 3
```

Le VPN est normalement bien configuré et le démon démarré automatiquement par pfSense. Il reste à exporter la configuration pour le client.

3.2 Exportation de la configuration client

On ajoute le paquet `openvpn-client-export` par le gestionnaire de paquets. Une fois l'application installée, on retourne dans le menu `VPN/OpenVPN` et on choisit l'onglet `Client Export` pour exporter la configuration relative à `alice`. Cliquer sur `Most Clients` pour exporter un fichier `.ovpn`.

4 Utilisation

Sur votre machine physique, installez un client OpenVPN :

- MacOS : Tunnelblick
- Windows : OpenVPN Connect
- Linux : en CLI

Téléchargez le fichier `.ovpn` pour vous connecter au VPN. A l'issue de tout ça, vous devez avoir accès à la `lxle` par son IP, voire peut-être par son entrée `DNS` (une MAJ des serveurs DNS de la machine hébergeant le client DNS sera peut-être à faire).
Au besoin, ajoutez une règle au firewall de la `pfsense` côté WAN pour autoriser les `pings` pour éviter la déconnexion automatique à `openVPN`.

5 Sécurité

Vérifiez que la connexion entre le client VPN et l'interface WAN de `pfSense` sont bien chiffrées (en reniflant l'interface WAN de la connexion).