

PROXY - PFSENSE

Installation et configuration



TANET Margaux

CPI 2024-2025

Table des matières

I-	Configuration initiale	3
a)	Mettre à jour PfSense	3
b)	Installation des packages	5
II-	Configuration de Squid en proxy transparent avec filtrage SSL	6
a)	Générer le certificat	6
b)	Configuration de Squid.....	8
III-	Configuration de SquidGuard Proxy Filter.....	10
a)	Mise en place du filtrage.....	11
IV-	Configuration LightSquid	13
V-	Tests.....	13
VI-	Conclusion.....	14

Introduction :

Dans ce document, nous verrons comment configurer un SquidGuard sur PfSense pour permettre à notre proxy Squid d'effectuer du filtrage de sites Web basé sur des catégories via une blacklist. Nous verrons donc comment configurer Squid en proxy transparent avec filtrage SSL, comment créer un CA et configurer LightSquid afin de superviser nos connexions.

❖ Qu'est-ce que Squid ?

Squid est un proxy de cache pour le Web prenant en charge HTTP, HTTPS, FTP. Squid optimise le flux de données entre le client et le serveur pour améliorer les performances.

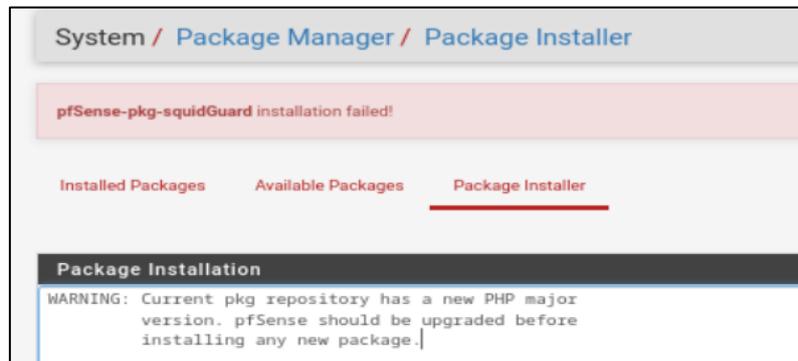
❖ Qu'est-ce que SquidGuard

SquidGuard est un logiciel de redirection d'URL, qui peut être utilisé pour le contrôle du contenu des sites Web auxquels les utilisateurs peuvent accéder. Il est écrit en tant que plug-in pour Squid et utilise des listes noires pour définir les sites pour lesquels l'accès est redirigé.

I- Configuration initiale

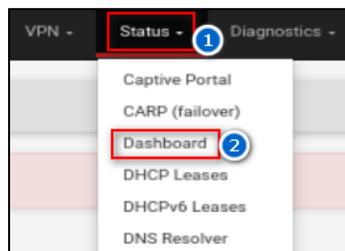
a) Mettre à jour PfSense

Pour l'installation des différents packages **Squid**, **SquidGuard** et **LightSquid** il faut mettre à jour **PfSense** sinon l'installation sera impossible :



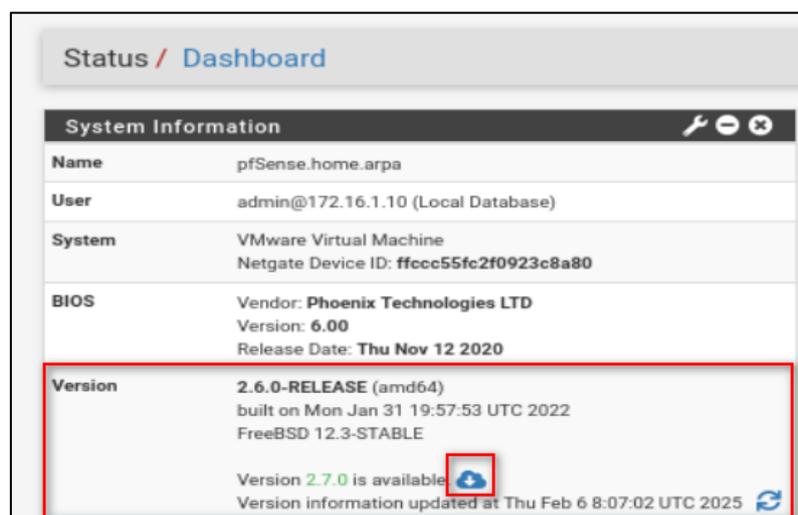
Avant la mise à jour, il faut penser à faire une snapshot de la VM et de désinstaller tous les packages additionnels.

- Se rendre dans **Status** puis **Dashboard** :



On voit que notre version est 2.6.0 et qu'une autre version 2.7.0 est disponible.

- Cliquer sur le nuage pour mettre à jour :



- Une nouvelle page s'affiche, nous confirmons l'installation de la mise à jour en cliquant sur le bouton "**Confirm**" :

The screenshot shows the 'System Update' page in pfSense. The 'Update Settings' tab is active. A confirmation message reads: 'Confirmation Required to update pfSense system.' Below this, there is a dropdown menu for 'Branch' set to 'Latest stable version (v2.7.0)'. A note below the dropdown says: 'Please select the branch from which to update the system firmware. Use of the development version is at your own risk!'. Below the note, there are two rows of information: 'Current Base System' with value '2.6.0' and 'Latest Base System' with value '2.7.0'. At the bottom, there is a 'Confirm Update' section with a green button containing a checkmark and the text 'Confirm'.

La mise à jour se lance :

The screenshot shows the 'Updating System' terminal window. It displays the following information:

```
Number of packages to be removed: 55
Number of packages to be installed: 58
Number of packages to be upgraded: 70
Number of packages to be reinstalled: 41

The process will require 58 MiB more space.
262 MiB to be downloaded.
[1/163] Fetching unbound-1.17.1_3.pkg: ..... done
[2/163] Fetching isc-dhcp44-client-4.4.3P1.pkg: ..... done
[3/163] Fetching php82-session-8.2.6.pkg: ..... done
[4/163] Fetching php82-gmp-8.2.6.pkg: ..... done
[5/163] Fetching wpa_supplicant-2.10_6.pkg: ..... done
[6/163] Fetching nginx-1.24.0_6,3.pkg: ..... done
[7/163] Fetching pfSense-base-2.7.0.pkg: s|
```

L'installation est un peu longue. Au bout de quelques minutes, l'interface web et notre VM PfSense se relancent. On constate que sur mon interface web la mise à jour a bien été effectuée, nous sommes bien en 2.7.0 :

Name	pfSense.home.arp
User	admin@172.16.1.10 (Local Database)
System	VMware Virtual Machine Netgate Device ID: ffccc55fc2f0923c8a80
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.7.0-RELEASE (amd64) built on Wed Jun 28 03:53:34 UTC 2023 FreeBSD 14.0-CURRENT

Si tout se passe bien, dans notre VM PfSense, lors du démarrage nous devrions avoir la version qui est affichée :

```

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.40.134/24
LAN (lan)      -> em1      -> v4: 172.16.1.1/24

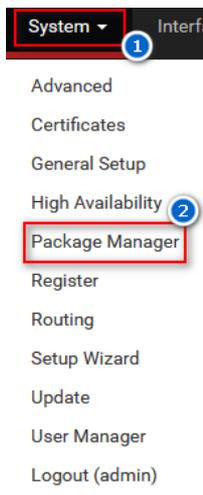
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Disable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

```

Tout s'est bien passé, j'ai mes différentes cartes qui sont remontées aussi nous pouvons continuer avec l'installation des packages.

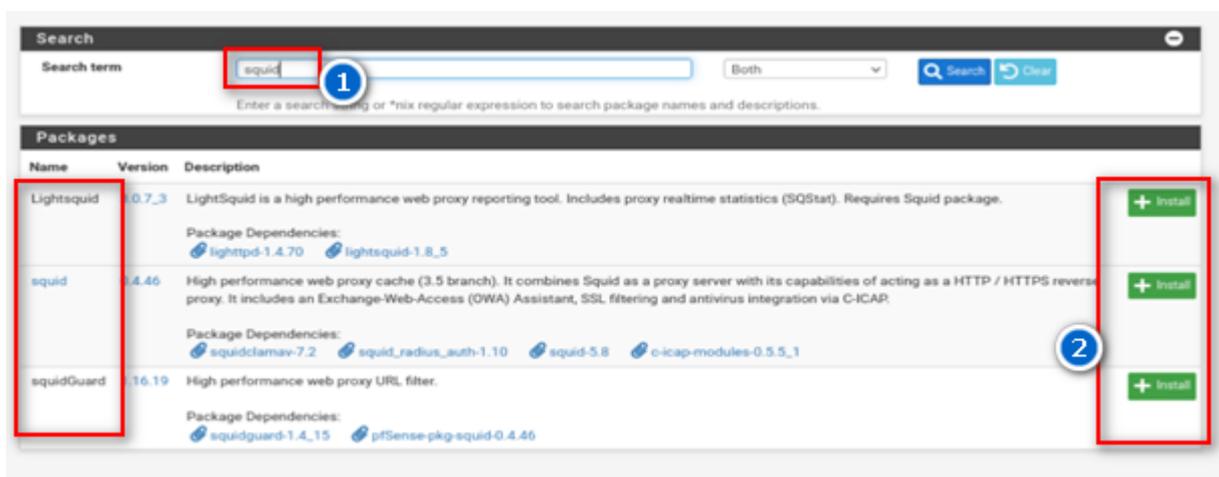
b) Installation des packages

Se rendre dans **System** puis **Package Manager** :



Puis dans **Available Packages** et saisir dans la barre de recherche « Squid » :

- Installer les différents packages **Squid**, **LightSquid** et **SquidGuard**.



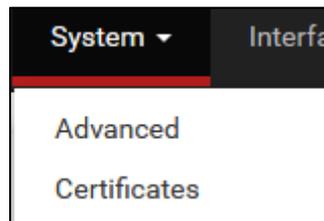
Les installations se sont bien faites :

Installed Packages					
Name	Category	Version	Description	Actions	
✓ Lightsquid	www	3.0.7_3	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package. Package Dependencies: lighttpd-1.4.72 lightsquid-1.8_5		
✓ squid	www	0.4.46	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP. Package Dependencies: squidclamav-7.2 squid_radius_auth-1.10 squid-6.3 c-icap-modules-0.5.5_1		
✓ squidGuard	www	1.16.19	High performance web proxy URL filter. Package Dependencies: squidguard-1.4.15 pfSense-pkg-squid-0.4.46		

II- Configuration de Squid en proxy transparent avec filtrage SSL

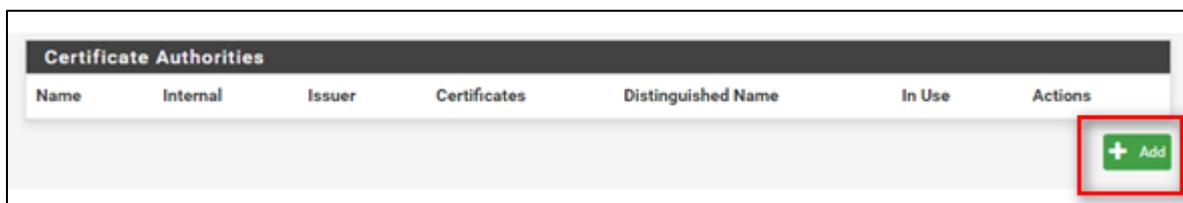
a) Générer le certificat

- Se rendre dans l'onglet **System** puis **Certificates** afin d'ouvrir le gestionnaire de certificats :



Nous allons créer une autorité de certification qui nous permettra ensuite de générer un certificat. Ce certificat sera distribué sur le client afin de rendre le proxy transparent.

- Dans l'onglet **Authorities**, cliquer sur le bouton « **Add** » :



- Ici, je remplis le nom de l'autorité de certification et j'indique que je veux créer une autorité de certification en sélectionnant **create an internal certificate authority** :

System / Certificate / Authorities / Edit

Authorities Certificates Revocation

Create / Edit CA

Descriptive name: certif authority

Method: Create an Internal Certificate Authority

Trust Store: Add this Certificate Authority to the Operating System Trust Store

Randomize Serial: Use random serial numbers when signing certificates

Internal Certificate Authority

Key type: RSA

2048

Digest Algorithm: sha256

Lifetime (days): 3650

Common Name: internal-ca

Country Code: None

Mon autorité de certification est créée :

- Cliquer sur l'étoile pour exporter le certificat.

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
certif authorities	✓	self-signed	0	CN=internal-ca Valid From: Thu, 06 Feb 2025 11:25:59 +0000 Valid Until: Sun, 04 Feb 2035 11:25:59 +0000	Squid (1)	

Le téléchargement se fait nous avons notre certificat :



- Se rendre dans les paramètres de notre navigateur et rechercher notre **gestionnaire de certificats**. Cliquer sur importer et injecter le certificat.

Gestionnaire de certificats

Vos certificats Décisions d'authentification Personnes Serveurs **Autorités**

Vous possédez des certificats enregistrés identifiant ces autorités de certification

Nom du certificat	Périphérique de sécurité
ACCRAIZ1	Builtin Object Token
Actalis S.p.A./03358520967	Builtin Object Token
AffirmTrust	Builtin Object Token

Voir... Modifier la confiance... **Importer...** Exporter... Supprimer ou ne plus faire confiance...

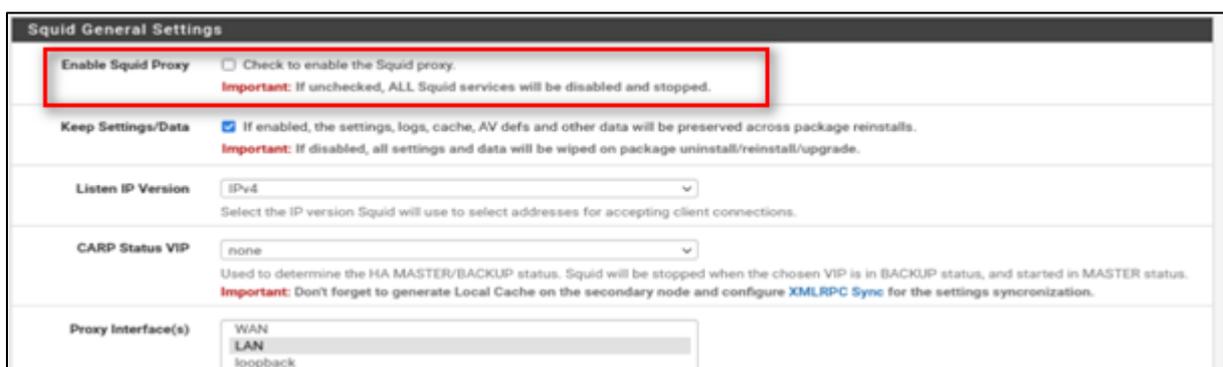
OK

b) Configuration de Squid

- Se rendre dans **Services** puis **Squid Proxy Server** :



- Sur la page générale de cet onglet, il faut cocher, dans la rubrique **Squid général Settings** : Enable Squid Proxy :



- Dans la rubrique **Transparent Proxy Settings**, cocher **Transparent http Proxy** :

Transparent Proxy Settings

Transparent HTTP Proxy Enable transparent mode to forward all requests for destination port 80 to the proxy server.

Transparent proxy mode works without any additional configuration being necessary on clients.
Important: Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below.
Hint: In order to proxy both HTTP and HTTPS protocols **without intercepting SSL connections**, configure WPAD/PAC options on your DNS/DHCP servers.

Transparent Proxy Interface(s)
 WAN
 LAN
 The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.

Bypass Proxy for Private Address Destination Do not forward traffic to Private Address Space (RFC 1918 and IPv6 ULA) destinations.
 Destinations in Private Address Space (RFC 1918 and IPv6 ULA) are passed directly through the firewall, not through the proxy server.

Bypass Proxy for These Source IPs
 Do not forward traffic from these source IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall.
Applies only to transparent mode. Separate entries by semi-colons (,)

Bypass Proxy for These Destination IPs
 Do not proxy traffic going to these destination IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall.
Applies only to transparent mode. Separate entries by semi-colons (,)

- Dans la rubrique **SSL Man in the Middle Filtering** cocher la case pour HTTPS/SSL Interception :

SSL Man In the Middle Filtering

HTTPS/SSL Interception Enable SSL filtering.

SSL/MITM Mode
 Splice Whitelist, Bump Otherwise
 The SSL/MITM mode determines how SSL interception is treated when 'SSL Man in the Middle Filtering' is enabled.
 Default: Splice Whitelist, Bump Otherwise. [Click info for details.](#)

SSL Intercept Interface(s)
 WAN
 LAN
 The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.

SSL Proxy Port
 3129
 This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129

- Enfin dans la rubrique **CA**, mettre l'autorité de certification que nous avons créé précédemment :

SSL Proxy Compatibility Mode
 Modern
 The compatibility mode determines which cipher suites and TLS versions are supported. Default: Modern. [Click info for details.](#)

DHParams Key Size
 2048 (default)
 DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.

CA
 certif authority
 Select Certificate Authority to use when SSL interception is enabled.

- Cliquer sur **save** pour sauvegarder les paramètres.
- Toujours dans l'onglet **Squid Server Proxy**, aller dans la rubrique **Local Cache** pour définir la taille qui sera dédiée au cache pour éviter les erreurs par la suite :

Package / Proxy Server: General Settings / General

General Remote Cache **Local Cache** Antivirus ACLs Traffic Mgmt Authentication Users Real Time Status

- Pour **Hard Disk Cache Size**, changer la taille du cache :

Squid Hard Disk Cache Settings

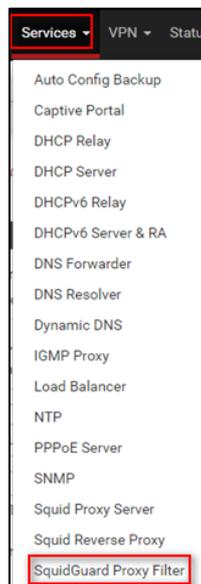
Hard Disk Cache Size
Amount of disk space (in megabytes) to use for cached objects.

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

Sauvegarder les paramètres réalisés.

III- Configuration de SquidGuard Proxy Filter

- Se rendre dans **Service** puis **SquidGuard Proxy Filter** :



- Dans **General Settings**, cocher la case **check this option to enable SquiGuard** et cliquer sur **Apply** pour démarrer le service :

Package / Proxy filter SquidGuard: General settings / General settings

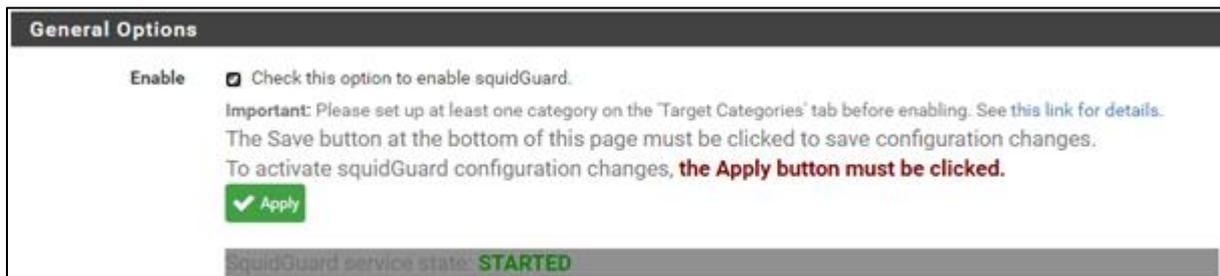
General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log XMLRPC Sync

General Options

Enable Check this option to enable squidGuard.
Important: Please set up at least one category on the 'Target Categories' tab before enabling. See [this link for details](#).
The Save button at the bottom of this page must be clicked to save configuration changes.
To activate squidGuard configuration changes, **the Apply button must be clicked.**

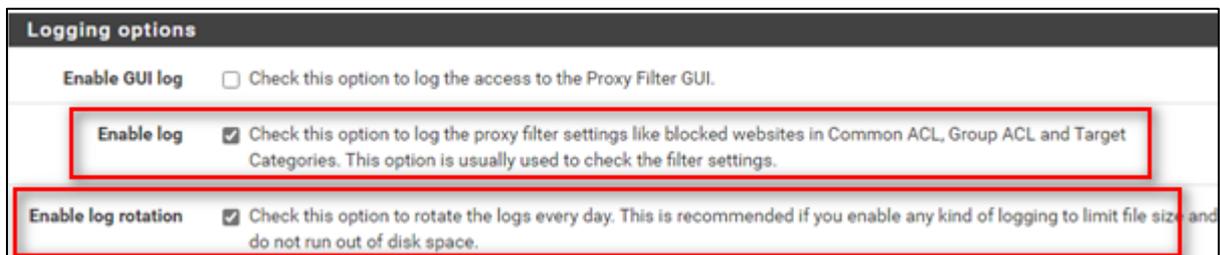
SquidGuard service state: **STOPPED**

Le service démarre :



Ne pas oublier de toujours faire **Apply** et **Save** après toutes modifications.

- Plus bas, cocher les cases **Enable log** et **enable log rotation** pour pouvoir suivre les évènements sur le proxy :



a) Mise en place du filtrage

Nous allons mettre en place une blacklist afin de bloquer la catégorie **social media** pour que l'utilisateur n'est pas accès à facebook.

- Pour cela, toujours dans **Proxy filter SquidGuard** les paramètres généraux, cocher la case **Blacklist** et renseigner la liste de l'université de Toulouse dans la ligne **Blacklist URL** :

URL de l'université de Toulouse : http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz



Sauvegarder les paramètres.

- Se rendre sur l'onglet **Blacklist**, renseigner l'URL utilisé précédemment. Cliquer sur le bouton **Download** pour que les filtres se téléchargent :

0 %

Enter FTP or HTTP path to the blacklist archive here.

- Se rendre dans l'onglet **Common ACL** et cliquer sur « +/- » pour dérouler le menu.
- Une liste apparaît, il faut trouver la ligne social network. Au bout de la ligne, renseigner accès **Deny** pour bloquer l'accès :

[blk_blacklists_marketingware]	access	---	▼
[blk_blacklists_mixed_adult]	access	---	▼
[blk_blacklists_mobile-phone]	access	---	▼
[blk_blacklists_phishing]	access	---	▼
[blk_blacklists_press]	access	---	▼
[blk_blacklists_publicite]	access	---	▼
[blk_blacklists_radio]	access	---	▼
[blk_blacklists_reaffected]	access	---	▼
[blk_blacklists_redirector]	access	---	▼
[blk_blacklists_remote-control]	access	---	▼
[blk_blacklists_residential-proxies]	access	---	▼
[blk_blacklists_sect]	access	---	▼
[blk_blacklists_sexual_education]	access	---	▼
[blk_blacklists_shopping]	access	---	▼
[blk_blacklists_shortener]	access	---	▼
[blk_blacklists_social_networks]	access	deny	▼
[blk_blacklists_special]	access	---	▼
[blk_blacklists_sports]	access	---	▼
[blk_blacklists_stalkerware]	access	---	▼
[blk_blacklists_strict_redirector]	access	---	▼
[blk_blacklists_strong_redirector]	access	---	▼
[blk_blacklists_translation]	access	---	▼
[blk_blacklists_tricheur]	access	---	▼

Laisser par défaut **Allow** :

[blk_blacklists_webmail]	access	---	▼
Default access [all]	access	allow	▼

- Cocher **Do not allow IP addresses in URL** pour empêcher les utilisateurs de contourner le filtrage dans le cas où ils utiliseraient leur adresse IP au lieu de leur nom de domaine pour l'accès au site.

Do not allow IP-Addresses in URL 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.

Proxy Denied Error

- Retourner sur **General Settings** pour enregistrer les modifications en faisant **Apply** et **Save**.

IV- Configuration LightSquid

- Se rendre dans l'onglet **Status** et cliquer sur **Squid Proxy Reports** :

Ici on peut changer nos identifiants de connexions et valider les changements :

Web Service Settings

Lightsquid Web Port
Port the lighttpd web server for Lightsquid will listen on. (Default: 7445)

Lightsquid Web SSL Use SSL for Lightsquid Web Access
This option configures the Lightsquid web server to use SSL and uses the WebGUI HTTPS certificate.

Lightsquid Web User
Username used to access lighttpd. (Default: admin)

Lightsquid Web Password
Password used to access lighttpd. (Default: pfsense)

Links [➔ Open Lightsquid](#) [➔ Open sqstat](#)

V- Tests

- Cliquer sur **Open Lightsquid**, une page s'ouvre contenant des informations.

[Squid rapport d'accès utilisateur](#)
Période de travail: **Fev 2025**

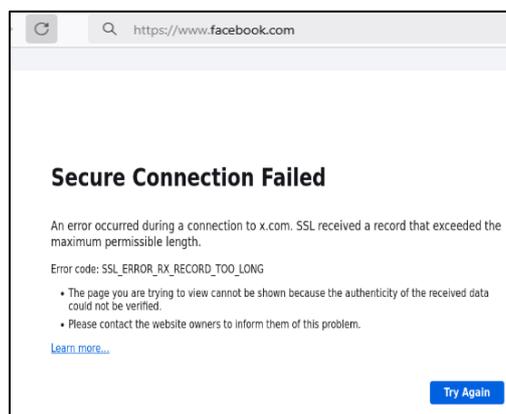
Calendar
2025
01 02 03 04 05 06 07 08 09 10 11 12

Date	Groupe Utilisateurs	Quota Dépassé	Octets	Moyenne	Hit %
06 Fev 2025	grp	1	1	78.7 M	78.7 M 0.00%
Total/Moyenne:		1	1	78.7 M	78.7 M 0.00%

[LightSquid v1.8](#) (c) Sergey Erokhin AKA ESL

Je n'ai pas réussi à accéder à l'adresse <http://172.16.1.1:7445> pour voir les informations sur les logs.

Testons de se connecter à facebook, normalement avec le filtrage on ne devrait pas accéder au site :



La requête pour facebook a bien été bloquée.

VI- Conclusion

Nous avons mis en place Squid en proxy transparent et activé le filtrage SLL en passant par la création de notre CA. Nous avons importé la blacklist de l'université de Toulouse pour bloquer la catégorie « social media » en testant une connexion sur Facebook. Nous avons vu que notre filtrage a fonctionné, nous n'avons pas d'accès à Facebook. Nous avons mis en place LightSquid afin de voir les connexions qui se faisaient.