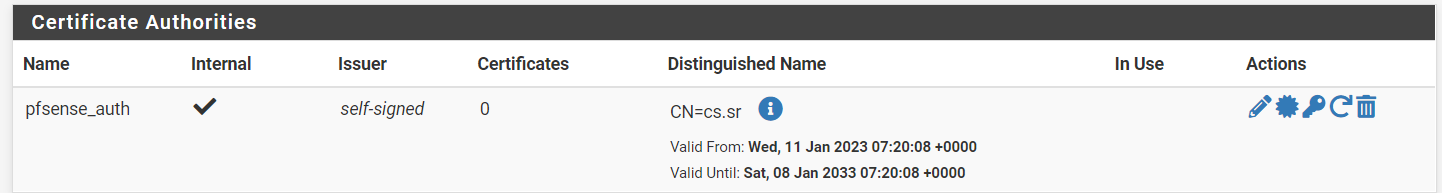
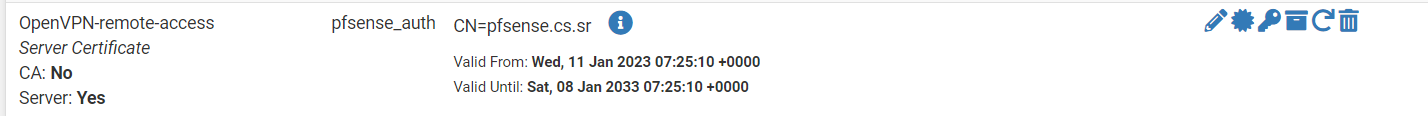
**TP 4 – OpenVPN**

On commence par créer le certificat d’autorité :



On s’en sert ensuite pour signer un nouveau certificat de serveur :



On créé ensuite l’utilisateur Alice, avec un certificat signé par le certificat d’autorité :



On créé ensuite la configuration OpenVPN sur le serveur :

Une image contenant texte

Description générée automatiquement

Ne pas oublier de configurer en « **remote access user** » :

Une image contenant texte

Description générée automatiquement

Pour installer le paquet **openvpn-client-export**, j’ai dû reconfigurer les adresses DNS dans la configuration pfSense pour qu’elles fonctionnent sur la connexion de l’université.

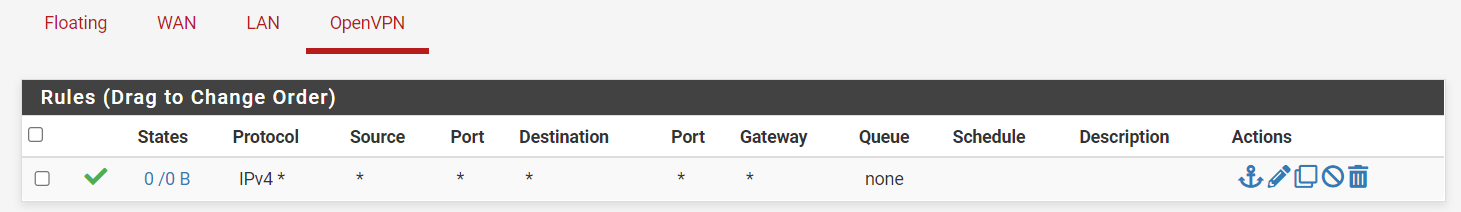
Configuration réseau :

|  |  |
| --- | --- |
| WAN | 192.168.5.130 |
| LAN | 192.168.126.10 |
| IPv4 tunnel net | 192.168.189.0/24 |

On n’oublie pas d’autoriser le port OpenVPN dans le parefeu :



On considère le réseau interne OpenVPN comme sûr parce qu’il n’y a que des administrateurs qui vont s’y connecter : on laisse donc passer tout le trafic :



On télécharge le fichier de configuration client, on le lance avec les identifiants d’Alice et on se retrouve connecté avec l’adresse 192.168.189.2 (gateway = 192.168.189.1).

Maintenant, lorsqu’on tente de communiquer avec l’hôte LXLE (192.168.126.11), tout le trafic transite par OpenVPN (capture Wireshark)

