Installation de Pfsense

Rémi RENARD

Date : 12/12/2023

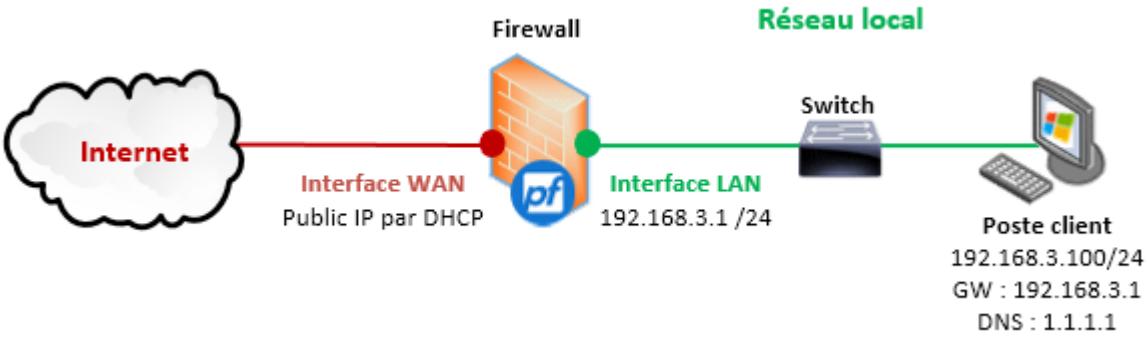
Table des matières

A quoi sert un pare-feu ?

PfSense est un *pare-feu open source faisant également fonction de routeur* appartenant à Rubicon Communications et Netgate. Il est basé sur le système d'exploitation FreeBSD issu de la famille d'Unix

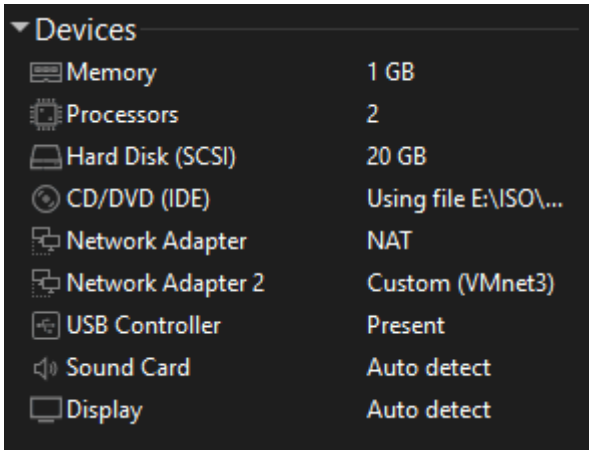
Un pare-feu, aussi nommé firewall, est un système de sécurité *(matériel ou logiciel)* qui va définir et contrôler les flux de données qui sont autorisés à entrer et sortir de votre réseau. Votre modem fournit par votre fournisseur d'accès à internet est un firewall matériel par exemple. Avec peu de fonction certes, mais c'est tout de même un firewall.

On dit globalement d'un firewall qu'il « applique la politique de sécurité de l'entreprise » grâce à des règles d'actions pour le trafic réseau. Pour simplifier, il va en fait accepter seulement les types de communications définies dans des règles et rejeter tout ce qui n'est pas explicitement autorisé.



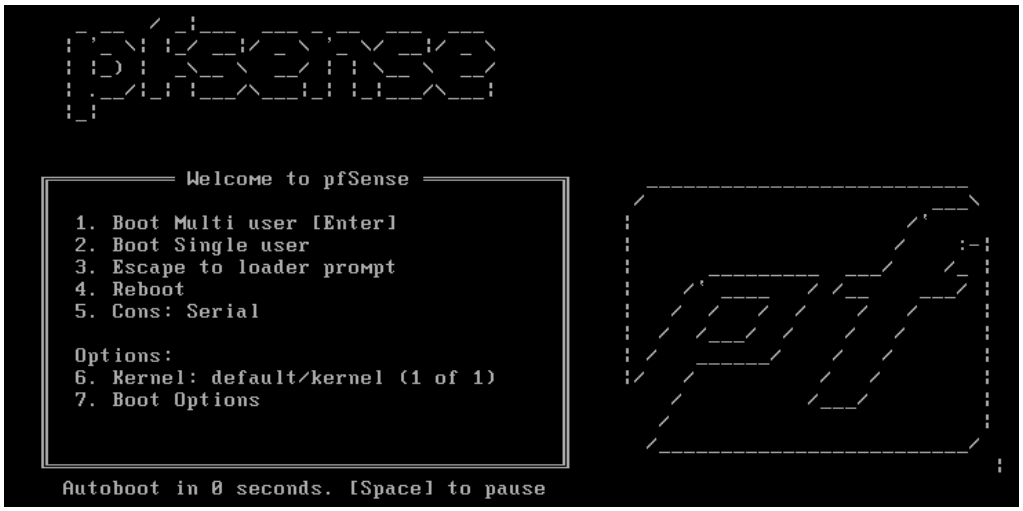
Installation de base de pfSense *(sur une VM)*

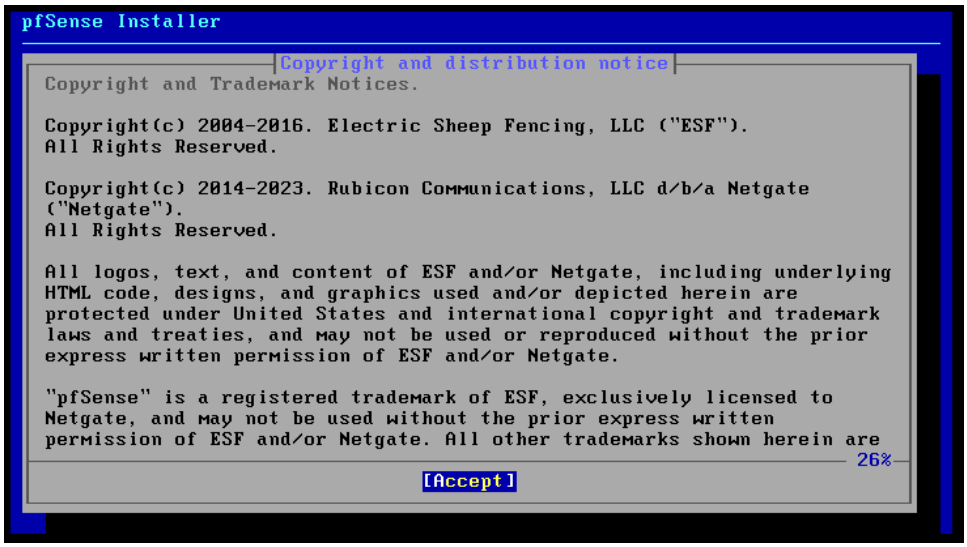
Au niveau de la configuration de la VM pfsense, elle est assez légère *(réalisé sous VMWare Workstation)* :

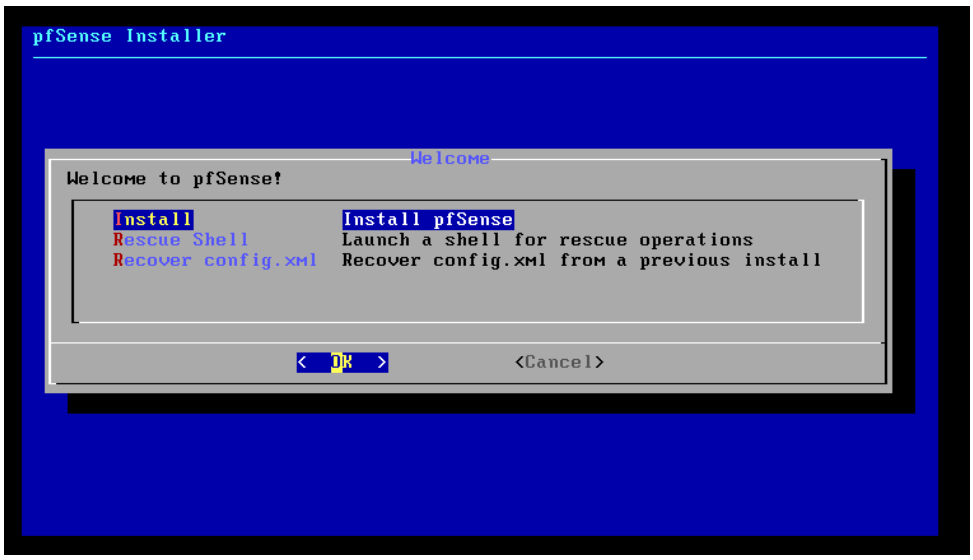


En revanche, pfsense agissant comme un routeur, **il est impératif d'avoir au moins 2 cartes réseaux, sur 2 réseaux différents** : le réseau WAN *(Internet)* et le réseau LAN *(local)*. **La première carte** va correspondre à l'interface WAN de pfsense, **elle a été positionnée en NAT** et **la seconde** sera l'interface LAN, elle est ici positionnée dans un **réseau privé** *(vmnet3)*.Nous utiliserons également une 3eme carte qui servira de DMZ.

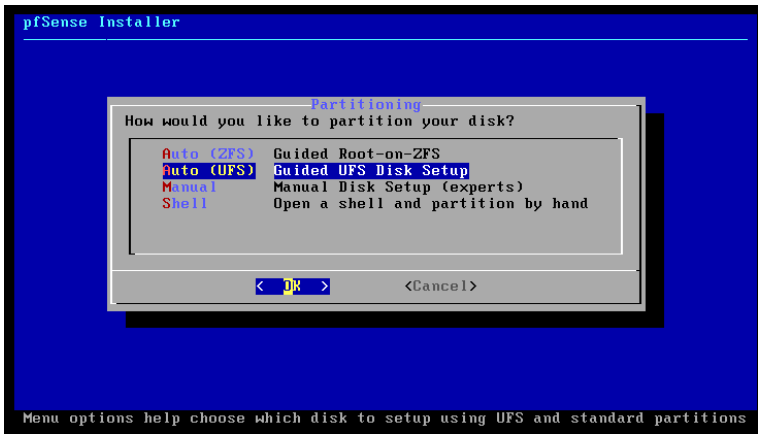
Commençons tout de suite par **installer pfsense**. Après avoir insérer l'ISO de pfsense dans VM dédiée, vous pouvez démarrer la machine. Le setup va démarrer automatiquement après quelques secondes .





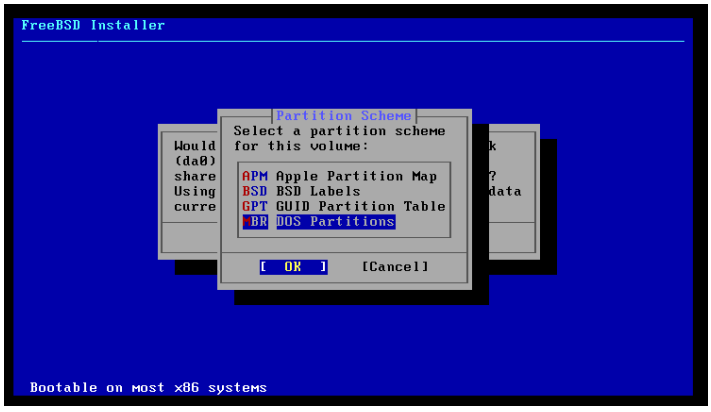


Le setup va vous demander de **partitionner le disque** de stockage de la machine. Avec les touches fléchées de votre clavier, allez sur **« Auto (UFS) » et appuyez sur Entrée**.

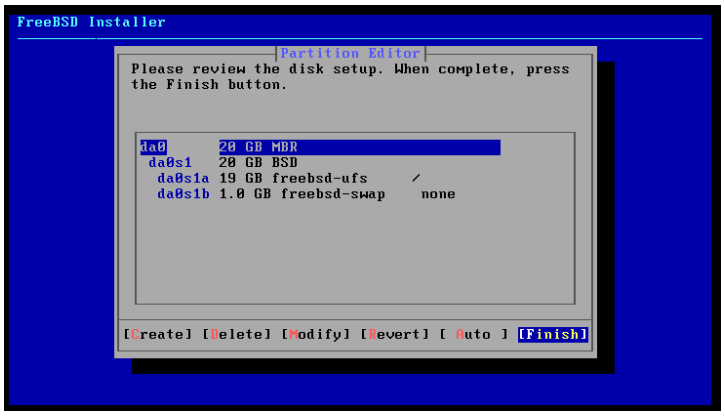


Vous pouvez confirmer que vous voulez utiliser le disque entier pour installer le système d'exploitation, pour cela, placez vous sur **« Entire Disk » et appuyez sur Entrée**.

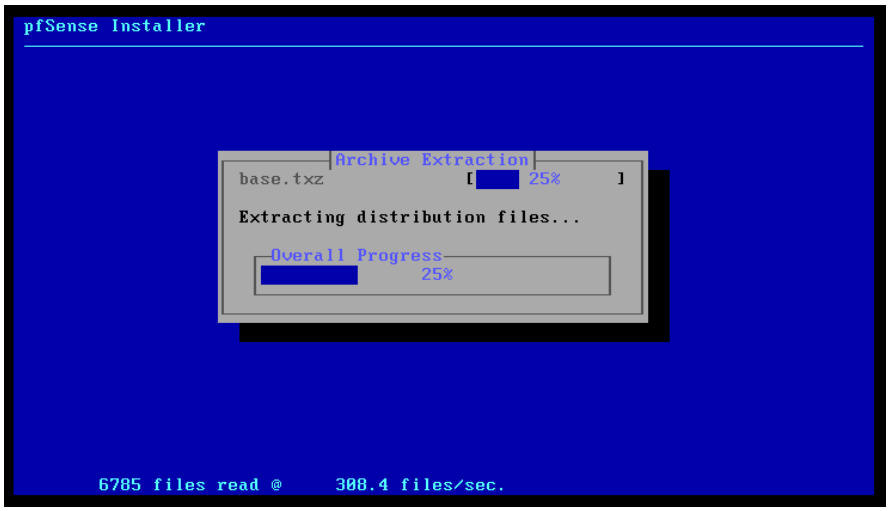
Ici je reste simplement sur **« MBR DOS Partitions » et appuyez sur Entrée** pour valider.

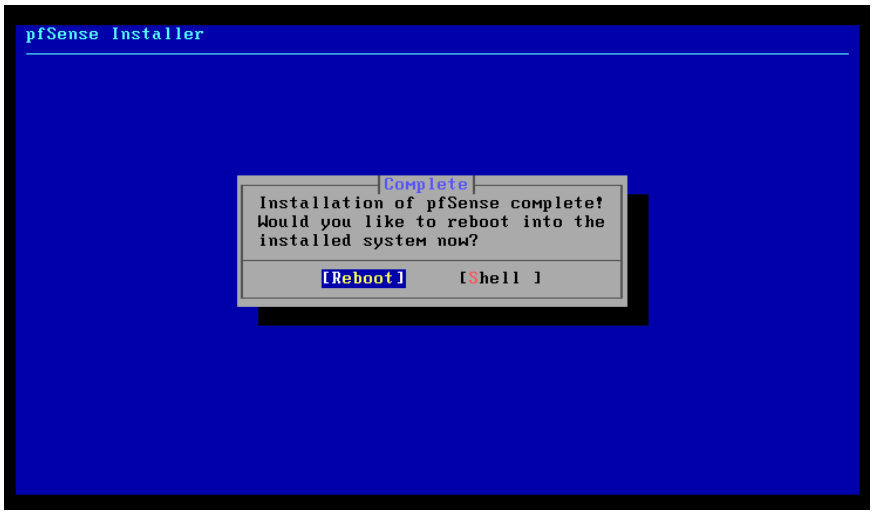


L'installer propose un découpage sur le disque 0 *(nommé ici da0)*, je n'ai pas besoin de modifier la proposition faites, placez vous sur **« Finish »** et appuyez sur Entrée.

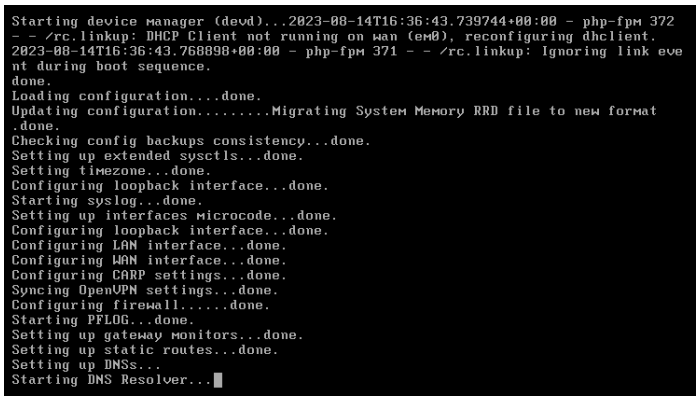


Un ultime avertissement sur le fait que le disque sera effacé pour faire face au système d'exploitation de pfsense. Placez vous sur **« Commit »** et appuyez sur Entrée.

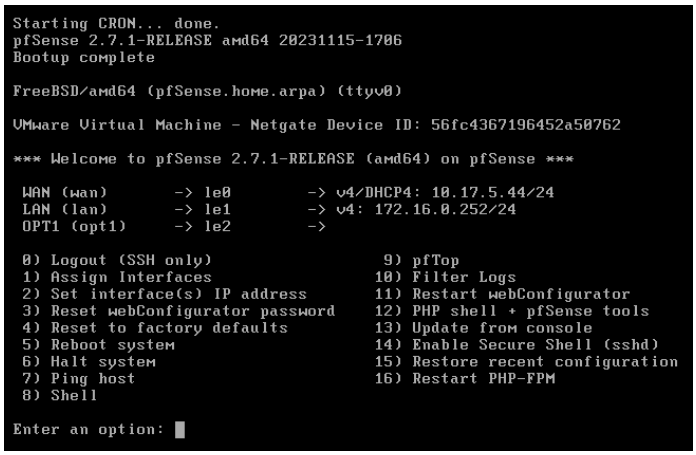




Au démarrage, **pfsense va se lancer, tester et configurer les services dont il a besoin**.

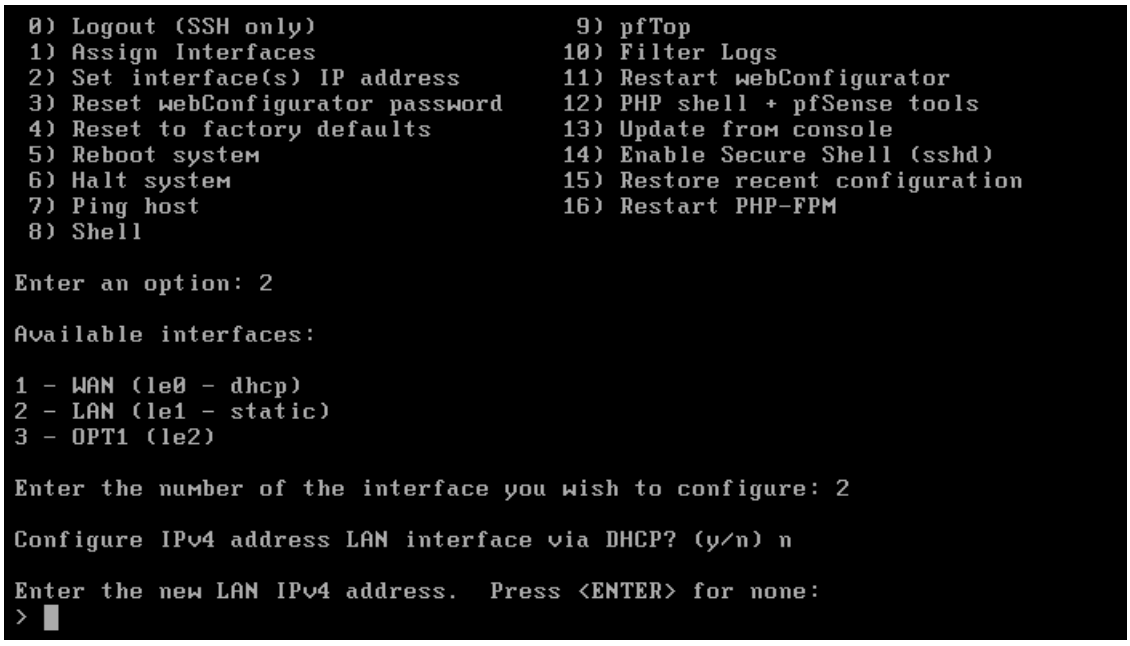


Une fois que le démarrage est finalisé, vous aurez la vue suivante sur la machine :

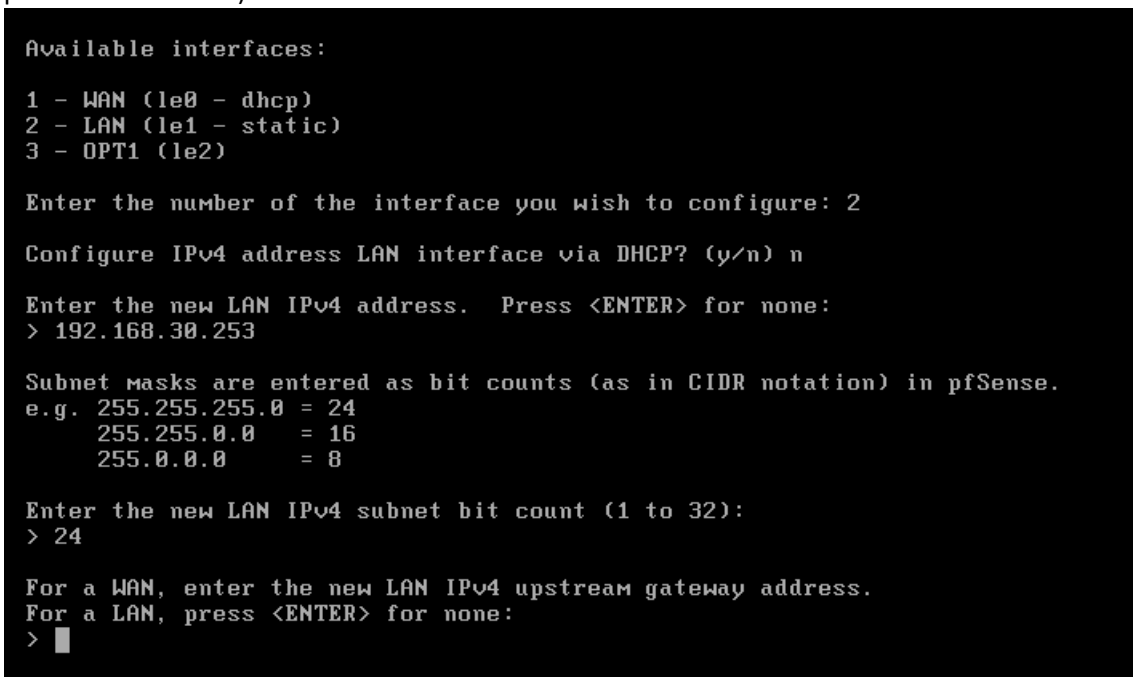


Configuration des Interfaces

L'interface « WAN » obtient une adresse IP grâce au DHCP de l'école. Nous voulons changer l'adresse IP « LAN » pour quelle corresponde a notre réseau local. Donc nous allons tapez 2 puis encore 2 pour choisir l'interface LAN.



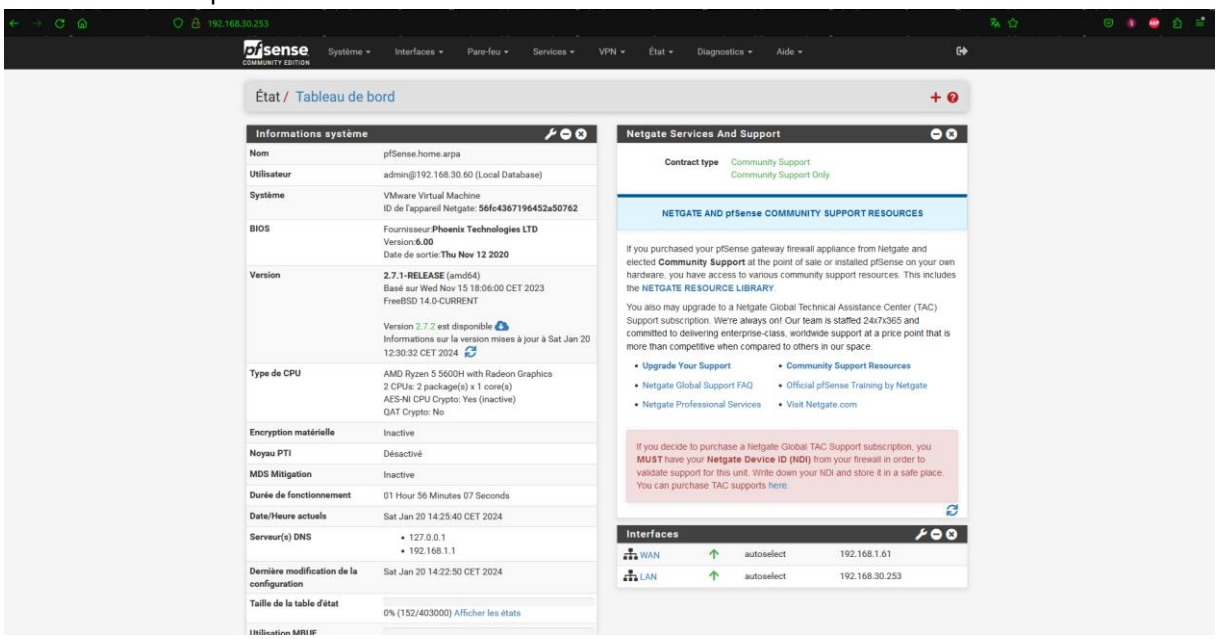
Nous ne voulons pas que l'adresse soit celle donnée par le DHCP, donc nous mettons "n" (pour non) et nous saisissons l'adresse que nous souhaitons pour la suite. Ensuite, le masque (en CIDR, donc 24 pour 255.255.255.0).



Pour la suite dans la configuration de l'interface nous répondons non partout ou juste entrer

```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 LAN address has been set to 192.168.30.253/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://192.168.30.253/

Press <ENTER> to continue.
```

Pour accéder à l'interface graphique de pfSense, il vous suffit d'entrer l'adresse IP de la carte LAN dans le navigateur de votre choix. N'oubliez pas d'aligner l'adresse IP de votre machine physique sur le même réseau que celui de la carte LAN.



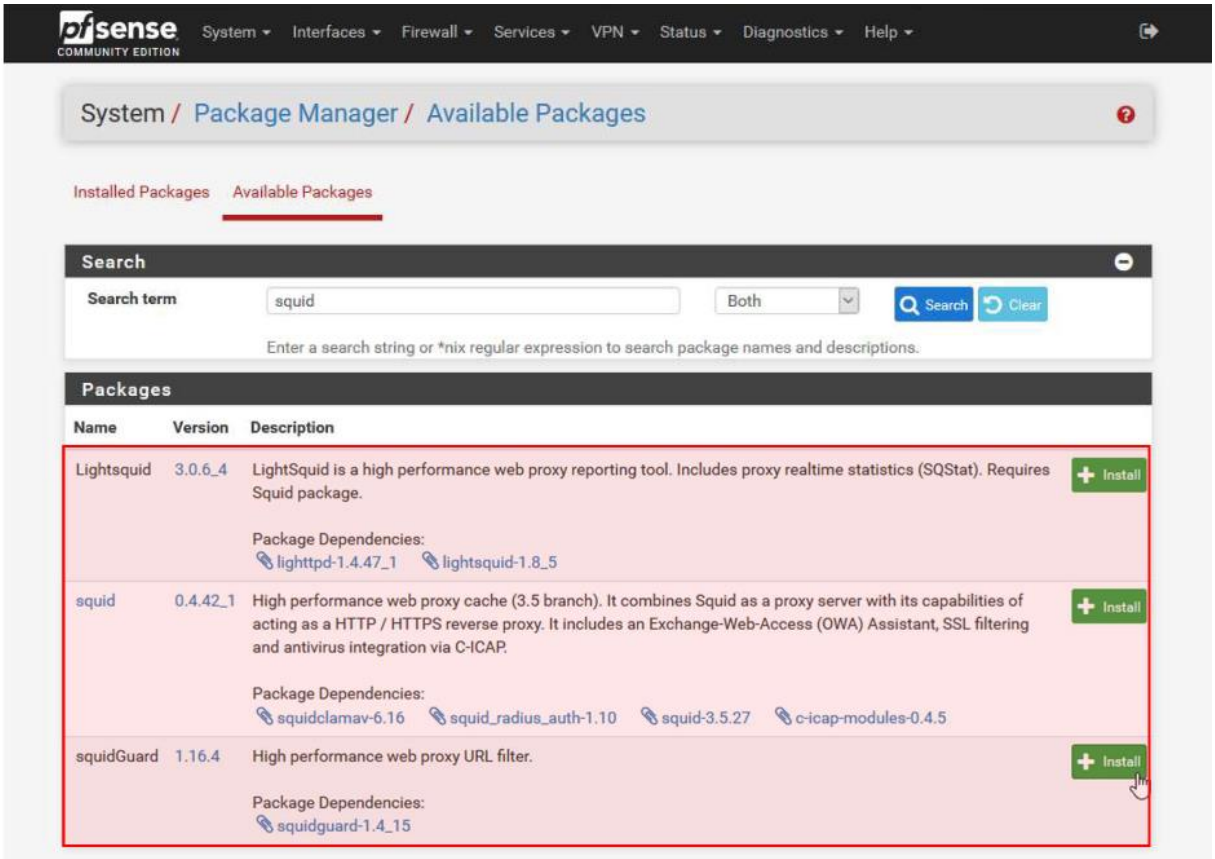
Mise en place de liste de blockage

Nous allons voir comment mettre en place une liste de blocage qui permet de refuser l'accès à certains sites web, en fonction des catégories telles que le téléchargement illégal, les sites d'achats, les sites pour adultes, etc.

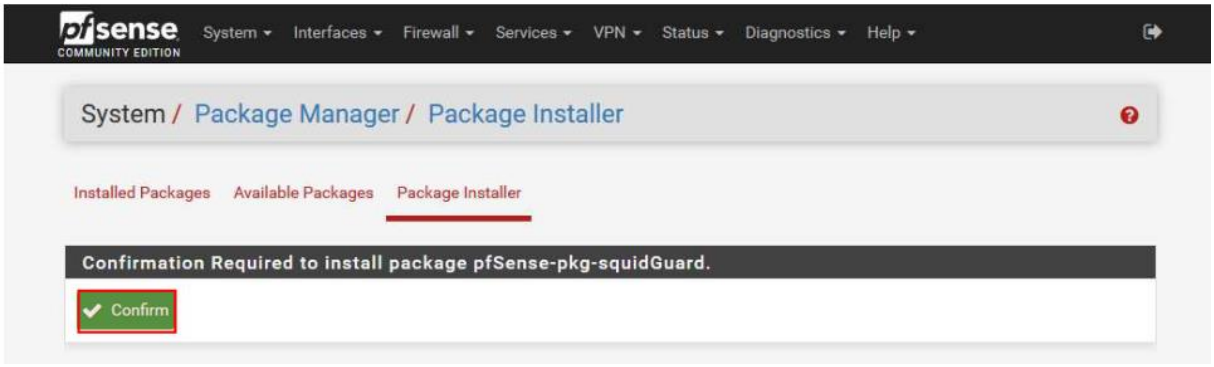
Pour cela, nous pouvons la créer ou utiliser une déjà prête élaborée par d'autres personnes ayant recensé ces sites. Afin de mettre en place ces listes de blocage, nous devons installer plusieurs packages. Sans ces paquets, il nous sera impossible d'imposer des restrictions grâce à ces listes.

Dans mon cas, je vais mettre en place la blacklist de Toulouse. Pour ce faire, nous devons installer les paquets en accédant à "Système / Gestionnaire de paquets".

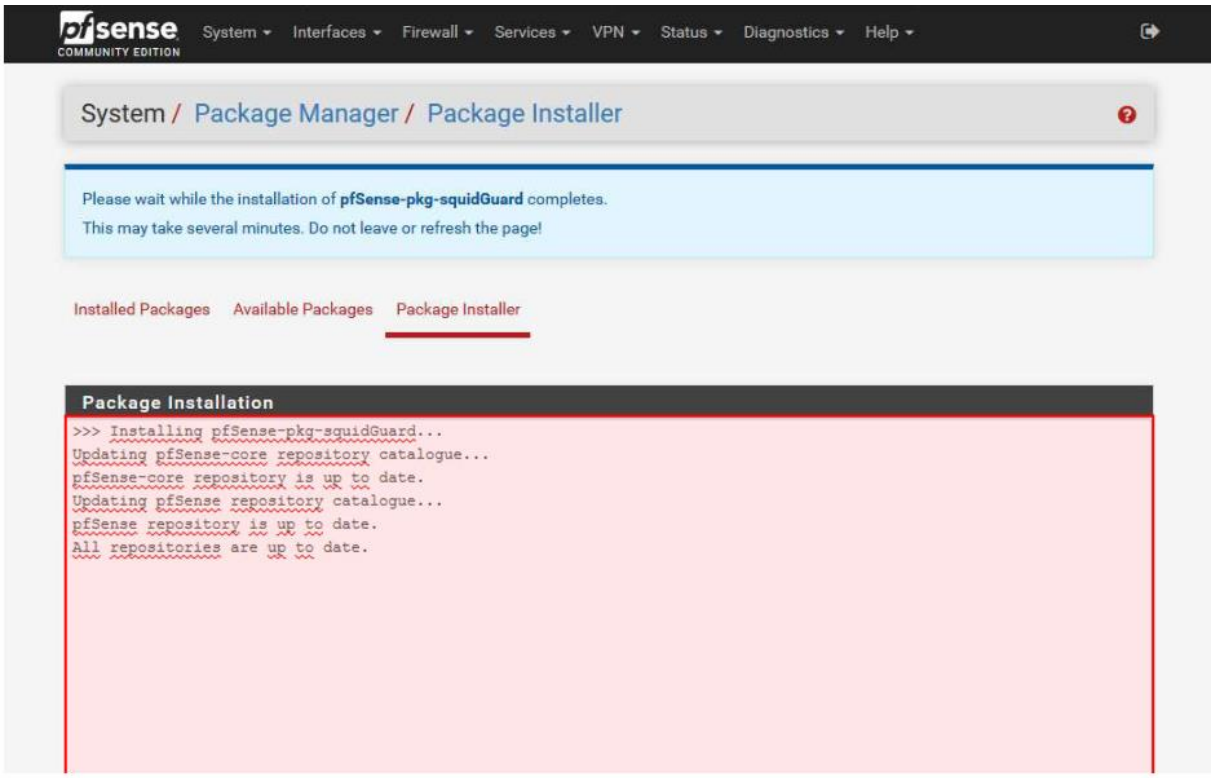
Une fois dans le gestionnaire, nous devons accéder à "Available Packages" et installer les paquets Squid, SquidGuard et Lightsquid. Nous pouvons rechercher ces paquets en utilisant le terme "squid". En l'absence de l'un de ces paquets, il nous sera impossible de mettre en place notre filtrage par rapport à nos sites web.



Pour chaque installation une demande de confirmation d'installation nous ai demander.

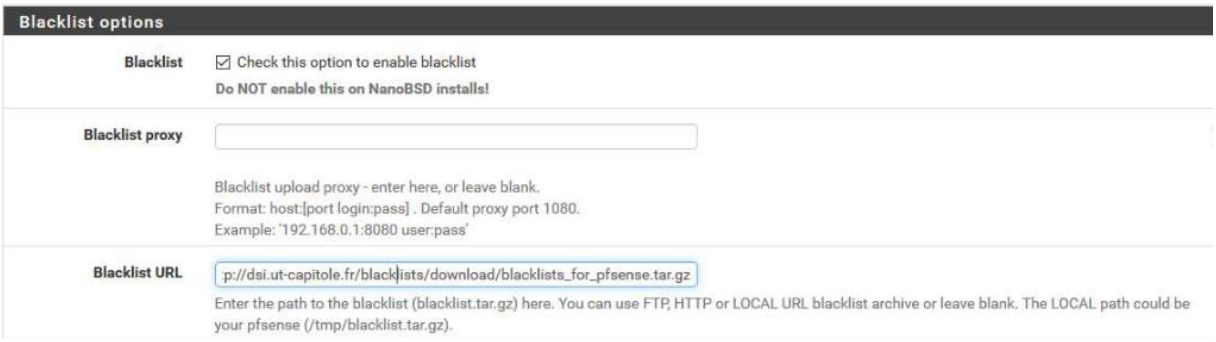


Pour chaque installation, nous avons l'avancement, il est important de ne pas fermer la page, si non l'installation échou.



Une fois les paquets installer, nous allons pouvoir installer notre blacklist, pour cela, nous devons aller dans "Services / SquidGuard Proxy Filter".

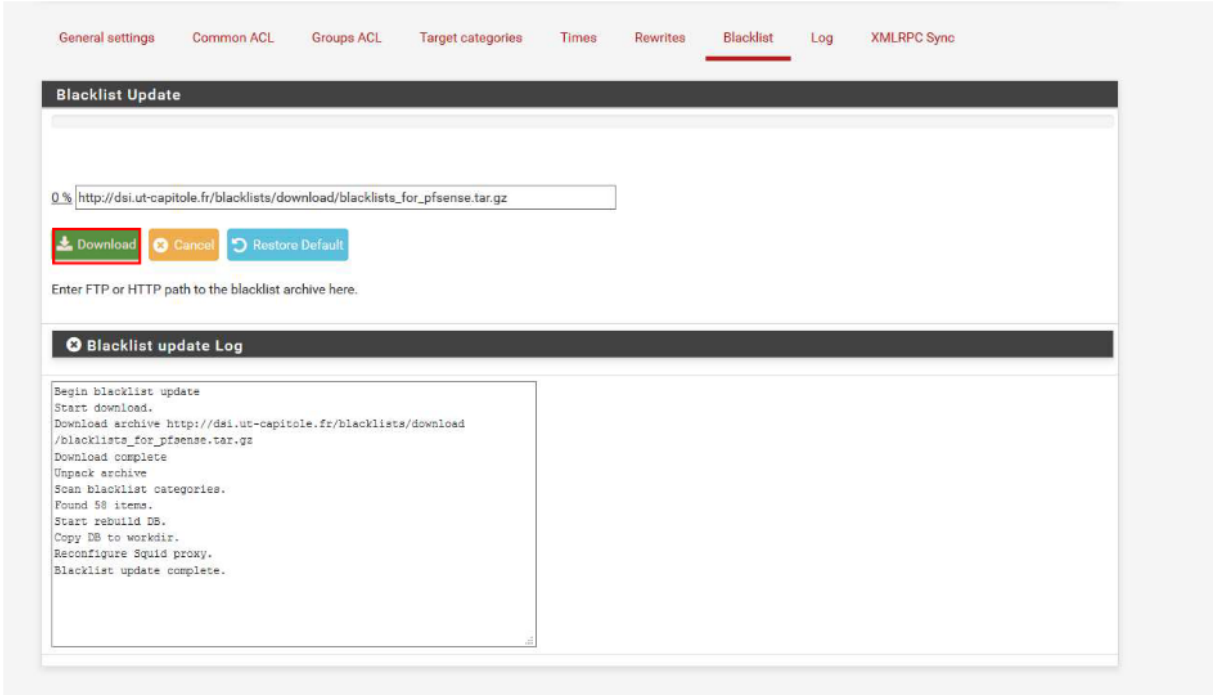
Nous devons activer la blacklist et nous devons mettre le lien de notre blackliste, ce qui nous permet de la mettre à jour facilement en cas de mise à jour de celle-ci



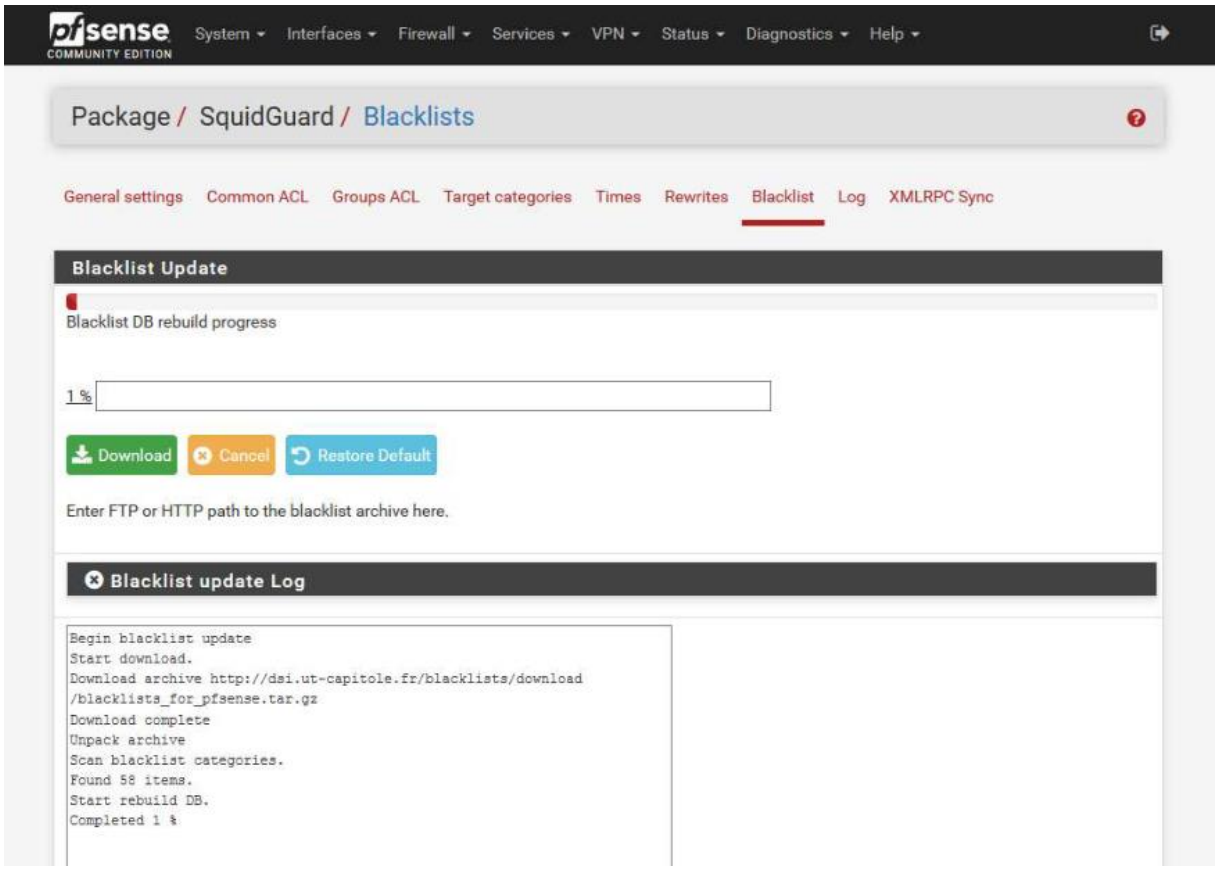
Lien de la blacklist : http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz

Ce n'est pas la seul blackliste existante, mais elle comprend beaucoup de site.

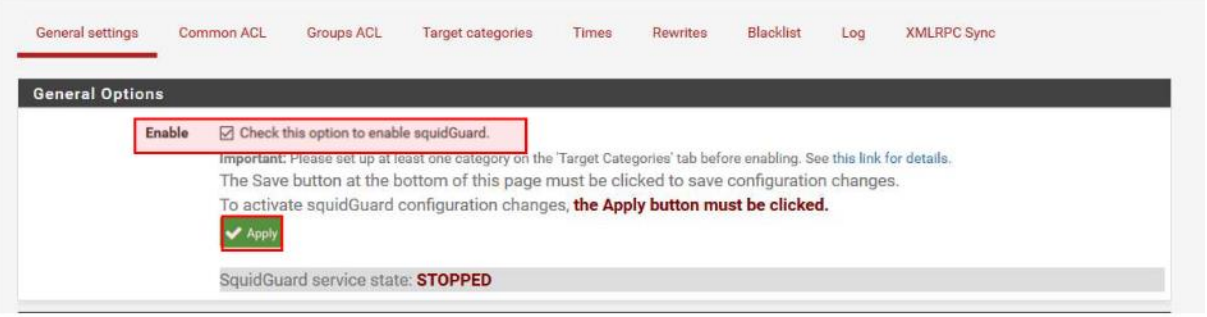
Maintenant, nous devons nous rendre dans "Système / Géneral / Blacklist", puis la télécharger



Un avancement du téléchargement est fait et la base de données ajoute les éléments de la liste



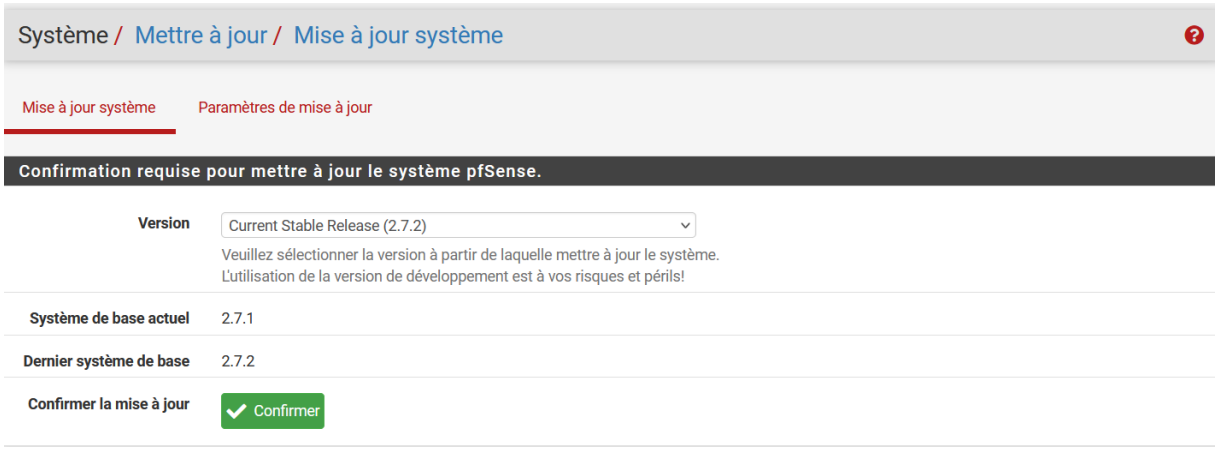
Une fois notre blackliste télécharger et ajouter, nous devons nous rendre dans "Services / SquidGuard Proxy Filter" et activer le service SquidGuard si il ne l'est pas



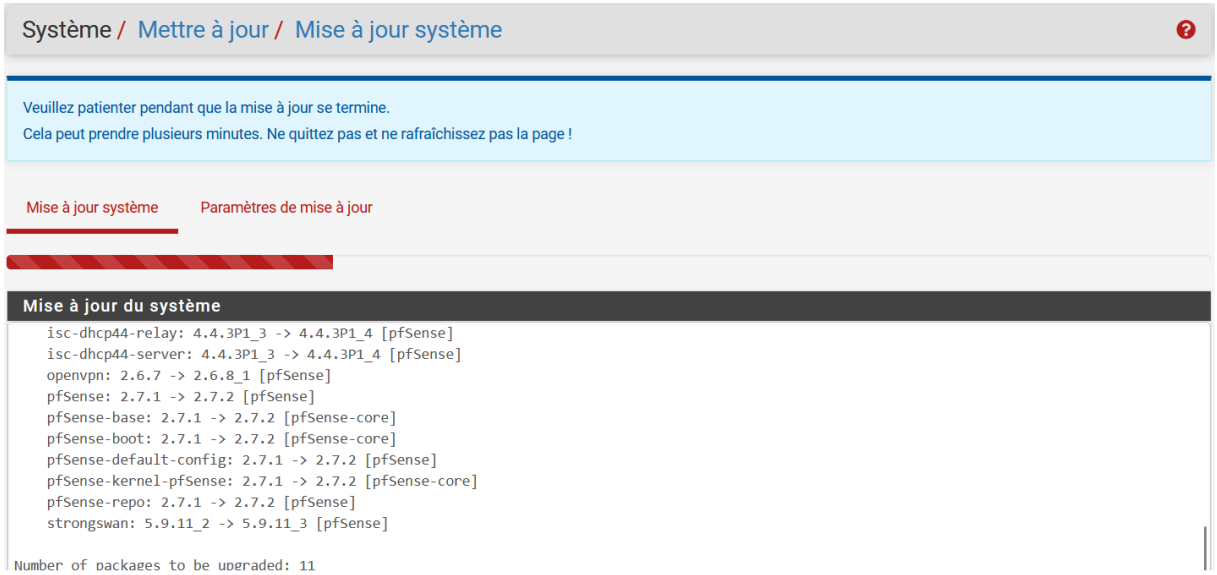
On verifie que notre paquet squidGuard soit bien actif

Mise à jour Pfsense

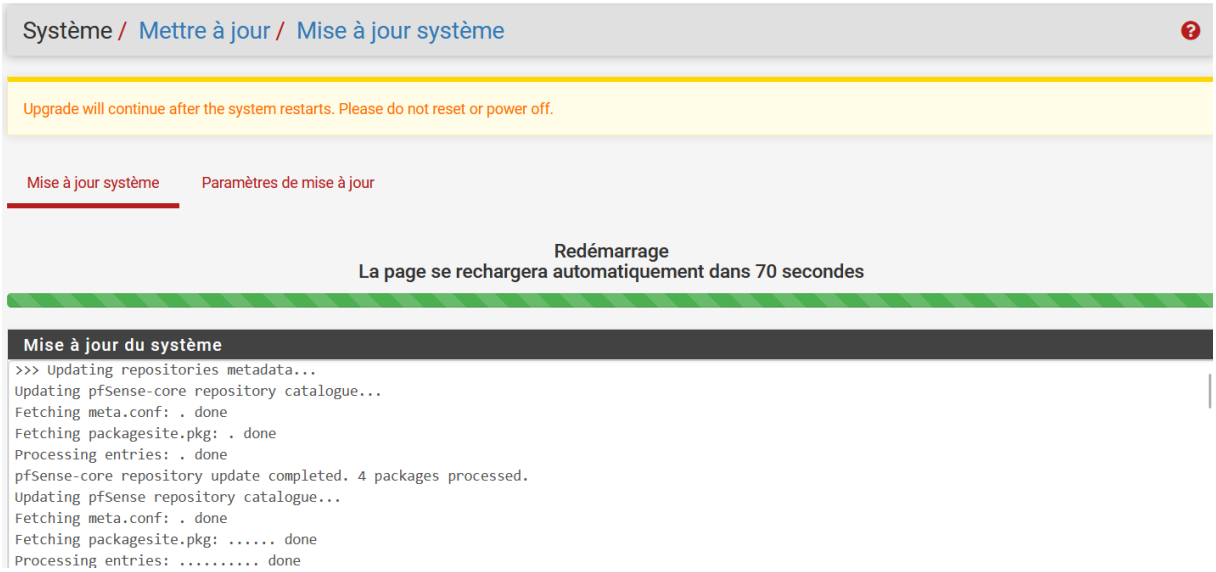
Les mises à jour sont importantes, tant au niveau des fonctionnalités que de la sécurité. La mise à jour de PFSENSE est facile à effectuer. Pour cela, nous devons nous connecter au panneau de contrôle, et sur le tableau de bord, nous trouvons la version actuelle. Comme on peut le constater, la version 2.7.2 est disponible, et nous pouvons donc la mettre à jour en cliquant sur le bouton 'Confirmer'



Puis l'installation se fait, mais on ne doit ni quitter ni fermer cette page car la mise à jour va s'arrêter et risque de planter PFSENSE.



Nous avons un message qui nous informe que la mise à jour est fini et que PFSENSE doit redémarrer.



La mise à jour à bien été faite.