## **PfSense**

- Un proxy Open Source avec PfSense
  - Introduction
  - Prérequis
  - <u>Installation</u>
  - Configuration de Squid
  - Configuration de SquidGuard
  - Configuration manuelle du proxy
  - Configuration automatique du proxy
  - <u>Références</u>

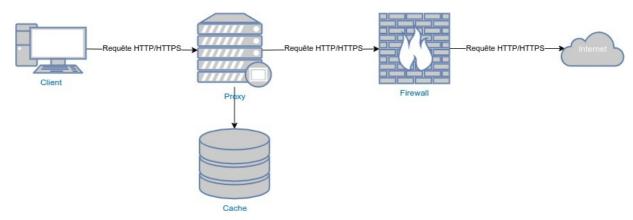
# Un proxy Open Source avec PfSense

### Introduction

Un **serveur mandataire** ou **proxy** (de l'anglais) est un serveur informatique qui a pour fonction de relayer des requêtes entre un poste client et un serveur. Les serveurs mandataires sont notamment utilisés pour assurer les fonctions suivantes :

- mémoire cache;
- la journalisation des requêtes (« logging ») ;
- la sécurité du réseau local ;
- le filtrage et l'anonymat.

L'utilité des serveurs mandataires est importante, notamment dans le cadre de la sécurisation des systèmes d'information.



Ce tuto va vous permettre de créer un proxy avec filtrage et logging. Nous allons utiliser <u>PfSense</u> comme base de travail.

A l'installation de base, nous allons ajouter les packages :

- Squid
- SquidGuard
- LightSquid

Un proxy Open Source avec PfSense

## Prérequis

- Une machine x86 physique ou virtuelle avec une interface réseau
  un serveur DNS
- un serveur DHCPun firewall

### Installation

Je vous invite à télécharger l'ISO de PfSense sur le site : https://www.pfsense.org/download/

PfSense peut être installé sur une machine physique ou sur une machine virtuelle. Pour ma part, il sera installé sur VWMware ESXi 6.5.



Le CLUF



Sélectionner « Install »



Choisir sa disposition de clavier



Choisir son type de système de fichiers



Patience...



Sélectionner « No »



#### Sélectionner « Reboot »

```
AMB Features2:0x1CLMS7)
Structured Extended Features2:0x0x0x0x0x138PB.STIBP.LIDFL.ARCH_CAP.SS8D>
Structured Extended Features2:0x0x0x0x0x138PB.STIBP.LIDFL.ARCH_CAP.SS8D>
IST2.ARCH_CAPS-NOW-CASSA_SKIP_LIDFL_VMC>
Repressor: Origin : "Marrothare"
Repressor: Origin :
```

#### Ne pas configurer de Vlan

#### Introduire le nom de l'interface réseau

```
Opfating configuration.....dome.
Harning: Configuration references interfaces that do not exist: end
Metwork interface mismatch -- Ranning interface assignment option.
Unlid interfaces are:
evel 08:8c:29:34:cb:98 (up) Intel(R) PRO/1808 Metwork Connection
No Unmer need to be set up first?
If VARNs until not be said, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLAMs later, if required.
Should VLAMs he set up now lyin1? a
If the names of the interfaces are not known, exto-detection cas
be said instead. To use acto-detection, place disconnect all
interfaces before pressing 'a' to begin the process.
Exter the LAMs interface name or 'a' for auto-detection
(and or a): sed!

Exter the LAMs interface name or 'a' for auto-detection
(STE: 1b): mobbles [fill firewoiling/HAT mode.
(a or nothing if finished):
```

#### Presser « Enter »

```
end BB:Bc:29:34:ch:98 (up) Intel(B) PES-1888 Natural Connection
bs NLONs need to be set up first?
If CLONs will not be seed, or only for optional interfaces, it is typical to
say so here and use the mebCasfigerator to configure ULANS later, if required.
Should ULANS be set up now (yint)?
If the seems of the interfaces are not known, exto-detection can
be seed instead. To use auto-detection, please disconnect all
interfaces before prossing 's' to begin the process.

Ester the LANS interface name or 'a' for auto-detection
Committee all seed
Exter the LANS interface name or 'a' for auto-detection
NOTE: this enables tull Firemelling-MHT mode.
C a or sothing if finished:
The interfaces will be assigned as follows:

LANS - well
Do you mant to proceed (yiel? y)
```

Enter « Y »

Sélectionner l'option 2 pour configurer l'adresse IP

Je sélectionne l'option DHCP pour attribuer une IP

Introduire « Y »

```
Restarting sebConfigurator...

The IPv4 SHH address has been set to dkcp
You can mear access the sebConfigurator by opening the following UEL is your set
browner:

http://dhcp/

Press CENTED to continue.
USBarr Virtual Hachine - Notgate Bevice 18: 73483694786fad913055

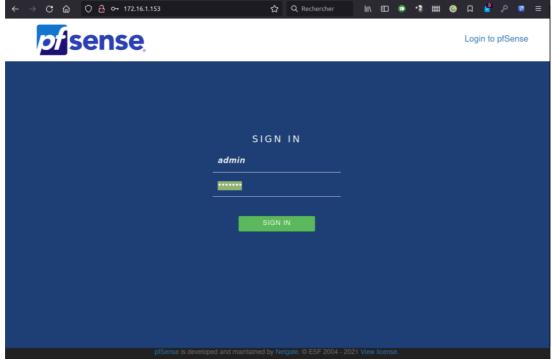
**** Melcome to pfSense 2.5.2-EELERSE (and64) on pfSense ***

LBM (ann) -> one -> v4/MECPv1: 172.16.1.153/16

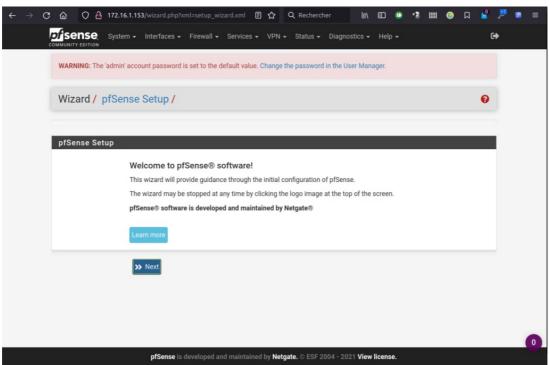
8) Legent (SSH salp)
1) Resign Interfaces
1) Restart sebConfigurator
2) Set interface(3) IP address 11 Bertart sebConfigurator
3) Benset to factory defaults 13) Update 1 concentration
4) Reset to factory defaults 13) Update 1 concentration
6) Holt system 150 Restart second 1 (sabd)
6) Holt system 150 Restart second 1 (sabd)
7) Fing host 151 Restart second 1 (sabd)
15 Shell 1 (sabd)
15 Restart recent configuration
16 Restart second 1 (sabd)
16 Restart second 1 (sabd)
17 Fing host 15 Restart second 1 (sabd)
18 Shell 1 (sabd)
19 Restart second 1 (sabd)
19 Restart second 1 (sabd)
10 Restart second 1 (sabd)
11 Restart second 1 (sabd)
12 Restart second 1 (sabd)
13 Restart second 1 (sabd)
14 Restart second 1 (sabd)
15 Restart second 1 (sabd)
15 Restart second 1 (sabd)
16 Restart second 1 (sabd)
17 Restart second 1 (sabd)
18 Restart s
```

Et voilà

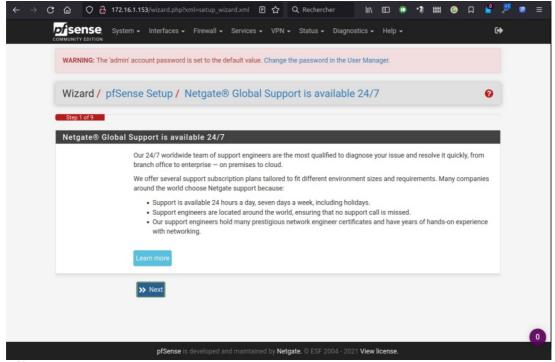
A présent, nous allons pouvoir passer via l'interface Web de management de PfSense via http://<IP> Pour Configurer PfSense et installer les packages nécessaires au fonctionnement du proxy.



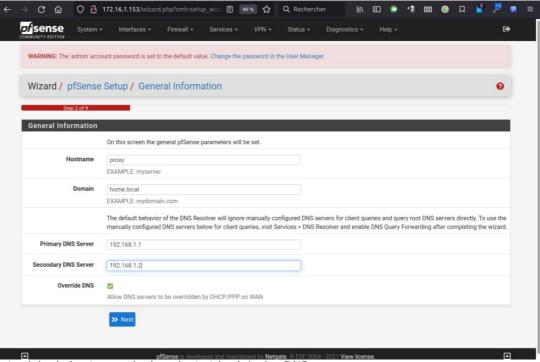
Le login/password et admin/pfsense



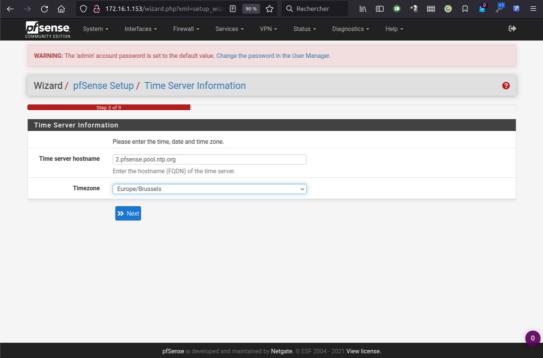
« Next »



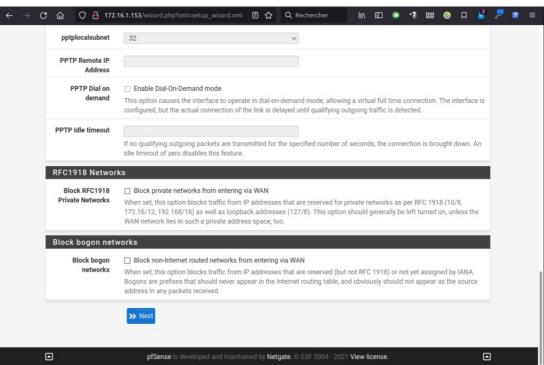
« Next »



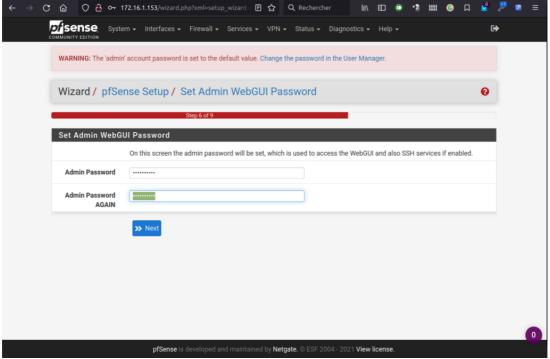
Introduire le hostname, le domainet et les ip's des DNS



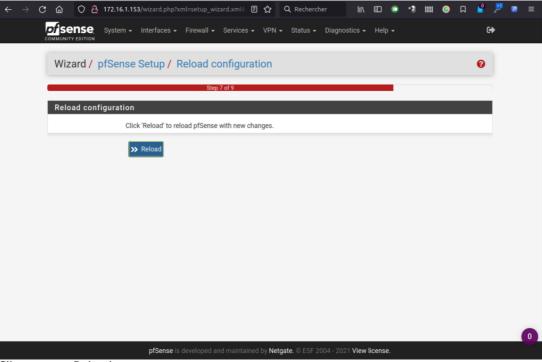
Choisir son serveur NTP et la timezone



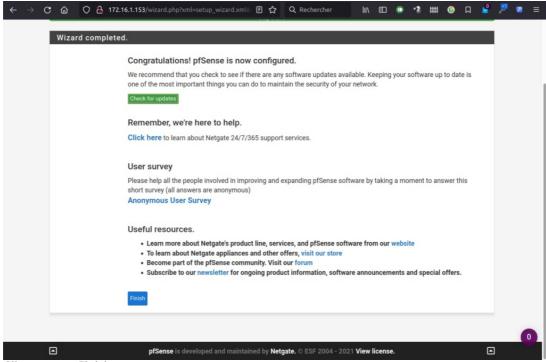
« Next »



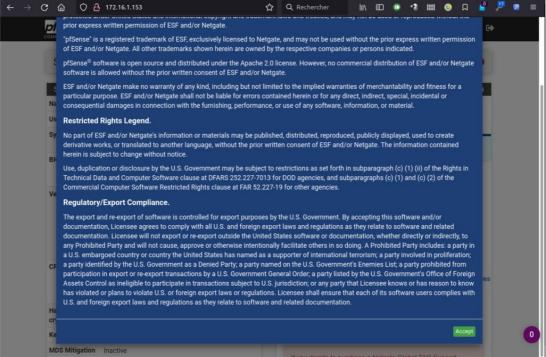
Introduire un nouveau mot de passe pour l'utilisateur « admin »



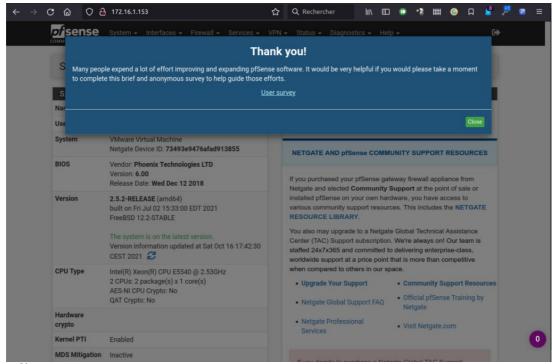
Cliquer sur « Reload »



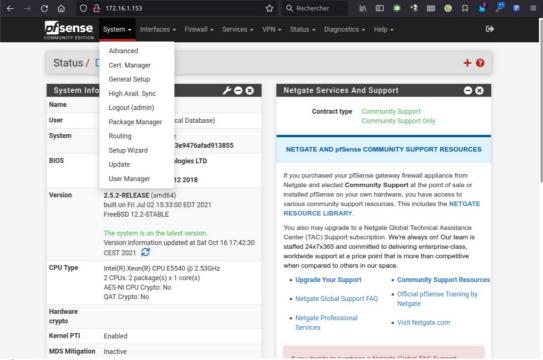
Cliquer sur « Finish »



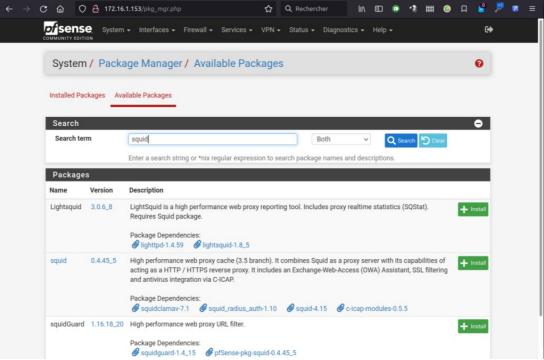
« Accept »



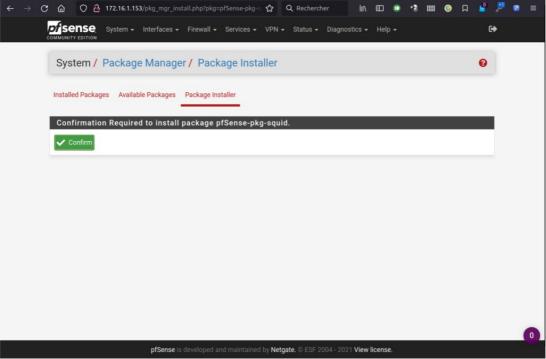
« Close »



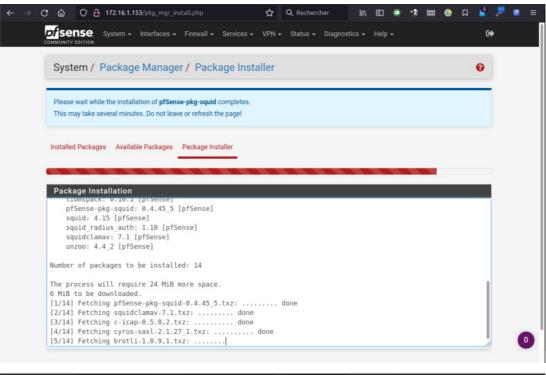
Sélectionner le « Package Manager »

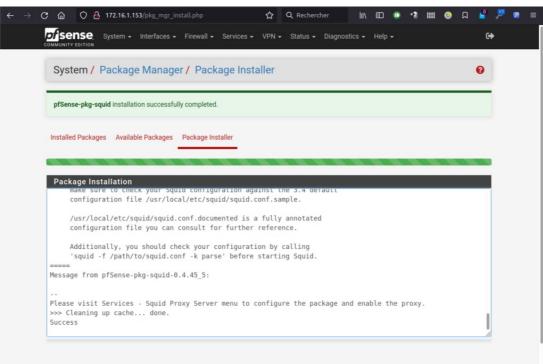


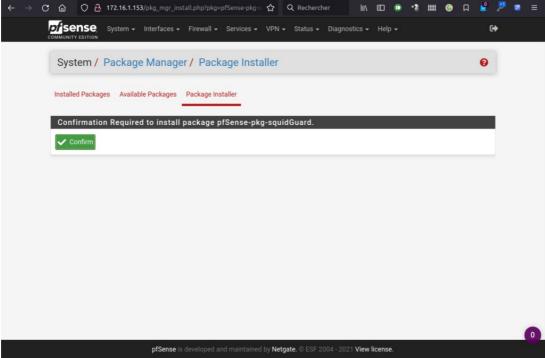
Dans « Available Packages ». rechercher les packages liés à Squid



Procéder à l'installation des pacakges

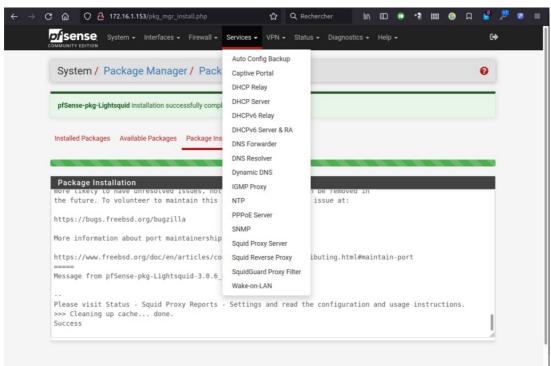




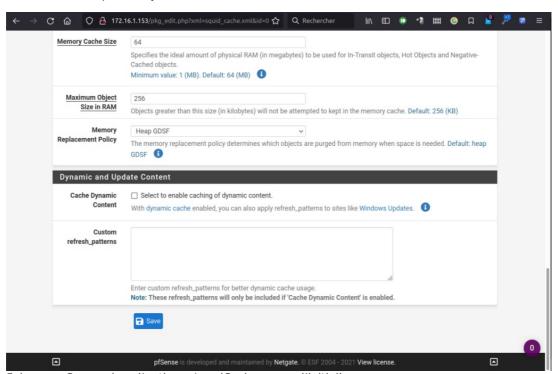


Et voilà...

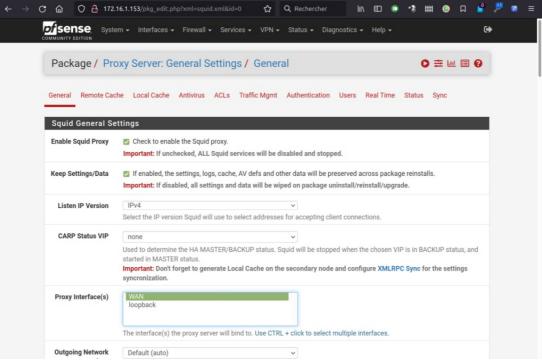
## Configuration de Squid



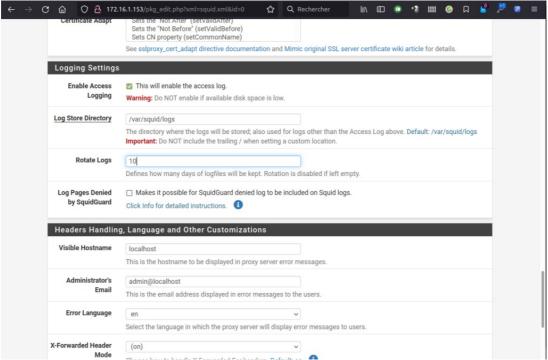
Sélectionner « Squid Proxy Server »



Faire un « Save » dans l'option « LocalCache » pour l'initialiser



Cocher « Check to enable the Squid proxy »

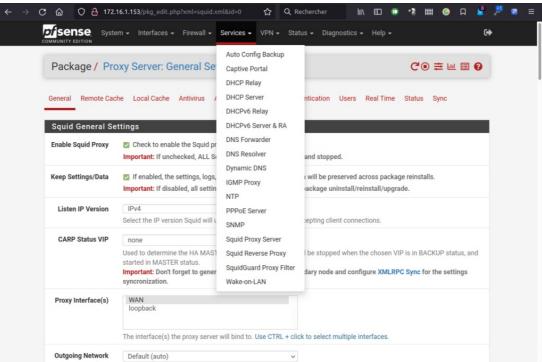


Coocher « This will enable the access log » et « Save »

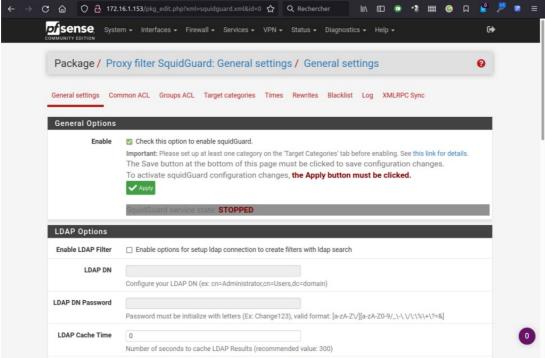
## Configuration de SquidGuard

SquiGuard est un « add-on » pour Squid qui va vous permeetre d'effectuer du filtrage basé sur des blacklists/whitelists.

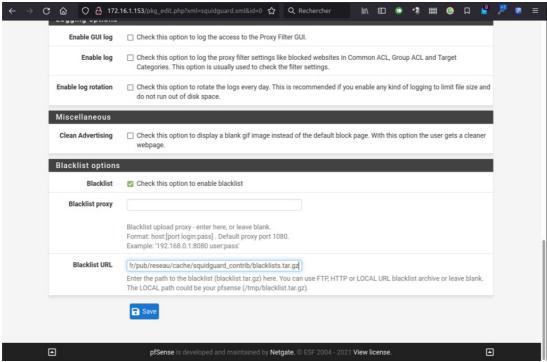
J'utilise la blacklist de L'Université de Toulouse. https://dsi.ut-capitole.fr/blacklists/



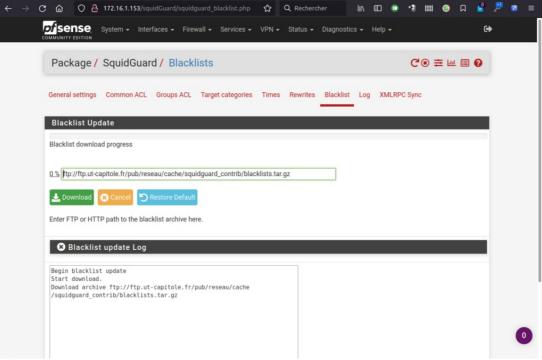
Sélectionner « SquiGuard Proxy Filter »



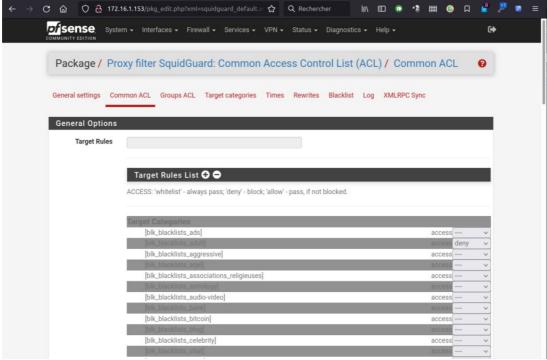
Cocher « Check this option to enable squidGuard »



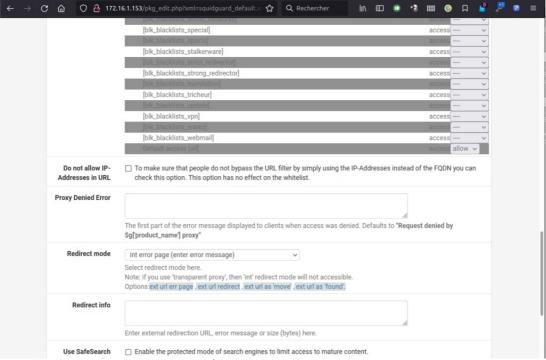
Cocher « Check this option to enable blacklist » et introduire l'URL de la blacklist



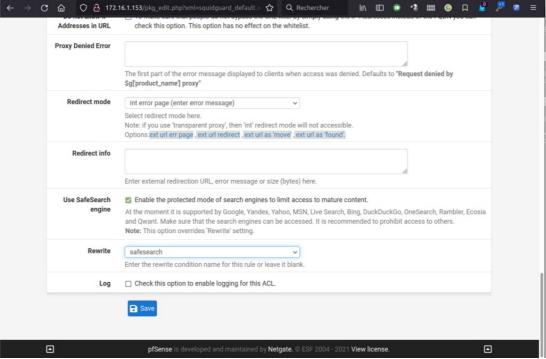
Effectuer le download de la blacklist



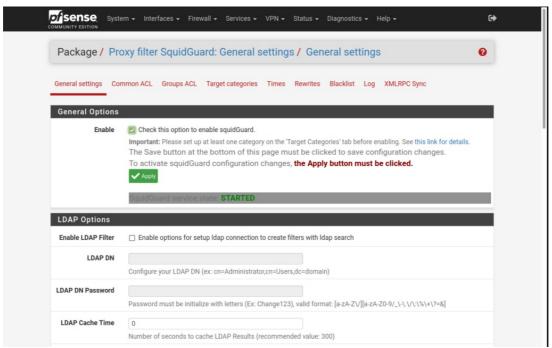
Sélectionner les catégories que vous désirez filtrer



Attention, le « all » est en deny par défaut, ce qui filtre tous les sites



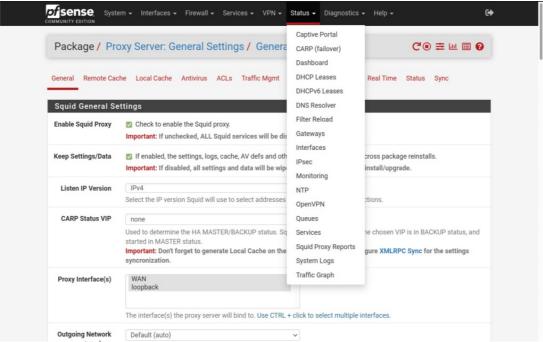
Activer le « safrsearch » pour rendre votre moteur de recherche « safe »



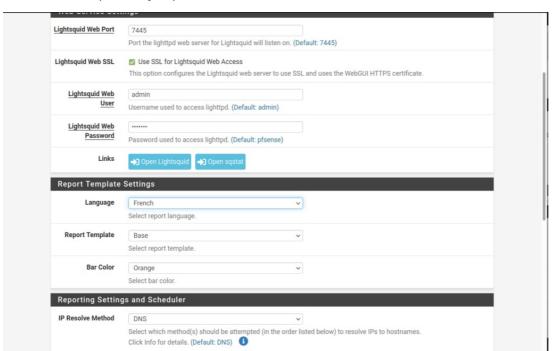
Ne pas oublier de cliquer sur « Save » pour valider la configuration

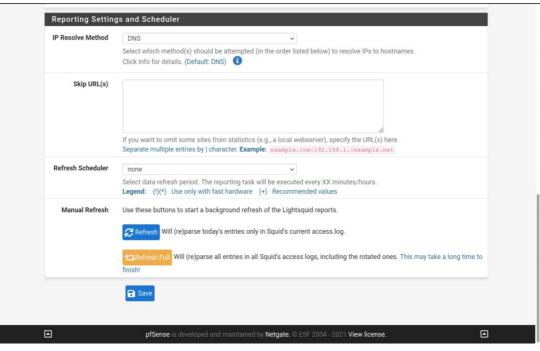
## Configuration de LightSquid

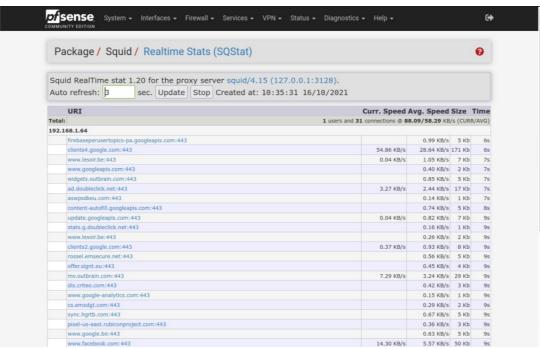
LightSquid va vous permettre de faire du reporting sur les accès Squid.



Sélectionner « Squid Proxy Reports »









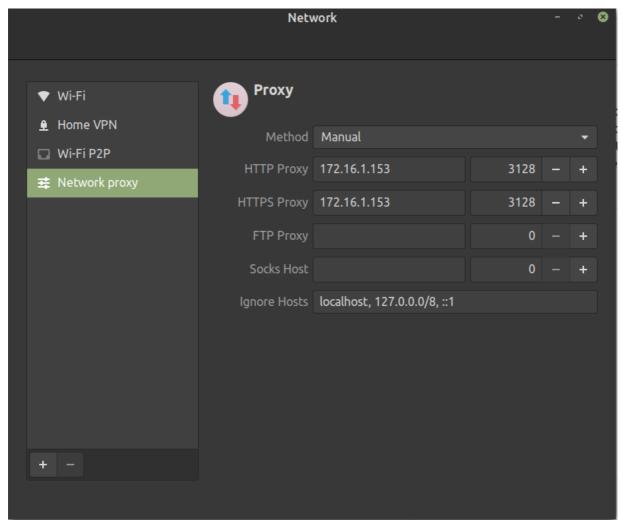
LightSquid v1.8 (c) Sergey Erokhin AKA ESL

## Configuration manuelle du proxy

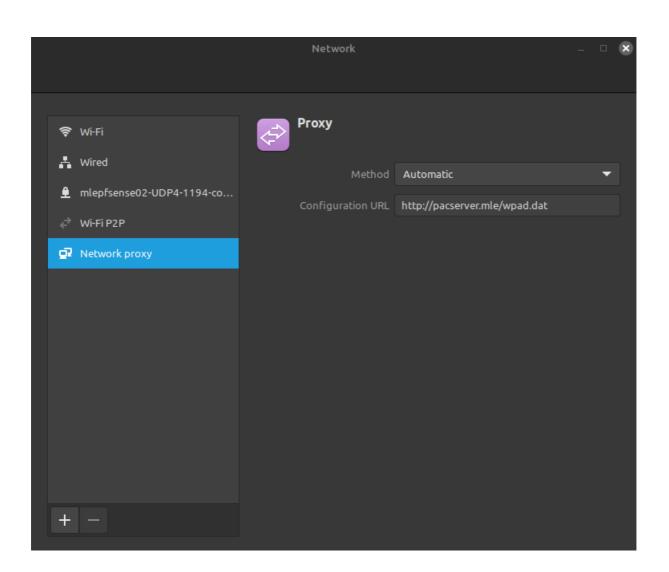
Les écrans ci-dessous sont propres à Linux

Vous avez 2 possibilités:

• La configuration manuelle du proxy



• par l'ajout de l'URL du serveur WEB hébergeant votre fichier de configuration



# Configuration automatique du proxy

#### Fichier PAC et WPAD

#### Introduction

Pour déployer automatiquement l'adresse de votre proxy, nous allons créer un un fichier proxy, pac.

Extrait de Wikipédia

https://fr.wikipedia.org/wiki/Fichier\_.PAC

Le <u>navigateur</u> va chercher ce fichier PAC en priorité. Les URL qu'il contient peuvent être configurées manuellement, ou déterminées automatiquement par le WPAD (<u>Web Proxy Autodiscovery Protocol (en)</u> $^{1}$ ).

Un fichier PAC contient une <u>fonction</u> en <u>JavaScript</u> appelée « FindProxyForURL(url, host) ». Cette <u>fonction</u> retourne une <u>chaîne de caractères</u> avec une ou plusieurs spécifications (règles) sur la façon d'y accéder. Ces règles amènent le <u>navigateur web</u> à utiliser un serveur <u>proxy</u> particulier ou à se connecter directement.

#### **Prérequis**

Un fichier proxy.pac doit être déployer à travers un serveur web. Perso, j'utilise un serveur Apache. Voici un lien pour vous aider à installer un serveur Apache sous Ubuntu :

https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-ubuntu-20-04-guickstart-fr

Pour l'extension .pac soit prise en charge par votre serveur Web Apache, il faut ajout un fichier .htaccess contenant :

```
AddType application/x-ns-proxy-autoconfig .pac
```

Dans le répertoire contenant votre fichier proxy.pac

Créez, également, un symbolic link wpad.dat vers votre fichier proxy.pac. Exemple:

In -s /var/www/html/proxy.pac /var/www/html/wpad.dat

#### Exemple de fichier proxy.pac

```
function FindProxyForURL(url, host)
//Les adresses privées n'utilisent pas le proxy
if (isInNet(host, "192.168.0.0", "255.255.0.0")) {
return "DIRECT"
if (isInNet(host, "10.0.0.0", "255.0.0.0")) {
return "DIRECT"
// les urls suffixées domain.local n'utilisent pas le proxy
if (shExpMatch(url, "*.domain.local//*"))
return "DIRECT";
} else {
// définition du proxy pour l'http et l'https
if (shExpMatch(url, "http:*"))
return "PROXY 172.16.1.153:3128";
if (shExpMatch(url, "https:*"))
return "PROXY 172.16.1.153:3128";
return "DIRECT";
```

#### Propagation via DNS

Remarque: La propagation de la configuration wpad/pac via DNS/DHCP n'est valable que pour des machines

Windows.

Pour propager votre configuration proxy via un serveur DNS. Vous devez créer une entrée wpad soit un A pointant vers l'IP du serveur web hébergeant le fichier wpad/pac ou un CNAME pointant vers le FQDN du serveur web hébergeant le fichier wpad/pac.

wpad.mle. IN A 172.16.1.1

ou

wpad.mle. IN CNAME pacserver.mle.

#### Propagation par DHCP

La propagation par DHCP de la configuration WPAD est principalement supporté par Windows.

Vous devez configurer l'option 252 qui pointera vers l'URL de votre fichier wpad.dat. Exemple : http://pacserver.mle/wpad.dat

Un proxy Open Source avec PfSense

## Références

http://findproxyforurl.com https://fr.wikipedia.org/wiki/Fichier\_.PAC https://www.pfsense.org/