Procédure - Mise en place d’un VPN OpenVPN sur pfSense

Objectif :

Permettre aux utilisateurs distants d’accéder de façon sécurisée aux ressources du réseau interne via un tunnel VPN chiffré, grâce à la solution OpenVPN intégrée à pfSense.

Prérequis :

- Un **pare-feu pfSense** installé et opérationnel.
- Accès à l’interface web d’administration de pfSense.
- Un nom de domaine ou une IP publique (ou dynamique avec DynDNS).
- Ports 1194 UDP ouverts sur la box ou le pare-feu extérieur.

Étapes détaillées :

1. Création de la CA (Autorité de Certification)

1. Aller dans **System > Cert. Manager > CAs**.
2. Cliquer sur **Add**.
3. Renseigner :
    - Descriptive name : `OpenVPN_CA`
    - Method : Create an internal Certificate Authority
    - Country, State, Common Name : remplir selon l’organisation.
4. Enregistrer.

---

2. Création du certificat serveur OpenVPN

1. Aller dans **System > Cert. Manager > Certificates**.
2. Cliquer sur **Add/Sign**.
3. Renseigner :
    - Descriptive name : `OpenVPN_Server_Cert`
    - Certificate authority : `OpenVPN_CA`
    - Type : Server Certificate
    - Common name : `vpn.mondomaine.local`
4. Enregistrer.

---

3. Configuration du serveur OpenVPN

1. Aller dans **VPN > OpenVPN > Servers**, puis **Add**.
2. Paramètres importants :
    - **Server Mode** : Remote Access (SSL/TLS + User Auth)
    - **Backend for auth.** : Local Database
    - **Protocol** : UDP
    - **Device Mode** : tun
    - **Interface** : WAN
    - **Local port** : 1194
    - **TLS Auth** : Enable
    - **Peer Certificate Authority** : OpenVPN_CA
    - **Server Certificate** : OpenVPN_Server_Cert
    - **IPv4 Tunnel Network** : `10.8.0.0/24` (plage utilisée pour les clients VPN)
    - **Redirect Gateway** : Cochez si vous voulez que tout le trafic client passe par le VPN.
3. Enregistrer et appliquer.

---

4. Création des utilisateurs VPN

1. Aller dans **System > User Manager > Users**, cliquer sur **Add**.
2. Renseigner le nom, mot de passe.
3. Cocher "Click to create a user certificate".
4. Sélectionner : Certificate Authority = OpenVPN_CA
5. Créer le certificat utilisateur.
6. Répéter pour chaque utilisateur VPN.

---

5. Ouverture du port dans le pare-feu pfSense

1. Aller dans **Firewall > Rules > WAN**, cliquer sur **Add**.
2. Interface : WAN
3. Protocol : UDP
4. Source : any
5. Destination port range : 1194
6. Destination : WAN address

7. Enregistrer et appliquer.

---

6. Génération du client de connexion OpenVPN

1. Aller dans **VPN > OpenVPN > Client Export** (installer le package si nécessaire).
2. Sélectionner l'utilisateur souhaité.
3. Choisir l'option correspondant à votre OS (Windows, Linux, etc.).
4. Télécharger le fichier `.ovpn` ou l'installeur préconfiguré.

---

7. Connexion et test du VPN côté client

1. Installer OpenVPN Client (Windows : openvpn.net).
2. Importer le fichier `.ovpn`.
3. Se connecter avec les identifiants créés.
4. Tester :
    - `ping 192.168.1.1` (routeur pfSense)
    - Accès aux fichiers ou services internes.

Compétences acquises :

- Administration d'un **pare-feu pfSense**.
- Configuration d'un **service VPN sécurisé avec OpenVPN**.
- Création et gestion de **certificats SSL/TLS**.
- Mise en place d'un **tunnel sécurisé pour accès distant**.
- Gestion des **règles de pare-feu et ports réseaux**.
- Authentification basée sur certificats + comptes utilisateurs.