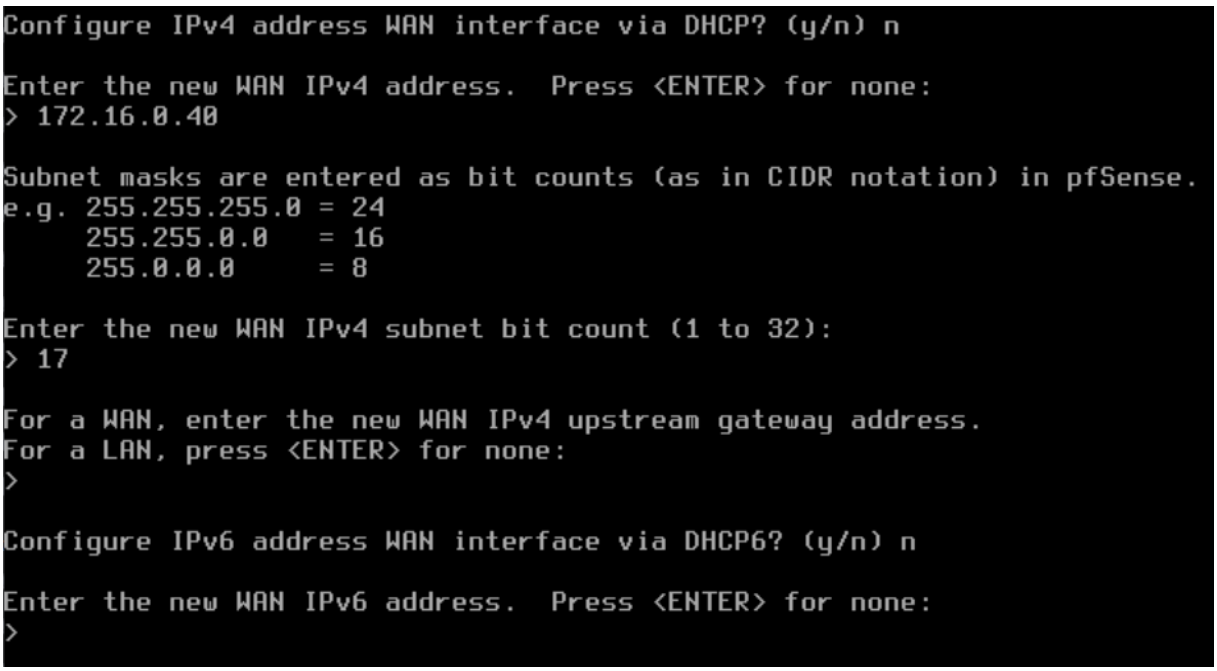
Configuration Certilab

Table des matières

1. Configuration IP et paramètres généraux

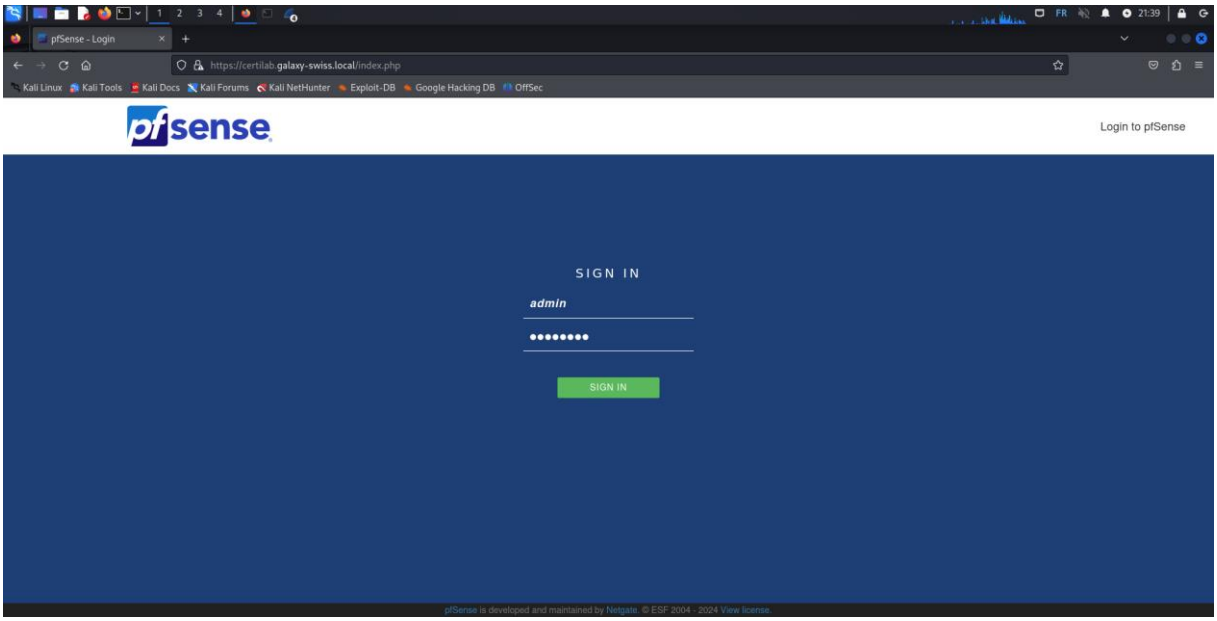
On va devoir mettre une adresse IP à l'interface principale de notre OS PfSense.

Ici on doit taper sur le 2, afin de mettre une adresse IP à l'interface em0 qui sera notre accès a l'interface Web pour continuer à l'administration de manière plus graphique et plus simple.

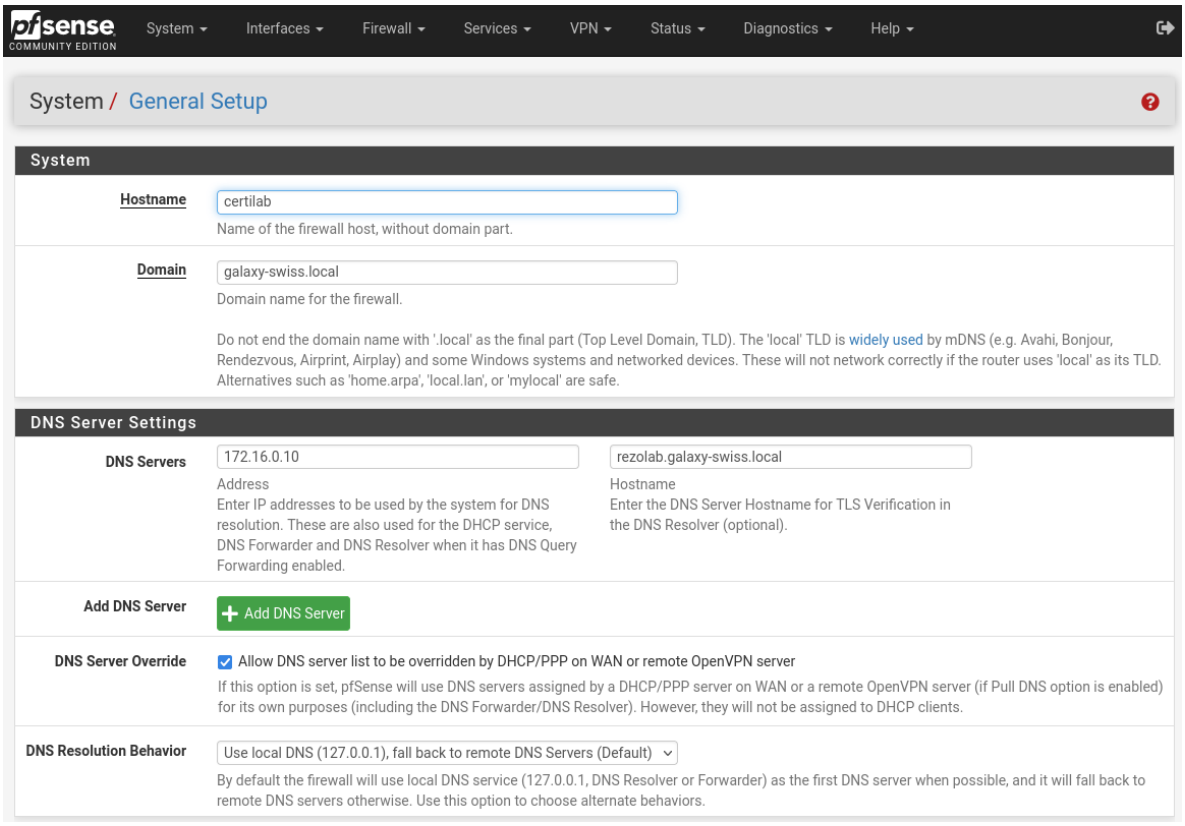


2. Administration sur l'interface Web

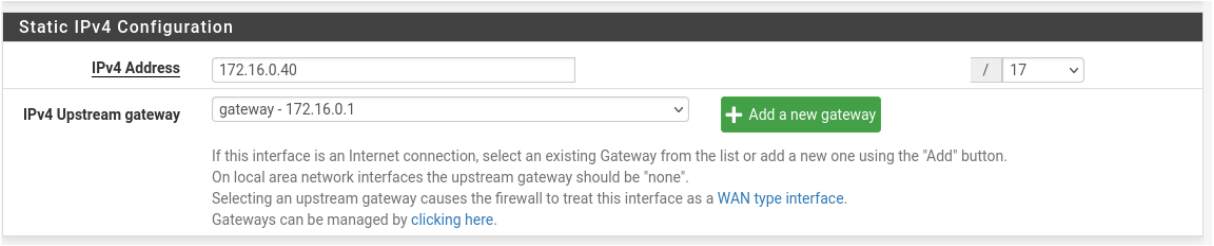
On va passer sur l'interface Web, on peut s'y connecter avec son FQDN grâce a son nom DNS :



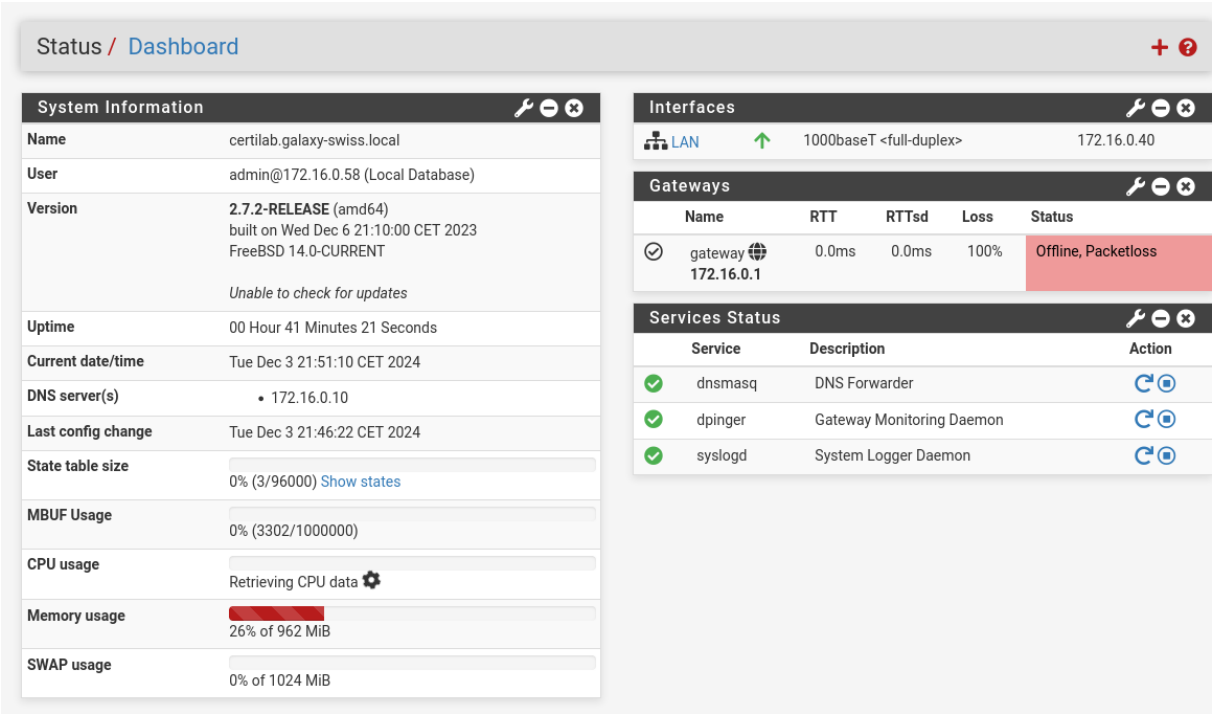
On va continuer la configuration IP Notamment en lui affectant notre serveur DNS qui est Rezolab



Et lui mettre une adresse de passerelle pour qu'elle puisse communiquer avec les autres réseaux :



On peut voir les informations générales du PFSense actuel

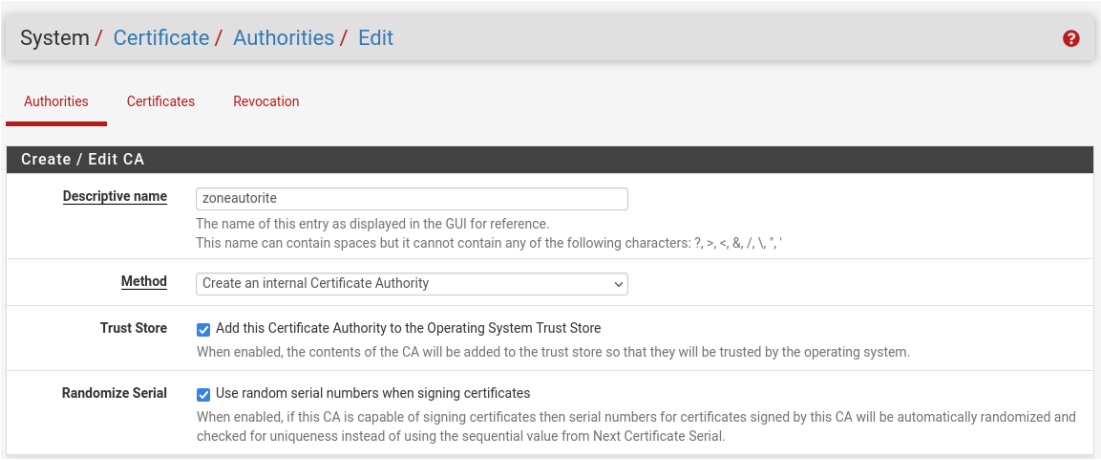


3. Création des Certificat d'autorité et Certificats Serveur

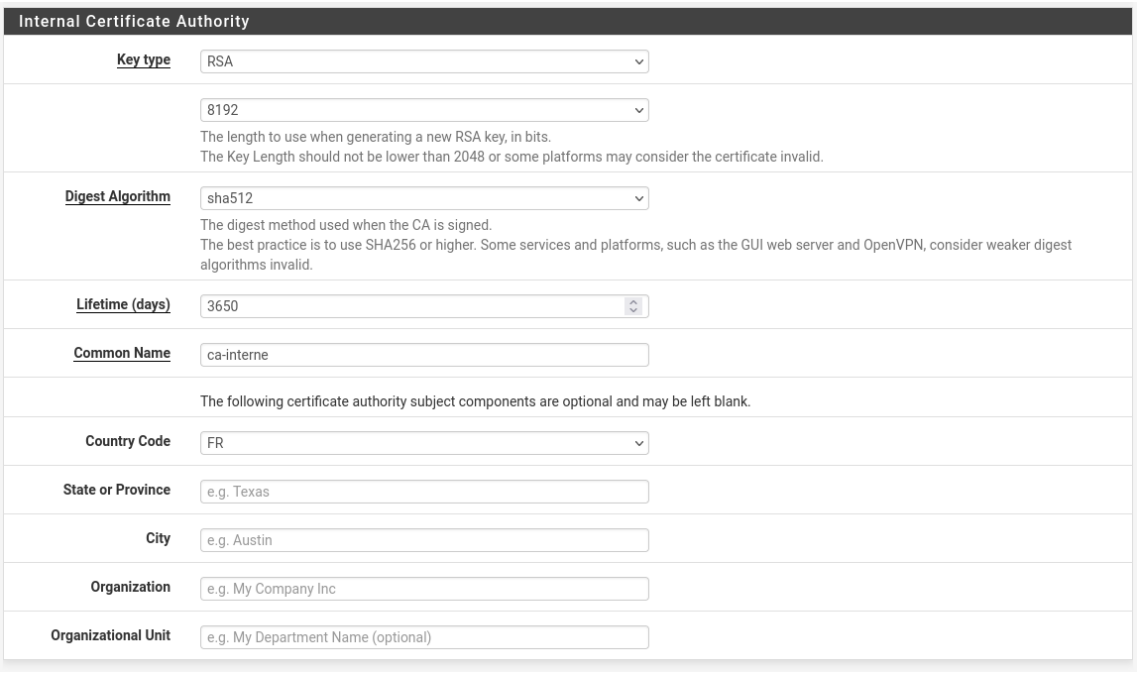
1. Certificat Autorité

Tout d'abord, nous devons créer un Certificat d'autorité autosigné afin de fournir aux différentes interfaces web une sécurisation en https.

On va créer une zone d'autorité appelée « zoneautorite » qu'on va déclarer comme un « Trust Store » qui va permettre à l'OS de faire confiance au certificat créé.

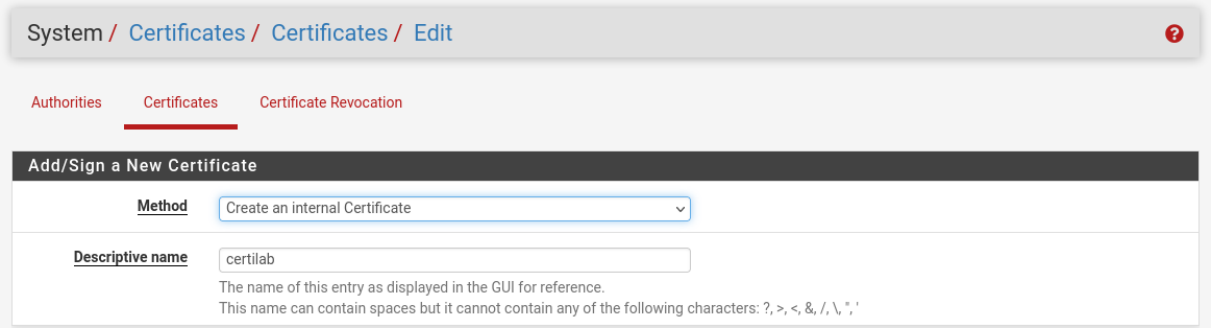


Ici on va définir les algos de chiffrement avec le type de clé, plus les bits sont élevés plus les échanges vont etre difficiles à déchiffrer. Ensuite on a les informations facultatives telles que la region etc...que nous allons pas remplir. Notre Certification d'Autorité est bien créée.

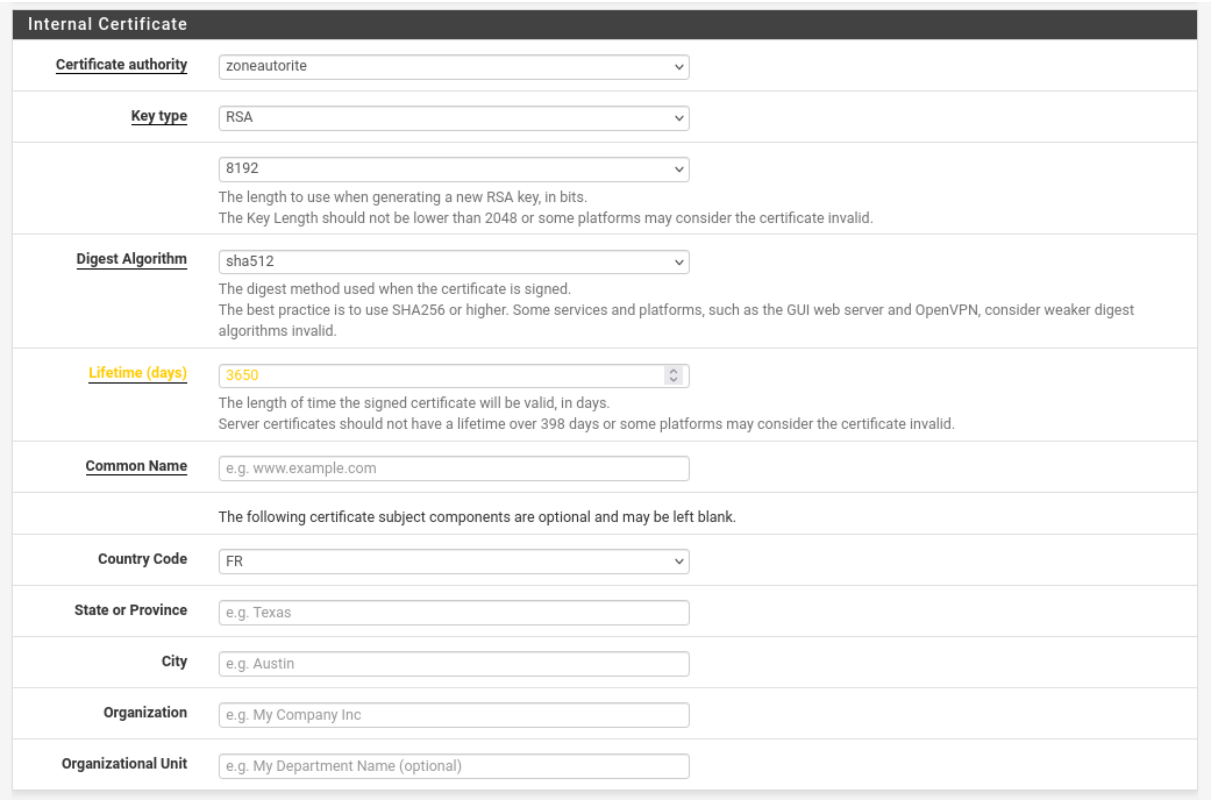


2. Certificats de Serveurs

Ensuite nous allons créer les Certificats de Serveurs, ici je déclare son nom et pour que cela soit explicite je mets le nom du serveur en question « Certilab ».

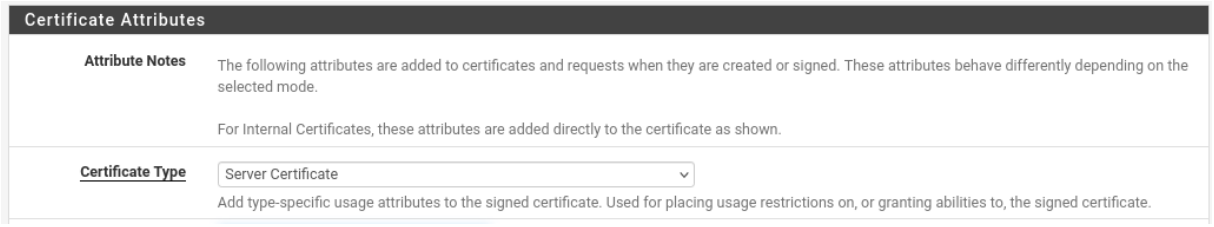


Ces Certificats doivent s'appuyer sur le Certificat d'autorité défini juste avant, alors nous déclarons donc que « zoneautorite » est le certificat qui sert d'autorité au certificat Certilab. On ne rentre pas les informations facultatives.



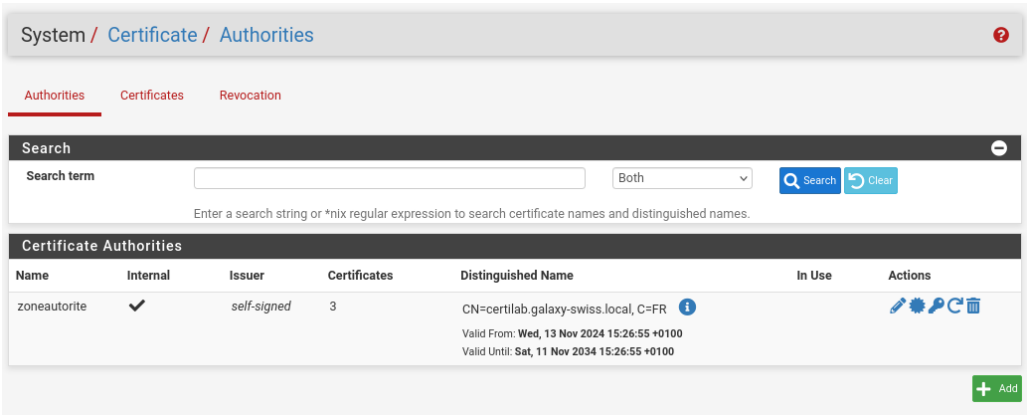
Ici, on veille à faire bien attention que ce soit un type de certificat « Server certificate » pour qu'on puisse les implanter dans les configurations de nos serveurs.

Après cela, le premier certificat de serveur est créé, on peut cliquer sur « save » et faire la même chose avec les autres :

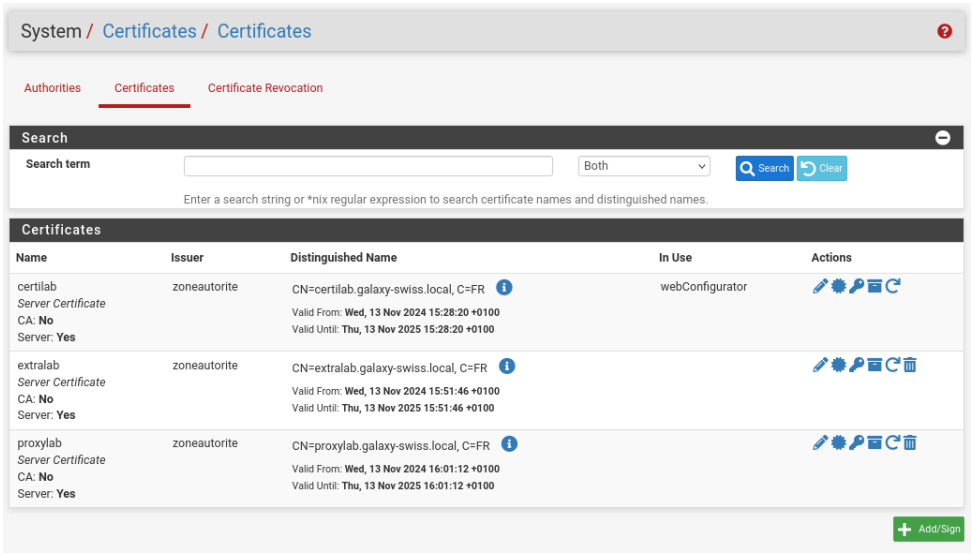


3. Liste des certificats :

Certificat D'autorité :

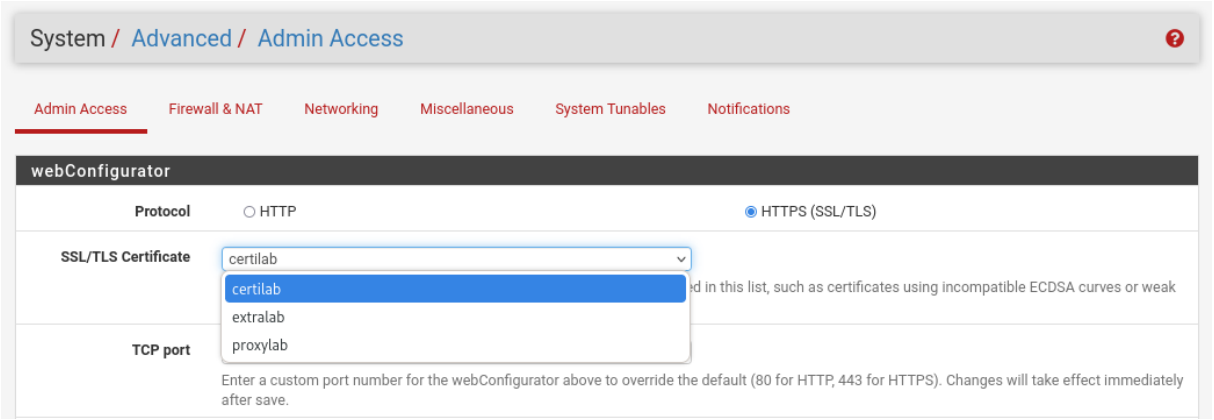


Certificats Serveurs :

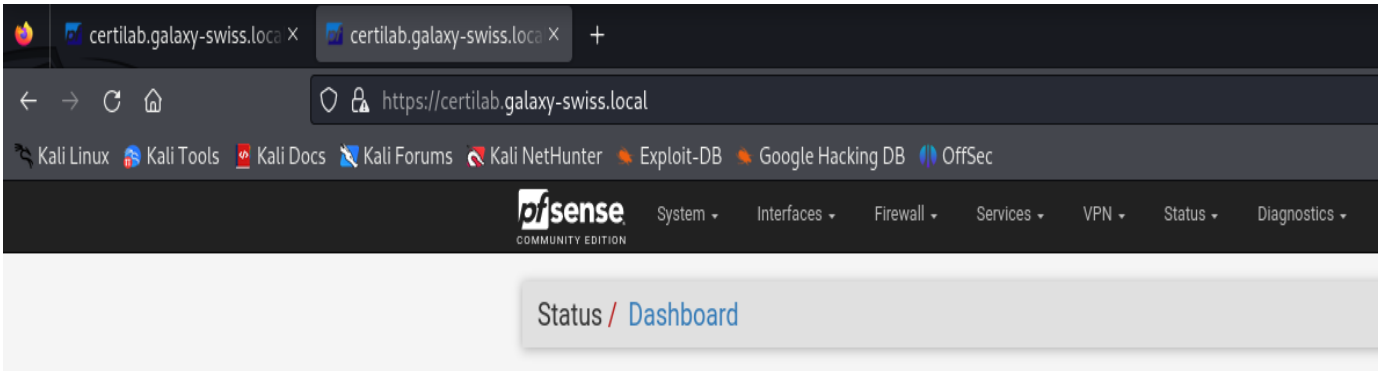


4. Mise en place du Certificat SSL sur le WebConfigurator du Certilab

Pour que l'interface Web sécurisée soit opérationnelle, nous devons sélectionner le protocole HTTPS dans les paramètres avancés et sélectionner le certificat correspondant au Certilab.



5. Test de la connexion en https :

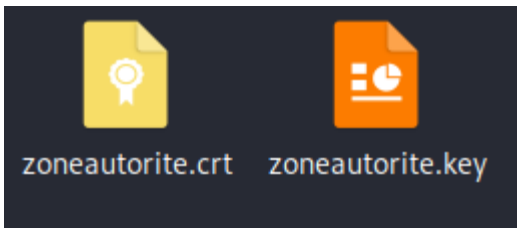


On peut voir que nous sommes connectés en https et qu'on ne peut pas nous connecter en http, ce qui sécurise donc les échanges entre ce serveur et les autres services.

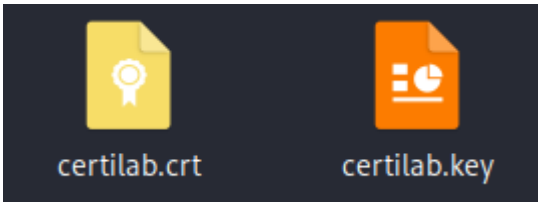
Nous allons évidemment faire la même chose sur les autres serveurs disposant d'une interface Web à sécuriser

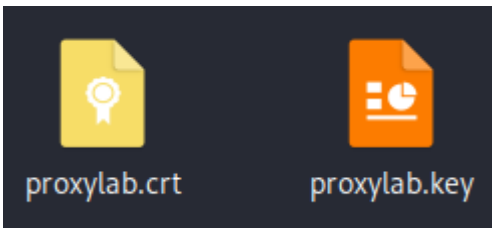
6. Contenu des certificats

Certificat d'autorité



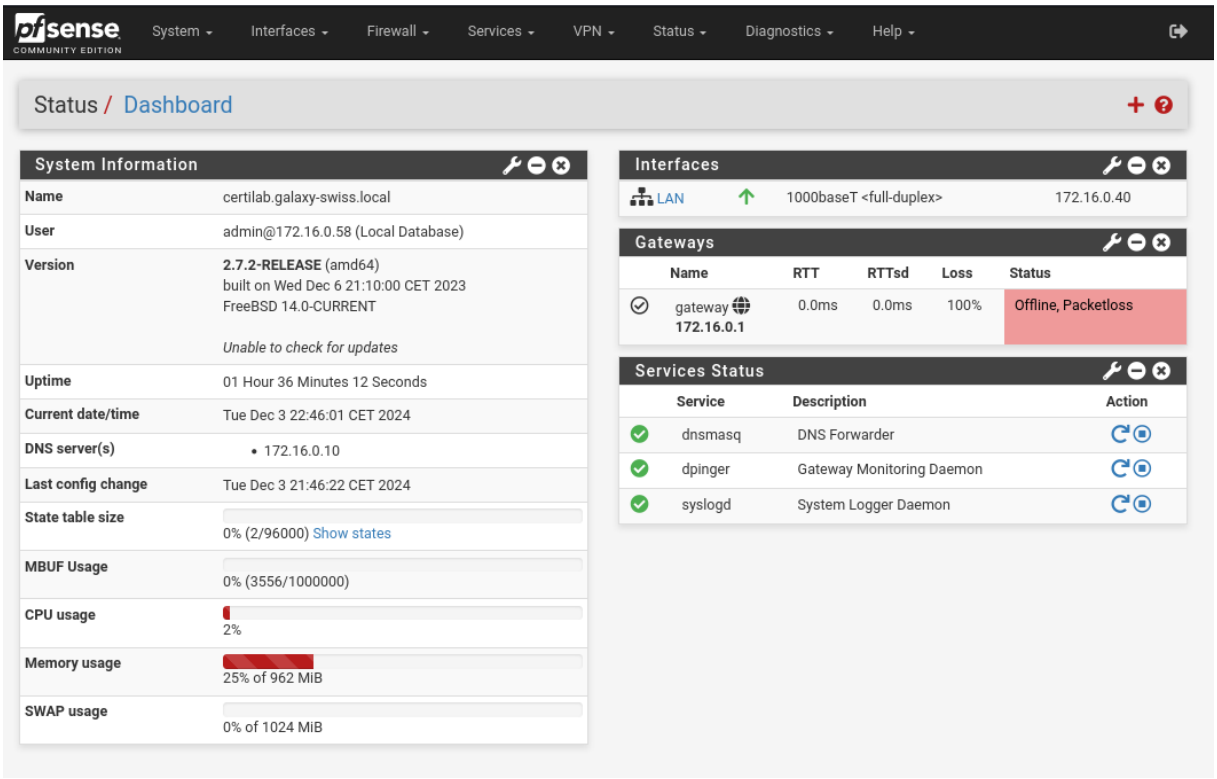
Certificats Serveurs



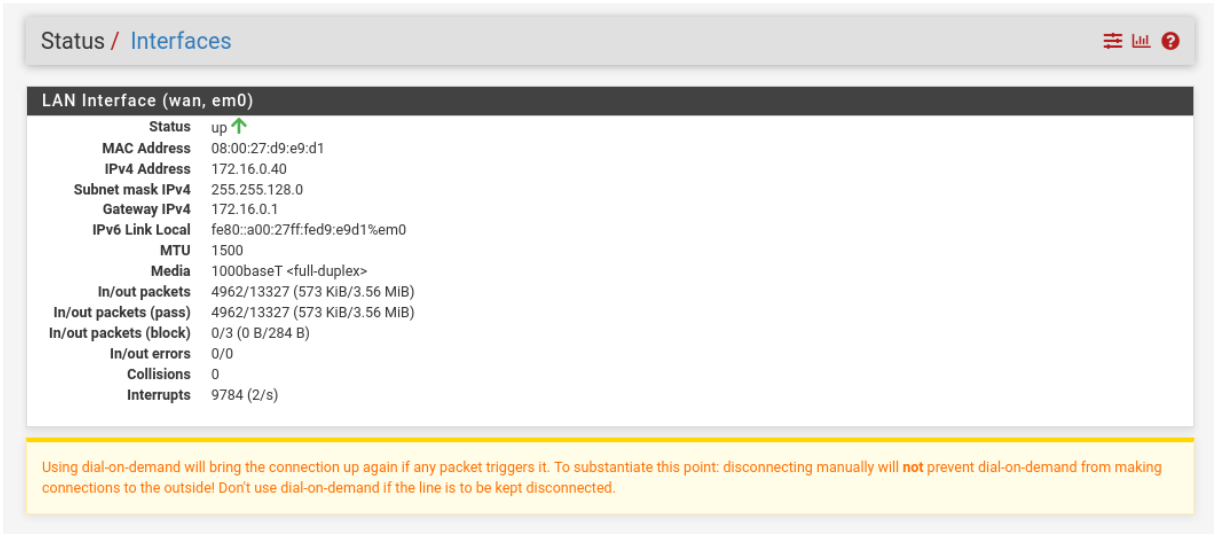


4. Dossier Technique de Configuration de Certilab

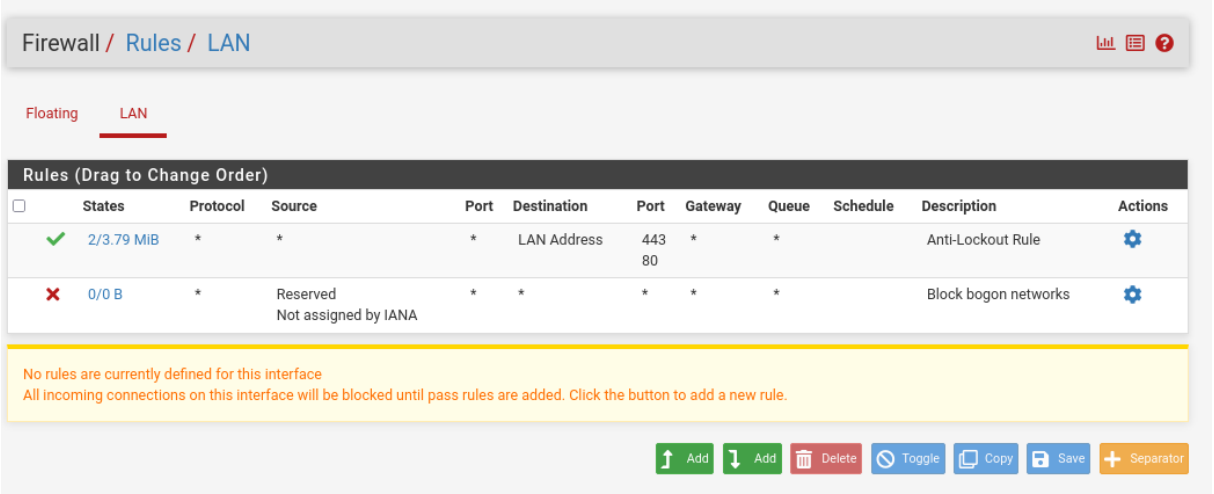
Screenshot Dashboard :



Screenshot Status Interfaces :



Screenshot Firewall/rules :



Screenshot Routing-Table :