PROXY

-

PFSENSE

Installation et configuration

TANET Margaux

CPI 2024-2025

Table des matières

Introduction :

Dans ce document, nous verrons comment configurer un SquidGuard sur PfSense pour permettre à notre proxy Squid d'effectuer du filtrage de sites Web basé sur des catégories via une blacklist. Nous verrons donc comment configurer Squid en proxy transparent avec filtrage SSL, comment créer un CA et configurer LightSquid afin de superviser nos connexions.

- **Qu'est-ce que Squid ?**

Squid est un proxy de cache pour le Web prenant en charge HTTP, HTTPS, FTP. Squid optimise le flux de données entre le client et le serveur pour améliorer les performances.

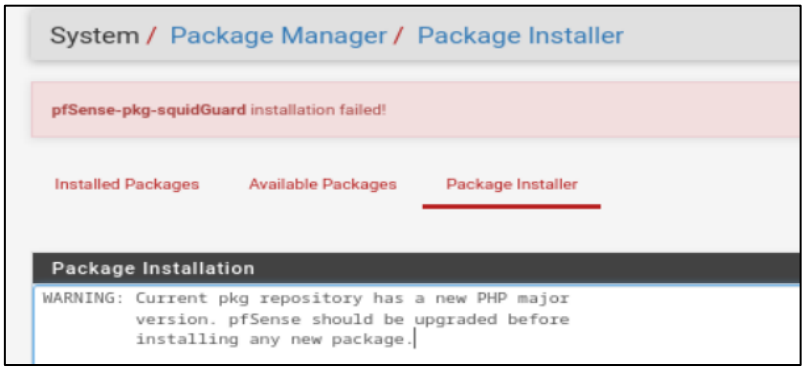
- **Qu'est-ce que SquidGuard**

SquidGuard est un logiciel de redirection d'URL, qui peut être utilisé pour le contrôle du contenu des sites Web auxquels les utilisateurs peuvent accéder. Il est écrit en tant que plug-in pour Squid et utilise des listes noires pour définir les sites pour lesquels l'accès est redirigé.

I- Configuration initiale

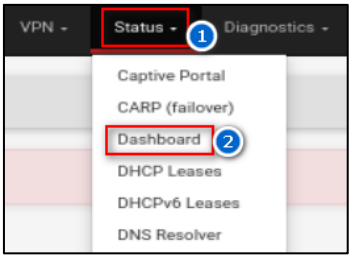
a) Mettre à jour PfSense

Pour l'installation des différents packages **Squid**, **SquidGuard** et **LightSquid** il faut mettre à jour **PfSense** sinon l'installation sera impossible :



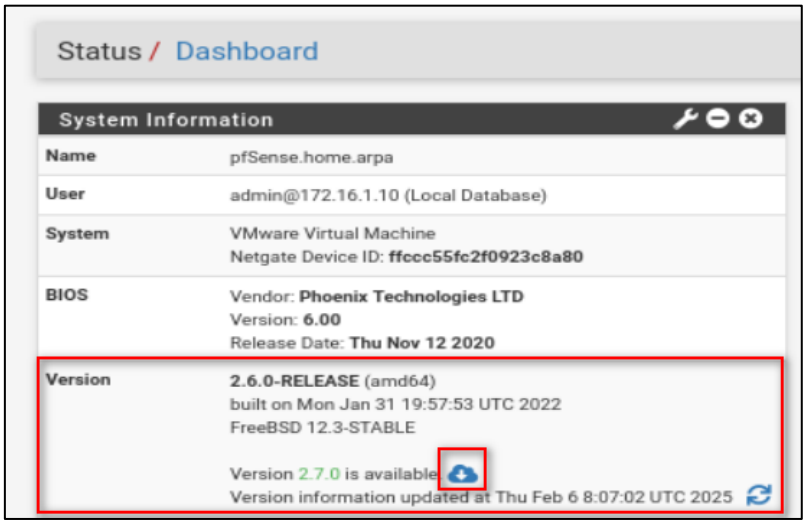
Avant la mise à jour, il faut penser à faire une snapshot de la VM et de désinstaller tous les packages additionnels.

- Se rendre dans **Status** puis **Dashboard :**

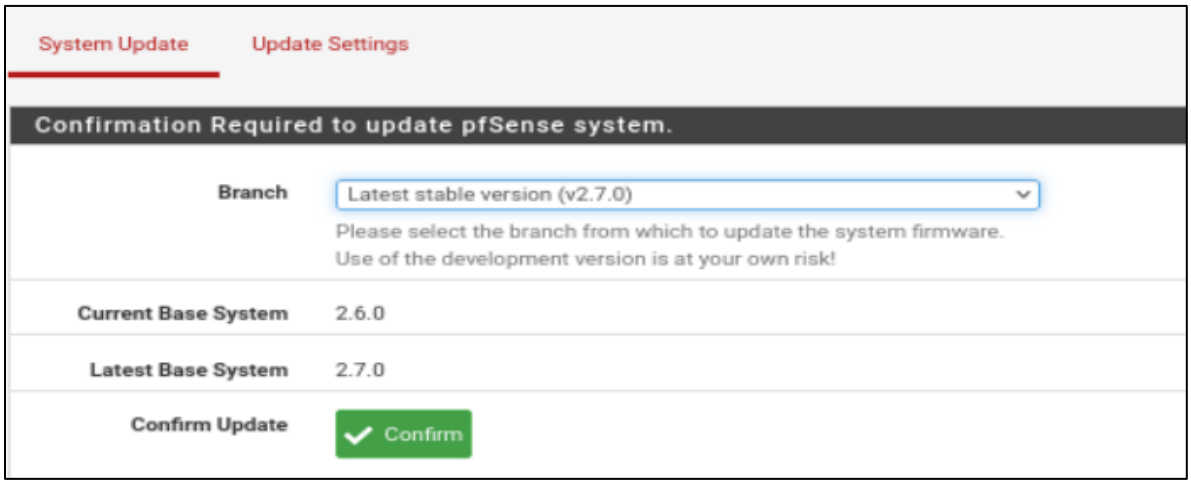


On voit que notre version est 2.6.0 et qu'une autre version 2.7.0 est disponible.

- Cliquer sur le nuage pour mettre à jour :

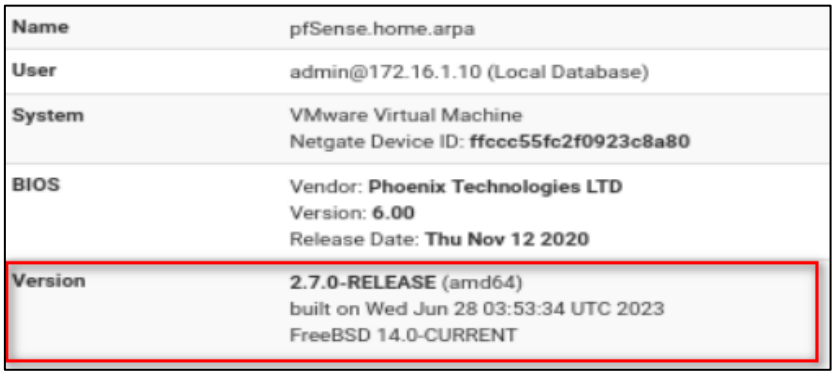


➢ Une nouvelle page s'affiche, nous confirmons l'installation de la mise à jour en cliquant sur le bouton "**Confirm**" :

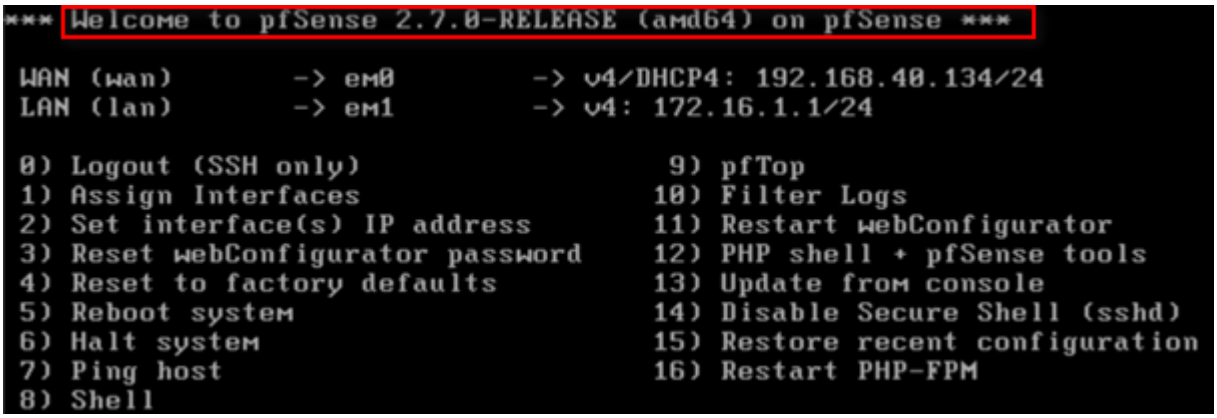


La mise à jour se lance :

L'installation est un peu longue. Au bout de quelques minutes, l'interface web et notre VM PfSense se relancent. On constate que sur mon interface web la mise à jour a bien été effectuée, nous sommes bien en 2.7.0 :



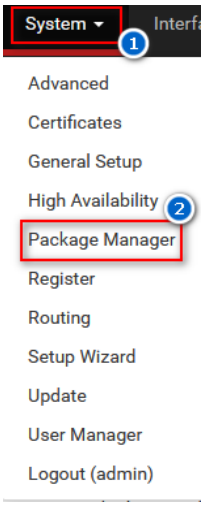
Si tout se passe bien, dans notre VM PfSense, lors du démarrage nous devrions avoir la version qui est affichée :



Tout s'est bien passé, j'ai mes différentes cartes qui sont remontées aussi nous pouvons continuer avec l'installation des packages.

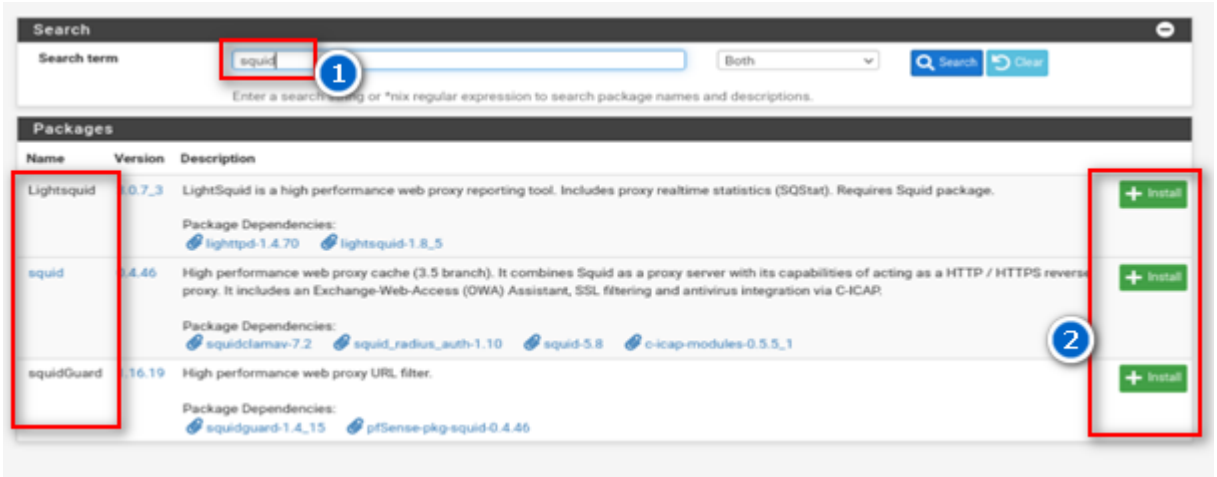
b) Installation des packages

Se rendre dans **System** puis **Package Manager** :

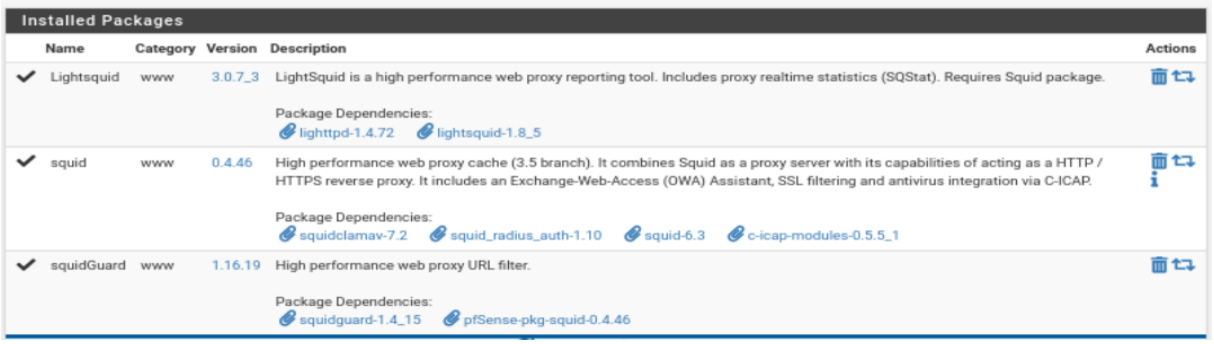


Puis dans **Available Packages** et saisir dans la barre de recherche « Squid » :

- Installer les différents packages **Squid**, **LightSquid** et **SquidGuard**.



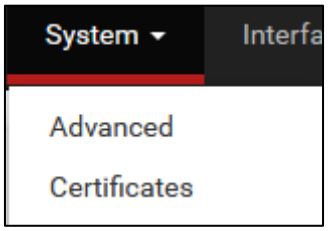
Les installations se sont bien faites :



II- Configuration de Squid en proxy transparent avec filtrage SSL

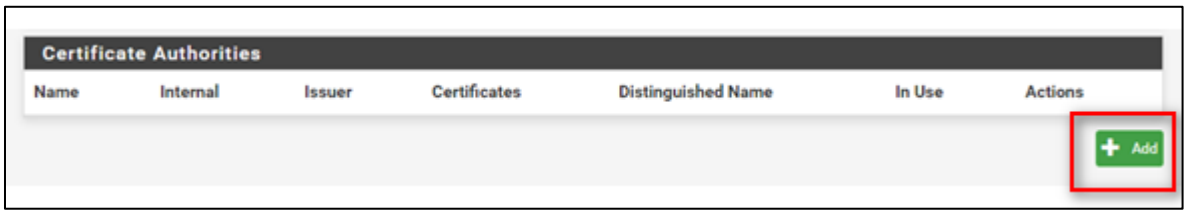
a) Générer le certificat

➢ Se rendre dans l'onglet **System** puis **Certificates** afin d'ouvrir le gestionnaire de certificats :

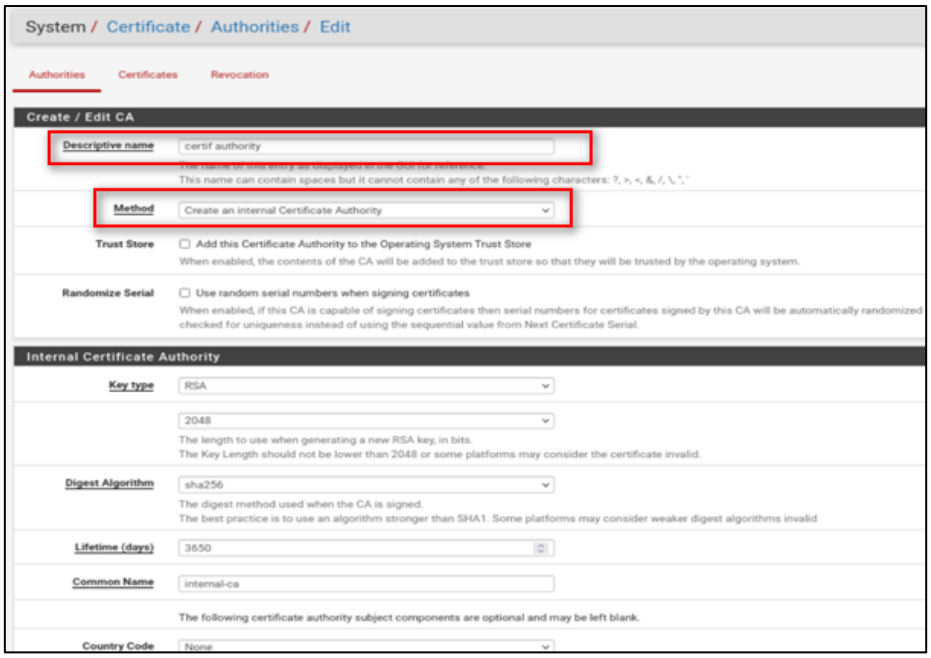


Nous allons créer une autorité de certification qui nous permettra ensuite de générer un certificat. Ce certificat sera distribué sur le client afin de rendre le proxy transparent.

➢ Dans l'onglet **Authorities**, cliquer sur le bouton « **Add** » :



➢ Ici, je remplis le nom de l'autorité de certification et j'indique que je veux créer une autorité de certification en sélectionnant **create an internal certificate authority** :

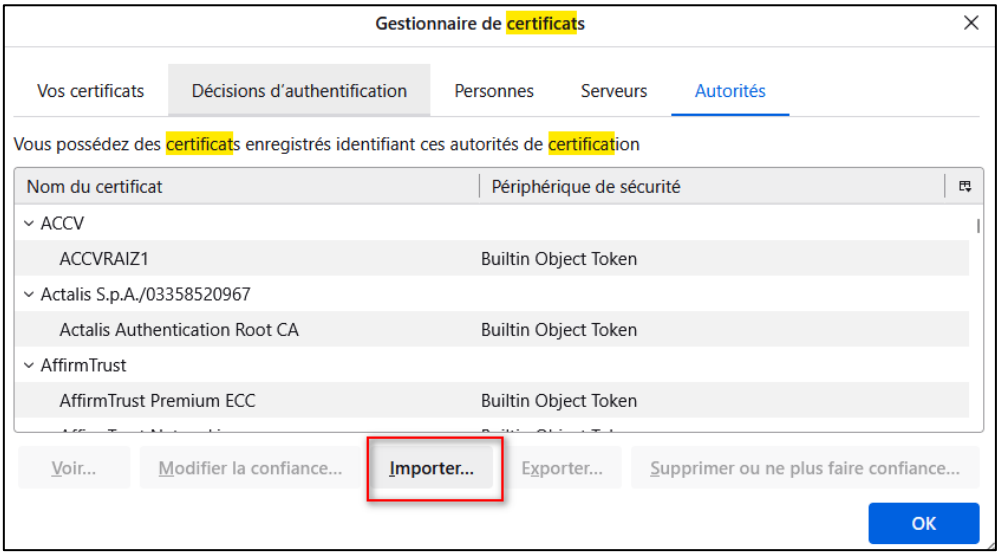


Mon autorité de certification est créée :

- Cliquer sur l'étoile pour exporter le certificat.

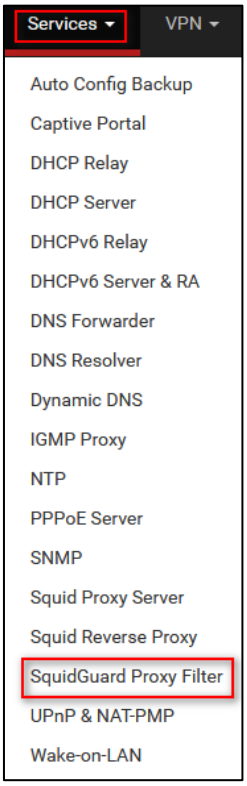
Le téléchargement se fait nous avons notre certificat :

- Se rendre dans les paramètres de notre navigateur et rechercher notre **gestionnaire de certificats**. Cliquer sur importer et injecter le certificat.

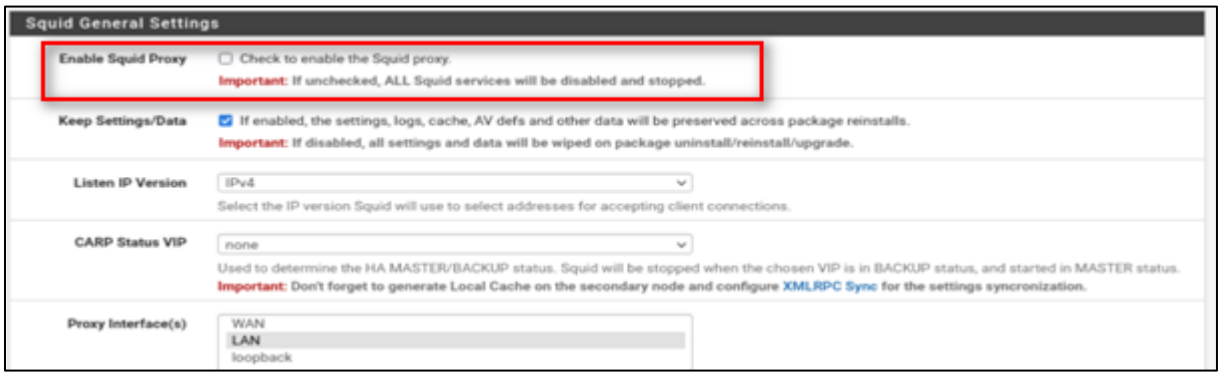


b) Configuration de Squid

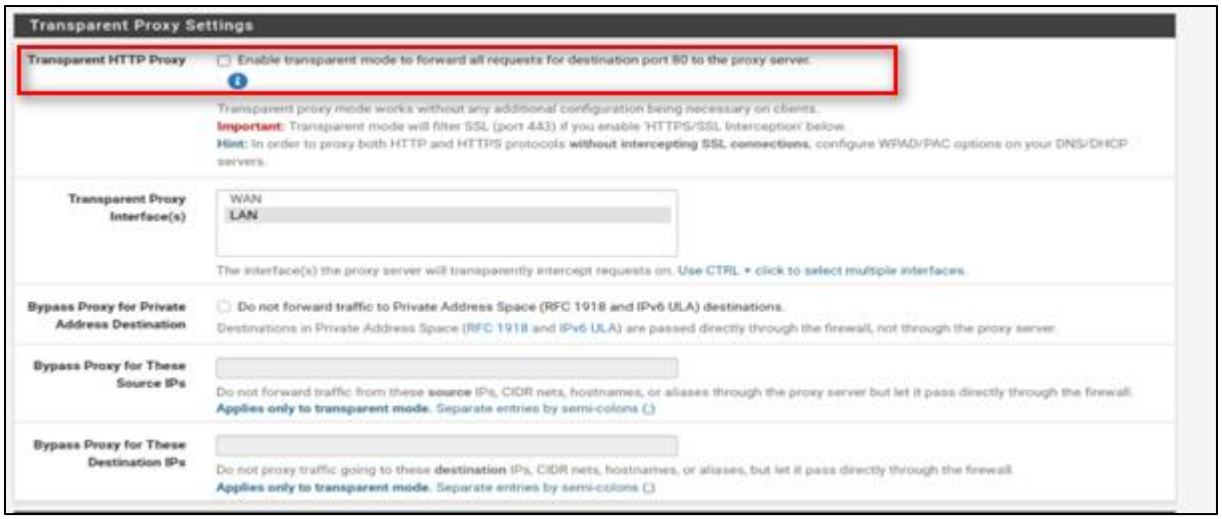
➢ Se rendre dans **Services** puis **Squid Proxy Server** :



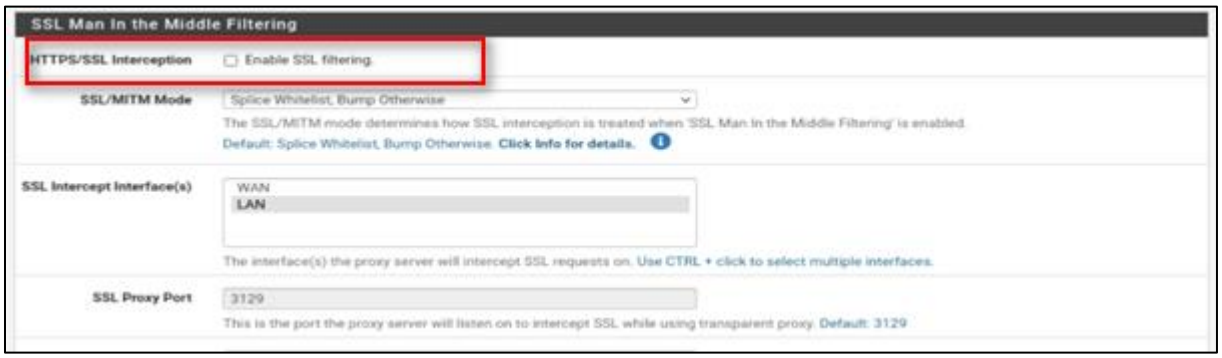
➢ Sur la page générale de cet onglet, il faut cocher, dans la rubrique **Squid général Settings** : Enable Squid Proxy :



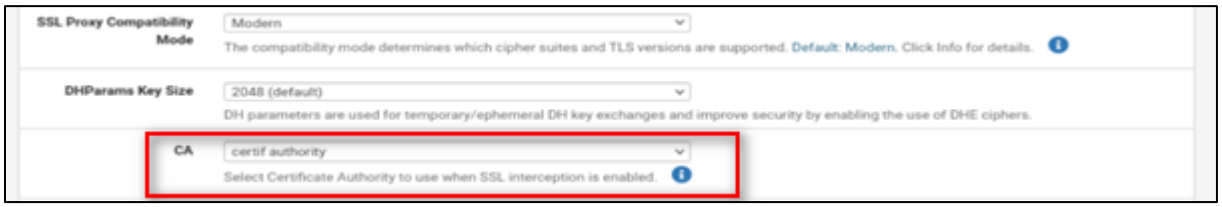
➢ Dans la rubrique **Transparent Proxy Settings,** cocher **Transparent http Proxy** :



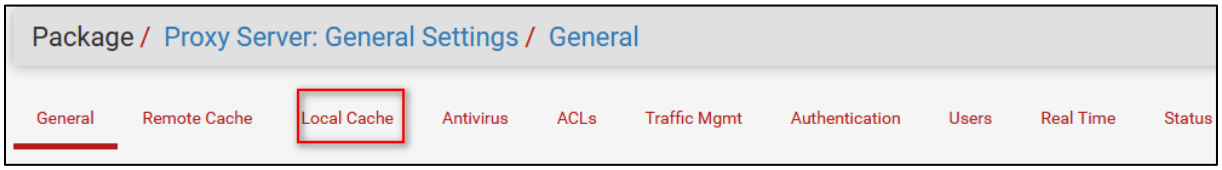
- Dans la rubrique **SSL Man in the Middle Filtering** cocher la case pour HTTPS/SSL Interception :



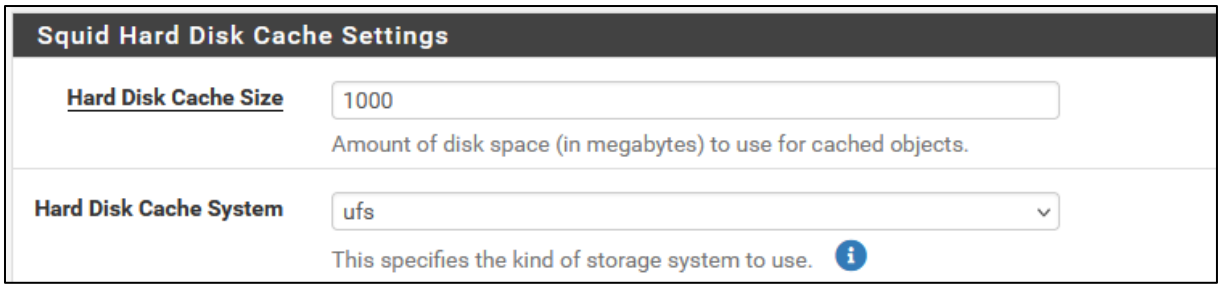
- Enfin dans la rubrique **CA,** mettre l'autorité de certification que nous avions créé précédemment :



- Cliquer sur **save** pour sauvegarder les paramètres.
- Toujours dans l'onglet **Squid Server Proxy**, aller dans la rubrique **Local Cache** pour définir la taille qui sera dédiée au cache pour éviter les erreurs par la suite :



- Pour **Hard Disk Cache Size,** changer la taille du cache :

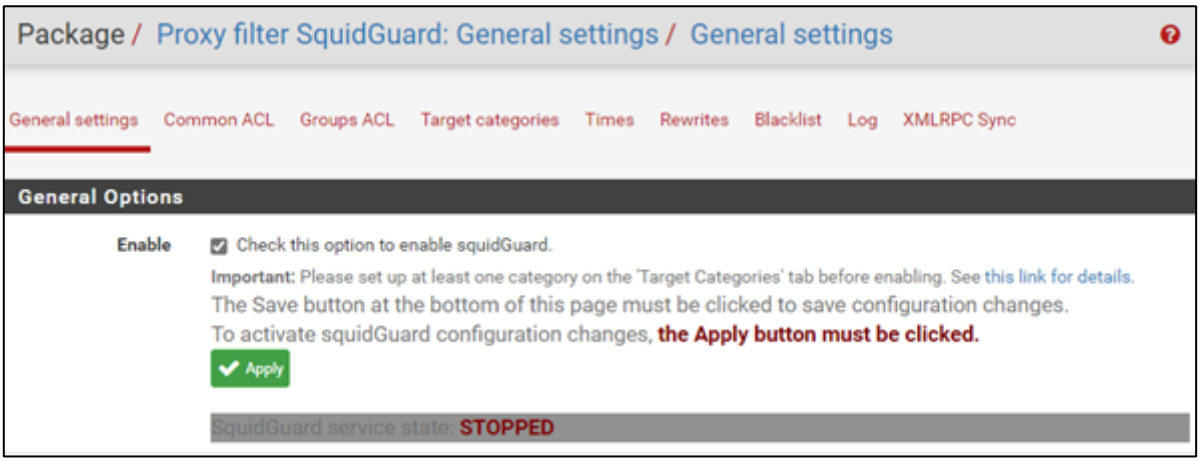


Sauvegarder les paramètres réalisés.

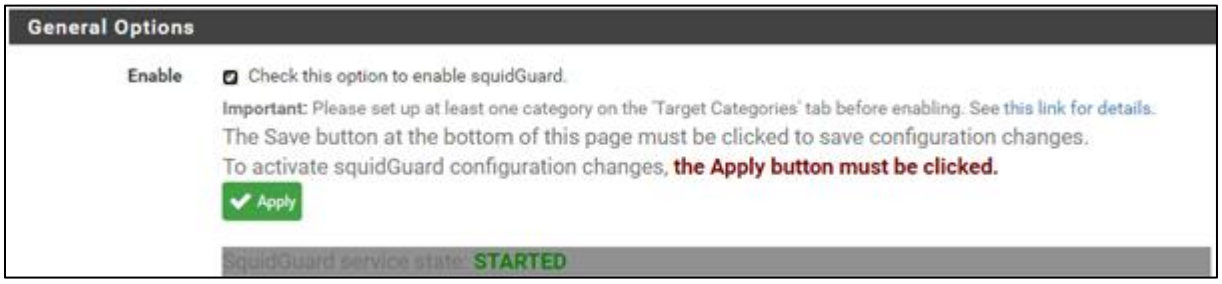
III- Configuration de SquidGuard Proxy Filter

➢ Se rendre dans **Service** puis **SquidGuard Proxy Filter** :

➢ Dans **General Settings,** cocher la case **check this option to enable SquiGuard** et cliquer sur **Apply** pour démarrer le service :

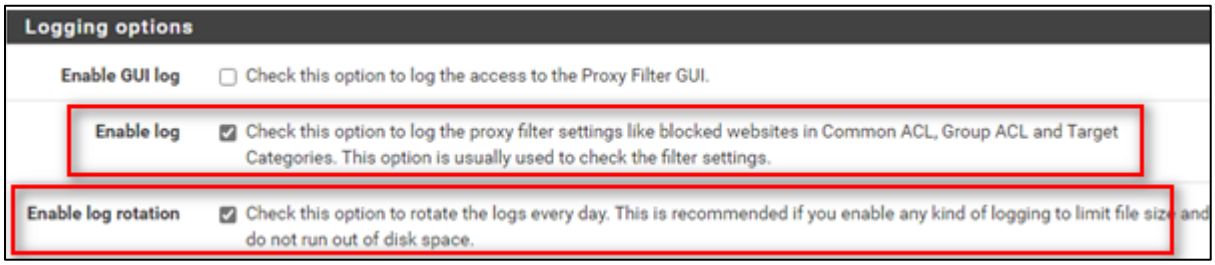


Le service démarre :



Ne pas oublier de toujours faire **Apply** et **Save** après toutes modifications.

- Plus bas, cocher les cases **Enable log** et **enable log rotation** pour pouvoir suivre les évènements sur le proxy :

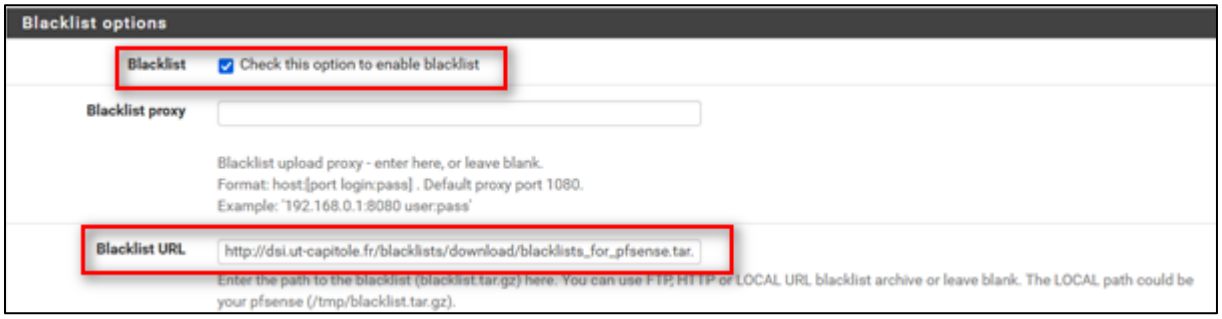


a) Mise en place du filtrage

Nous allons mettre en place une blacklist afin de bloquer la catégorie **social media** pour que l'utilisateur n'est pas accès à facebook.

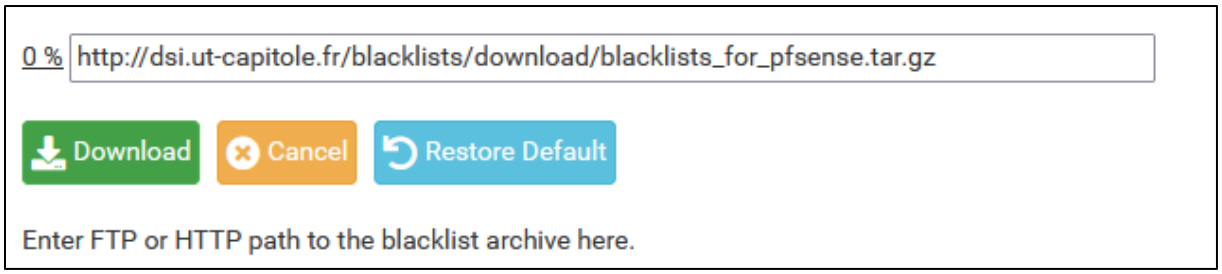
- Pour cela, toujours dans **Proxy filter SquidGuard** les paramètres généraux, cocher la case **Blacklist** et renseigner la liste de l'université de Toulouse dans la ligne **Blacklist URL :**

URL de l'université de Toulouse : http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz



Sauvegarder les paramètres.

- Se rendre sur l'onglet **Blacklist**, renseigner l'URL utilisé précédemment. Cliquer sur le bouton **Download** pour que les filtres se téléchargent :



- Se rendre dans l'onglet **Common ACL** et cliquer sur « +/- » pour dérouler le menu.
- Une liste apparaît, il faut trouver la ligne social network. Au bout de la lgine, renseigner accès **Deny** pour bloquer l'accès :

Laisser par défaut **Allow** :

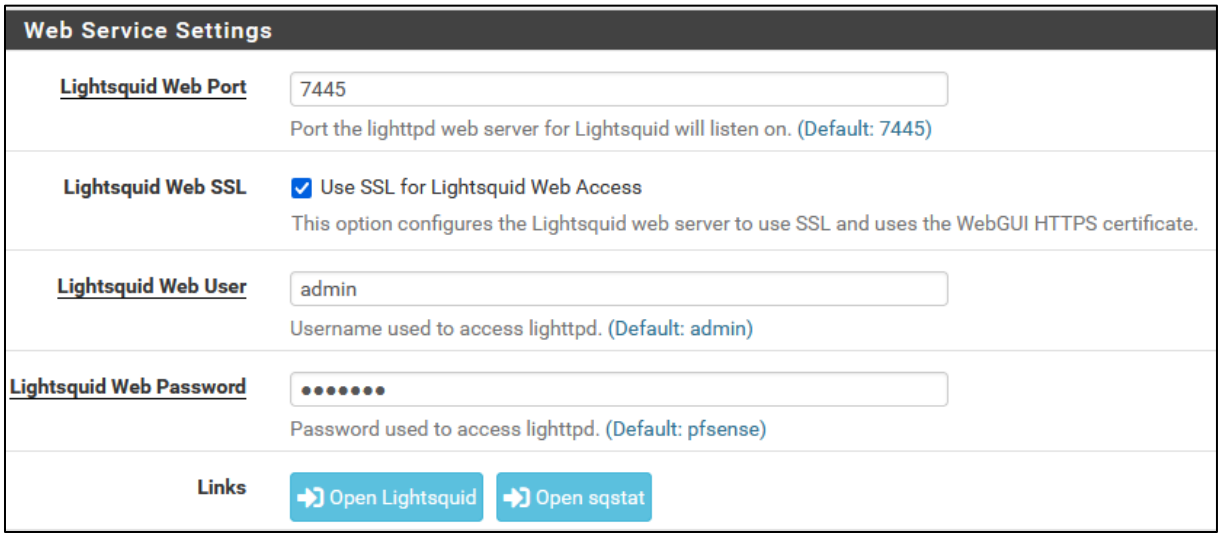
- Cocher **Do not allow IP addresses in URL** pour empêcher les utilisateurs de contourner le filtrage dans le cas où ils utiliseraient leur adresse IP au lieu de leur nom de domaine pour l'accès au site.

- Retourner sur **General Settings** pour enregistrer les modifications en faisant **Apply** et **Save**.

IV- Configuration LightSquid

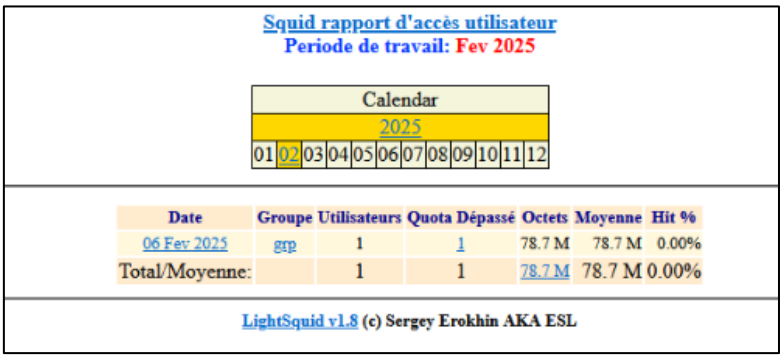
➢ Se rendre dans l'onglet **Status** et cliquer sur **Squid Proxy Reports** :

Ici on peut changer nos identifiants de connexions et valider les changements :



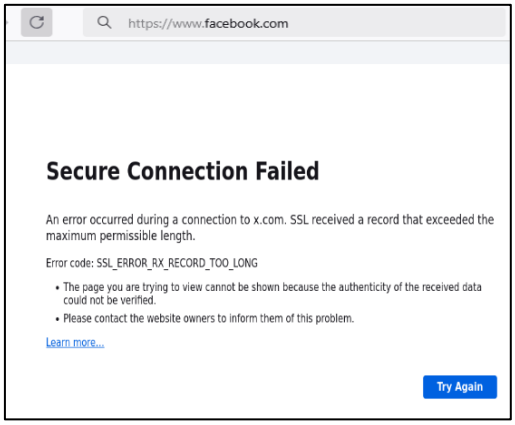
V- Tests

➢ Cliquer sur **Open Lightsquid**, une page s'ouvre contenant des informations.



Je n'ai pas réussi à accéder à l'adresse http://172.16.1.1:7445 pour voir les informations sur les logs.

Testons de se connecter à facebook, normalement avec le filtrage on ne devrait pas accéder au site :



La requête pour facebook a bien été bloquée.

VI- Conclusion

Nous avons mis en place Squid en proxy transparent et activer le filtrage SLL en passant par la création de notre CA. Nous avons importé la blacklist de l'université de Toulouse pour bloquer la catégorie « social media » en testant une connexion sur Facebook. Nous avons vu que notre filtrage a fonctionné, nous n'avions pas d'accès à Facebook. Nous avons mis en place LightSquid afin de voir les connexions qui se faisaient.