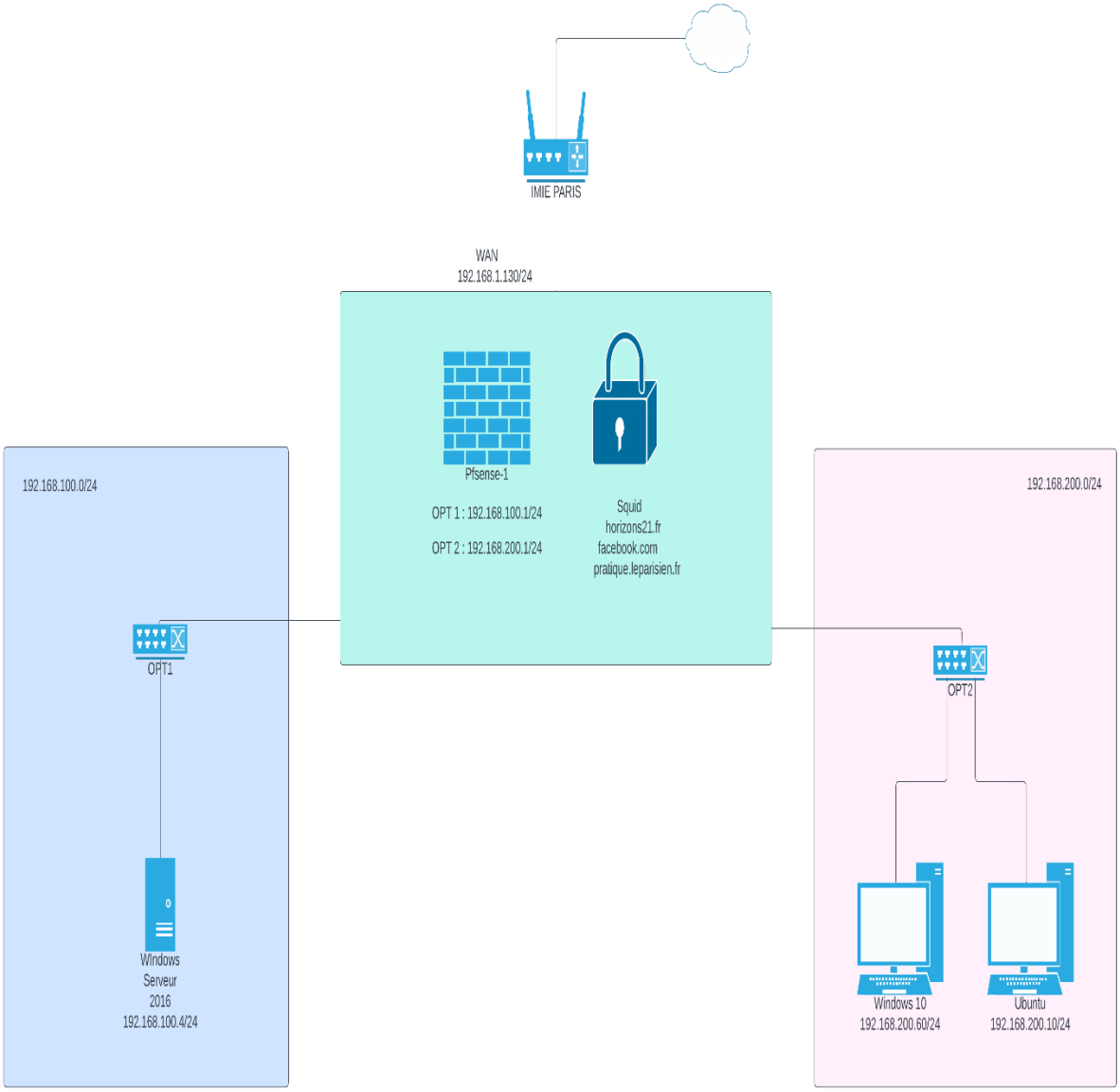
PROJET PERSONNEL ENCADRE n°1

MISE EN PLACE DE SQUID, SQUIDGUARD, LIGHTSQUID SUR PFSENSE

Abdoul-Aziz MANE

Schéma de l’infrastructure réseau



Abdoul-Aziz MANE

PPE n°1 : Mise en place de Squid sur Pfsense

Introduction :

Squid est un serveur proxy open-source populaire qui est couramment utilisé pour le cache et la filtration web.

Fonctionnement de SQUID

Lorsque Squid est installé sur pfSense, il peut être utilisé pour améliorer les performances de navigation web en mettant en cache le contenu web fréquemment consulté. Cela peut réduire la quantité de bande passante utilisée par les clients sur le réseau et accélérer les temps de chargement des pages. De plus, Squid peut être configuré pour bloquer l'accès à certains sites web ou catégories de contenu, offrant ainsi une couche supplémentaire de filtrage et de sécurité web.

Installation de SQUID

L'installation de Squid sur pfSense implique la configuration du paquet Squid dans l'interface de gestion basée sur le web de pfSense. Une fois installé, Squid peut être configuré pour répondre aux besoins spécifiques du réseau, notamment en définissant le contenu à mettre en cache et pendant combien de temps le conserver, en configurant les contrôles d'accès et les restrictions, ainsi qu'en configurant les journaux et la surveillance.

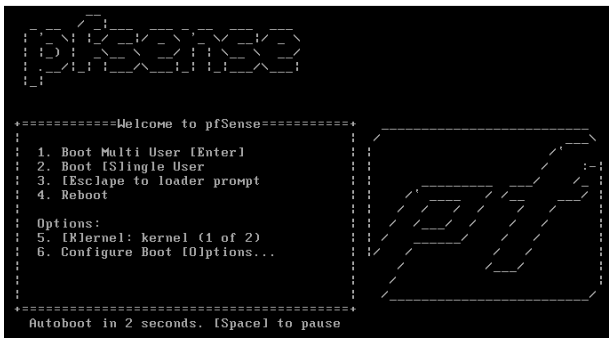
Avantages de SQUID

Dans l'ensemble, l'utilisation de Squid avec pfSense peut fournir des avantages significatifs pour les réseaux en termes de performances, de sécurité et de contrôle sur le contenu web.

Abdoul-Aziz MANE

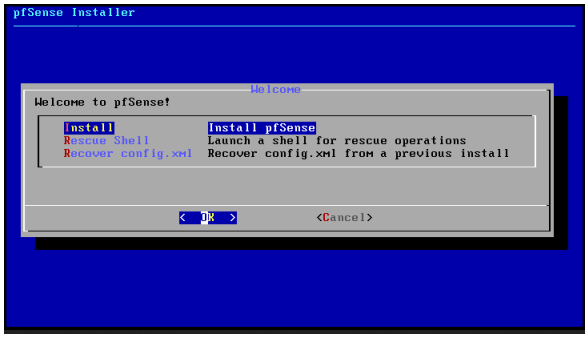
Taches à effectuer :

1) Commençons tout de suite par **installer pfsense**. Après avoir insérer l'ISO de pfsense dans VM dédiée, vous pouvez démarrer la machine. Le setup va démarrer automatiquement après quelques secondes.

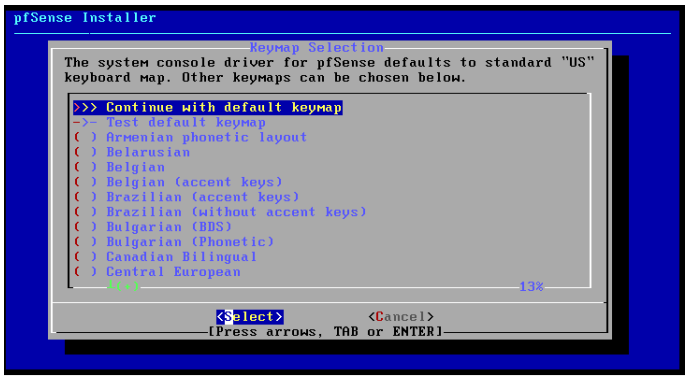


2) **L'installation va s'effectuer au clavier.** Appuyez sur la touche **Entrée pour Accepter**.

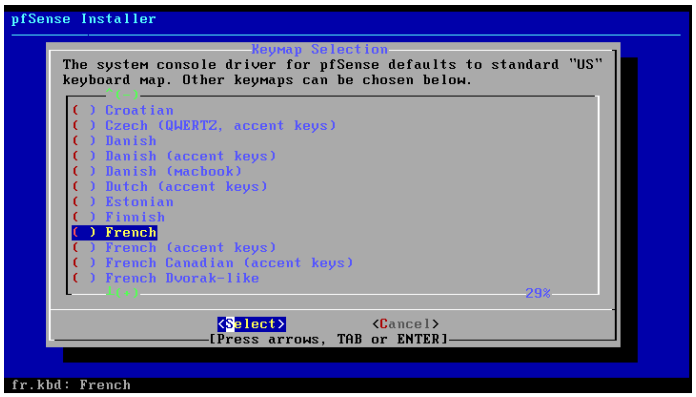
3) Vérifiez que vous êtes bien sur « **Install** » *(doit être sélectionné en bleu foncé comme dans l'image ci-dessous, sinon déplacez-vous avec les flèches de votre clavier)* et appuyez sur **Entrée pour faire OK**.



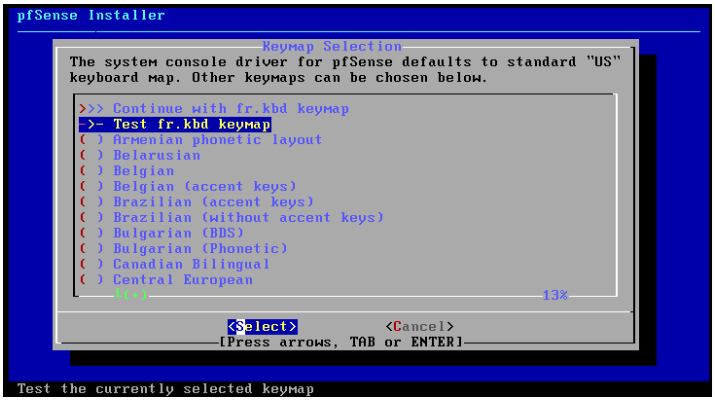
4) Il faut **sélectionner le clavier**



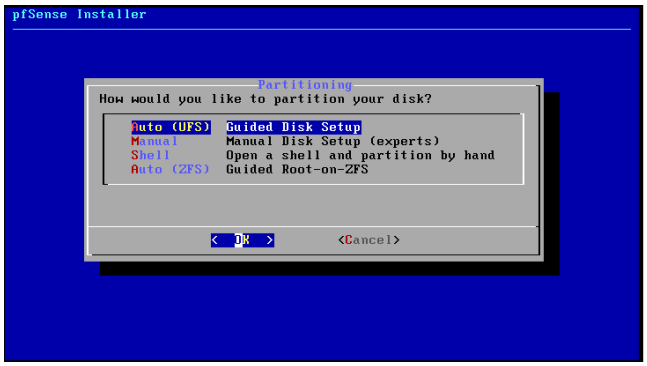
5) **Descendez avec les flèches** jusqu'à « French » et appuyez sur **Entrée.**



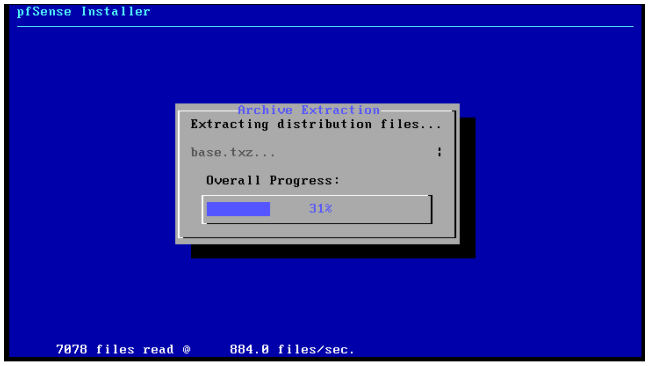
6) Vous verrez dans les 2 premières lignes que le clavier « **fr.kdb** » a été sélectionné. Vous pouvez le tester si besoin. Pour poursuivre, remontée sur la ligne « **Continue with…** » et appuyez sur Entrée.



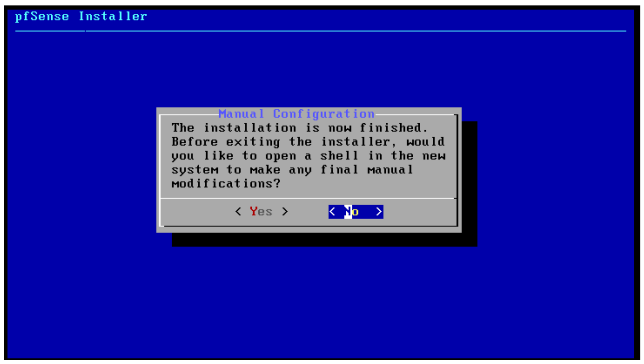
7) Le setup va vous demander de **partitionner le disque** de stockage de la machine. Sauf si vous avez besoin d'une configuration bien spécifique, **restez sur « Auto (UFS) » et appuyez sur Entrée**.



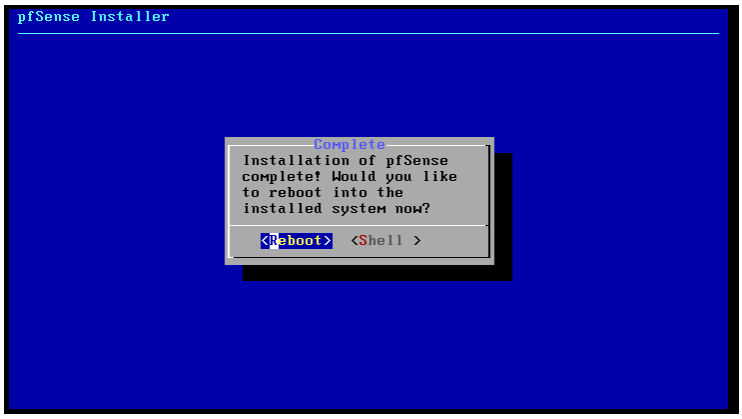
8) L'installation est désormais lancée. **Patientez quelques secondes**, c'est très rapide.



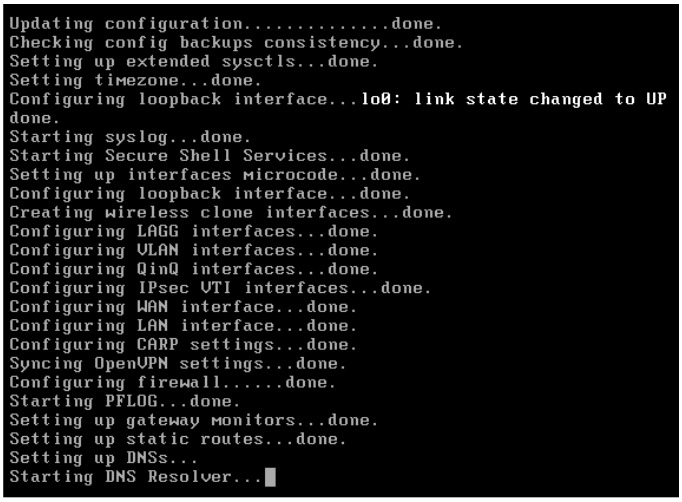
9) Il vous sera ensuite proposer d'ouvrir un shell *(terminal)* si vous souhaitez apporter des modifications. Passez sur la case « **No** » et appuyez sur **Entrée.**



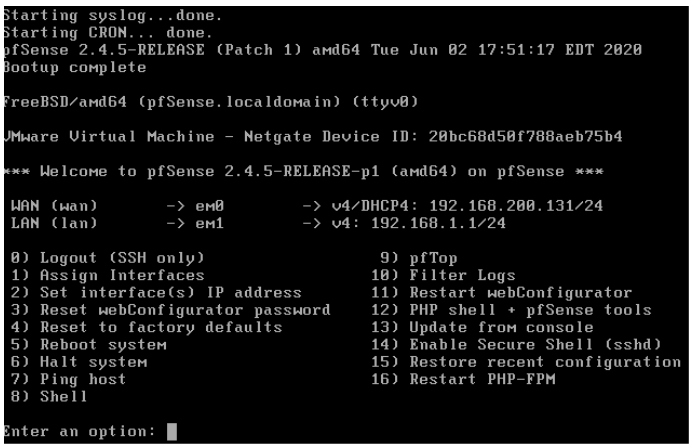
10) Et pour terminer cette installation du système, **appuyez une dernière fois sur Entrée pour rebooter et démarrer directement sur le nouveau pfsense** fraîchement mis en place ;



11) Au démarrage, **pfsense va se lancer, tester et configurer les services dont il a besoin**. Par exemples dans l'image ci-dessous, on peut voir que pfsense à tester la présence de l'interface WAN *(ligne Configuring WAN interface…done.)* et l'a configuré, idem pour l'interface LAN. Il a également lancé le service DNs pour la résolution de nom de domaine *(ligne Configuring DNS Resolver…).*

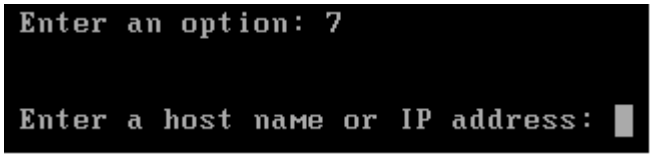


12) Une fois que le démarrage est finalisé, vous aurez la vue suivante sur la machine :



13) On voit bien nos **deux interfaces réseaux** *(WAN et LAN)*. On voit également que **l'interface WAN a bien récupéré une adresse IP automatiquement depuis un DHCP** *(ce qui correspond à l'adresse IP publique)*. Nous devons aussi modifier l'adresse IP du WAN et la définir en statique. Concernant le LAN, il attribue une adresse statique par défaut que nous allons changer.

Vous avez **16 menus** qui vont permettre de faire différentes **actions et configurations**. Pour les utiliser, il faut **saisir leur numéro et appuyez sur Entrée.** Testons ensemble avec le menu **ping**. Saisissez au clavier le **chiffre 7** puis la touche **Entrée.**



Lançons un ping vers google.fr pour tester l'accès à internet et le bon fonctionnement de la résolution de nom.

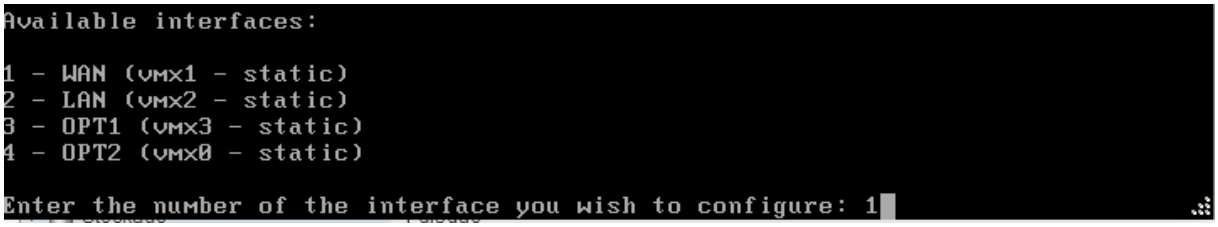
Info ++ : Attention, malgré la configuration du clavier en français, celui-ci se retrouve par défaut en qwerty ! Pour saisir le point, il faut appuyez sur la touche « / ».

Vous pouvez **arrêter le ping** en appuyant **simultanément sur les touches Ctrl et C**. On voit que le ping passe sans problème, l'interface WAN est donc fonctionnelle.

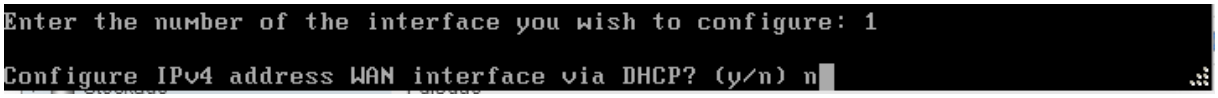
Nous avons une dernière petite chose à faire avant de passer sur l'interface web de Pfsense pour la configuration finale. Il faut **assigner la bonne adresse IP à l'interface WAN**, c'est-à-dire celle qui correspond à notre réseau externe *(pour moi dans le cadre de ce tuto, 192.168.1.130).*

Pour cela, au choix des menus, **tapez 2 puis Entrée**.

On me demande **quelle interface je veux modifier**. L'interface WAN est ici vmx1, donc je tape 1 et j'appuie sur Entrée.



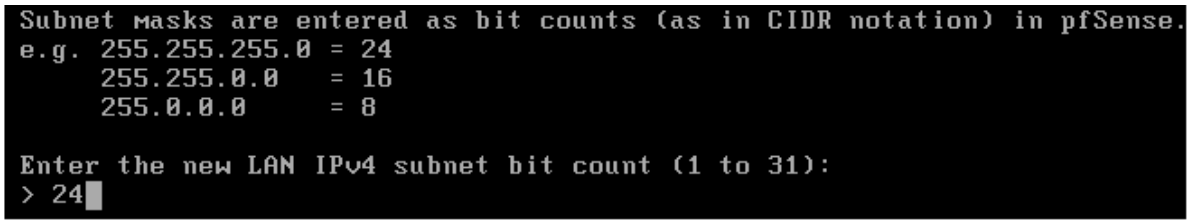
Dans mon cas, je ne mets pas de DHCP sur le WAN alors j'appuie sur N :



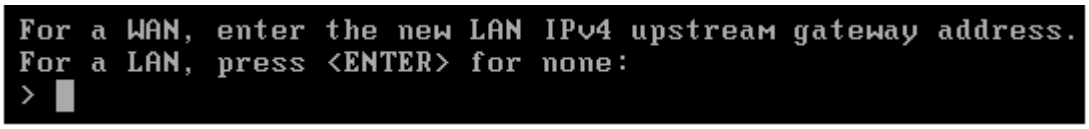
<u>Info +</u> : le service DHCP peut être activé et configuré plus simplement par la suite via l'interface web.

Ensuite **saisissez l'adresse IP que vous donnez à cette interface**

Définissez le masque de sous-réseau du réseau local **en notation CIDR uniquement**, donc 24 pour moi.



Pfsense demande ensuite si le réseau dispose d'une passerelle vers laquelle renvoyer les flux. Pour mon cas l'interface WAN doit avoir comme Gateway 192.168.1.1 (l'adresse du routeur de l'école)



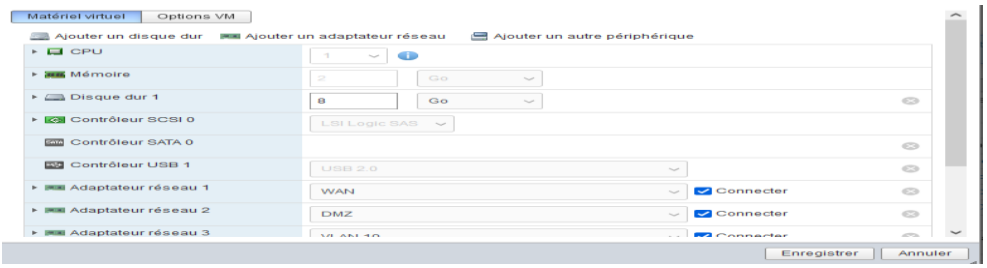
Répéter la même opération pour le LAN en lui mettant comme adresse ip 192.168.2.1/24

On n'active pas le dhcp sur le LAN

Et enfin, la dernière question concerne le **protocole utilisé pour aller sur l'interface web**. Par défaut, il est en **HTTPS** donc sécurisé. Vous pouvez choisir de le passer en HTTP si vous le souhaitez en répondant « y » pour « Yes ». Personnellement je vais répondre « n ».

```
Disabling IPv4 DHCPD...Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n)
```

14) Ajouter des cartes réseaux qui se nommeront OPT1 et OPT2.



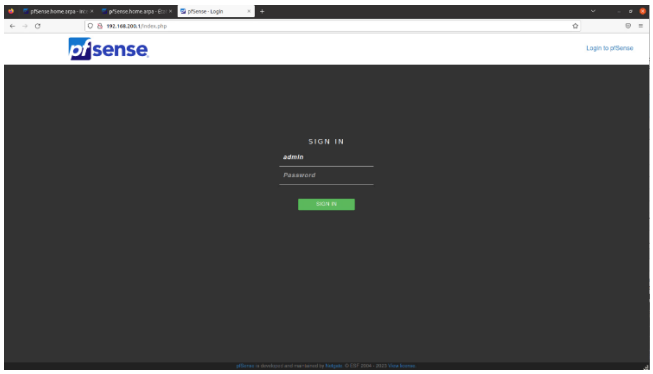
Faire la même configuration pour OPT1, en lui mettant comme adresse 192.168.100.1 et pareil pour OPT2 avec comme adresse 192.168.200.1 et OPT3 10.1.10.2/24 ce qui doit donner ça à la fin :

```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 596128dfe071b09d8ce5

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vmx1       -> v4: 192.168.1.130/24
 LAN (lan)       -> vmx3       -> v4: 192.168.150.1/24
 OPT1 (opt1)     -> vmx4       -> v4: 192.168.100.1/24
 OPT2 (opt2)     -> vmx0       -> v4: 192.168.200.1/24
 SYNC (opt3)     -> vmx2       -> v4: 10.1.10.2/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Disable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

La configuration de l'interface LAN est terminée. Je vois à l'écran l'**URL à utiliser pour aller sur pfsense qui est donc ici https://192.168.150.1/**, soit son adresse IP.

La configuration de pfsense en **lignes de command**e est maintenant terminée, passons sur l'interface web.

Depuis un PC sur le réseau local disposant d'une adresse IP fixe si le DHCP n'est pas actif, **ouvrez un navigateur internet et accédez à votre pfsense.**

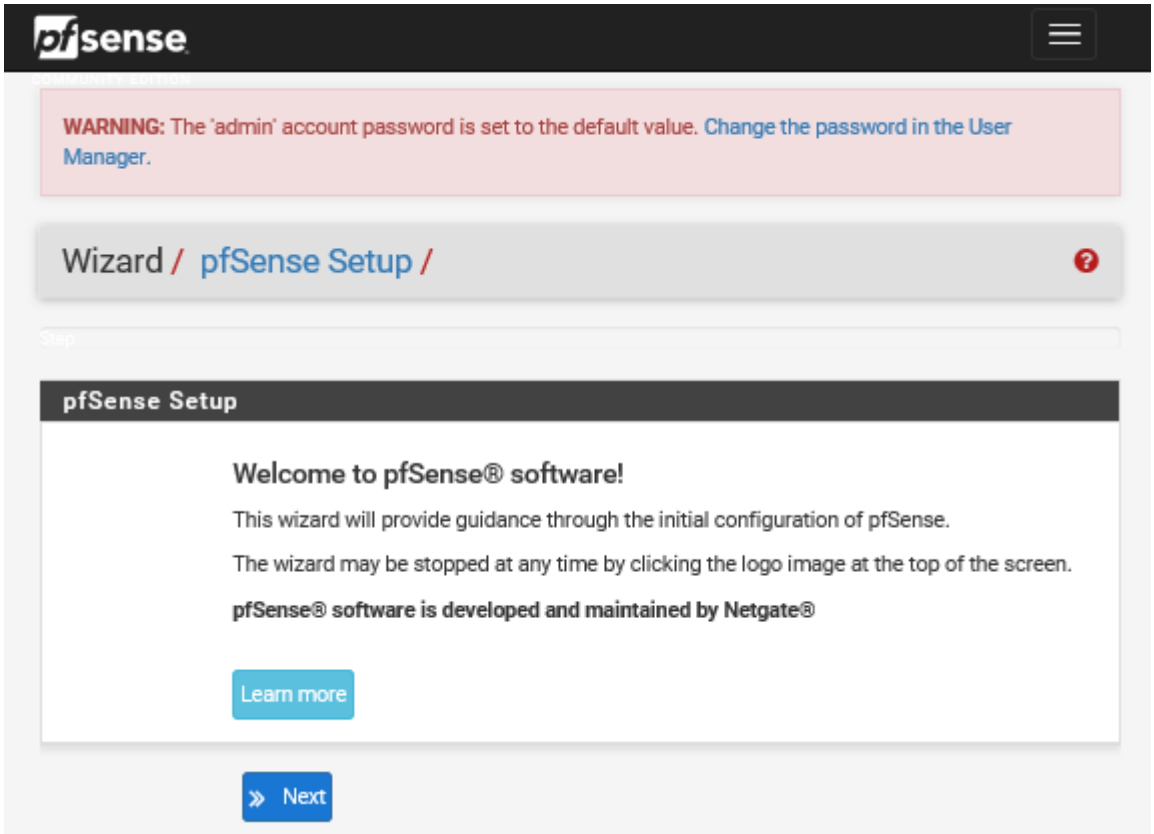


<u>Info ++</u> : Si vous avez laissé le protocole HTTPS, vous aurez une erreur de certificat qui est tout à fait normal. Le navigateur va vous prévenir qu'il y a un problème mais rien ne vous empêche de poursuivre votre navigation (méthode variable selon le navigateur) pour accéder à pfsense.

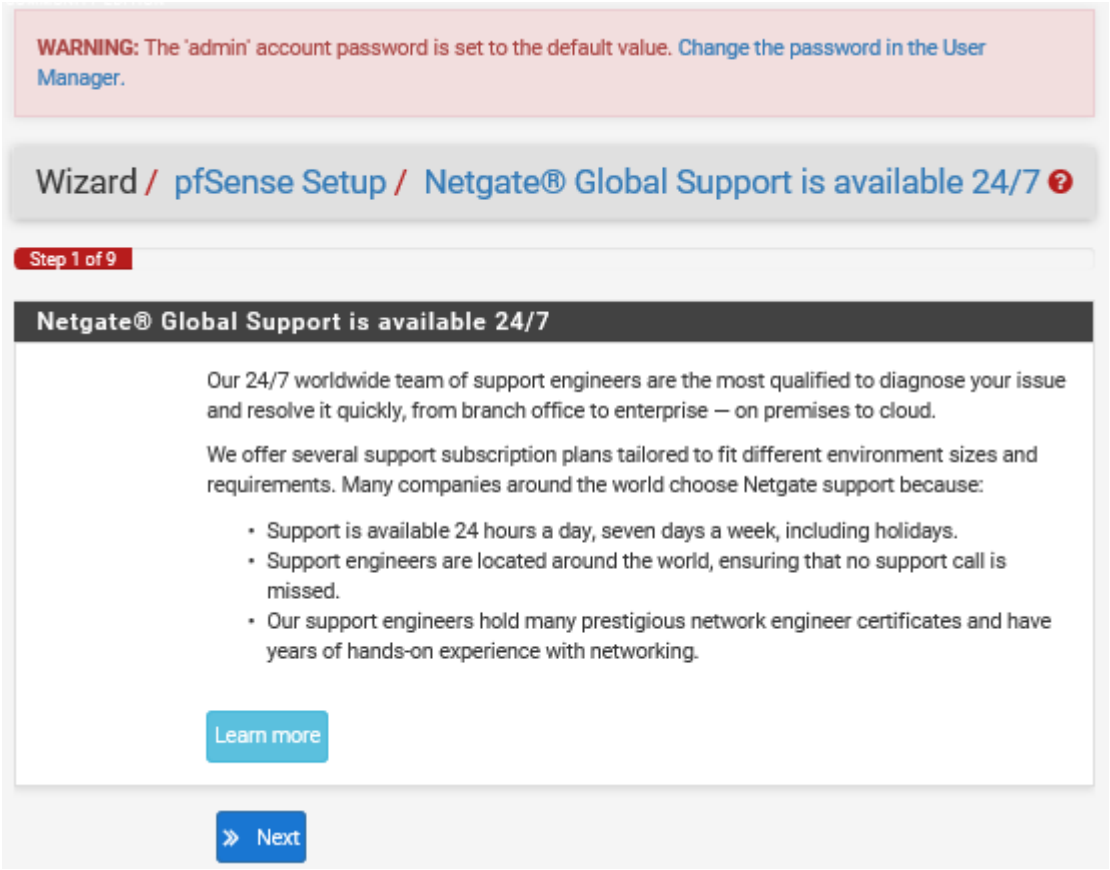
Les **identifiants par défaut de pfsense** sont les suivants :

-
  - **Login** : admin
  - **Mot de passe** : pfsense

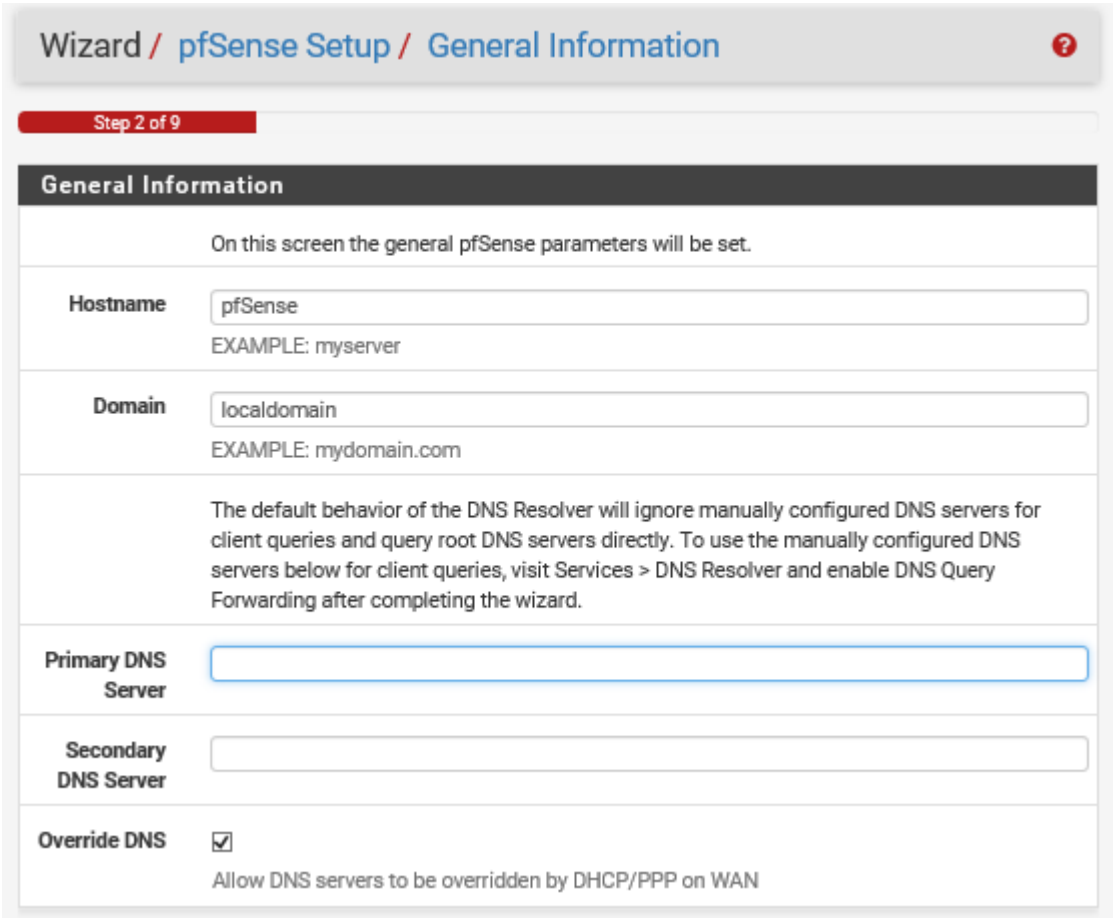
Vous arrivez sur l'**assistant de configuration** de pfsense qui va nous permettre de finaliser l'installation de notre firewall. Cliquez sur le bouton « **Next** ».



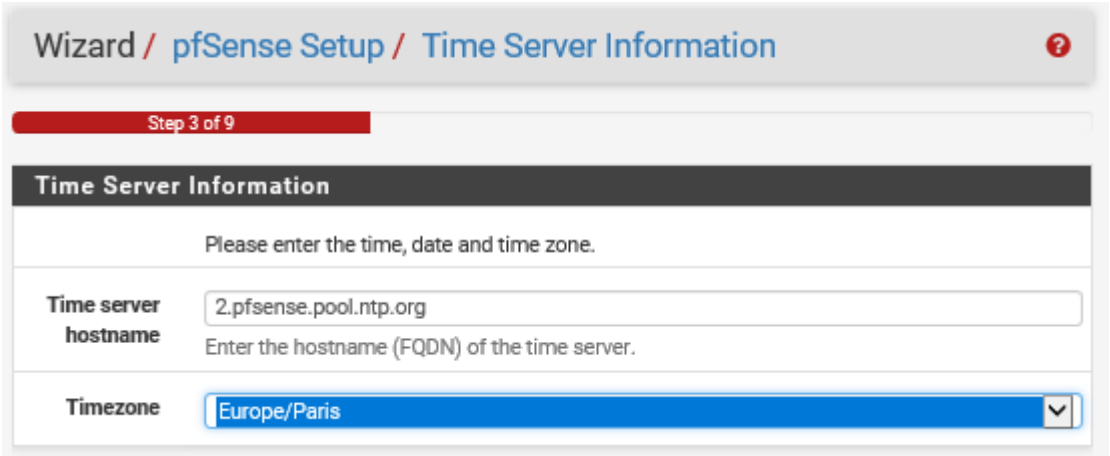
L’assistant nous informe qu’il est possible d’avoir un **support technique sous condition de souscrire un contrat**. Cliquez de nouveau sur **Next**.



Au niveau de la partie des **informations générales**, vous pouvez modifier le **nom du firewall** et déclarer votre **nom de domaine si vous en avez un** dans votre réseau. Ici également vous pouvez **déclarer un serveur DNS local** *(ce n’est pas mon cas, j’utile le DNS de mon AD pour ce tuto)*. Je ne modifie ici aucun champ.

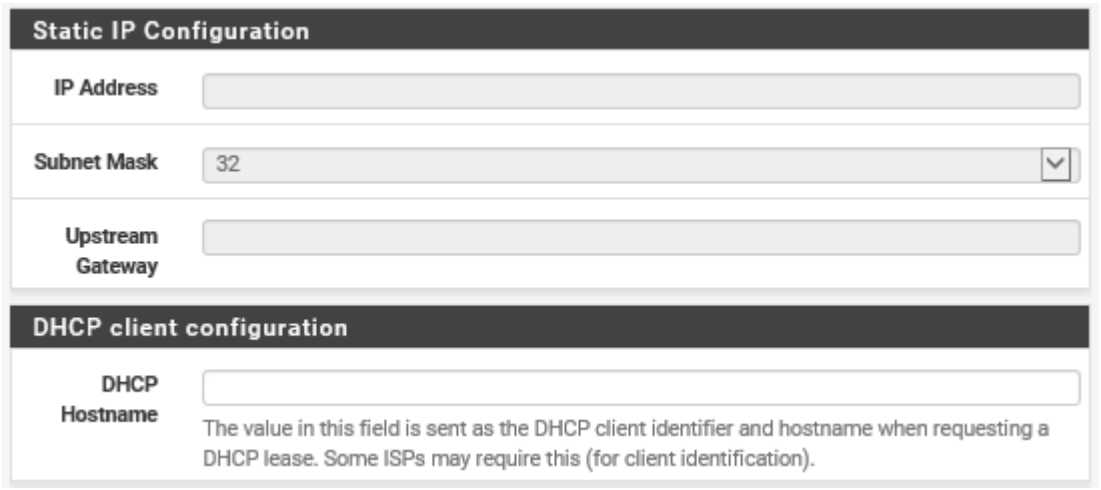


Choisissez « **Europe/Paris** » dans la **Timezone** et poursuivez.

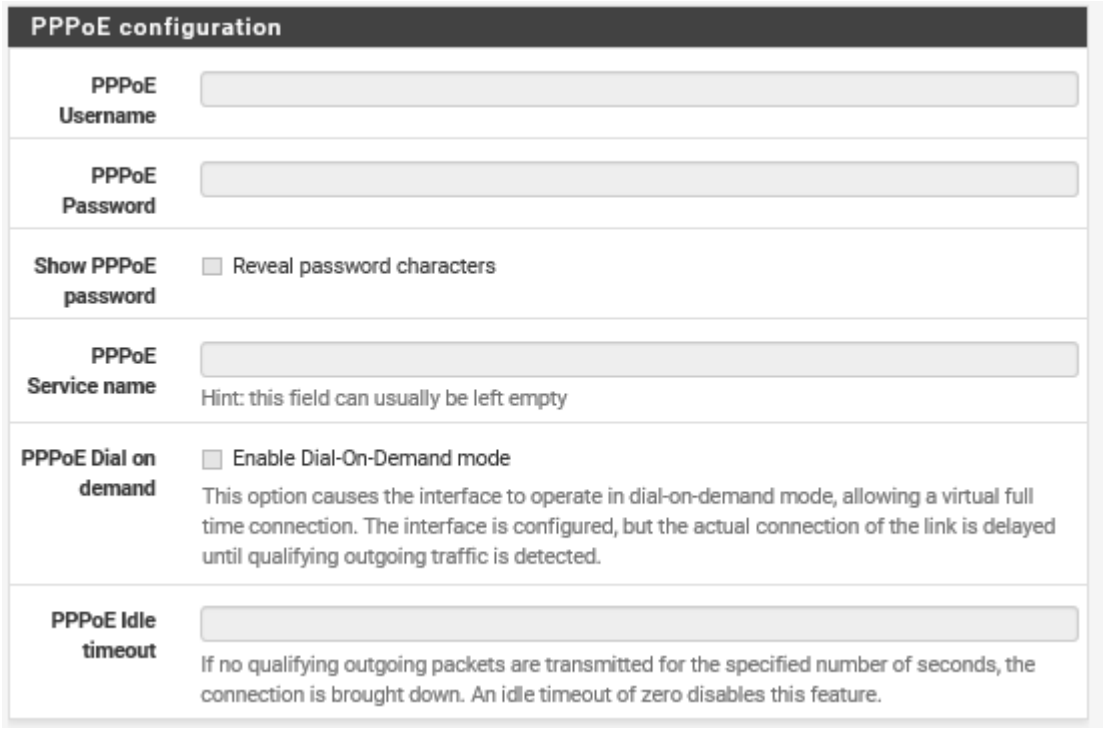


Ensuite nous arrivons à la configuration de l'**interface WAN**. Elle est **configurée automatiquement par DHCP donc je ne vais le remettre en statique**.

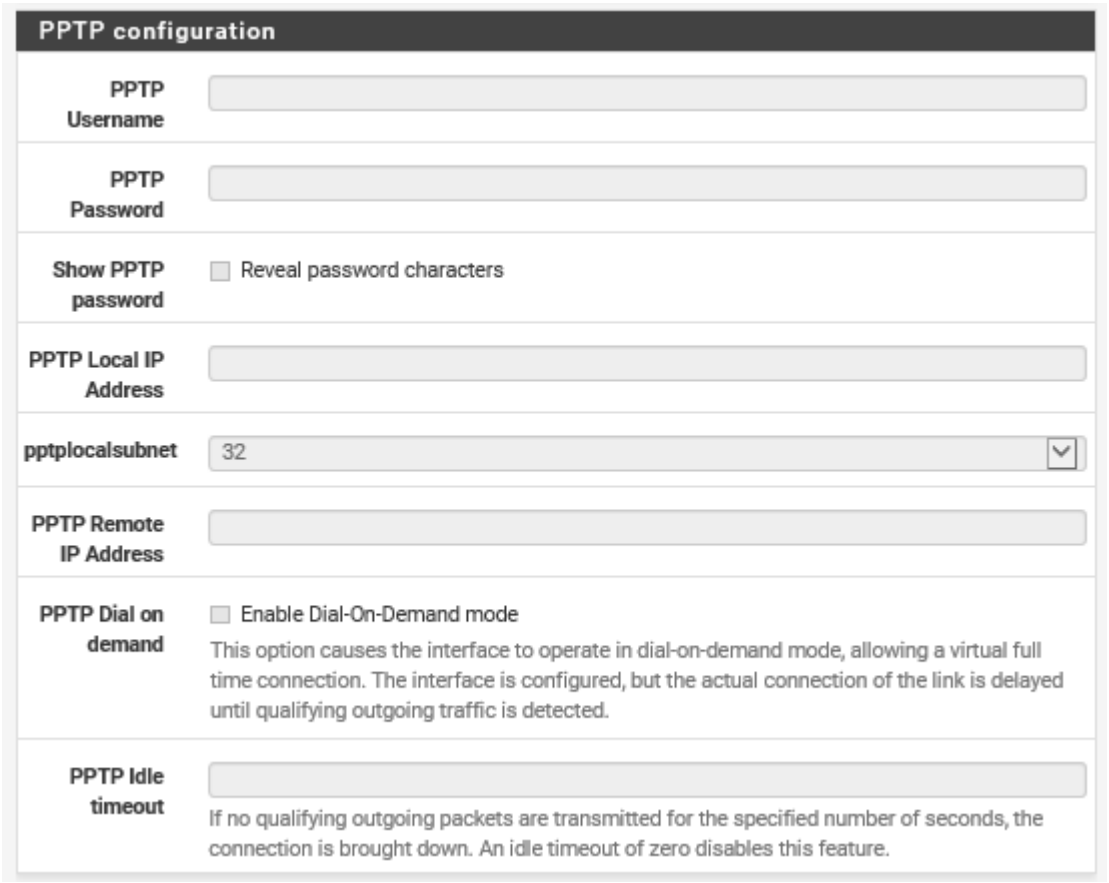
Si vous avez besoin d'attribuer une IP fixe à cette interface, c'est dans cette partie que ça se définit.



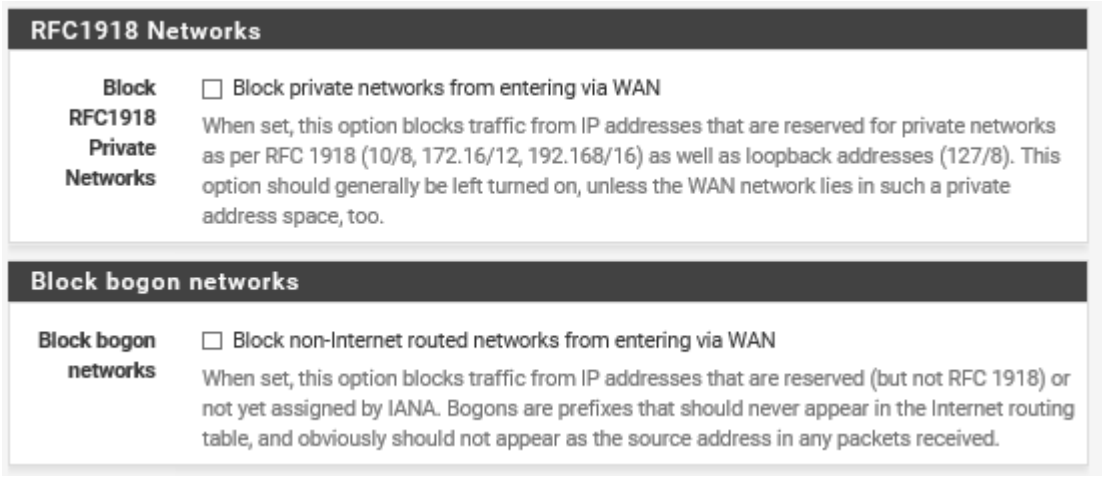
La partie « **PPPoE configuration** » sert en général à mettre les **identifiants fournis par votre FAI**. Ce sont ces identifiants qui sont définis dans votre box internet actuellement. Si vous souhaitez placer un firewall à la place de la box, il sera nécessaire de remplir cette partie.



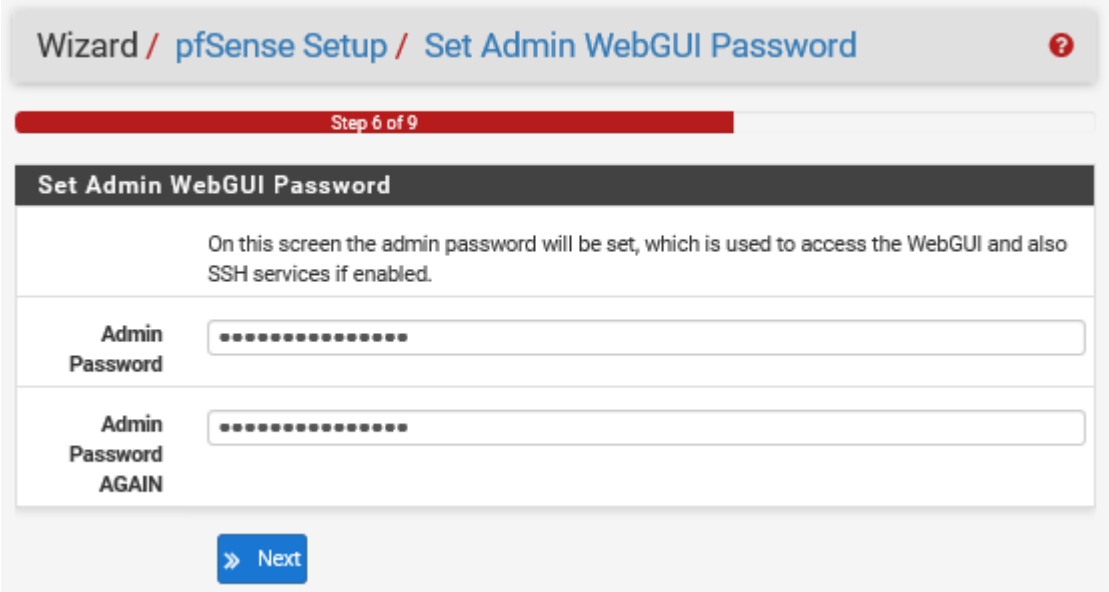
La partie suivante « **PPTP configuration** » servira plutôt au **montage d'un VPN point à point** *(Protocole de tunnel point-à-point, à éviter car peu sécurisé, plutôt privilégier son petit frère IPSEC).*



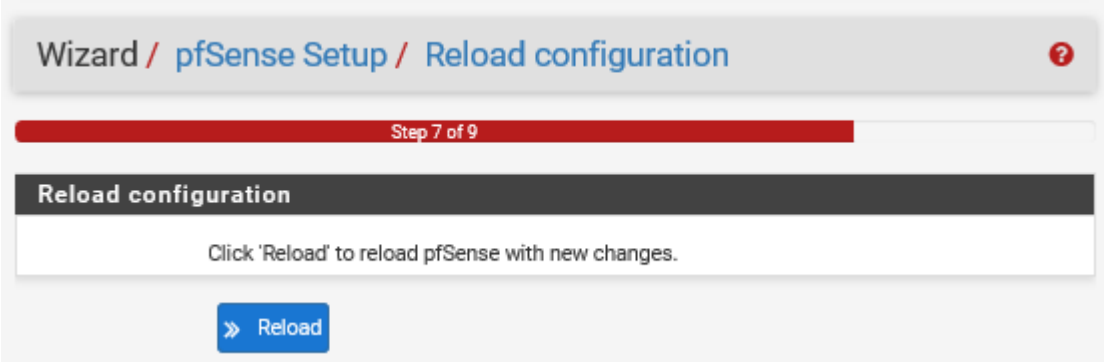
Les deux dernières options de cette page définissent que tout trafic entrant sur l'interface WAN et venant d'une classe d'adresse réseau privé est automatiquement bloqué. **Comme mon infra est ici virtuelle, je vais obligatoirement faire communiquer des réseaux privés, je n'utilise pas réellement une adresse publique**. Il est donc **nécessaire dans le cadre d'un labo de décocher ces 2 cases** sinon vous pourrez avoir des petits couacs.



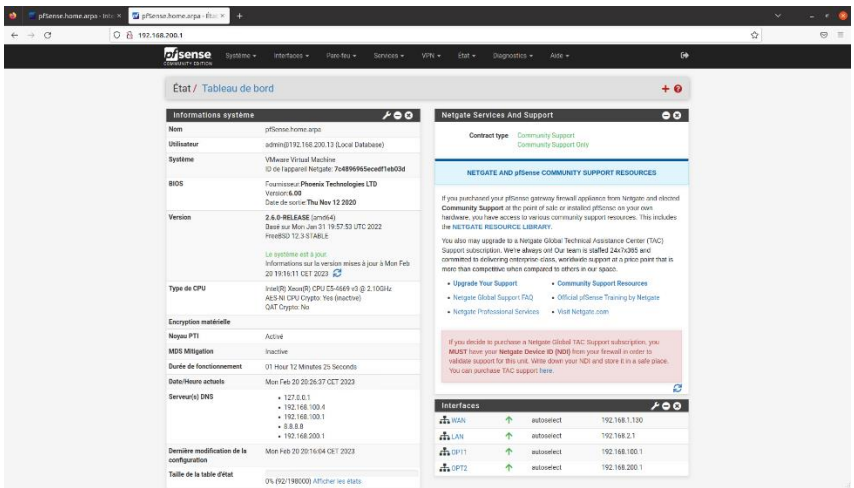
Durant la phase de configuration, il est également **nécessaire de changer les identifiants par défaut du compte admin** de pfsense.



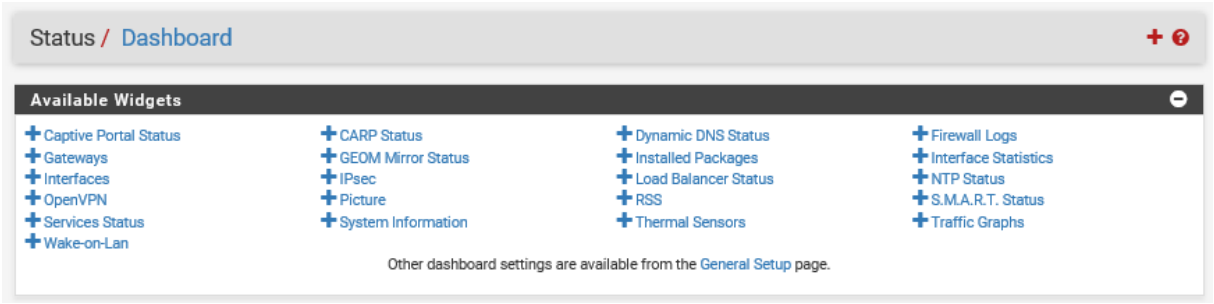
La phase finale de l'installation de pfsense est terminée. Cliquez sur **Reload** pour recharger pfsense. A la fenêtre suivante, vous pourrez simplement cliquer sur le bouton **Finish**.



Vous arrivez donc sur le **tableau de bord de votre pfsense**. Vous retrouvez ici des **infos sur l'utilisation des ressources de la machine** elle-même, ses **différentes adresses IP**, sa **version** et ses **mises à jour** si nécessaire etc…

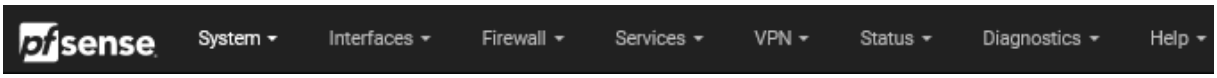


Cette **vue est personnalisable** est cliquant sur le **petit + en haut à droite** dans la barre de titre.



Vous pouvez ajouter des graphiques, des infos sur les load balancer, le trafic, les logs, les VPN etc…

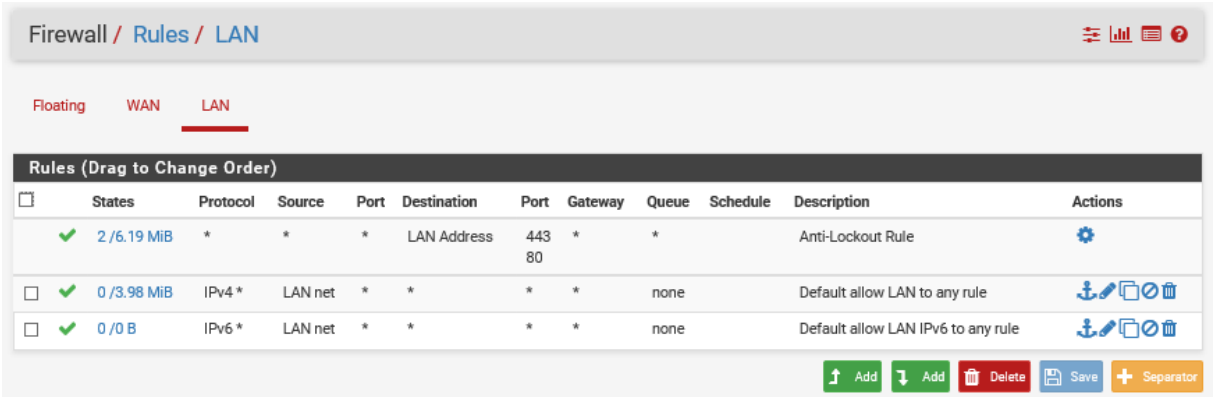
Les **différents menus** vont vous permettre de faire toutes sortes de choses sur votre firewall.



-
  - Mettre en place des VPN *(IPSEC, OpenVPN…)*
  - Activer des services *(DHCP, DNS, NLB, NTP, WOL…)*
  - Faire du NAT et du port forwarding
  - Ajouter des routes
  - Définir des règles pour le trafic entrant/sortant
  - Surveiller précisément ce même trafic
  - Ajouter des plugins qui vont apporter d'autres fonctionnalités *(filtrage Squidguard par exemple)*
  - …

Info + : Pour modifier la langue de pfsense, allez dans le menu System et General Setup.

Par défaut lors de son installation, tout le trafic est ouvert. On peut voir ceci dans le **menu « Firewall », sous-menu « Rules » et partie « LAN ».**



Les règles présentes ici **définissent que tout le trafic IPv4 et IPv6, tout protocole confondu, venant sur réseau local** *(LAN Net)* **sur n'importe quel port et vers n'importe quelle destination est autorisé**.

D'ailleurs si vous avez correctement suivi ce tuto et que depuis le PC client vous faites un ping vers google.fr, le ping va bien aboutir, preuve en est que le trafic peut sortir sans intervention de votre part.

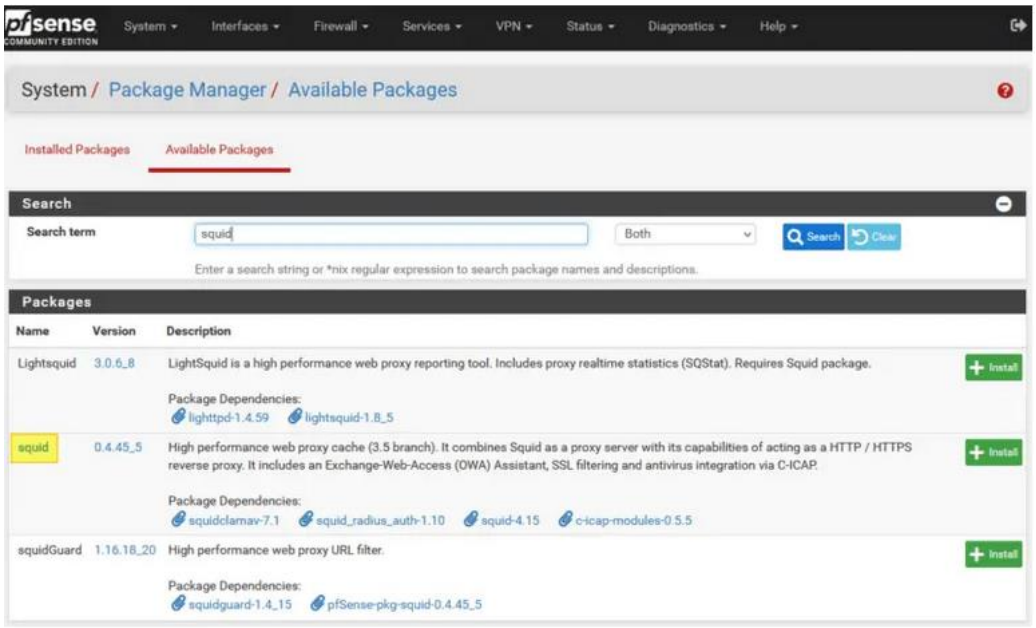
Il est plus que conseillé de brider ce trafic pour n'autoriser que les protocoles/port nécessaires. Le but d'un firewall étant de sécuriser ce qui entre et sort de son réseau, si c'est porte ouverte, il n'y a pas vraiment d'intérêt…

I.INSTALLATION DE SQUID

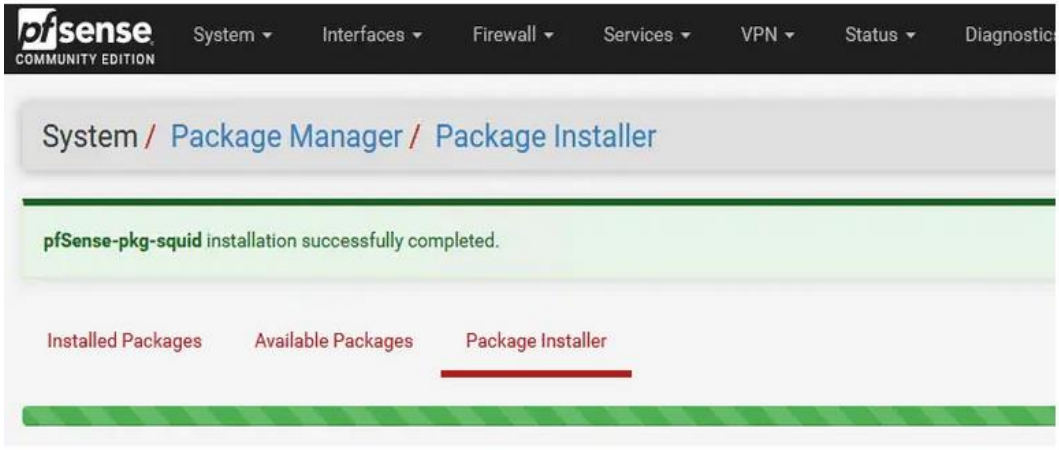
Connectez-vous sur l'interface d'administration de PfSense afin d'installer le paquet "*squid*". Pour cela, sous "**System**", cliquez sur "**Package Manager**" et ensuite sur l'onglet "**Available Packages**".

`System > Package Manager > Available Packages`

Recherchez "**squid**" et cliquez sur le bouton "**Install**" à droite, au niveau de la ligne correspondante.



À la fin de l'installation, le message "**pfSense-pkg-squid installation successfully completed**" doit s'afficher.



Le paquet étant installé, on peut passer à la configuration.

II.CONFIGURATION DE SQUID

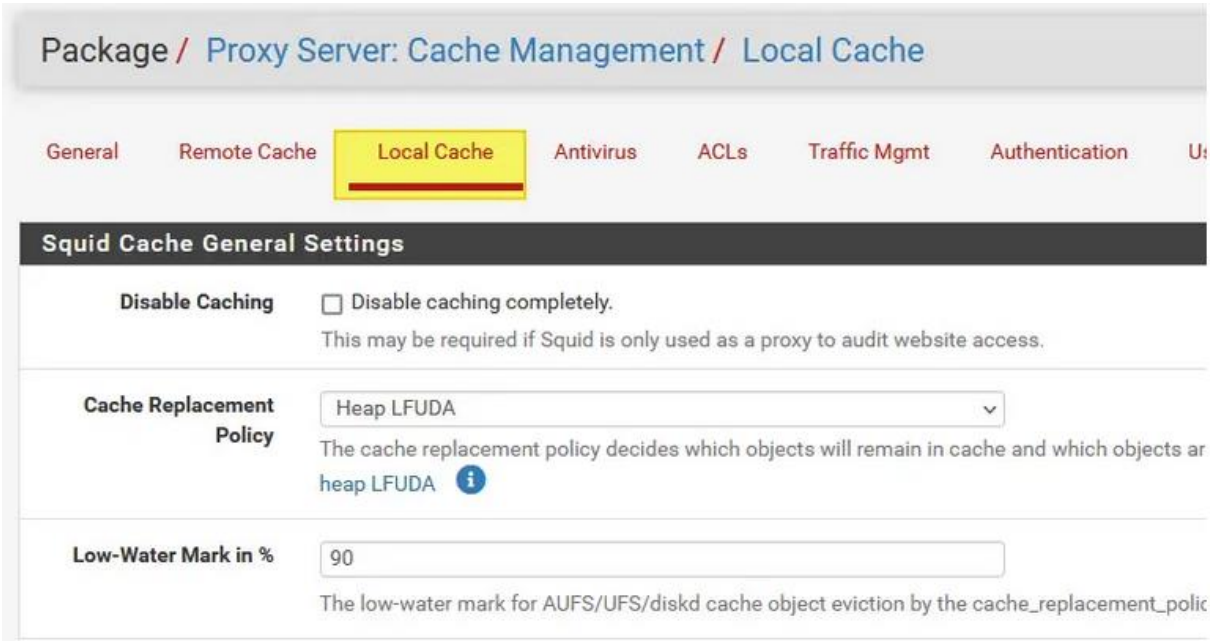
La configuration de Squid s'effectue via le menu "**Services**" :

```
Services > Squid Proxy Server
```

La configuration est découpée en plusieurs onglets. Afin de pouvoir activer Squid, il faut **configurer le cache local sinon le démarrage du processus Squid échouera**. Cliquez sur l'onglet "**Local Cache**". Comme pour chaque section, nous retrouvons de nombreux paramètres... Pour le cache, j'attire votre attention sur ces options :

- **Hard Disk Cache Size** : par défaut sur "100" pour 100 Mo, cette valeur correspond à la taille maximale du cache sur l'espace disque. Vous pouvez augmenter cette valeur à **1024 Mo** pour avoir 1 Go de cache.
- **Hard Disk Cache Location** : l'emplacement du cache, à savoir par défaut "*/var/squid/cache*".

Que vous décidiez de modifier ou non l'un des paramètres de la section "**Local Cache**", vous devez cliquer sur le bouton "**Save**" en bas de la page.

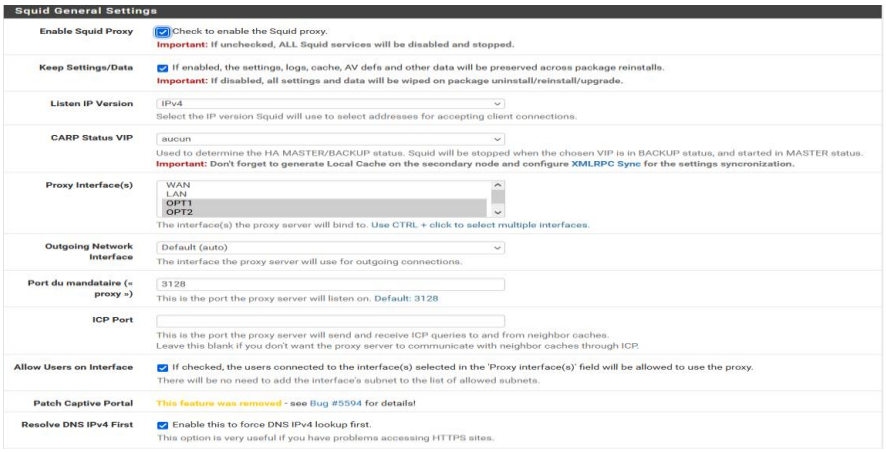


Ensuite, cliquez sur l'onglet "**General**". Là encore, il y a de nombreuses options. Voici ce qu'il faut configurer à minima :

- **Enable Squid Proxy** : cochez la case pour activer Squid sur le pare-feu, ce qui signifie qu'il va démarrer
- *[facultatif]* **Listen IP Version** : écouter en IPv4, en IPv6 ou les deux
- **Proxy interface(s)** : sur quelle interface souhaitez-vous activer le proxy ? Ici, ce sera s sur les interfaces "**OPT1**" et "**OPT2**" donc je les sélectionne. Vous pouvez en

sélectionner un seul si besoin, mais dans tous les cas le "WAN" ne sera pas sélectionné.

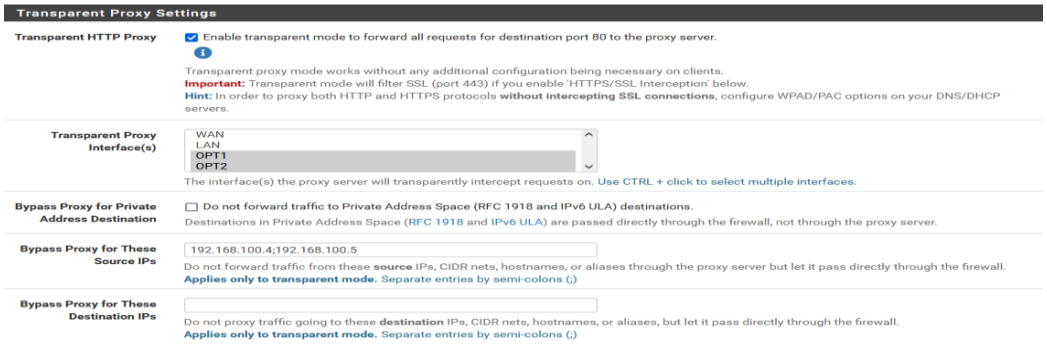
- **Proxy Port** : on laisse le port par défaut, à savoir 3128, mais il ne devra pas être déclaré sur les postes clients puisque l'on va configurer Squid en mode proxy transparent.
- **Allow Users on interface** : cochez cette case pour autoriser implicitement les utilisateurs connectés sur le réseau "OPT1" et "OPT2" à utiliser le proxy. Cela évite de déclarer le réseau dans un second temps.



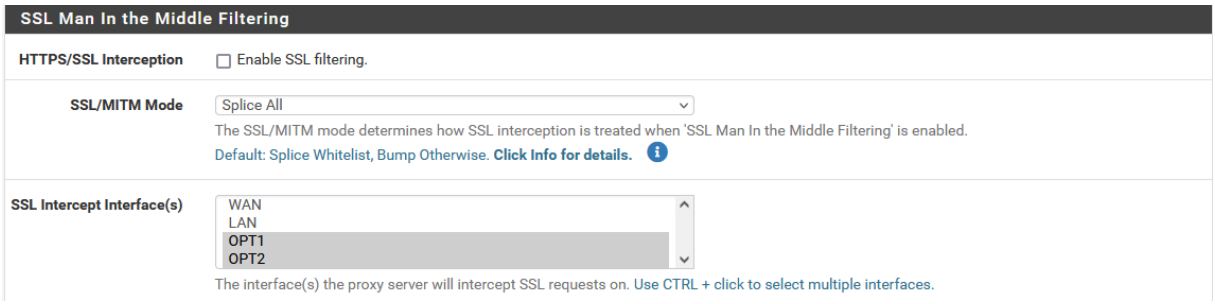
Descendez dans la page... et cochez l'option "**Transparent HTTP Proxy**" pour activer le mode proxy transparent pour le protocole HTTP. Pour l'activer pour le protocole HTTPS, il faudra cocher une autre option (nous en parlerons par la suite).

Dans le même esprit qu'au début de la configuration, sélectionnez "**OPT1**" et "**OPT2**" pour l'option "**Transparent Proxy Interface(s)**".

En configurant l'option "**Bypass Proxy for these Source IPs**", vous avez la possibilité de déclarer des adresses IP sources (ou un sous-réseau source) qui peuvent passer outre le proxy et accéder en direct à Internet, ici on va mettre les 2 AD's avec 192.168.100.4 et 192.168.100.5 car les salariés ne sont pas censés y avoir accès. Dans le même esprit, l'option "**Bypass Proxy for these Destination IPs**" permet d'outrepasser le proxy pour certaines destinations.

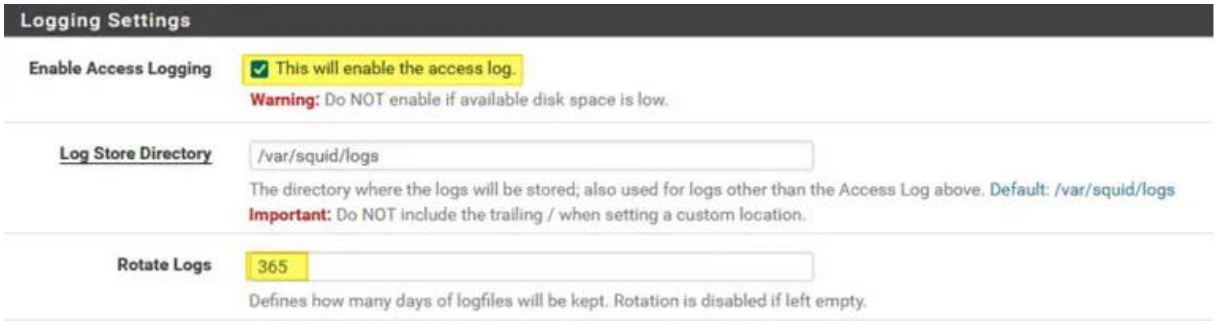


Pour le moment, laissez l'option "**Enable SSL filtering**" décochée.



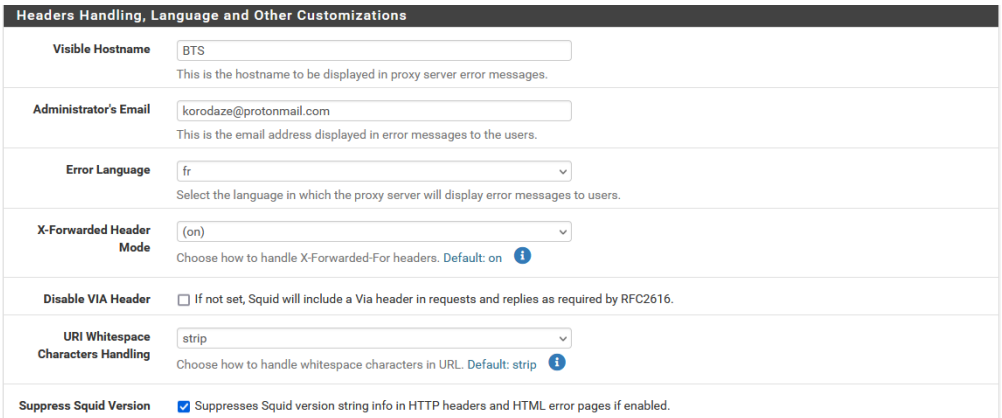
Continuez de descendre dans la page... Activez les journaux comme ceci :

- **Enable Access Logging** : cochez l'option pour activer les journaux, ce qui va permettre de savoir qui fait quoi sur Internet.
- **Rotate Logs** : pendant combien de jours souhaitez-vous conserver les logs ? Pour les établissements scolaires, c'est pendant 365 jours qu'il faut conserver les logs (sauf erreur de ma part).



Ensuite, la section "**Headers Handling, Language and Other Customizations**" permet de configurer les messages Squid. Le champ "**Visible Hostname**" correspond au nom d'hôte qui peut s'afficher côté client, notamment sur les pages de blocage Squid, tout comme l'e-mail spécifié pour l'option "**Administrator's Email**". Pour les messages d'erreurs justement, précisez la langue française au niveau de l'option "**Error Language**".

Pour des raisons de sécurité, on va masquer les informations sur Squid, notamment la version, en cochant l'option "**Suppress Squid Version**". Ce qui donne :

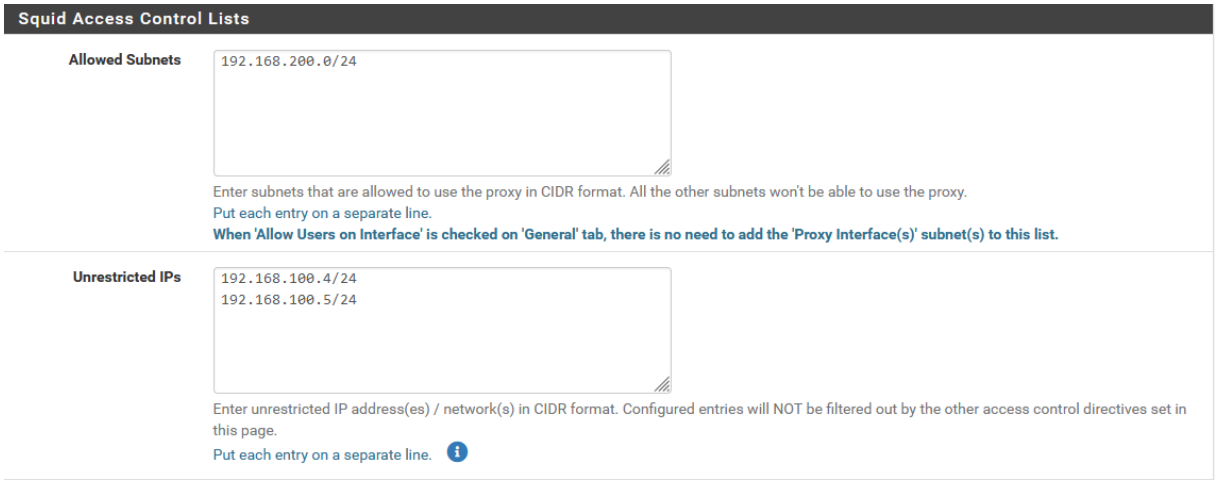


Voilà, on est arrivé au bout de la page de configuration ! Cliquez sur "**Save**" pour appliquer cette nouvelle configuration.

IV. Tester le proxy transparent Squid

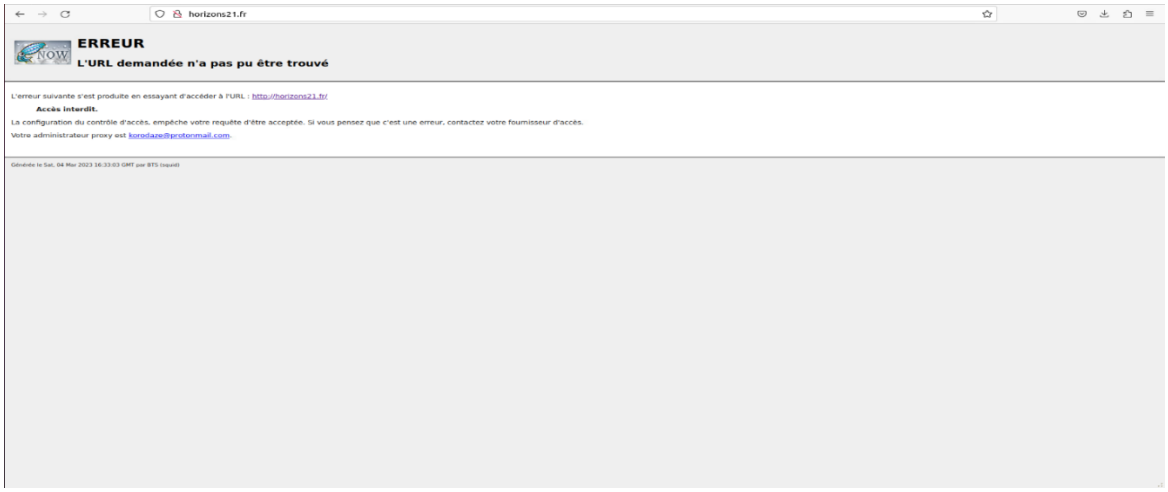
Pour tester le bon fonctionnement de notre proxy transparent HTTP, on peut tout simplement s'amuser à naviguer sur Internet. Pour que ce soit plus parlant, on va bloquer un nom de domaine.

Cliquez sur l'onglet "**ACLs**", toujours dans la configuration de Squid. C'est ici que vous pouvez déclarer les sous-réseaux autorisés à utiliser le proxy (**Allowed Subnets**) mais pour nous on renseignera le réseau 192.168.200.0/24 car on veut que tous les clients utilisent le proxy. Pour autoriser une ou plusieurs adresses IP (ou sous-réseau) à passer outre les restrictions, renseignez l'option "**Unrestricted IPs**" ici on va mettre les réseaux 192.168.100.4/24 et 192.168.100.5/24 car ce sont les 2 serveurs AD de notre infra et on ne veut pas qu'ils aient une restriction.



Ce qui m'intéresse pour ce test, c'est l'option "**Blacklist**" puisqu'elle permet d'indiquer un ou plusieurs domaines à bloquer. Pour ce test, il nous faut un site en HTTP (ce qui est de plus en plus "rare", enfin surtout au niveau des sites connus). J'ai pris le site "*horizons21.fr*", au hasard, et je l'ai ajouté comme ceci :

Ensuite, on sauvegarde la configuration... Puis, à partir d'un poste de travail situé sur le réseau local, on tente d'accéder au site horizons21.fr. Et là, on peut voir que ça ne fonctionne pas ! On peut voir qu'une page "**Accès interdit**" renvoyée par Squid s'affiche !



On peut aussi suivre les logs en temps réel côté Squid, via l'onglet "**Real Time**". On voit très bien nos requêtes à destination du site "*horizons21.fr*" depuis l'hôte *192.168.200.150 :* c'est la preuve irréfutable que notre PC passe bien par le proxy transparent !

Squid Access Table

Squid - Access Logs

Date	IP	État	Adresse	Utilisateur	Destination
05.03.2023 14:00:38	192.168.200.150	NONE/200	34.120.208.123:443	-	-
05.03.2023 14:00:38	192.168.200.150	NONE/200	35.241.9.150:443	-	-
05.03.2023 14:00:37	192.168.200.150	TCP_DENIED/403	http://horizons21.fr/favicon.ico	-	-
05.03.2023 14:00:36	192.168.200.150	TCP_DENIED/403	http://horizons21.fr/	-	-
05.03.2023 14:00:03	192.168.100.6	NONE/200	34.117.237.239:443	-	-
05.03.2023 13:59:59	192.168.100.60	NONE/000	error:transaction-end-before-headers	-	-
05.03.2023 13:59:59	192.168.100.60	NONE/409	v10.events.data.microsoft.com:443	-	-
05.03.2023 13:59:59	192.168.100.60	NONE/200	13.69.109.131:443	-	-
05.03.2023 13:58:26	192.168.100.61	NONE/000	error:transaction-end-before-headers	-	-
05.03.2023 13:58:26	192.168.100.61	NONE/409	v10.events.data.microsoft.com:443	-	-

V. Configurer Squid en proxy transparent HTTPS (SSL Inspection)

C'est bien beau notre configuration, mais notre proxy transparent fonctionne seulement sur le protocole HTTP. Depuis quelques années maintenant, la tendance est au HTTPS (et on ne va pas s'en plaindre) alors c'est indispensable que l'on permette à notre proxy transparent de travailler le HTTPS.

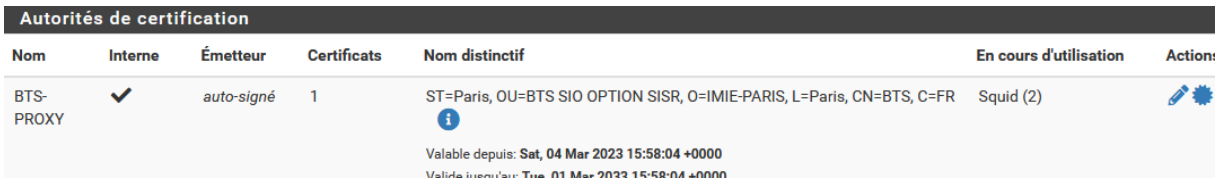
Cela est un peu plus complexe qu'une simple case à cocher dans les options du proxy, car il faut faire ce que l'on appelle du **SSL Inspection**. Puisqu'un flux HTTPS est chiffré, le proxy ne peut pas seulement regarder les trames passer. En effet, pour chaque connexion, il doit déchiffrer le flux, l'inspecter puis le chiffrer à nouveau afin de l'acheminer : une tâche d'envergure et gourmande en ressources.

A. Créer l'autorité de certification PfSense

Pour commencer, il faut créer une autorité de certification sur notre pare-feu PfSense. Rendez-vous dans le menu "**System**" puis "**Cert. Manager**" et dans l'onglet "**CAs**". Cliquez sur "**Add**" et renseignez les différents champs : c'est tout simple.

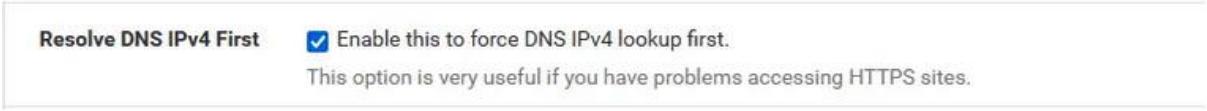
Note : si vous avez une autorité de certification Active Directory, il doit être possible d'ajouter un certificat existant directement.

Vous obtenez une autorité de certification, comme la mienne nommée "*BTS-PROXY*".



B. SSL Inspection avec Squid

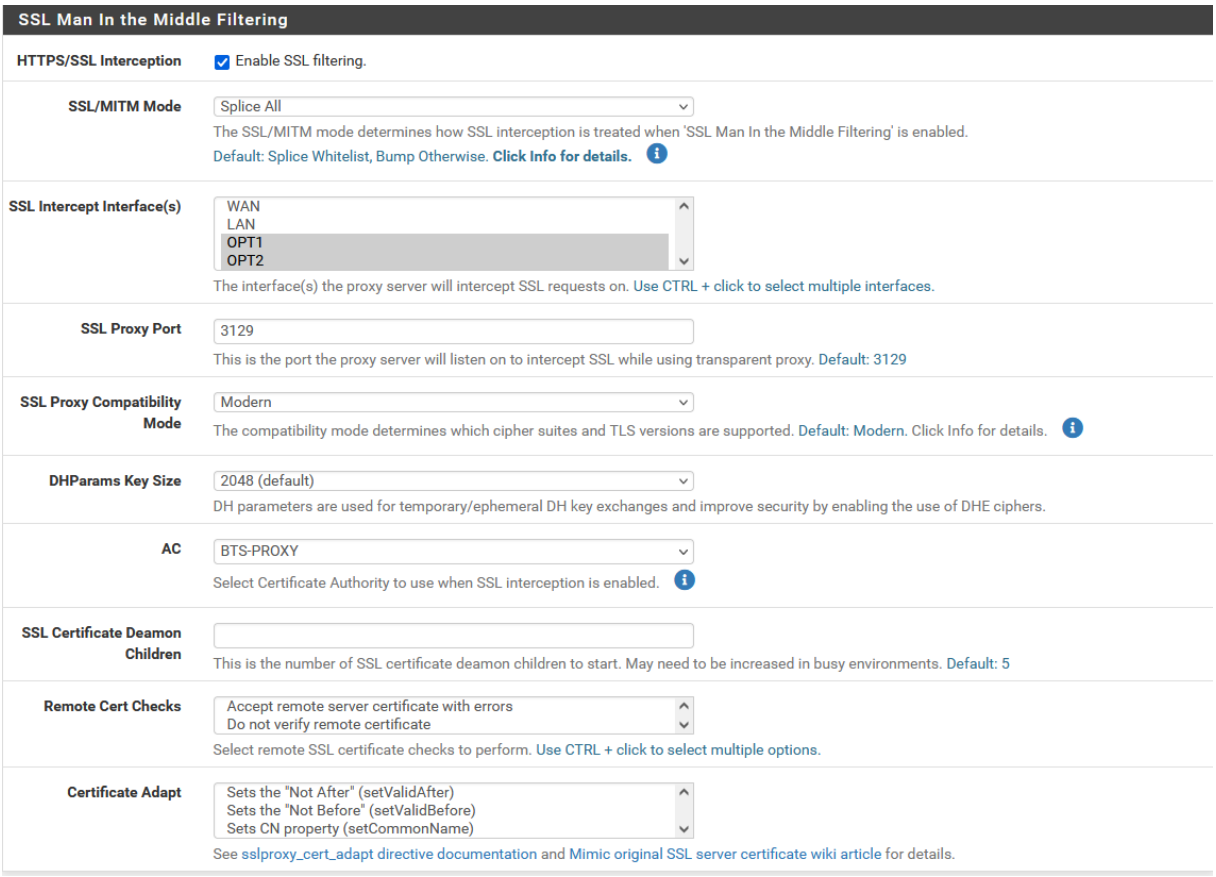
Retournez dans la configuration de Squid, via le menu "**Services**". Cochez l'option "**Resolve DNS IPv4 First**" pour activer la résolution DNS en amont du filtrage, ce qui est recommandé lorsque l'on filtre le HTTPS (ce que l'on s'apprête à faire).



Ensuite, activez l'option "**Enable SSL filtering**". Pour le mode "**SSL/MITM Mode**", choisissez le mode "**Splice All**" : c'est le mode le moins contraignant à mettre en œuvre, car il ne nécessite pas de déployer le certificat de l'autorité de certification sur l'ensemble des postes clients. C'est aussi le mode recommandé lorsque l'on prévoit de déployer Squid Guard, ce qui sera le cas dans la seconde partie de ce tutoriel.

Remarque : si vous prenez l'autre mode, il faut exporter le certificat de la CA créée précédemment et le déployer sur toutes les machines qui vont passer par le proxy transparent.

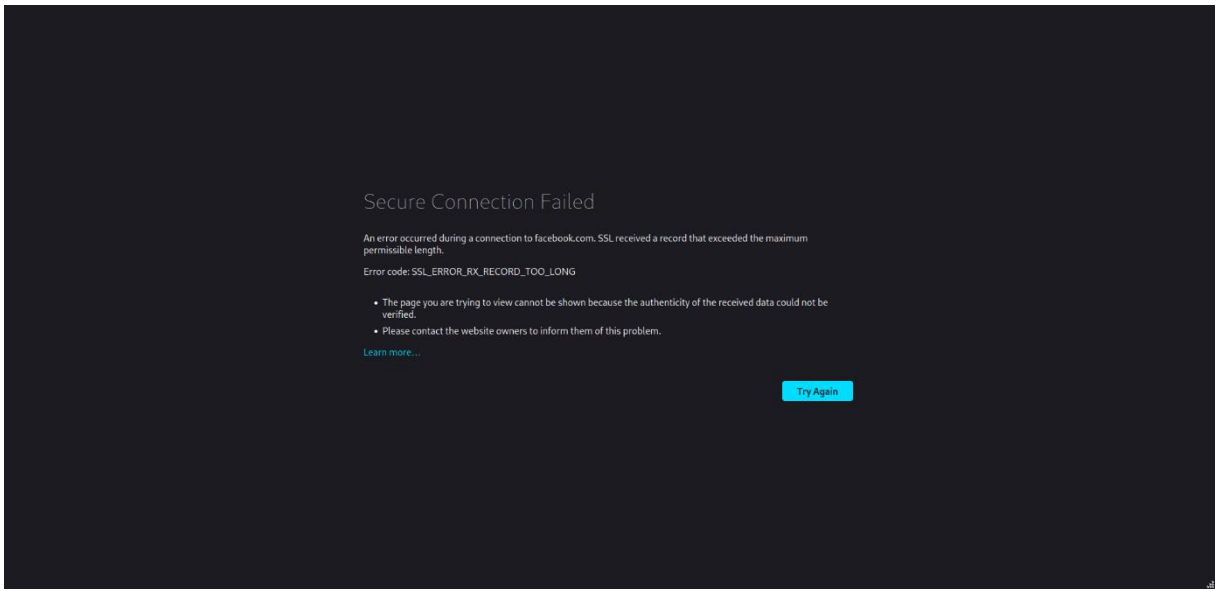
Sélectionnez l'autorité de certification créée précédemment au niveau de l'option "**CA**".



Sauvegardez via le bouton en bas de page.

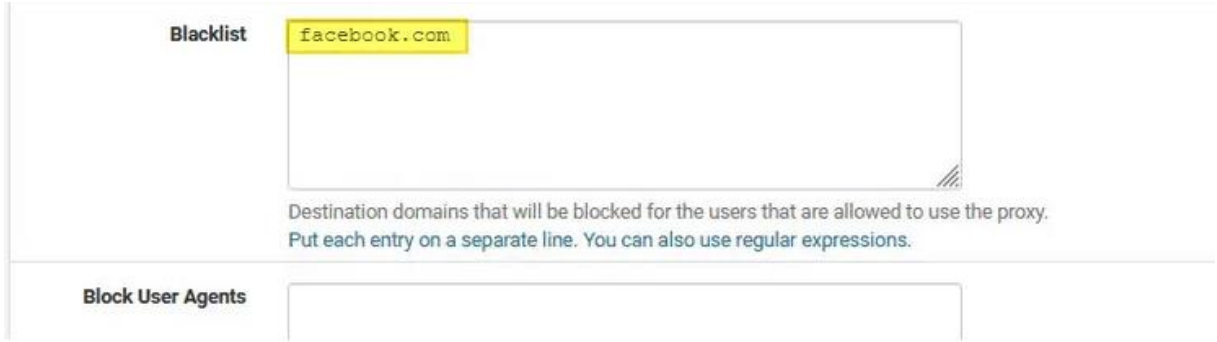
C. Tester l'accès à Internet

Maintenant, retournez sur votre poste de travail qui passe par le proxy puis tentez de naviguer sur un site en HTTPS. Vous allez très probablement obtenir le message d'erreur "**SSL_ERROR_RX_RECORD_TOO_LONG**". Ce qui confirme que le proxy fonctionne.



E. ACL : bloquer un site HTTPS dans Squid

Comme toute à l'heure, on va retourner dans l'onglet "**ACLs**" au niveau de la section "**Blacklist**". Cette fois-ci, on va bloquer un domaine où le site tourne en HTTPS : "*facebook.com*", à tout hasard. Ce qui donne :



On sauvegarde et on tente d'accéder à Facebook... Voici le message que l'on obtient :

I. Présentation

Dans ce tutoriel, nous allons voir comment installer et configurer Squid Guard sur un pare-feu PfSense pour permettre à notre proxy Squid d'effectuer du filtrage de sites Web basé sur des catégories, via une blacklist.

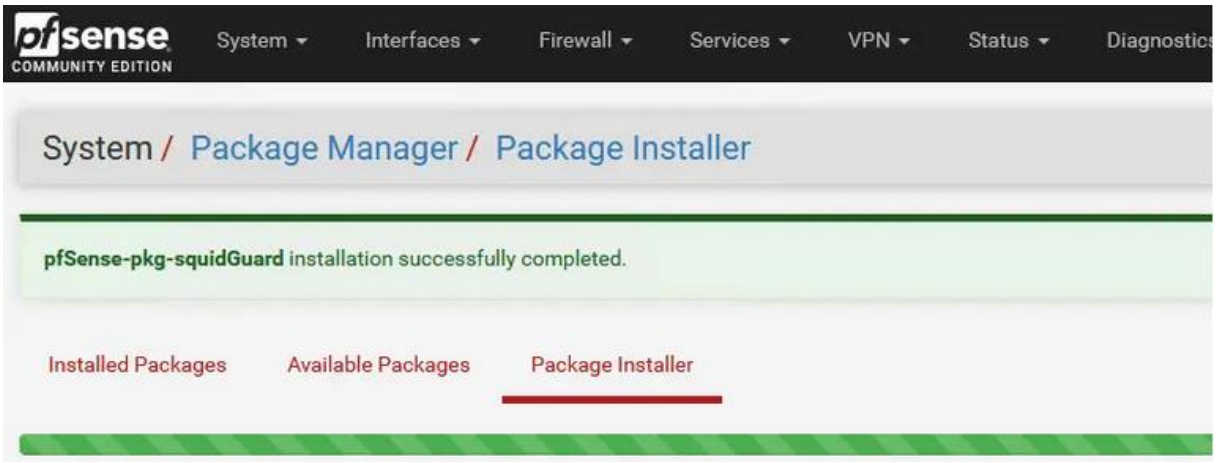
Au sein de Squid, sans Squid Guard donc, on peut mettre en place des ACLs et notamment bloquer des noms de domaine. Le problème, c'est que l'on ne peut pas créer de catégories pour regrouper plusieurs domaines, et on ne peut pas non plus créer des restrictions selon des plages horaires. Embêtant.

Grâce à Squid Guard, on va pouvoir utiliser une Blacklist existante, c'est-à-dire **une liste noire de domaines organisés par catégories**, afin d'affiner le filtrage au sein de notre proxy Squid. En complément, on pourra mettre en place des règles en fonction de plages horaires, de groupes utilisateurs, etc. De cette façon, vous allez pouvoir configurer votre proxy de manière à bloquer tous les sites liés à la pornographie.

La mise en place de Squid Guard nécessite au préalable d'avoir mis en place un proxy avec Squid puisque ce paquet vient en complément.

II. Installation de Squid Guard sur PfSense

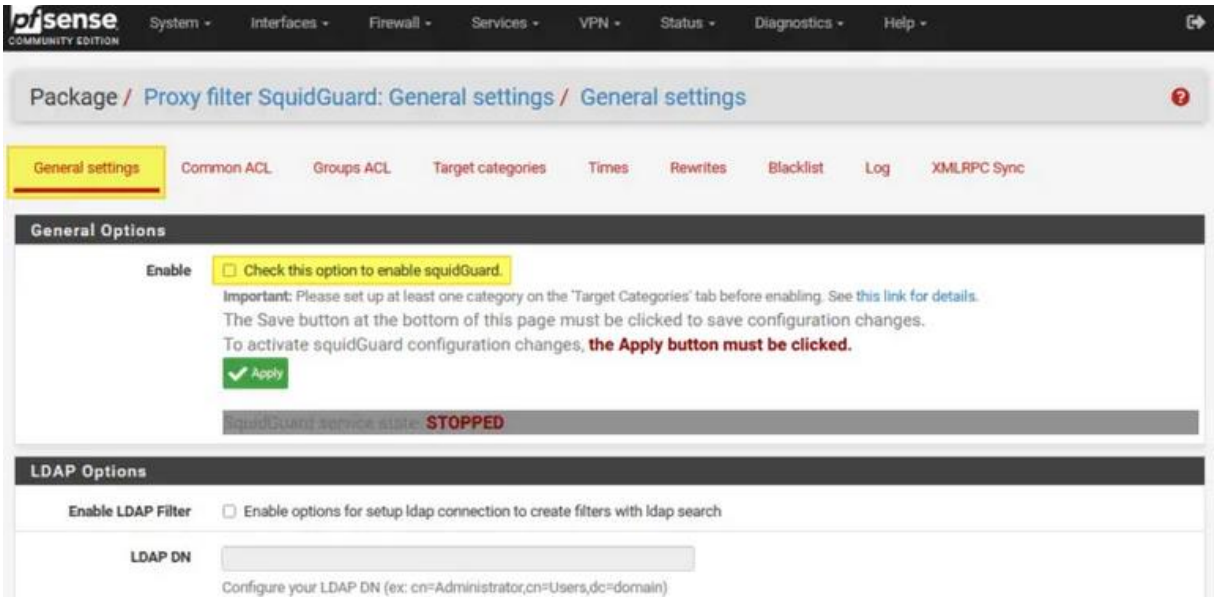
L'installation de ce paquet sur PfSense passe par le menu habituel sous "**System**", puis "**Package manager**". Dans la section "**Available Packages**", recherchez "*squid*" et vous devriez voir le paquet Squid Guard apparaître. Il ne reste plus qu'à cliquer sur le bouton "**Install**".



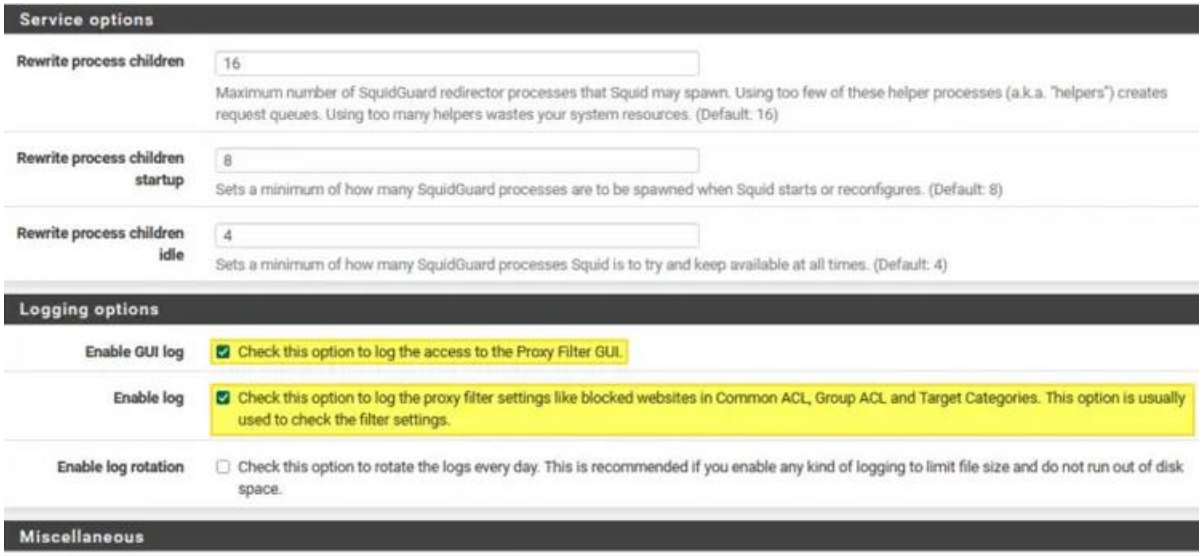
Une fois que c'est fait, nous pouvons passer à la configuration via le menu "**Services**" où se trouve une entrée "**SquidGuard Proxy Filter**".

III. Configuration de Squid Guard sur PfSense

Pour le moment, on va s'intéresser à l'onglet "**General Settings**". N'allez pas trop vite : **ne cochez pas l'option "Check this option to enable SquidGuard" pour le moment, car il faut le préconfigurer avant de l'activer.**



Cochez les deux options suivantes pour activer les logs : "**Enable GUI Log**" et "**Enable log**".

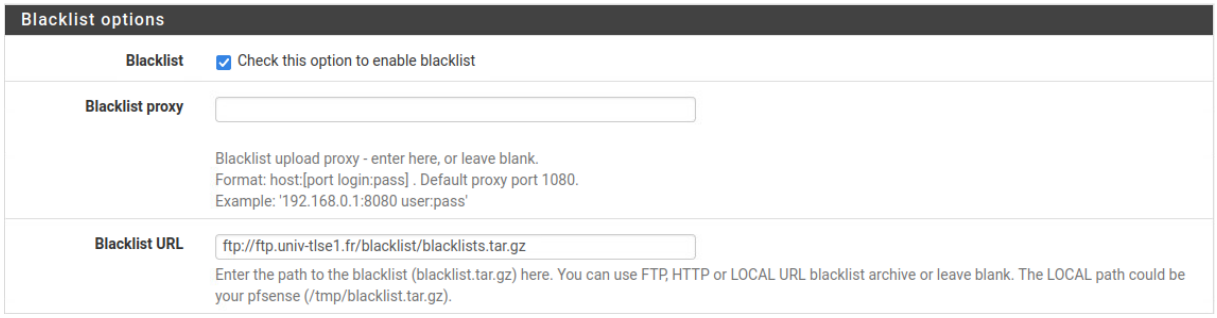


Au sein de la section "**Blacklist**", cochez l'option "**Check this option to enable blacklist**" afin d'activer l'utilisation d'une blacklist, c'est-à-dire une liste noire. Nous allons utiliser **la liste noire de L'Université Toulouse Capitole**, car elle est française, fiable et elle existe depuis depuis plusieurs années. **Elle contient de nombreuses catégories afin de répartir les sites et permettre un blocage ciblé selon certaines catégories.**

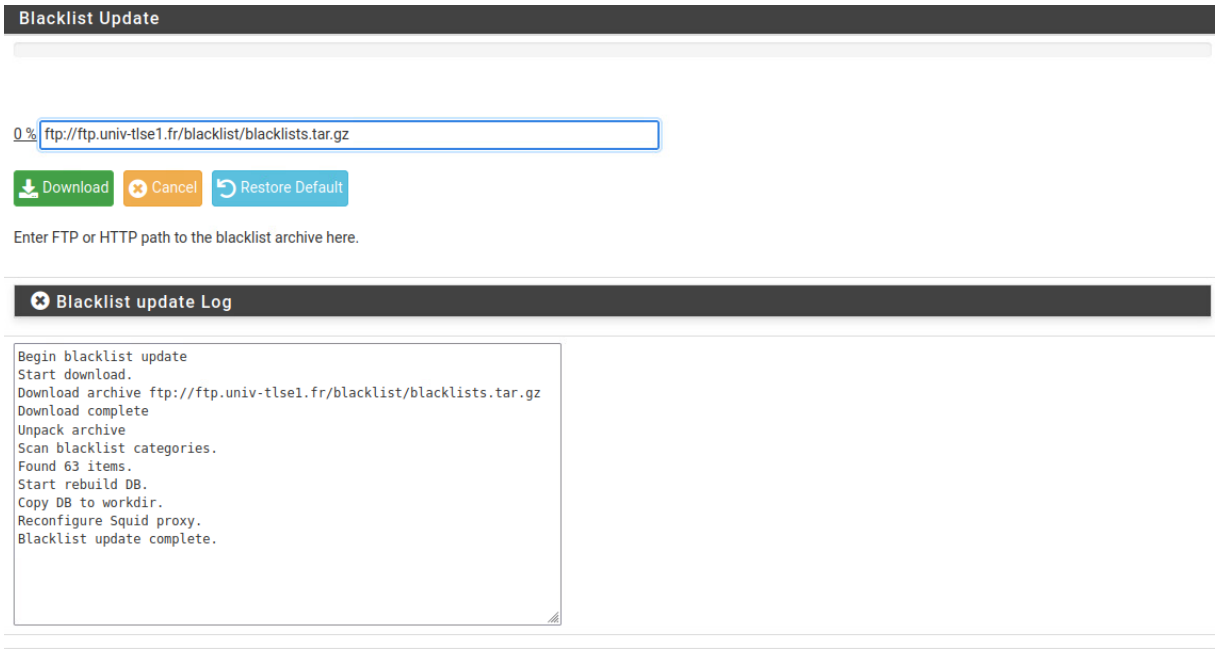
Ensuite, renseignez l'option "**Blacklist URL**" avec l'URL suivante :

```
ftp://ftp.univ-tlse1.fr/blacklist/blacklists.tar.gz
```

Enfin, cliquez sur le bouton "**Save**".

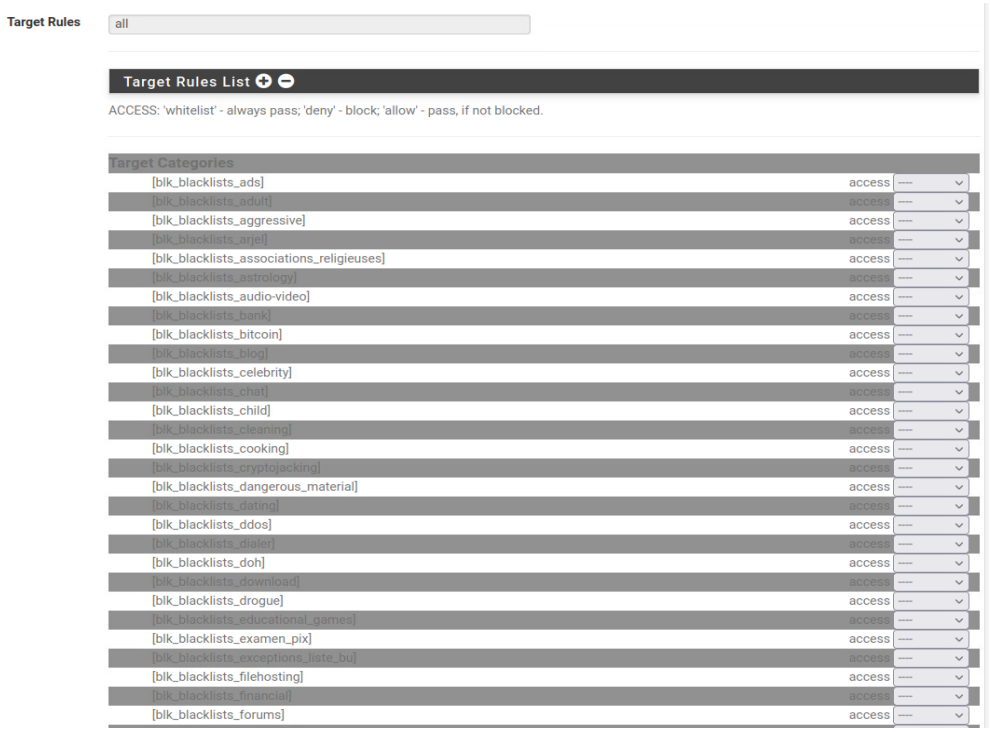


Maintenant, basculez sur l'onglet "**Blacklist**" de SquidGuard. Cliquez sur le bouton "**Download**" pour télécharger la dernière version de la liste noire que nous avons renseignée dans les paramètres de SquidGuard.



Afin d'exploiter la liste noire, nous devons créer des règles sous la forme d'ACL. Cliquez sur "**Common ACL**" afin de créer une règle de base et commune au sein de Squid, tandis que la section "**Groups ACL**" permet de créer des ACL ciblées avec plusieurs critères (par exemple : "*bloquer une catégorie selon une plage horaire spécifique*" ou "*bloquer une catégorie à tous les membres d'un groupe Active Directory*").

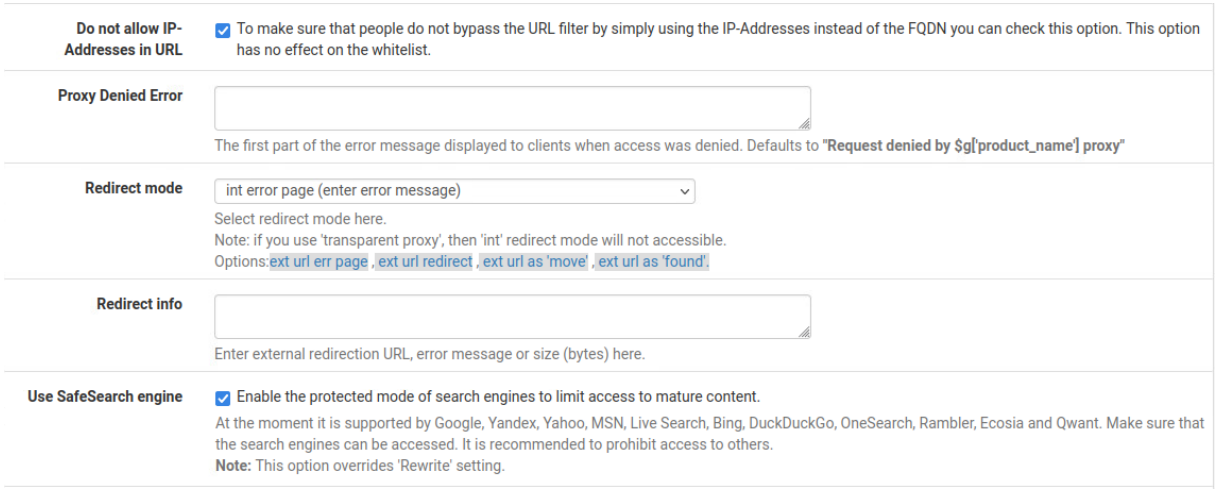
Au sein du champ "**Target Rules List**", vous avez la liste de toutes les catégories récupérées à partir de la blacklist toulousaine.



Je vous propose de bloquer la catégorie "**VPN**" correspondante à "**[blk_blacklists_vpn]**", il faut donc modifier la valeur du champ "**access**" pour

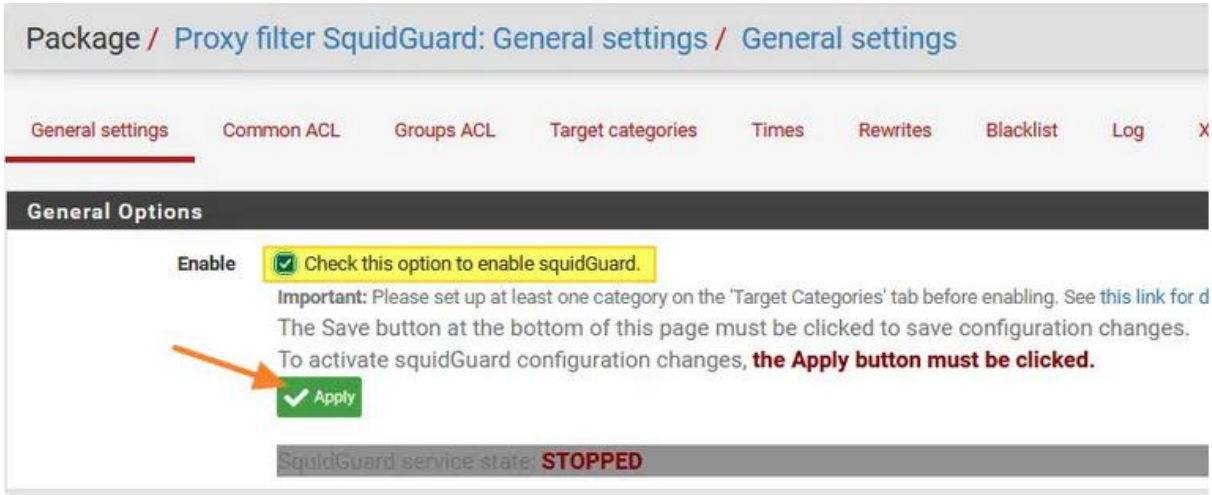
préciser "**deny**". En complément, pensez à configurer la valeur du champ "**Default access [all]**" sur "**allow**" pour autoriser toutes les autres catégories (par défaut).

Afin d'éviter qu'un petit malin contourne la restriction en précisant l'adresse IP du serveur distant à la place du nom de domaine, cochez l'option "**Do not allow IP-Addresses in URL**". En complément, si vous souhaitez utiliser la fonction SafeSearch des moteurs de recherche, cochez la case "**Use SafeSearch Engine**", tout en sachant que cela permet d'utiliser Google, Bing, DuckDuckGo, Qwant, etc.



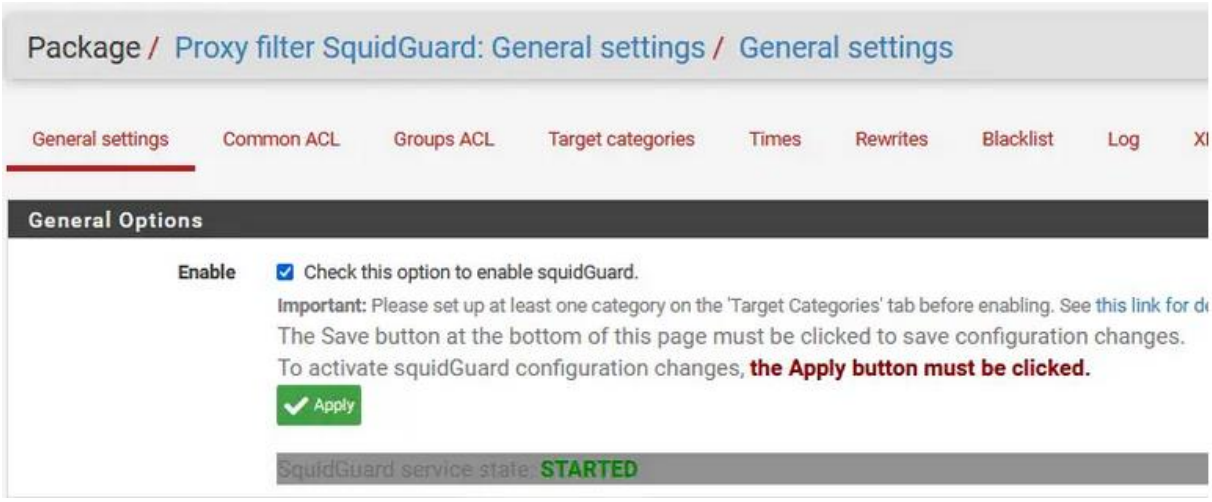
Enfin, activez les logs pour cette règle en cochant l'option "**Log**" tout en bas, puis cliquez sur "**Save**".

La configuration étant prête, retournez dans "**General Settings**", cochez l'option "**Check this option to enable SquidGuard**" et cliquez sur "**Apply**".

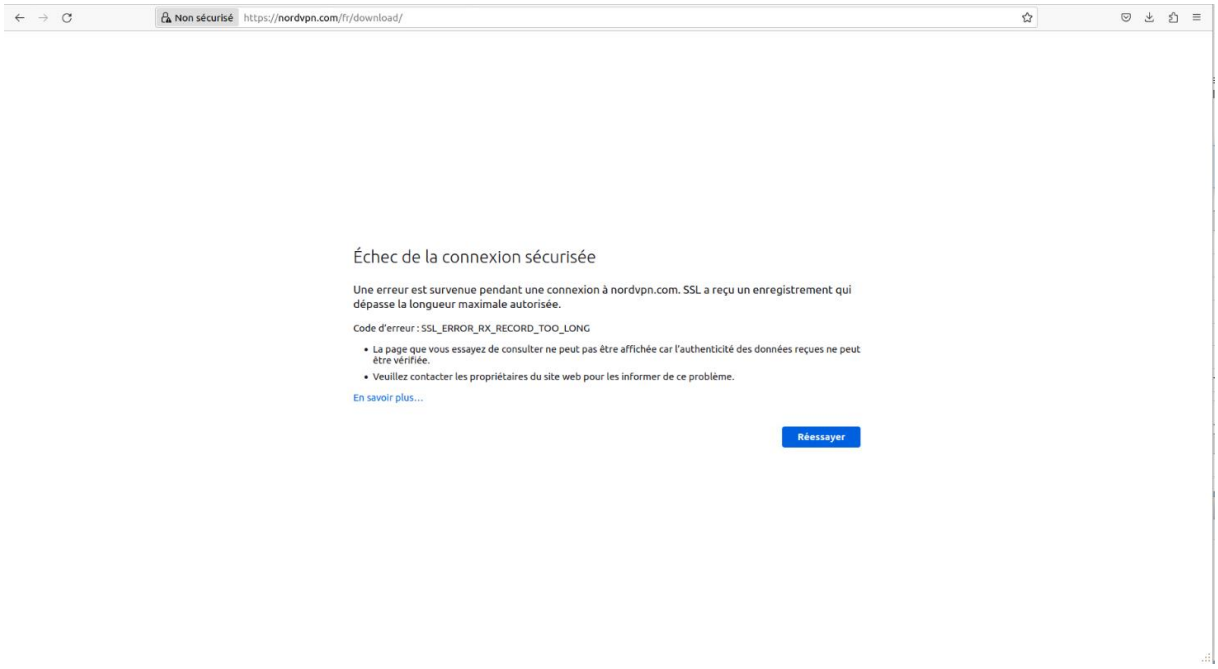


Le statut du service SquidGuard doit changer et passer sur "**STARTED**". Si ce n'est pas le cas, vérifiez que Squid est bien démarré de son côté.

Remarque importante : à chaque fois que vous modifiez la configuration de Squid Guard (exemple : bloquer une catégorie supplémentaire), il faut impérativement venir dans l'onglet "**General Settings**" pour cliquer sur le bouton "**Apply**" sinon les modifications ne sont pas prises en compte !

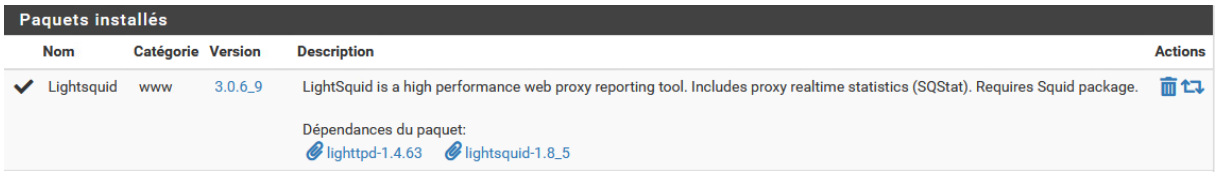


À partir d'un poste client, tentez d'accéder à un site en rapport avec la thématique "**VPN**", comme le site de NordVPN et vous verrez que la connexion est en erreur. En réalité, c'est SquidGuard qui est intervenu pour bloquer la connexion à ce site, conformément à la politique de filtrage mise en place.



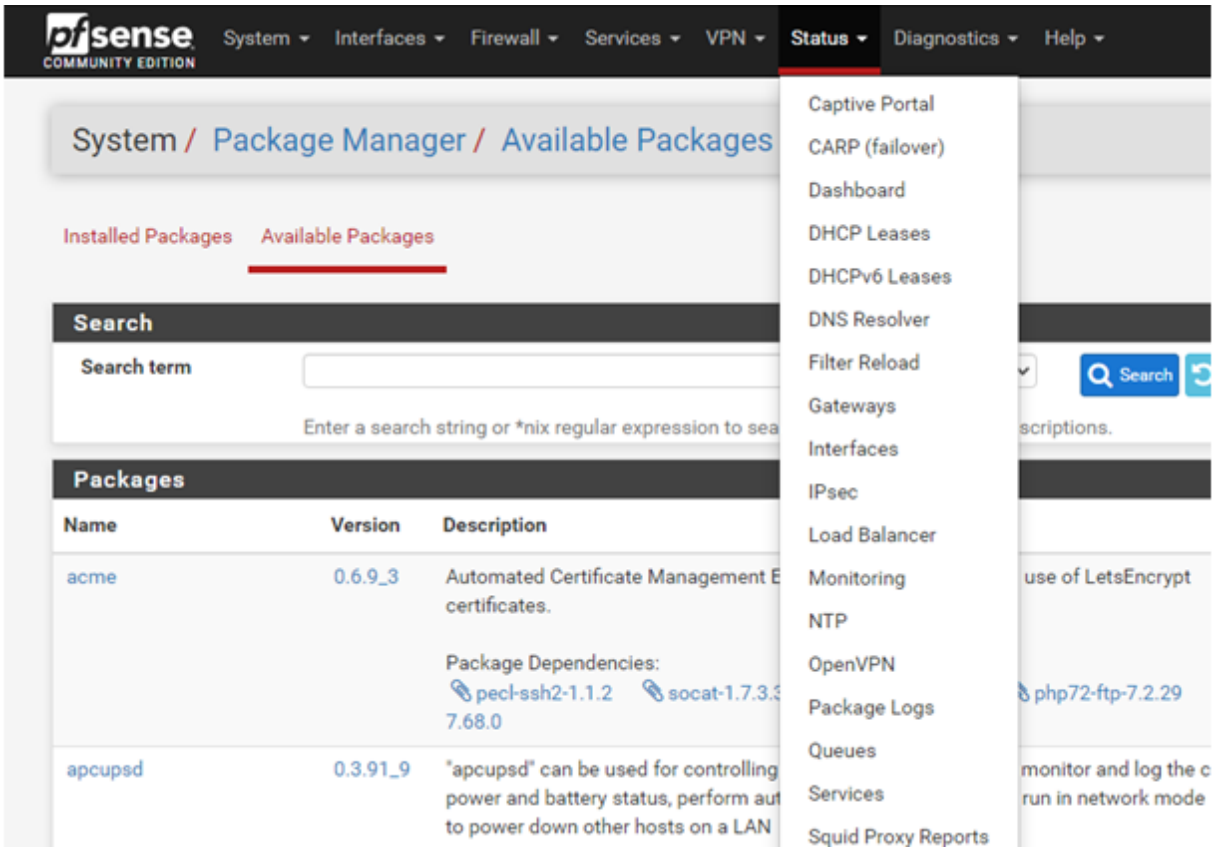
Pour aller plus loin, je vous invite à regarder deux onglets en particulier : "**Times**" pour créer des plages horaires" et "**Groups ACL**" pour créer des règles basées sur plusieurs critères. Sachez également que la section "**Target categories**" vous permet de créer des listes personnalisées.

IV. Installation et Configuration de LightSquid

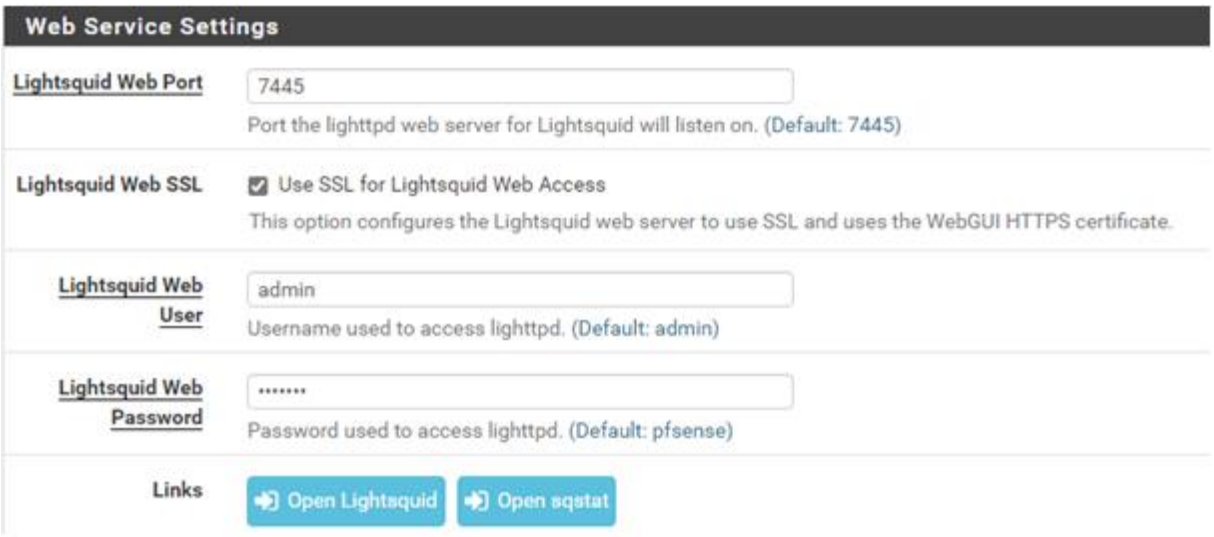


Tout d'abord installer le packet LightSquid.

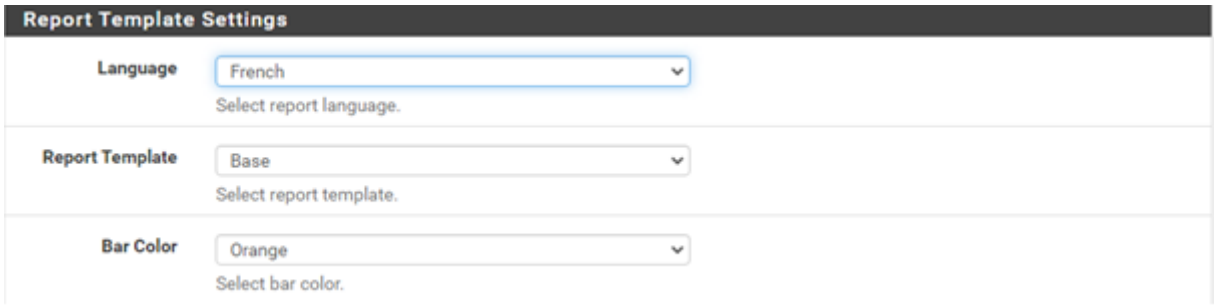
Nous allons désormais configurer Lightsquid. Dans l'onglet « Status », cliquez sur « Squid Proxy Reports ».



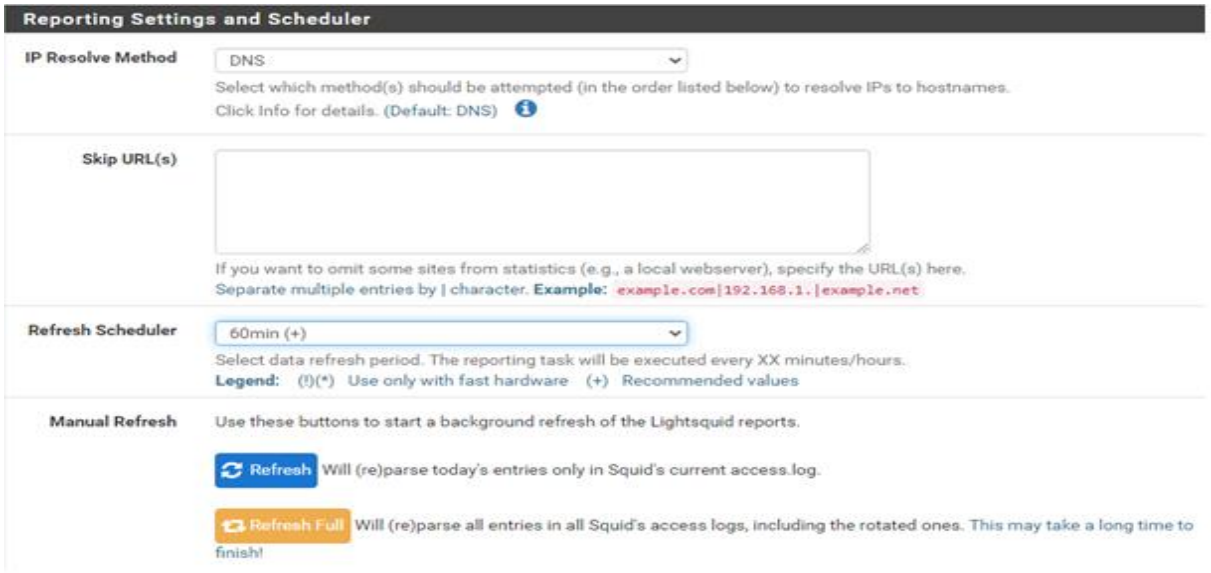
Vous pouvez ici changer les identifiants de connexion à la page Lightsquid. Par défaut, il s'agira des identifiants de PFSENSE.



Vous pouvez ensuite changer la langue de l'interface.

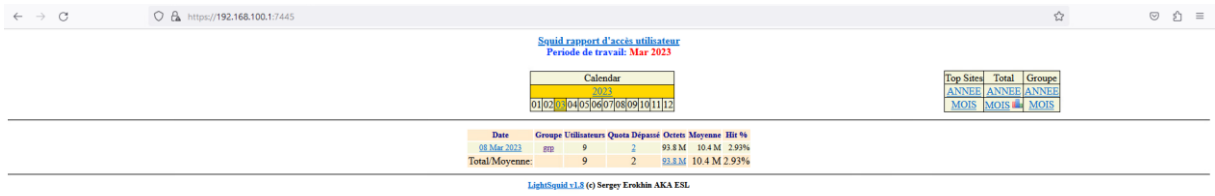


Indiquez ensuite une période de rafraichissement des données dans l'interface dans « Refresh Scheduler ».



Cliquez enfin sur « save » et « refresh ».

Cliquez ensuite sur « Open Lightsquid ». Une page contenant les informations de Logs devrait s'afficher.



Redémarrez ensuite PFSENSE. Dans l'onglet « Diagnostics », cliquez sur « Reboot ».