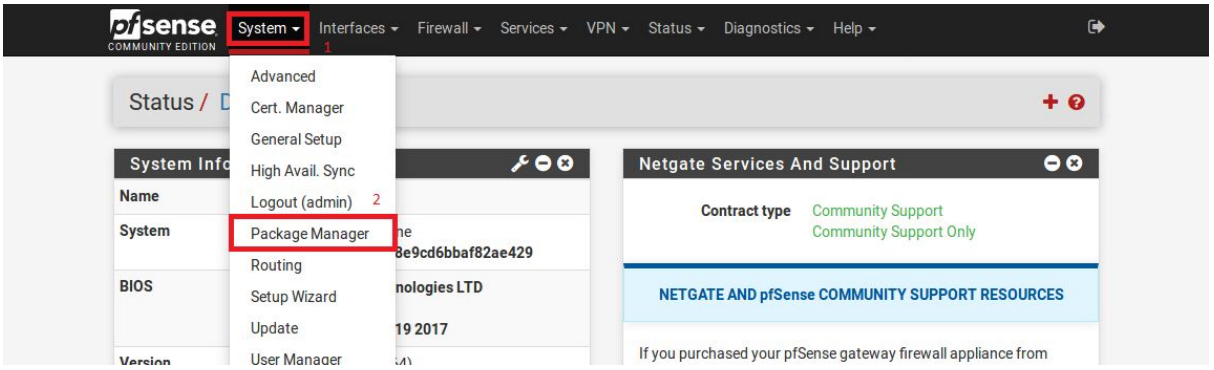
Situation professionnelle en PPE 3 : Filtrage des accès internet vers internet via un PROXY

Documentation n°2 : Journalisation des connexions utilisateurs.

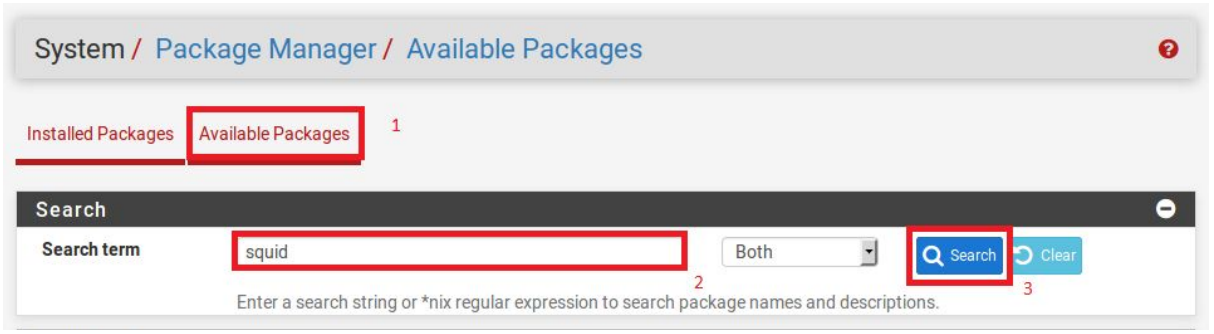
Auteur : Guillaume Orlando
Date : 14/11/2017

I. Mise en place du filtrage HTTP :

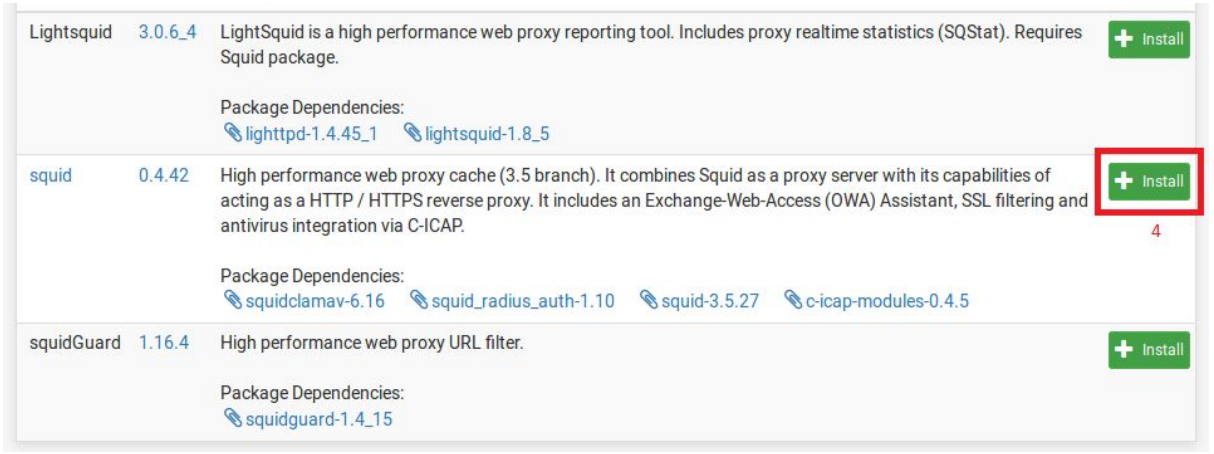
Si ce n'est pas encore fait, le paquet SQUID doit être installé sur la machine via l'utilitaire d'extensions Pfsense. Pour ajouter des fonctionnalités au travers de nouveaux paquets, il faudra se rendre dans le gestionnaire de paquets :



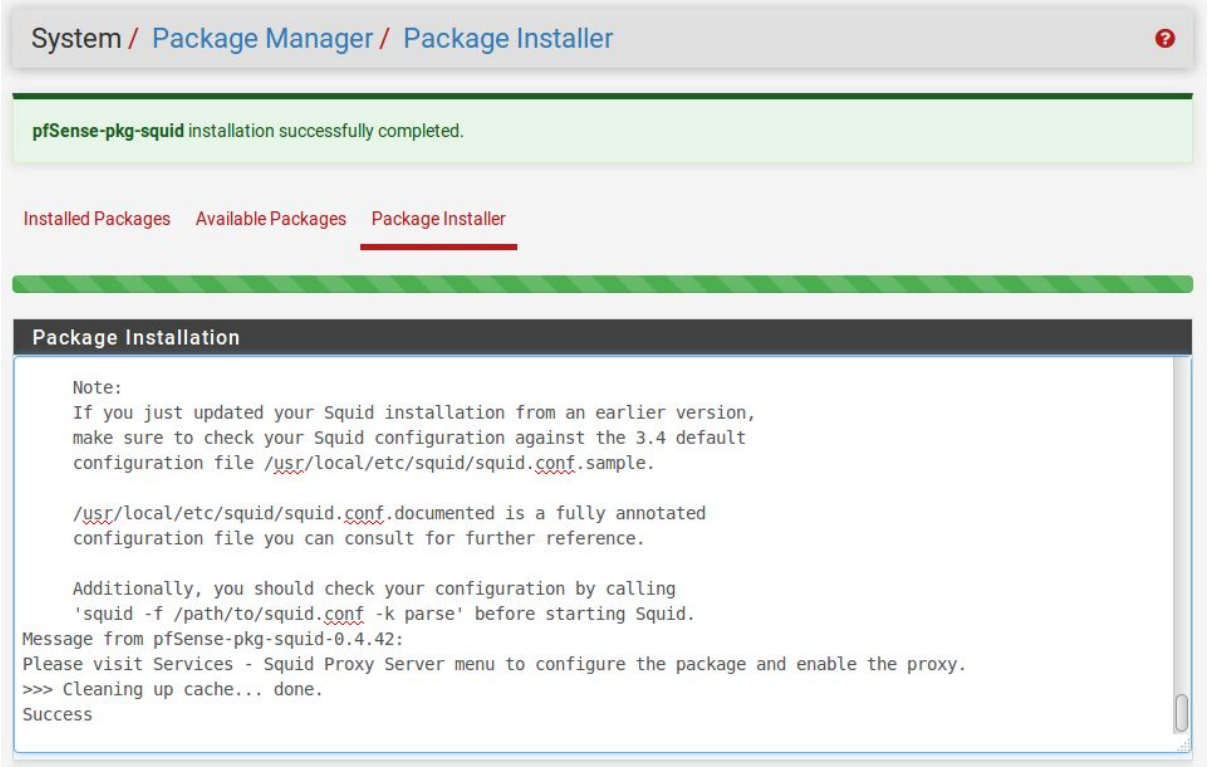
Puis sous l'onglet "Availables packages", nous allons pouvoir chercher de nouveaux paquets à installer. Dans notre cas, nous effectuons une recherche avec le terme "squid" :



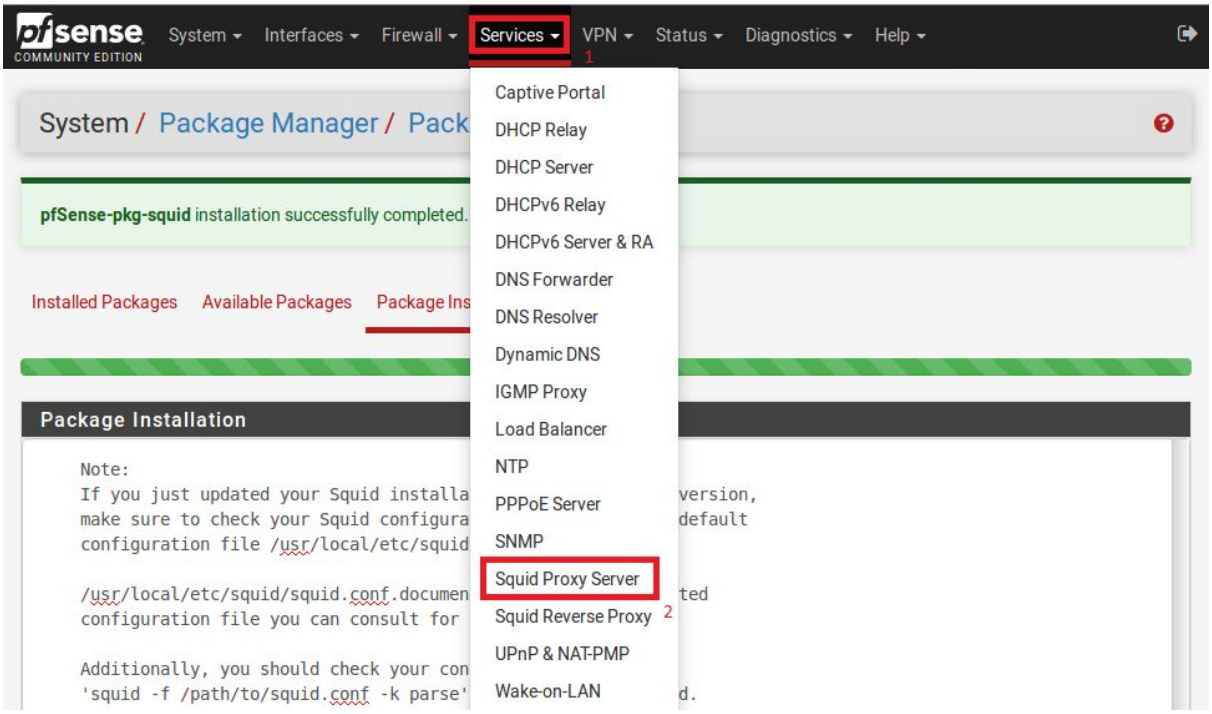
Nous installons le paquet suivant :



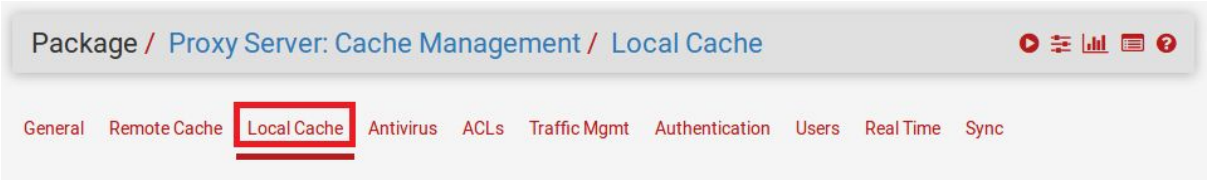
Après quelques temps d'attente, l'installation va se terminer d'elle même :



Nous allons maintenant entamer la configuration du proxy Squid pour filtrer les connexion sortantes utilisants le protocoles HTTP. la configuration du service se fait dans l'onglet "Service" puis sous "Squid proxy Server" :



Avant même de configurer le filtrage à proprement parlé, il va falloir configurer le cache local de la machine. Ce cache va contenir les logs utilisateurs. les informations sont situés dans le sous-onglet "Local Cache" :



Les options de configurations suivantes sont utilisés dans le contexte actuel :

Squid Cache General Settings

Cache Replacement Policy
Heap LFUDA
The cache replacement policy decides which objects will remain in cache and which objects are replaced to create space for the new objects. Default: heap LFUDA

Low-Water Mark in %
90
The low-water mark for AUFS/UFS/diskd cache object eviction by the cache_replacement_policy algorithm.

High-Water Mark in %
95
The high-water mark for AUFS/UFS/diskd cache object eviction by the cache_replacement_policy algorithm.

Do Not Cache
Enter domain(s) and/or IP address(es) that should never be cached. Put each entry on a separate line.

Enable Offline Mode
Enable this option and the proxy server will never try to validate cached objects.
Offline mode gives access to more cached information than normally allowed (e.g., expired cached versions where the origin server should have been contacted otherwise).

External Cache Managers
Enter the IPs for the external Cache Managers to be granted access to this proxy. Separate entries by semi-colons (;)

Squid Hard Disk Cache Settings

Hard Disk Cache Size
2000
Amount of disk space (in megabytes) to use for cached objects.

Hard Disk Cache System
ufs
This specifies the kind of storage system to use.

Clear Disk Cache NOW
Hard Disk Cache is automatically managed by swapstate_check.php script which is scheduled to run daily via cron.
If you wish to clear cache **immediately,** click this button **once**: Clear Disk Cache NOW

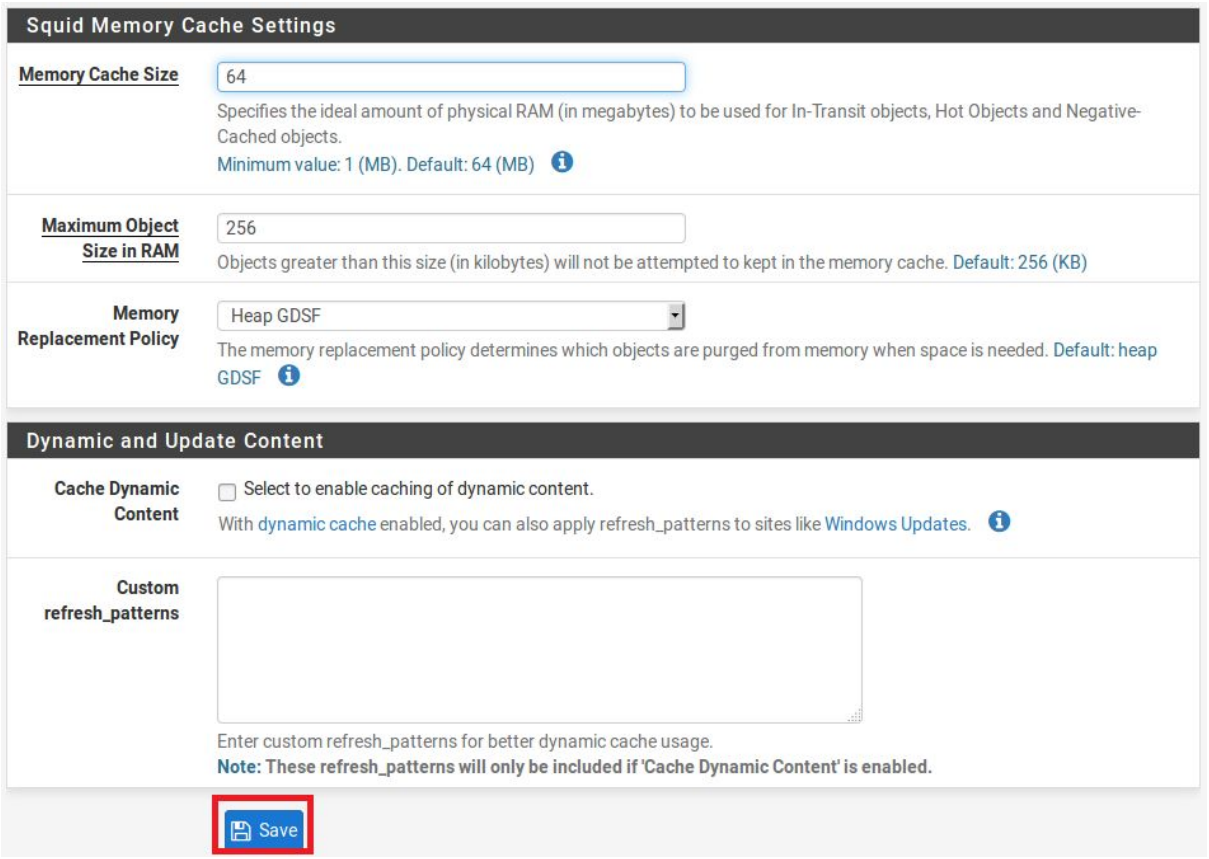
Level 1 Directories
16
Specifies the number of Level 1 directories for the hard disk cache.

Hard Disk Cache Location
/var/squid/cache
This is the directory where the cache will be stored. Default: /var/squid/cache

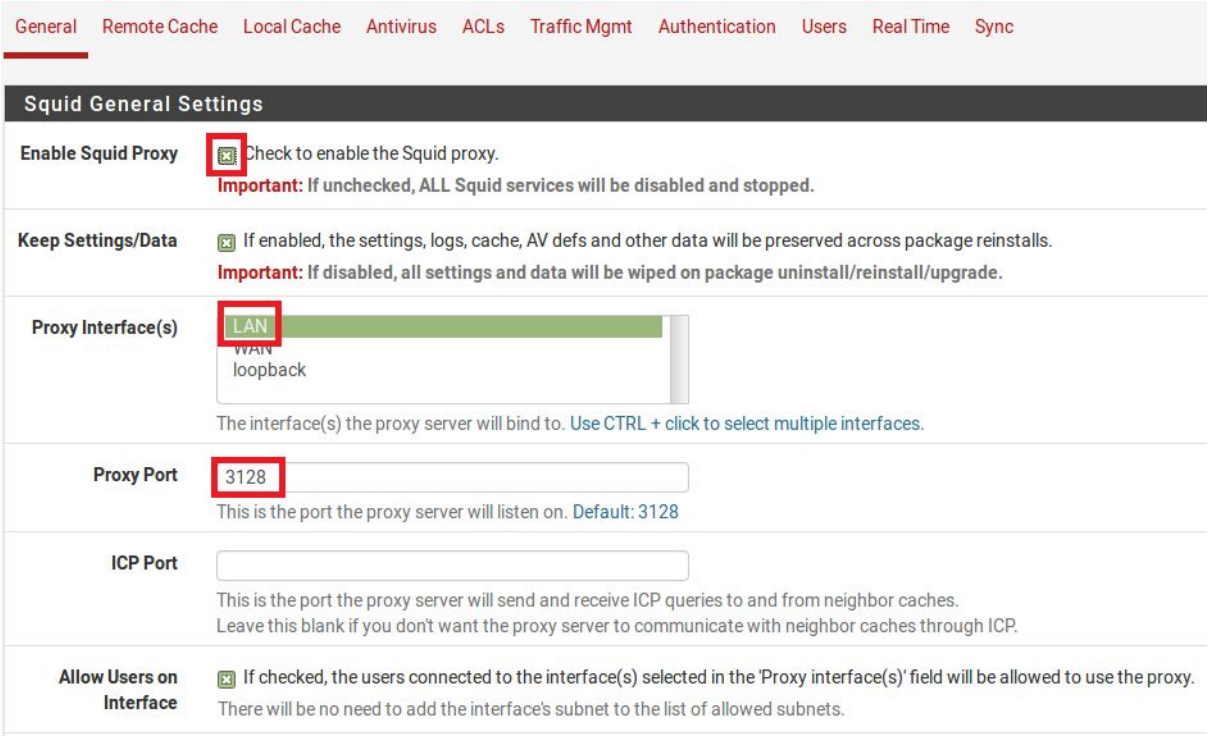
Minimum Object Size
0
Objects smaller than the size specified (in kilobytes) will not be saved on disk. Default: 0 (meaning there is no minimum)

Maximum Object Size
4
Objects larger than the size specified (in megabytes) will not be saved on disk. Default: 4 (MB)

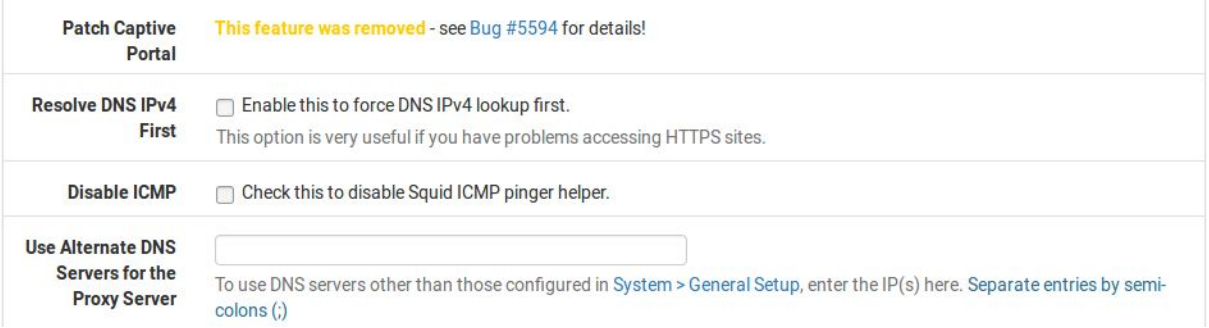
Attention à bien modifier la taille attribuée au cache. Ici, puisqu'il s'agit d'un prototype, nous allons attribuer 2Go. Les autres options peuvent rester tels quels. Nous terminons en sauvegardant les modifications :



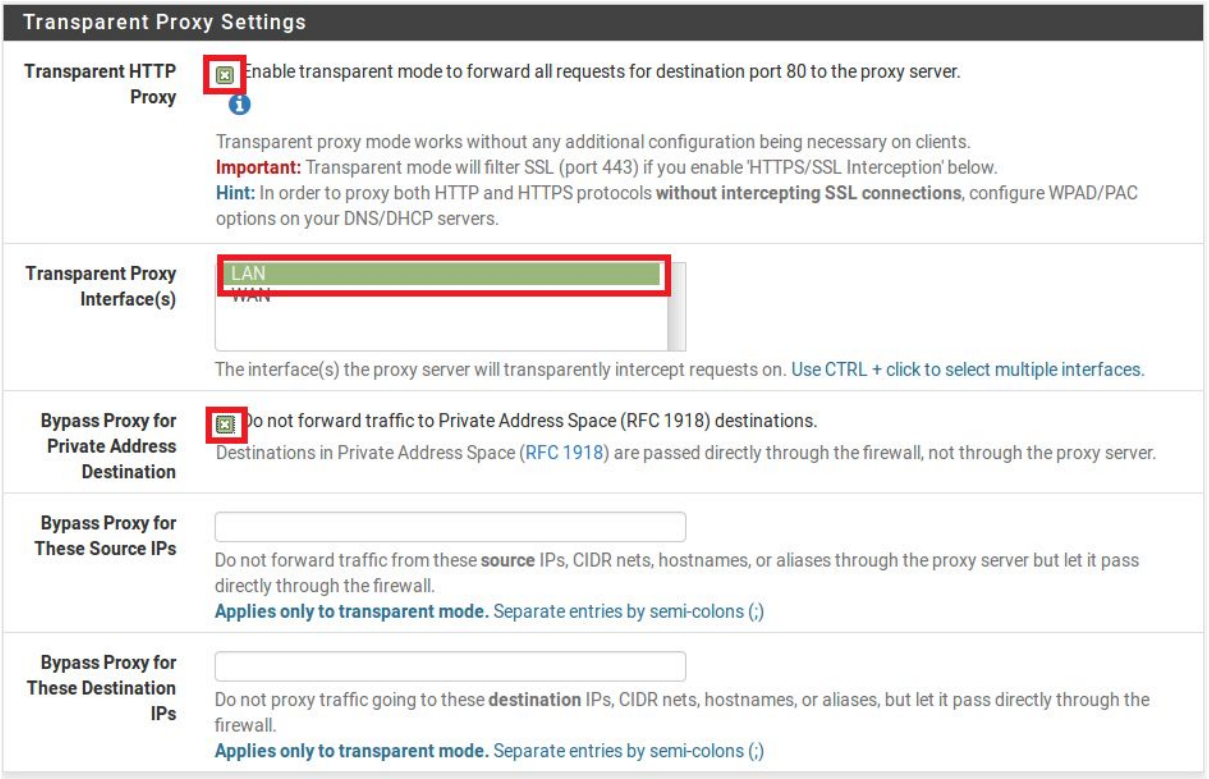
Nous pouvons maintenant revenir sur l'espace de configuration général pour activer l'interception HTTP. La configuration générale est la suivante :



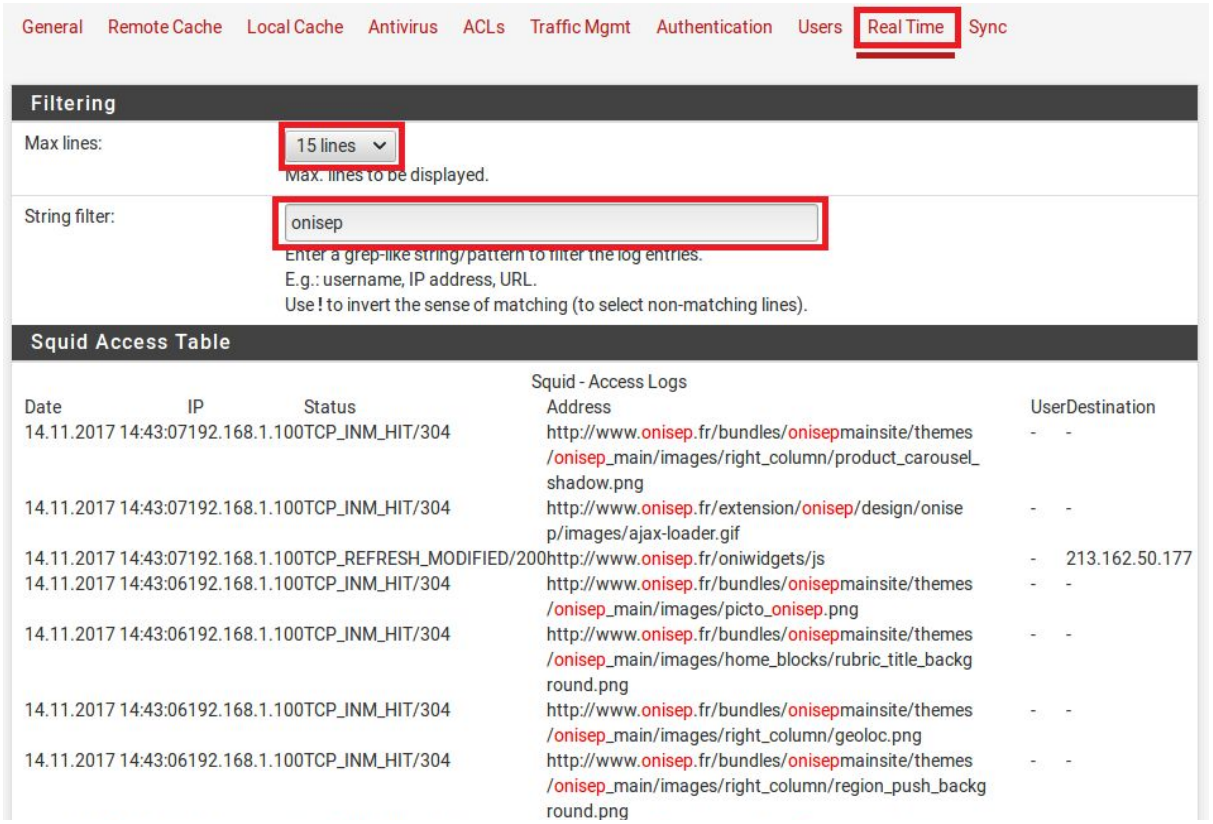
Commençons par activer le proxy Squid en cochant la case “Enabled Squid Proxy”. L’interface sélectionné sera la LAN, puisque le filtrage aura lieu sur le trafic sortant du LAN en direction du WAN. Attention aussi à ne pas modifier le port par défaut de SQUID, sans quoi beaucoups d’applications utilisateurs seront à reconfigurer.



Les options permettant de configurer l'interception du trafic HTTP se fait via les options “Transparent proxy Settings”. nous activons le proxy transparent et redirigeons le trafic entrant. L’interface d’écoute reste ici la LAN :

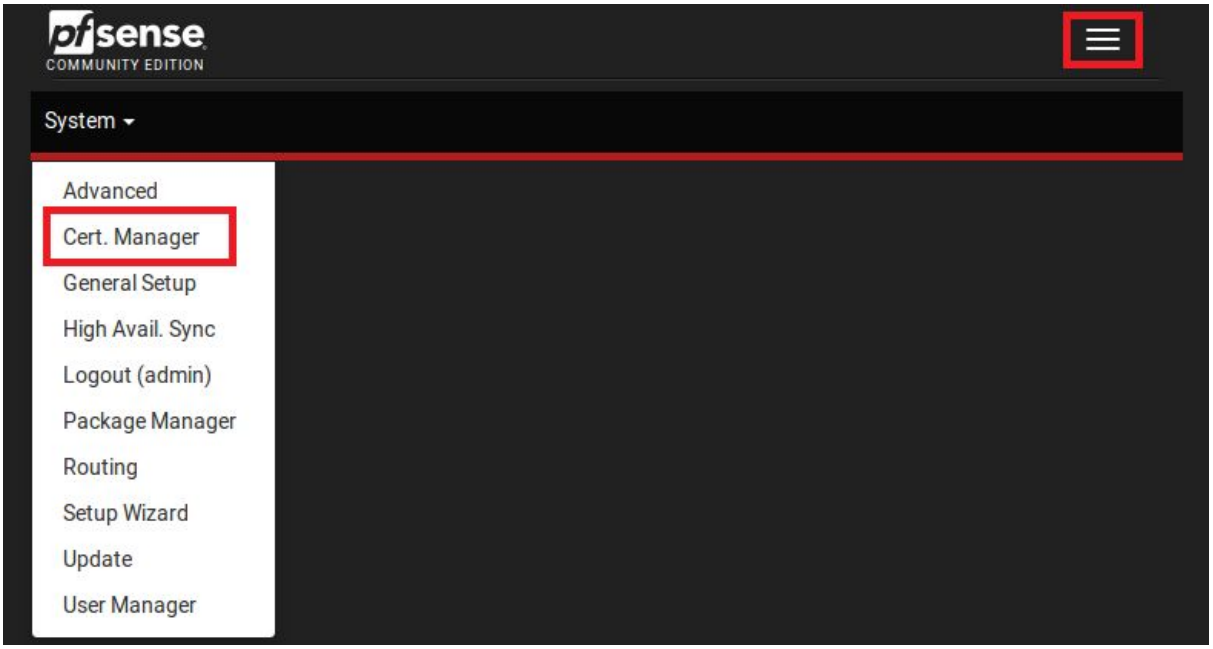


L'interception HTTP est maintenant terminée. Nous pouvons sauvegarder via le bouton correspondant, tout en bas de la page.
Pour tester que tout est effectif, rendons-nous dans l’onglet “Real-Time” du service squid. Cet onglet nous permet de voir en temps-réel les requêtes des utilisateurs du LAN. Nous devrions être capable d’observer en clair les connexions HTTP. Le test sera fait avec le site de l’onisep sur notre machine client (il n’utilise pas le protocole HTTPS).

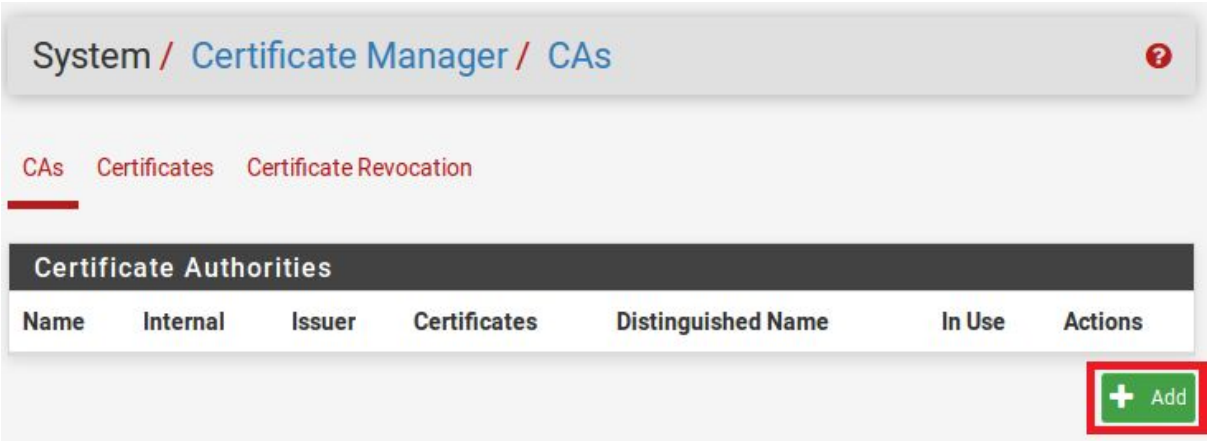


II. Mise en place du filtrage HTTPS :

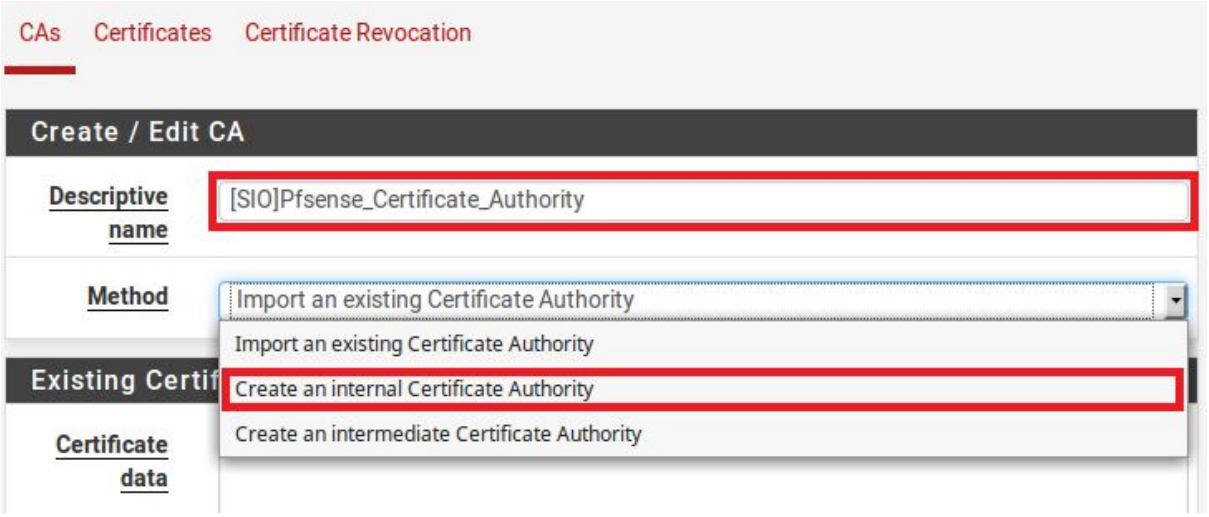
Pour filtrer les requêtes HTTPS, nous allons commencer par créer un certificat SSL sur la machine Pfsense et installer le certificat sur l'interface et les postes du LAN concernés.
Commençons par créer une autorité de certification pour notre Pfsense.
Cela va servir aux utilisateurs du LAN, de façon à confirmer l'identité du routeur Pfsense.
Pour créer l'autorité de certification, rendez-vous dans l'onglet "Cert-Manager" dans le menu "System" :



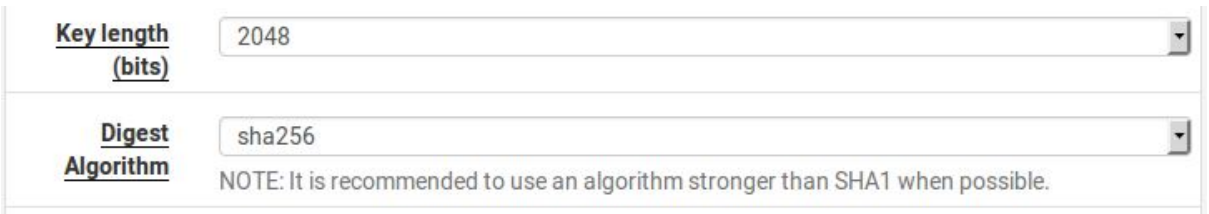
La liste des certificats installés ou créés sur la machine devrait apparaître. Si la machine est vierge, la liste devrait être vide. Nous ajoutons une autorité de certification avec le bouton “Add” :



La première des étapes va être de nommer correctement l’autorité de certification. Attention à renseigner un nom explicite. L’importance des toutes la saisie d’informations qui va suivre est primordiale. En effet, grâce à ces informations, les utilisateurs vont pouvoir déterminer s’ils sont filtrés par le bon proxy sur le bon réseau,et non par une tierce personne se faisant passer pour le proxy. Enfin, puisque nous souhaitons créer une nouvelle autorité de certification, il faudra l’indiquer :

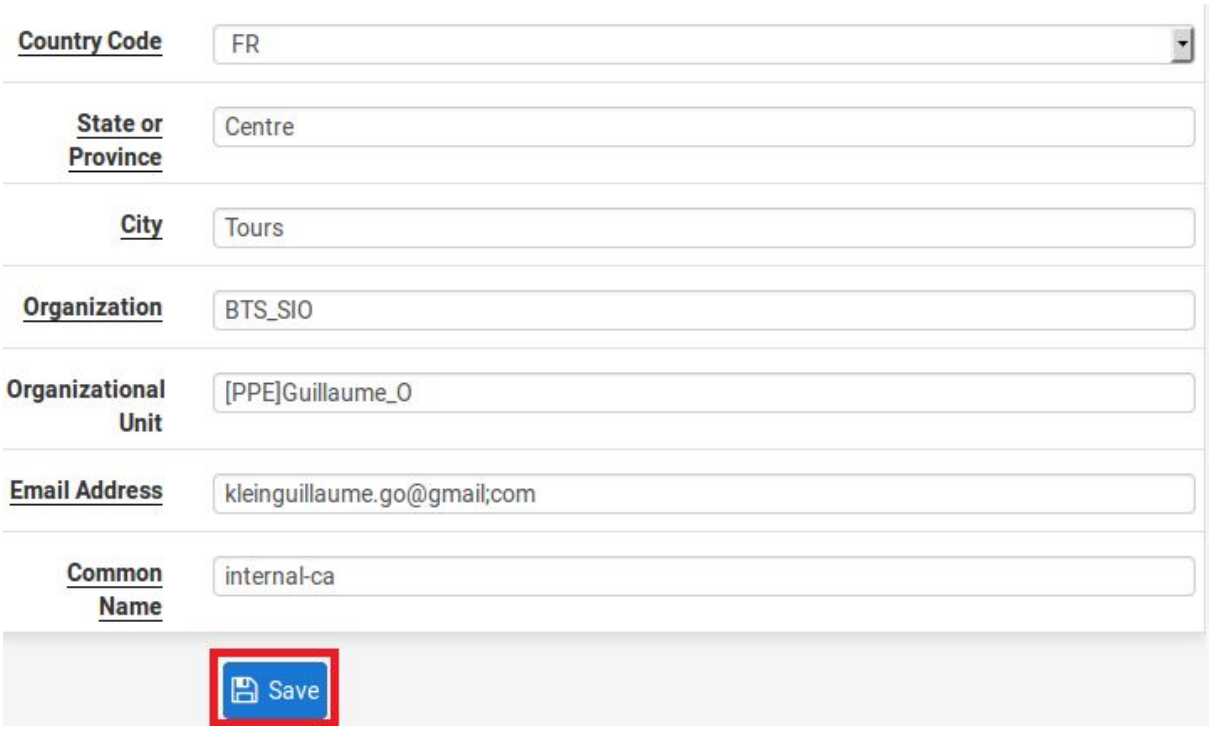


De nouvelles options vont s’offrir à nous. Encore une fois, la plus grande attention est requise pour remplir les champs. Les premiers choix vont concerner le choix des clés. Plus la longueur de la clé est élevée, plus le flux sera sécurisé, mais plus la machine va consommer de ressources. Nous utilisons ici une longueur intermédiaire de 2048 bits. Le choix de la fonction de hachage est également primordiale, puisque certaines fonctions de hachages sont aujourd’hui complètement obsolète. Nous utiliserons ici l’algorithme de hachage SHA-512 :

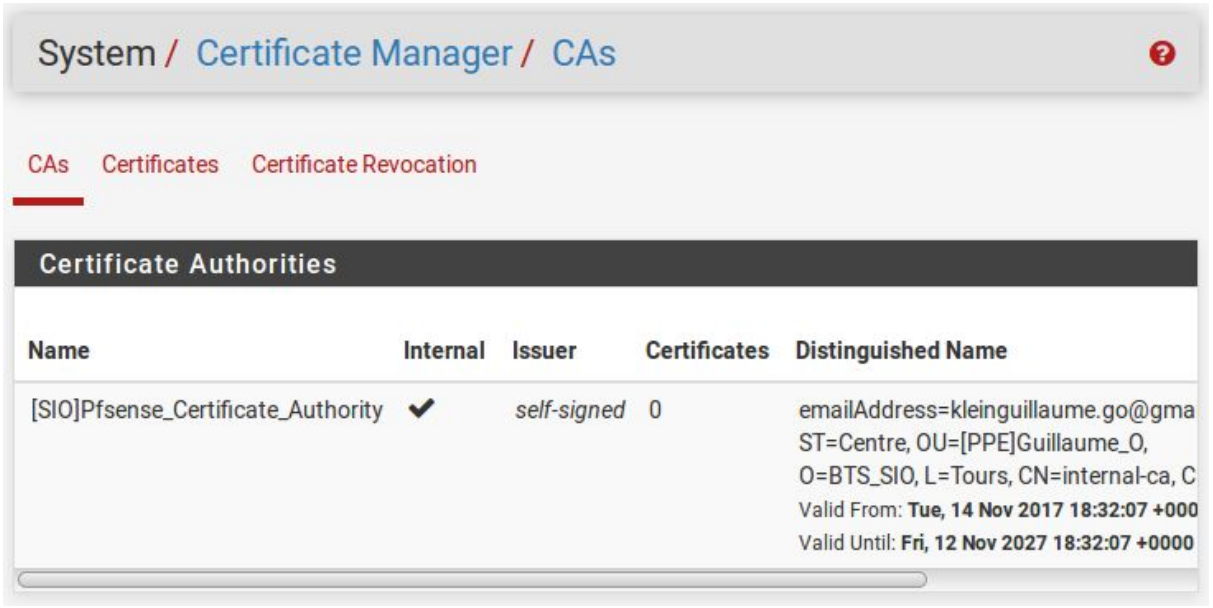


Viens ensuite la durée de validitée de l'autorité. nous la laissons sur la durée par défaut :

Pour finir, des informations d'identification de l'autorité sont demandées afin de pouvoir générer l'autorité de certification :



L'autorité est maintenant visible sous l'onglet "Cert Manager" :

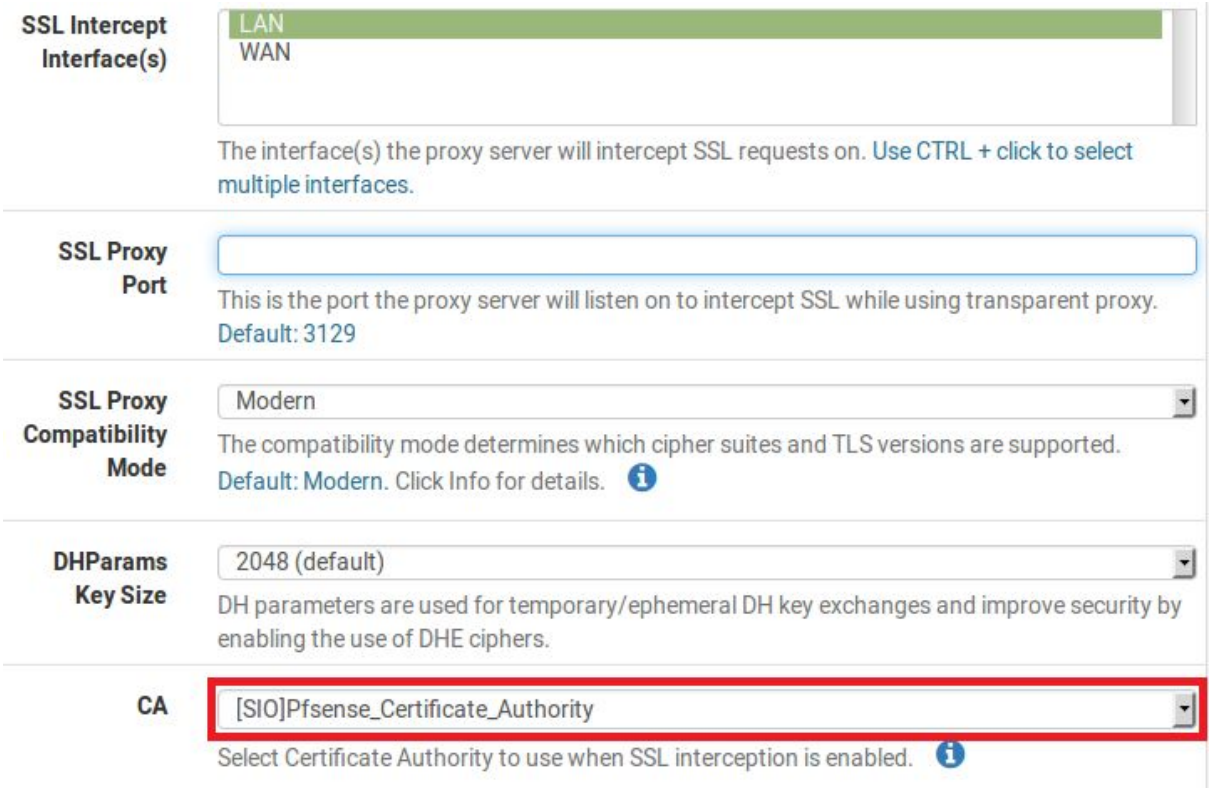


Nous pouvons désormais configurer les options de filtrage HTTPS.

Retournons dans les paramètres de configuration du service Squid, sous"Service/squid/general".

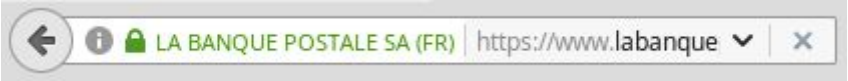
Un groupe d'option se nomme "SSL Man in The Middle Filtering". C'est ce groupe d'option que nous allons configurer. Premièrement, nous activons le filtrage SSL en cochant la case"HTTPS/SSL Interception". Le mode de filtrage doit être réglé sur "Splice all". Ce mode permet à Pfsense de capturer le flux sortant en temps réel, sans avoir à effectuer de manipulations sur les postes clients concernés :

Nous laisson les autres paramètres par défaut, à l'exception de la rubrique "CA", ou nous sélectionnons l'autorité de certification faite précédemment :



N'oubliez pas de sauvegarder les modification avec le bouton "Save" en bas de la page pour que les changements prennent effets.

Pour vérifier le fonctionnement de notre prototype, les étapes sont les mêmes qu'avec le filtrage HTTP. Rendez-vous sur une machine cliente côté LAN, et naviguez sur un site web utilisant le protocole HTTPS. Sur le dashboard Pfsense, observez le trafic en temps réel via l'onglet "Service/Squid/real time". Pour la vérification, j'ai ici utilisé le site de la banque postale :



Le résultat est positif, nous observons les URL web visités en clair, même lorsque le site en question utilise le protocole HTTPS :

Squid Access Table

Squid - Access Logs

Date	IP	Status	Address	User	Destination
14.11.2017 18:49:49	192.168.1.102	TCP_TUNNEL/200	www.labanquepostale.fr:443	-	83.206.67.137
14.11.2017 18:49:49	192.168.1.102	TCP_TUNNEL/200	www.labanquepostale.fr:443	-	83.206.67.137
14.11.2017 18:49:48	192.168.1.102	TCP_TUNNEL/200	pixel.tapad.com:443	-	185.57.60.186
14.11.2017 18:49:48	192.168.1.102	TCP_TUNNEL/200	match.adsrvr.org:443	-	54.247.118.100
14.11.2017 18:49:47	192.168.1.102	TCP_TUNNEL/200	ad.yieldlab.net:443	-	92.122.180.198
14.11.2017 18:49:47	192.168.1.102	TCP_TUNNEL/200	tracker.adotmob.com:443	-	54.154.37.108
14.11.2017 18:49:47	192.168.1.102	TCP_TUNNEL/200	gum.criteo.com:443	-	178.250.0.67
14.11.2017 18:49:45	192.168.1.102	TCP_TUNNEL/200	groupelapostefranalytics.	-	91.216.195.218

III. Configuration d'un serveur distant pour réception des logs :

Maintenant que nous sommes capable d'observer les connexions sortant du notre réseau LAN, il serait préférable d'exporter l'ensemble des logs sur un serveur de stockage externe. En effet, la machine Pfsense doit rester la plus légère possible, et la conservation / manipulations des logs y est très peu trivial. Nous allons donc mettre en place un serveur distant capable de recevoir les logs générés par pfsense, puis l'historique des connexions web utilisateurs filtrés par Squid. La machine est ici un Linux Mint (pour la légèreté), mais n'importe quel OS Linux fera l'affaire en production.

Depuis notre OS fraîchement installé, nous allons commencer par mettre à jour la liste des paquets disponibles en lançant un "apt-get update". Une fois ceci fait, nous allons pouvoir installer le service "syslog-ng" via le gestionnaire de paquets apt. Attention ,il sera certainement nécessaire d'installer les dépendances suivantes avant d'installer le service :
syslog-ng-mod-json, syslog-ng-mod-mongodb, syslog-ng-mod-sql, syslog-ng-mod-core.

Une fois les paquets installés, nous allons éditer le fichier de configuration de syslog-ng sous /etc/syslog-ng/syslog-ng.conf.

Nous commençons par commenter la ligne "internal();" :

```
# Sources
#########################
# This is the default behavior of sysklogd package
# Logs may come from unix stream, but not from another machine.
#
source s_src {
        system();
#       internal();
```

Juste en dessous, nous ajoutons les trois lignes suivantes :

```
source s_net { udp(port(514)); };
destination pfsense { file("/var/log/pfsense/pfSense.log"); };
log { source(s_net); destination(pfsense); };
```

Le serveur syslog va donc écouter sur le port UDP 514 pour recevoir les logs distants. Ceux-ci seront placés dans le fichier “pfSense.log” sous “/var/log/pfsense”. Attention à bien créer le dossier et le fichier pfSense.log manuellement.

Nous pouvons désormais redémarrer le service syslog-ng pour appliquer les modifications, et être tenu au courant en cas de problèmes dans le fichier de configuration édité :

```
user-virtual-machine user # service syslog-ng restart
```

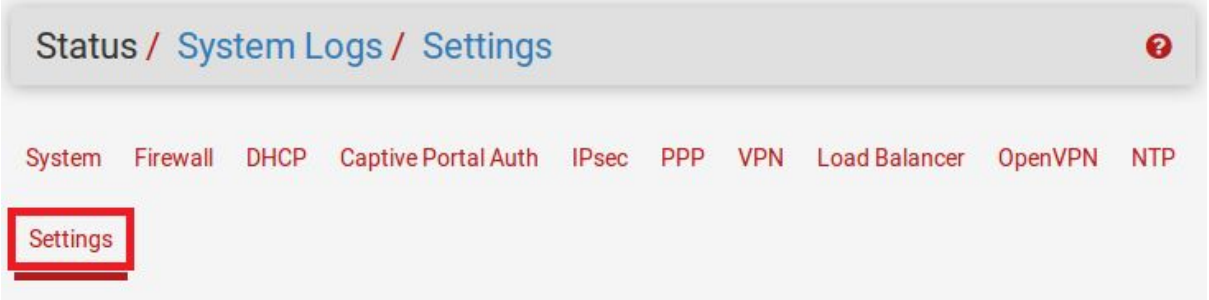
Enfin, avec la commande “netstat- patun” nous allons observer tous les ports d’écoutes de notre serveur, pour vérifier que le port 514 y est bien présent :

```
Proto Recv-Q Send-Q Adresse locale          Adresse distante        Etat
ID/Program name
tcp        0      0 127.0.1.1:53            0.0.0.0:*               LISTEN
1118/dnsmasq
udp        0      0 0.0.0.0:5353            0.0.0.0:*
752/avahi-daemon: r
udp        0      0 0.0.0.0:56163           0.0.0.0:*
752/avahi-daemon: r
udp        0      0 0.0.0.0:514             0.0.0.0:*
7571/syslog-ng
udp        0      0 127.0.1.1:53            0.0.0.0:*
1118/dnsmasq
udp        0      0 0.0.0.0:68              0.0.0.0:*
5321/dhclient
```

Si tout est bon, la configuration côté serveur syslog est maintenant terminée. pensez à noter l’adresse IP de ce serveur (et à la basculer en adressage fixe si ce n’est pas déjà fait), nous allons en avoir besoin pour la suite.

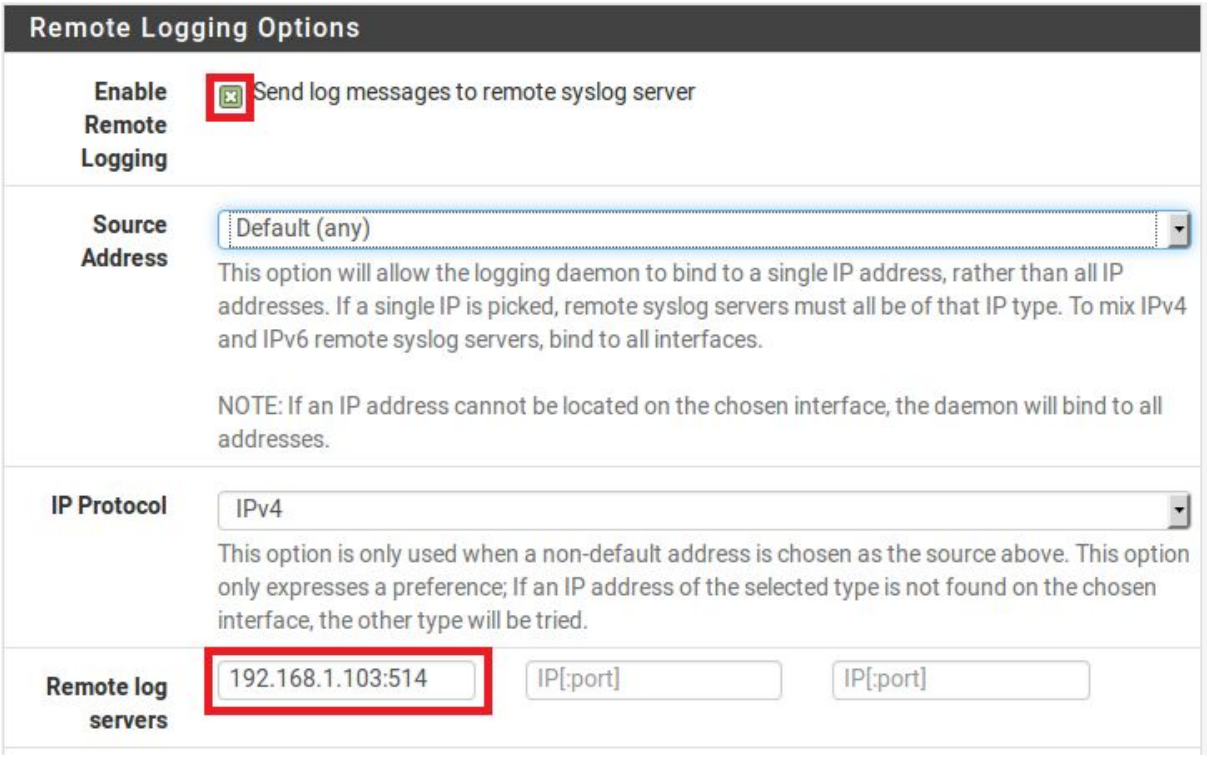
IV. Exportation des logs Pfsense vers le serveur syslog distant :

De retours sur notre dashboard Pfsense, nous allons configurer l’envoi des logs. Pour ce faire, rendez-vous dans “Statut/system Logs” puis “Settings” :

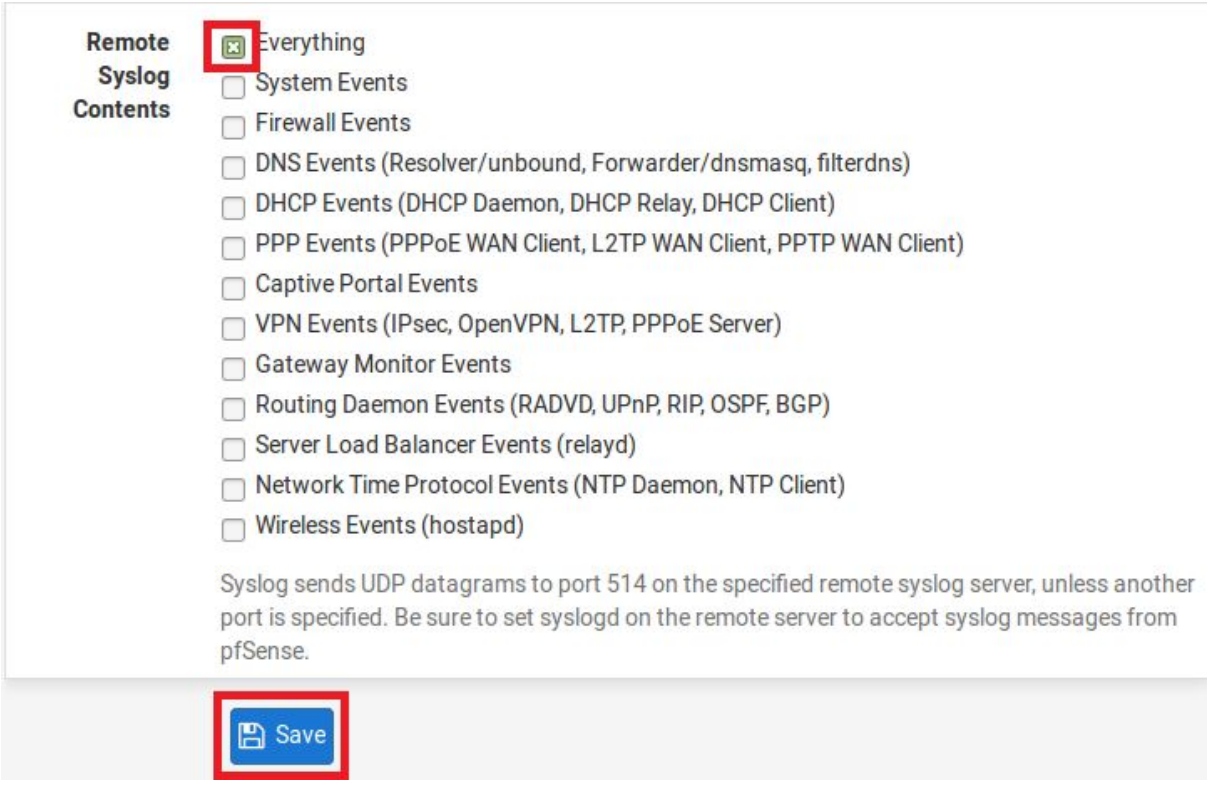


Dans la catégorie “Remote Logging Options”, cocher la case “Enabled Remote Logging”. Ceci aura pour effet de faire apparaître de nouvelles options de configurations.

Nous renseignons l'adresse ip et le port d'écoute de notre serveur syslog sous le format *ip:port* :



Enfin, nous pouvons sélectionner quels types de logs sont à transmettre au serveur distant. Nous choisissons de tout envoyer vers le serveur distant pour soulager la machine Pfsense :



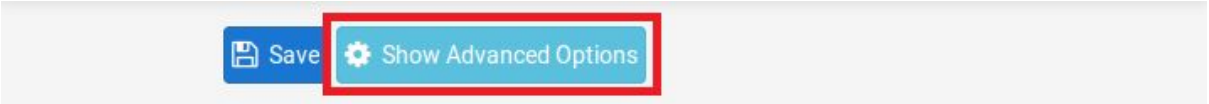
Désormais les logs d'état de Pfsense sont transmis sur le serveur syslog. Pour vérifier que tout fonctionne correctement, connectez vous sur le serveur distant, et entrez la commande "tail -f /var/log/pfsense/pfSense;log" pour observer la réception des logs en direct.
Si tout c'est bien passé et que les deux serveurs communiquent correctement, quelques premiers logs devraient être présents :

```
user@user-virtual-machine ~ $ tail -f /var/log/pfsense/pfSense.log
Nov 15 19:33:15 192.168.1.1 filterlog: 62,,,12000,em0,match,block,in,4,0x0,,1,0,
0,none,2,igmp,28,192.168.0.1,224.0.0.1,datalength=8
Nov 15 19:33:15 192.168.1.1 filterlog: 62,,,12000,em0,match,block,in,4,0x0,,1,0,
0,none,2,igmp,32,192.168.0.1,224.0.0.1,datalength=12
Nov 15 19:33:15 192.168.1.1 filterlog: 62,,,12000,em0,match,block,in,4,0x0,,1,0,
0,none,2,igmp,28,192.168.2.1,224.0.0.1,datalength=8
```

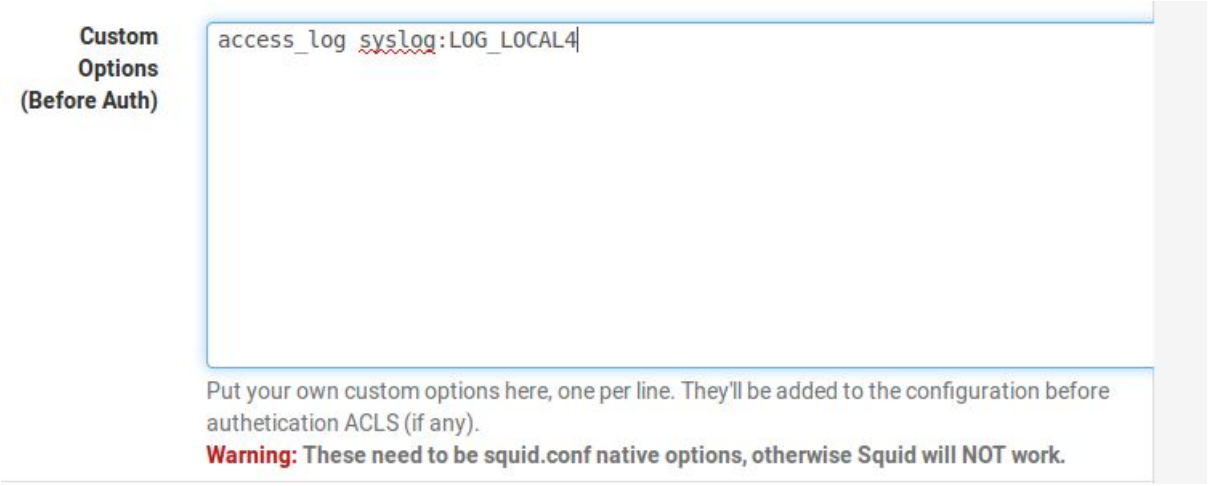
Nous allons ensuite conclure sur l'export des logs web des utilisateurs du LAN générés par Squid.

V. Exportation des logs Squid vers le serveur syslog distant :

Les modifications à faire vont être très simples, mais celles-ci ne sont pas relatives à quelconques options pré-définis sous Pfsense. Sur le dashboard Pfsense, rendez-vous dans l'onglet "Service/Squid proxy Server", puis tout en bas des options general, dans les options avancés :



Dans le champ "Custom Options Before Auth", nous allons ajouter la commande suivante "access_log syslog:LOG_LOCAL4" :

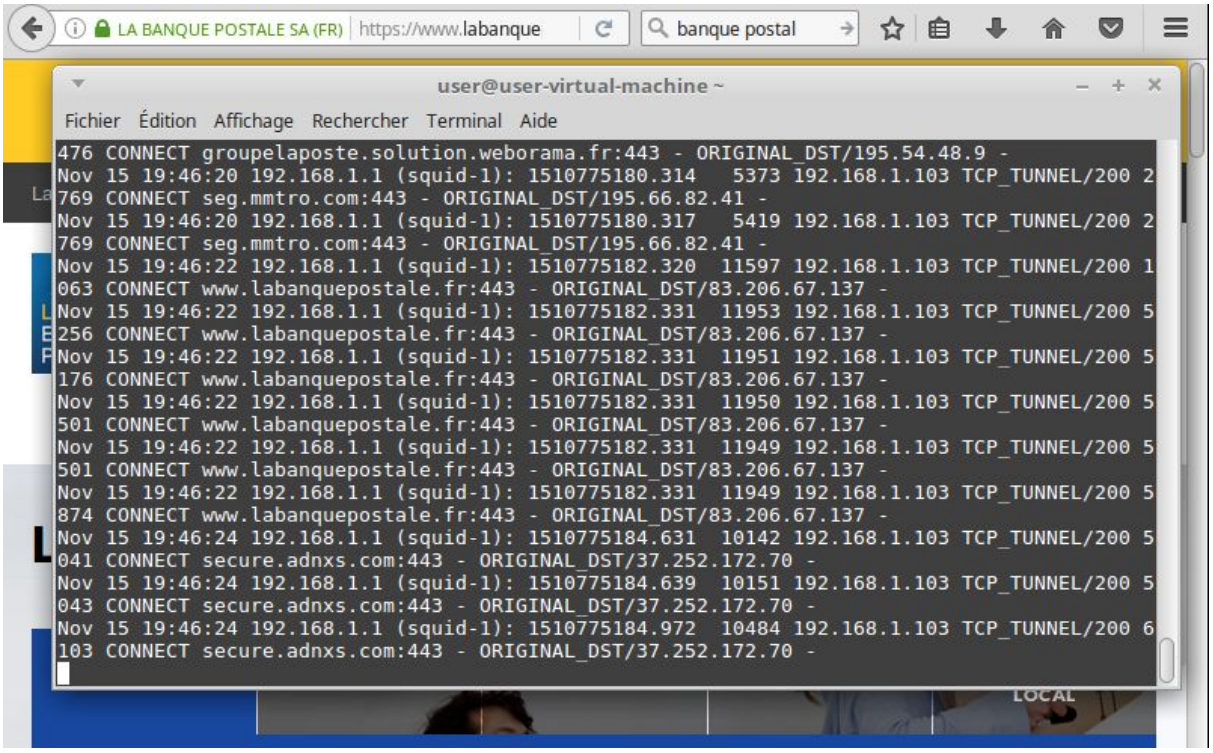


Cela aura pour effet de simuler l'ajout de nouvelles options au sein du fichier de configuration de Squid. Cette ligne permet d'exporter les logs fournis par Squid en suivant le schéma des autres logs Pfsense, et donc d'atterrir dans le fichier "pfSense.log" présent sur le serveur syslog distant.

Pensez à sauvegarder les modification avant d'effectuer le dernier test. la sauvegarde aura pour effet de redémarrer le service Squid Proxy, et donc de générer de nouveaux fichier logs:

```
Nov 15 19:43:31 192.168.1.1 check_reload_status: Reloading filter
Nov 15 19:43:31 192.168.1.1 php-fpm[310]: /pkg_edit.php: [squid] Adding cronjobs ...
Nov 15 19:43:31 192.168.1.1 php-fpm[310]: /pkg_edit.php: [squid] Antivirus features disable
d.
Nov 15 19:43:31 192.168.1.1 php-fpm[310]: /pkg_edit.php: [squid] Removing freshclam cronjob
.
Nov 15 19:43:31 192.168.1.1 php-fpm[310]: /pkg_edit.php: [squid] Stopping any running proxy
 monitors
Nov 15 19:43:32 192.168.1.1 php-fpm[310]: /pkg_edit.php: [squid] Reloading for configuratio
n sync...
Nov 15 19:43:33 192.168.1.1 php-fpm[310]: /pkg_edit.php: [squid] Starting a proxy monitor s
cript
```

rendez vous maintenant sur une machine cliente connectée au LAN, et naviguez sur des sites HTTPS. Toujours en prenant l'exemple du site de la banque postal, nous observons les logs liés à la demande de cette page web dans notre fichier pfSense.log sur le serveur syslog distant :



Les logs sont maintenant interprétables, datés, relatifs aux adresses IP de notre réseau LAN, et stockés en dur sur une machine distante propice à la duplication ou à la redondance. Les différentes étapes obligatoires et juridiques liés à la mise à disposition de notre matériel informatique aux employés est donc terminée.

Pensez enfin à vider le cache local de Pfsense des logs potentiellements archivés durant les différentes étapes de configuration.