

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



**Documentation n°3 : Filtrage des connexions internet indésirables.**

**Auteur :** Guillaume Orlando

**Date :** 16/11/2017

## I. Introduction :

Le fait de bloquer l'accès à certains sites-web en entreprise permet aux utilisateurs de ne pas être distraits par certains réseaux-sociaux, de ne pas naviguer sur des sites webs dangereux, ou totalement illégaux. Le blocage d'URL se fait de deux manières.

D'un côté, la whitelist permet de définir à l'avance quels sites webs sont autorisés sur le réseau, et de bloquer tous les autres. Cette méthode est la plus sécurisée puisque l'accès web est totalement contrôlé. En revanche, la mise en place d'une whitelist n'offre pas de flexibilité aux utilisateurs, et risque de les brider si la liste n'est pas assez exhaustive.

La deuxième solution, que nous allons retenir par la suite, consiste en la mise en place d'une blacklist. À l'inverse de la whitelist, certains sites sont interdits, et tout le reste du trafic est autorisé par les utilisateurs. Bien que plus permissive, la blacklist se doit d'être correctement configurée et d'être constamment maintenu à jour. Nous allons voir dans cette documentation comment installer et déployer un filtrage web via une blacklist sur notre machine PfSense. Pour ce faire, nous utiliserons une extension du proxy Squid, Squidguard.

## II. Installation de Squid-Guard :

SquidGuard peut être installé via le gestionnaire de paquets PfSense. Celui-ci est situé sous l'onglet "System/Package Manager". Dans la liste des paquets disponibles, nous renseignons "squidguard" pour trouver le paquet correspondant :

The screenshot shows the PfSense Package Manager interface. At the top, the breadcrumb navigation is "System / Package Manager / Available Packages". Below this, there are two tabs: "Installed Packages" and "Available Packages", with the latter being selected. A search bar is present with the text "Search term" and a search button. The search term "squidguard" is entered in the search bar. Below the search bar, there is a table of packages. The table has three columns: "Name", "Version", and "Description". The first row shows "squidGuard" with version "1.16.4" and description "High performance web proxy URL filter.". To the right of the description, there is a green button with a plus sign and the text "Install". Below the table, there is a section for "Package Dependencies:" which shows "squidguard-1.4\_15".

Name	Version	Description
squidGuard	1.16.4	High performance web proxy URL filter.

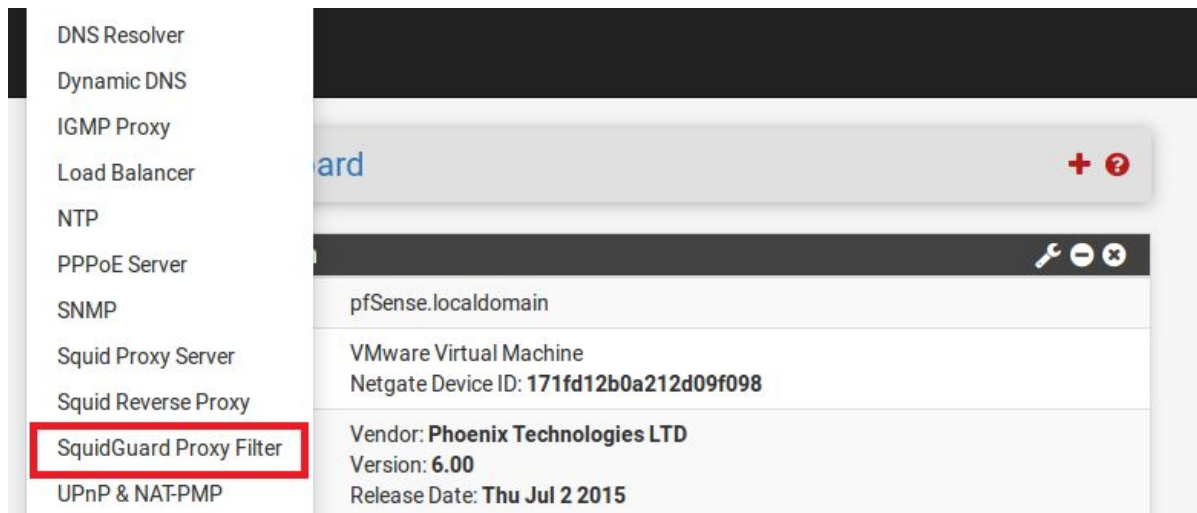
Package Dependencies:  
squidguard-1.4\_15

Après avoir confirmé l'installation de SquidGuard, et le temps que le processus d'installation se déroule, nous devrions être prêt pour la configuration de la blacklist.

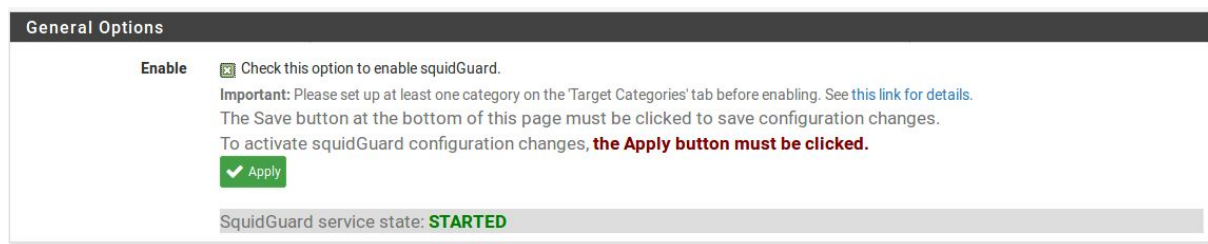
pfSense-pkg-squidGuard installation successfully completed.

### III. Mise en place d'une blacklist :

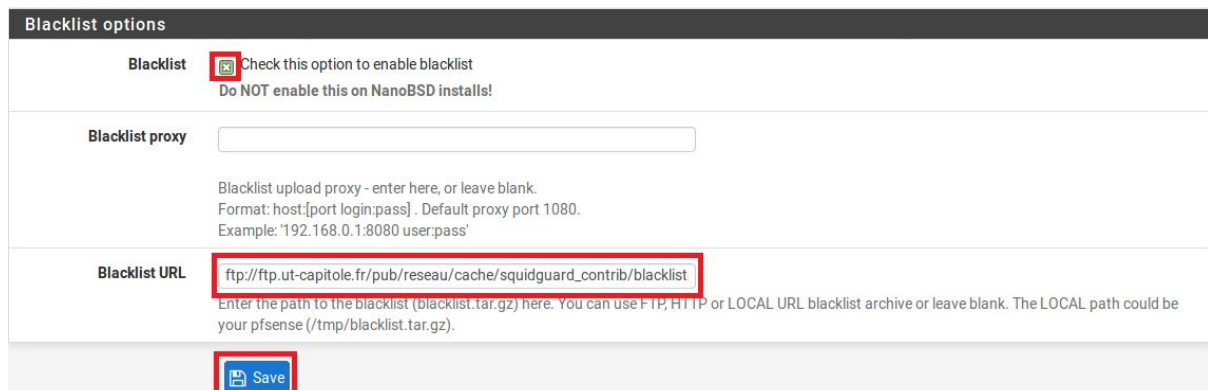
Maintenant que le paquet est installé, un nouvel onglet nommé "SquidGuard Proxy Filter" devrait être disponible dans le menu "System" :



Nous commençons par activer SquidGuard :

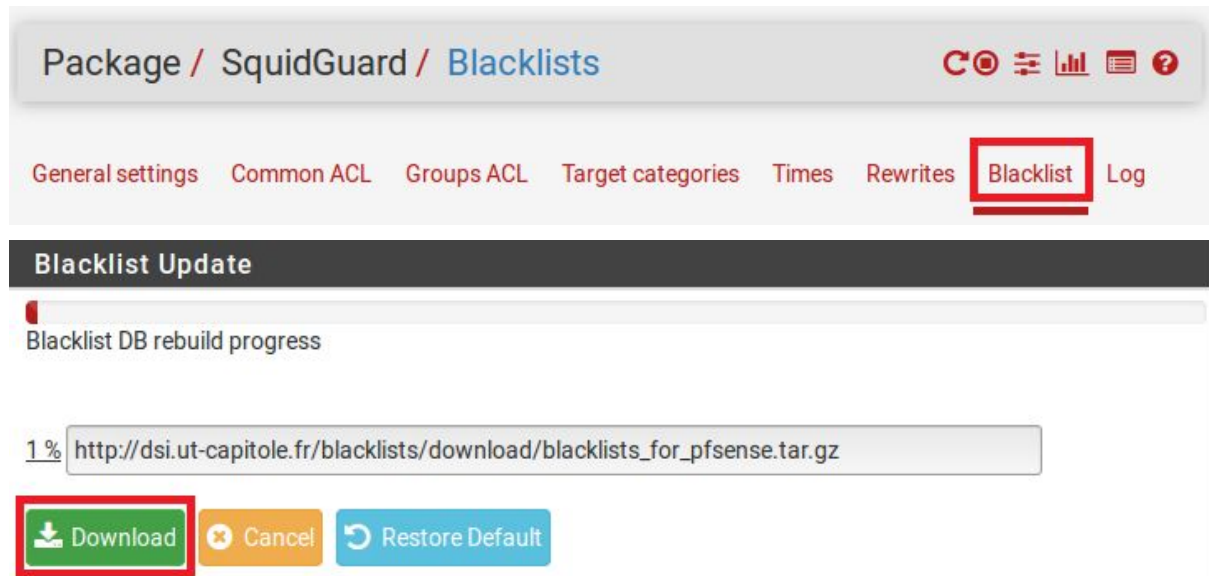


Le reste des options de SquidGuard vont rester par défaut pour le moment. Rendez-vous directement tout en bas de la page, dans la rubrique "Blacklist Options". Pensez à bien activer la blacklist en cochant la case correspondante. Le lien de la blacklist imposé, celle de l'université de Toulouse, est disponible ici : "http://dsi.ut-capitole.fr/blacklists/download/blacklists\_for\_pfsense.tar.gz". Nous la collons dans l'option "blackList URL".

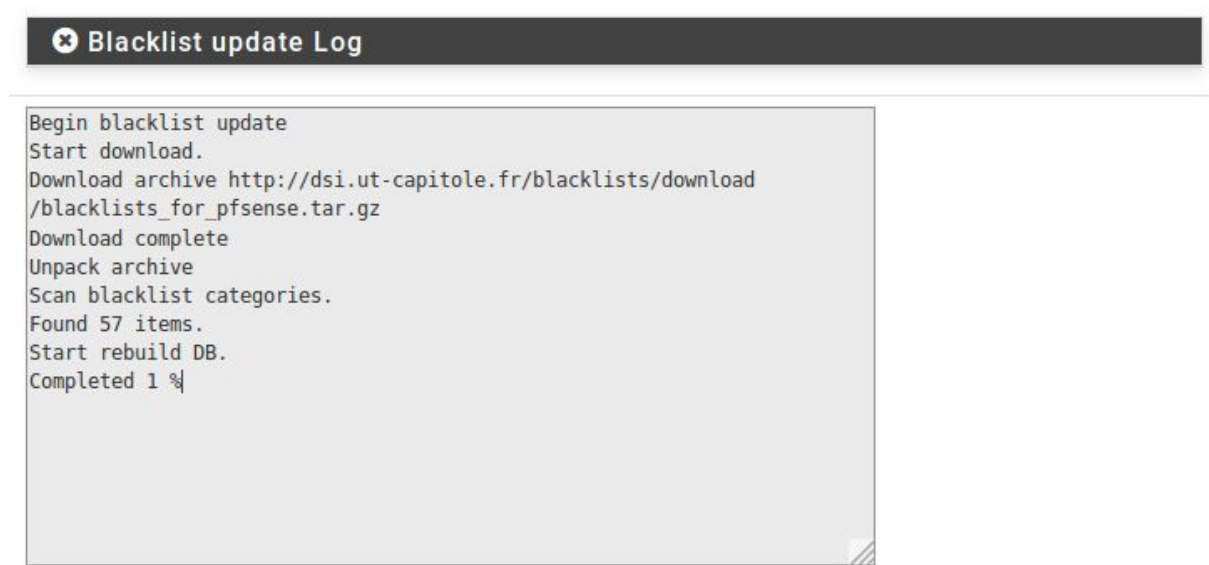


Pensez à appliquer les changements avant de quitter la page.

Nous allons maintenant importer le contenu de la blacklist de l'université de Toulouse en accédant à l'onglet "Blacklist", toujours sur la page de configuration de SquidGuard. pour lancer le téléchargement des fichiers de la blacklist, cliquez sur "Download" :

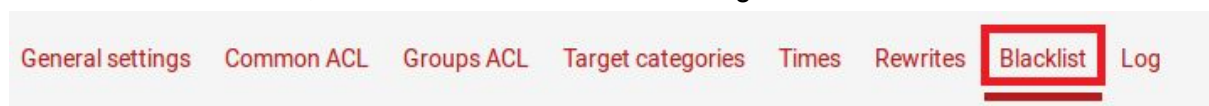


Le téléchargement devrait prendre quelques temps, mais l'avancement de l'opération est affiché dans la console présente juste en dessous :



Une fois la blacklist importée, il ne reste plus qu'à configurer les règles ACL Pfsense lorsque celui-ci va rencontrer une page contenu dans une des nombreuses listes de sites inappropriés.

Pour ce faire, rendez-vous sous l'onglet "Common ACL" :



Un icon "+" précédé de la mention "Target Rules List" va nous permettre d'observer la liste des catégories de sites disponibles. Il faudra manuellement appliquer un filtre sur chacun d'entre eux, en spécifiant si le site est autorisé : "allow", ou non-autorisé : "deny" :

General Options

Target Rules

!blk\_adult all

Target Rules List

1

ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.

Target Categories

[blk_blacklists_ads]	access	----	▼
[blk_blacklists_adult]	access	----	▼
[blk_blacklists_aggressive]	access	----	▼
[blk_blacklists_agressif]	access	whitelist	▼
[blk_blacklists_arjel]	access	deny	3 ▼
[blk_blacklists_associations_religieuses]	access	allow	▼
[blk_blacklists_astrology]	access	----	▼


Attention à bien appliquer les filtres en fonction du contenu concerné. En effet, certaines catégories n'ont clairement pas besoin d'être non-autorisés. Les catégories "Economy", "Press" ou encore "Webmail" ne sont pas susceptibles d'être inappropriées dans le cadre du travail des employés utilisateurs du LAN.

Puisque nous configurons une blacklist, attention à bien régler le reste des sites web accessibles :

[blk_blacklists_special]	access	deny	▼
[blk_blacklists_sports]	access	allow	▼
[blk_blacklists_strict_redirector]	access	deny	▼
[blk_blacklists_strong_redirector]	access	deny	▼
[blk_blacklists_translation]	access	allow	▼
[blk_blacklists_tricheur]	access	deny	▼
[blk_blacklists_update]	access	allow	▼
[blk_blacklists_violence]	access	deny	▼
[blk_blacklists_warez]	access	deny	▼
[blk_blacklists_webmail]	access	allow	▼
Default access [all]	access	allow	▼


Pour terminer, nous cochons quelques fonctionnalités additionnelles de façon à renforcer notre blacklist ::

<b>Do not allow IP-Addresses in URL</b>	<input checked="" type="checkbox"/> To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.
<b>Use SafeSearch engine</b>	<input checked="" type="checkbox"/> Enable the protected mode of search engines to limit access to mature content. At the moment it is supported by Google, Yandex, Yahoo, MSN, Live Search and Bing. Make sure that the search engines can be accessed. It is recommended to prohibit access to others. <b>Note:</b> This option overrides 'Rewrite' setting.
<b>Rewrite</b>	<div>none (rewrite not defined)</div> <div>Enter the rewrite condition name for this rule or leave it blank.</div>
<b>Log</b>	<input checked="" type="checkbox"/> Check this option to enable logging for this ACL.



Maintenant que tout est configuré comme il faut, nous terminons par appliquer les changements sur le service SquidGuard dans l'onglet général :

**General Options**

<b>Enable</b>	<input checked="" type="checkbox"/> Check this option to enable squidGuard. <b>Important:</b> Please set up at least one category on the 'Target Categories' tab before enabling. See <a href="#">this link for details</a> . The Save button at the bottom of this page must be clicked to save configuration changes. To activate squidGuard configuration changes, <b>the Apply button must be clicked.</b> <div style="text-align: center; margin-top: 10px;">  </div>
---------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

SquidGuard service state: **STARTED**

Essayons maintenant de naviguer vers un site interdit, tel que le service de proxy gratuits "hide.me" par la blacklist depuis un poste client du LAN :

### **Request denied by pfSense proxy: 403 Forbidden**

#### **Reason:**

**Client address:** 192.168.1.103  
**Client name:** 192.168.1.103  
**Client group:** default  
**Target group:** blk\_blacklists\_redirector  
**URL:** http://hide.me/fr/proxy

La configuration du filtrage d'URL est maintenant terminé !