
Installation de Squid Proxy et Anti-virus

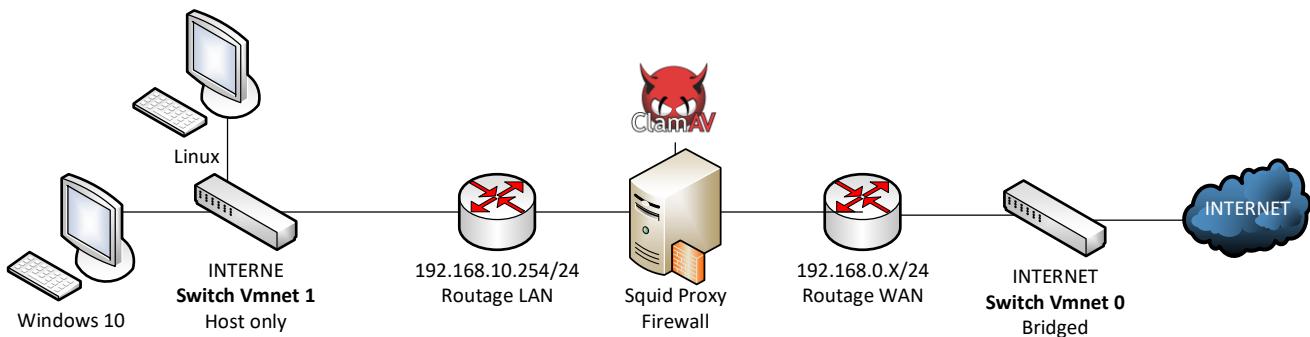
Objectifs traités

| | |
|--|------|
| <i>Installation des packages</i> | 2-2 |
| <i>Mise en place filtrage HTTPS</i> | 2-5 |
| <i>Configuration de Squid Proxy Server</i> | 2-7 |
| <i>Configuration de SquidGuard</i> | 2-11 |
| <i>Configuration de LightSquid</i> | 2-15 |
| <i>Configuration du NAT pour un serveur WEB en DMZ</i> | 2-17 |
| <i>Configuration de ClamAV Anti-virus</i> | 2-20 |

Installation des packages

Nous allons installer un Proxy transparent, pourquoi transparent, tout simplement car il est entre le réseau local et le réseau internet (mondiale) ce qui de ce fait, oblige toutes les requêtes à passer à son travers et permet de n'avoir aucune configuration à faire sur les machines du réseau local.

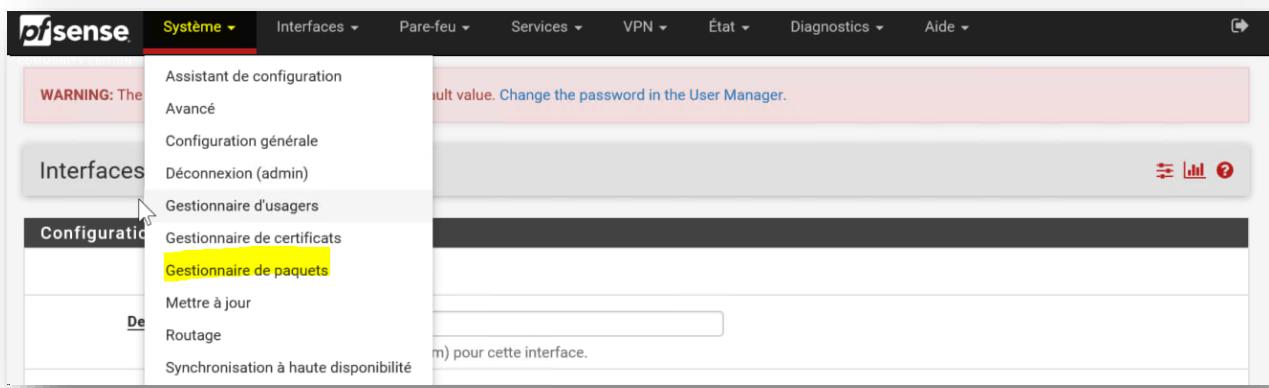
Les clients pensent se connecter au serveur final alors que c'est le proxy qui traite leurs requêtes en se faisant passer par le serveur final.



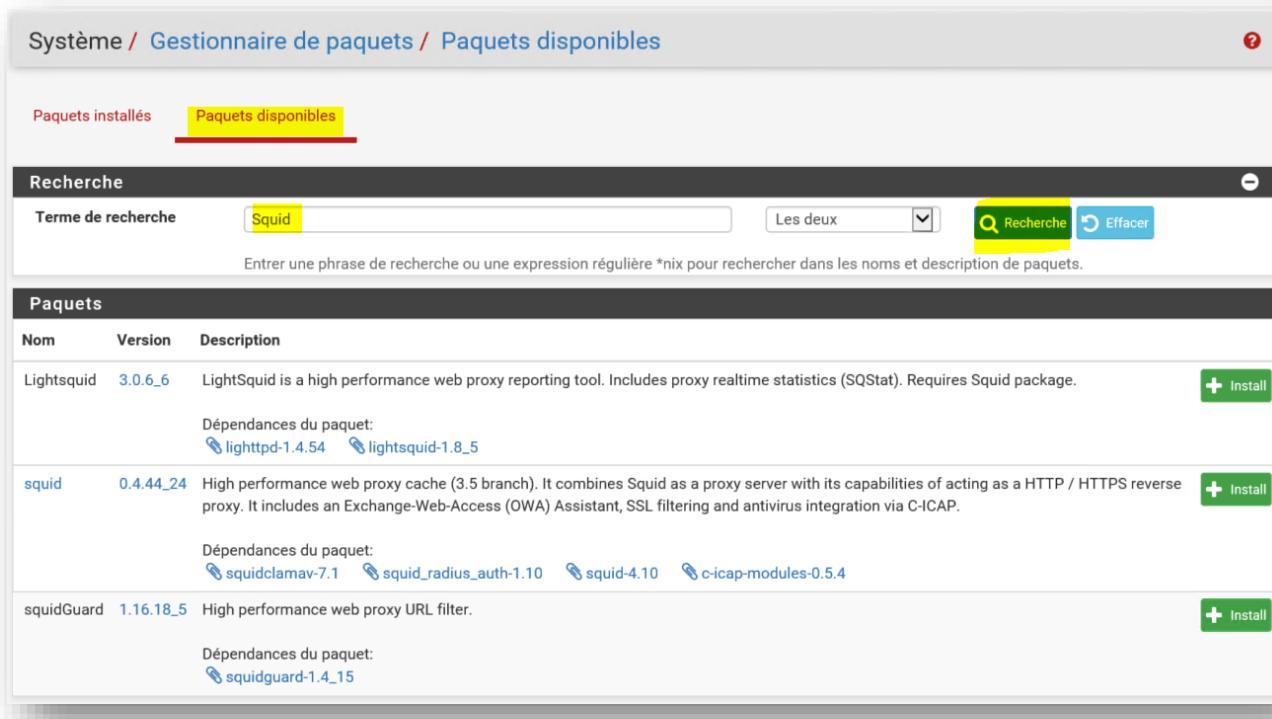
Dans les Packages d'installation nous allons installer 3 packages qui sont :

- **Squid** qui sera le proxy transparent contenant aussi ClamAV Antivirus
- **SquidGuard** qui servira à filtrer les accès vers le réseau extérieur (internet permettant ainsi de bloquer des sites en fonction de la politique de l'entreprise).
- **LightSquid** qui jouera le rôle d'analyseur son forme de site web utilisant le port **7445** ce qui permettra de voir les sites consultés en fonction de l'adresse IP du client.

L'installation des packages se trouve dans système puis **Gestionnaire de paquets**



Cliquer sur **Paquets disponibles** puis dans la recherche taper **Squid** puis **Recherche**
 Cliquer ensuite sur chaque **Install** de chaque paquet  pour qu'il soit installer un par un



Système / Gestionnaire de paquets / Paquets disponibles

Paquets installés Paquets disponibles

Recherche

Terme de recherche Squid Les deux Recherche Effacer

Entrer une phrase de recherche ou une expression régulière *nix pour rechercher dans les noms et description de paquets.

Paquets

| Nom | Version | Description | |
|--|-----------|---|---|
| Lightsquid | 3.0.6_6 | LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package. |  |
| Dépendances du paquet: | | | |
|  lighttpd-1.4.54  lightsquid-1.8_5 | | | |
| squid | 0.4.44_24 | 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. |  |
| Dépendances du paquet: | | | |
|  squidclamav-7.1  squid_radius_auth-1.10  squid-4.10  c-icap-modules-0.5.4 | | | |
| squidGuard | 1.16.18_5 | High performance web proxy URL filter. |  |
| Dépendances du paquet: | | | |
|  squidguard-1.4_15 | | | |

Cliquer sur **confirmer** pour démarrer l'installation

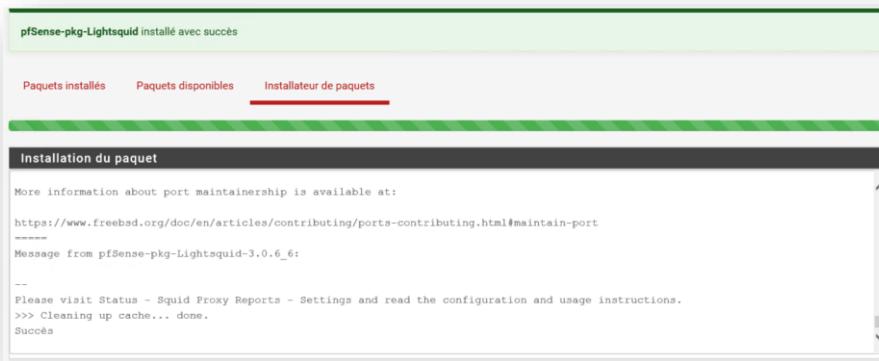


Paquets installés Paquets disponibles Installateur de paquets

Confirmation requise pour installer le paquet pfSense-pkg-Lightsquid.



Installation du premier paquet est installer, répéter la même opération pour les 2 autres



pfSense-pkg-Lightsquid installé avec succès

Paquets installés Paquets disponibles Installateur de paquets

Installation du paquet

More information about port maintainership is available at:
<https://www.freebsd.org/doc/en/articles/contributing/ports-contributing.html#maintain-port>

Message from pfSense-pkg-Lightsquid-3.0.6_6:

--
 Please visit Status - Squid Proxy Reports - Settings and read the configuration and usage instructions.
 >>> Cleaning up cache... done.
 Succès

Voici le résultat obtenu à la fin de l'installation des 3 packages dans **Paquet installés**.

Système / Gestionnaire de paquets / Paquets installés

Paquets installés Paquets disponibles

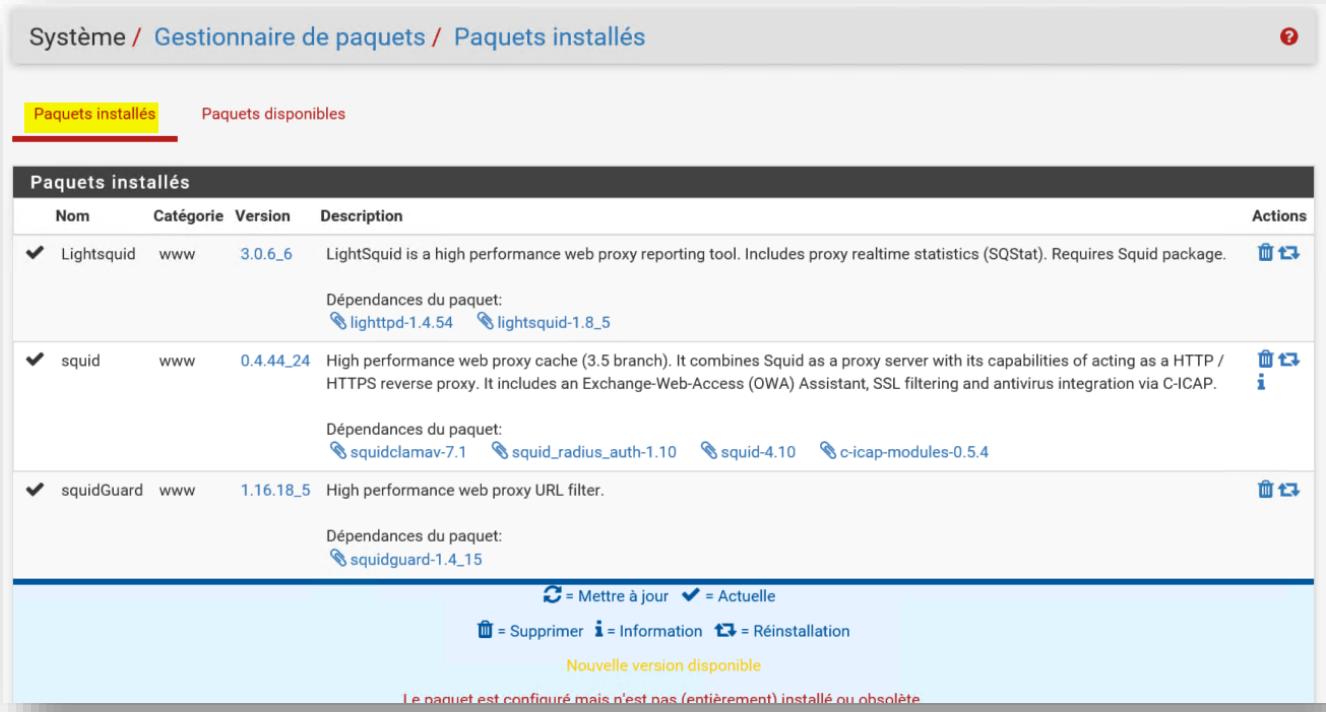
| Paquets installés | | | | Actions |
|---|-----------|-----------|---|---------|
| Nom | Catégorie | Version | Description | |
| ✓ Lightsquid | www | 3.0.6_6 | LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package. | |
| Dépendances du paquet: | | | | |
| lighttpd-1.4.54 lightsquid-1.8_5 | | | | |
| ✓ squid | www | 0.4.44_24 | 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. | |
| Dépendances du paquet: | | | | |
| squidclamav-7.1 squid_radius_auth-1.10 squid-4.10 c-icap-modules-0.5.4 | | | | |
| ✓ squidGuard | www | 1.16.18_5 | High performance web proxy URL filter. | |
| Dépendances du paquet: | | | | |
| squidguard-1.4_15 | | | | |

= Mettre à jour = Actuelle

= Supprimer = Information = Réinstallation

Nouvelle version disponible

Le paquet est configuré mais n'est pas (entièrement) installé ou obsolète



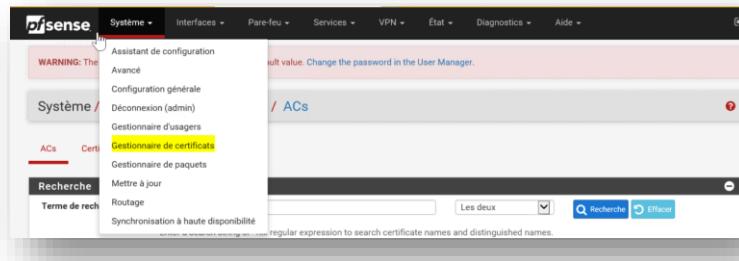
Mise en place du certificat filtre HTTPS

Comme nous voulons avec squidguard filtrer des pages HTTP, il faut mettre en place un certificat pour intercepter SSL sur le réseau et bloquer certains sites en HTTPS.

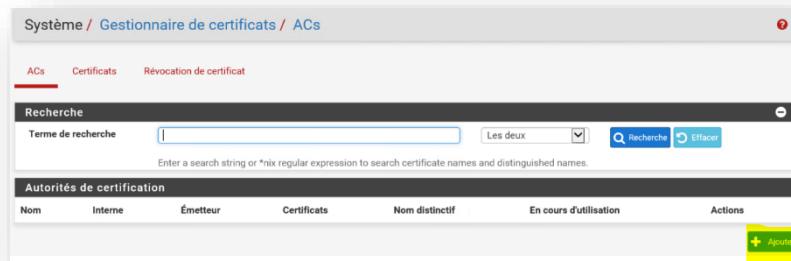
Sans cela aucune interception en HTTPS n'est possible.

Il faut créer une autorité de certification dans pfSense car c'est lui qui est routeur principal sur le réseau et oblige tous les utilisateurs passe par lui pour accéder au réseau internet.

Pour créer le certificat aller dans **système** puis **gestionnaire de certificats**



Cliquer sur **Ajouter**



Remplir le champs **description Name** les autres sont facultatif et cliquer sur **enregistrer**

Le certificat est créé et prêt pour son utilisation.

The screenshot shows the pfSense web interface with the following details:

- Header:** Système, Interfaces, Pare-feu, Services, VPN, État, Diagnostics, Aide.
- Warning Message:** WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
- Breadcrumbs:** Système / Gestionnaire de certificats / ACs
- Navigation:** ACs (selected), Certificats, Révocation de certificat.
- Search Bar:** Recherche, Term de recherche (empty), Les deux, Recherche, Effacer.
- Table Headers:** Autorités de certification, Nom, Interne, Émetteur, Certificats, Nom distinctif, En cours d'utilisation, Actions.
- Table Data:** CA-LUIS (selected), checked, auto-signé, 0, ST=Île de France, O=Formation, L=Melun, CN=internal-ca, C=FR, Valable depuis: Sat, 09 May 2020 16:47:07 +0000, Valide jusqu'au: Tue, 07 May 2030 16:47:07 +0000.
- Buttons:** Ajouter (Add).

Configuration de Squid Proxy Server

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

La configuration se fait en allant dans les **Services** puis **Squid proxy server**



Aller dans **local cache** et paramétrer le **hard disks cache size à 600 Mo** puis cliquer sur **enregistrer**

Squid Cache General Settings

- Cache Replacement Policy: Heap LFUDA
- Low Water Mark in %: 90
- High Water Mark in %: 95
- Do Not Cache: (empty input field)
- Enable Offline Mode: (checkbox unchecked)
- External Cache Managers: (empty input field)

Squid Hard Disk Cache Settings

- Hard Disk Cache Size: 600
- Hard Disk Cache System: ufs
- Clear Disk Cache NOW: (button)
- Level 1 Directories: 16
- Hard Disk Cache Location: /var/squid/cache
- Minimum Object Size: 0
- Maximum Object Size: 4

Squid Memory Cache Settings

- Memory Cache Size: 64
- Maximum Object Size in RAM: 256
- Memory Replacement Policy: Heap GDDF

Dynamic and Update Content

- Cache Dynamic Content: (checkbox unchecked)
- Custom refresh_patterns: (empty input field)

Enregistrer (Save)

Aller ensuite sur l'onglet **General** et activer **Enable squid proxy** et **Resolve DNS IPV4 First**

Squid General Settings

- Enable Squid Proxy** Check to enable the Squid proxy.
Important: If unchecked, ALL Squid services will be disabled and stopped.
- Keep Settings/Data** If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.
Important: If disabled, all settings and data will be wiped on package un/install/reinstall/upgrade.
- Listen IP Version** IPv4
Select the IP version Squid will use to select addresses for accepting client connections.
- Proxy Interface(s)** LAN
OPT1
WAN
boucle locale
The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.
- Port du mandataire (proxy)** 3128
This is the port the proxy server will listen on. Default: 3128
- ICP Port**
This is the port the proxy server will send and receive ICP queries to and from neighbor caches.
Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.
- Allow Users on Interface** If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy.
There will be no need to add the interface's subnet to the list of allowed subnets.
- Patch Captive Portal** This feature was removed - see Bug #5594 for details!
- Resolve DNS IPV4 First** Enable this to force DNS IPv4 lookup first.
This option is very useful if you have problems accessing HTTPS sites.
- Disable ICMP** Check this to disable Squid ICMP pinger helper.
- Use Alternate DNS Servers for the Proxy Server**
To use DNS servers other than those configured in System > General Setup, enter the IP(s) here. Separate entries by semi-colons (;)

Activer **Transparent http proxy**

Transparent Proxy Settings

- Transparent HTTP Proxy** Enable transparent mode to forward all requests for destination port 80 to the proxy server.
 - Info** 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)** LAN
OPT1
WAN
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 (;)

Cocher **HTTPS/SSL Interception/SSL filtering** puis sélectionner **Splice All** et enfin ajouter le **certificat** créer précédemment.

Le mode « Splice ALL » permet à pfSense de capturer à la volée et d'effectuer le contrôle sur le flux sans manipulation sur les machines clientes, il permet aussi de bloquer les sites web interdits via la rubrique « ACL » de Squid.

Cocher **Enable Access Logging** puis définir le nombre de jours ou les logs peuvent être conservé ici **180** Jours.

Dans **Error Language** selectionner **fr** et cocher **Suppress Squid Version** puis **enregistrer** le tout

Headers Handling, Language and Other Customizations

| | | |
|---|-------------------------------------|---|
| Visible Hostname | localhost | This is the hostname to be displayed in proxy server error messages. |
| Administrator's Email | admin@localhost | This is the email address displayed in error messages to the users. |
| Error Language | fr | Select the language in which the proxy server will display error messages to users. |
| X-Forwarded Header Mode | (on) | Choose how to handle X-Forwarded-For headers. Default: on i |
| Disable VIA Header | <input type="checkbox"/> | If not set, Squid will include a Via header in requests and replies as required by RFC2616. |
| URI Whitespace Characters Handling | strip | Choose how to handle whitespace characters in URL. Default: strip i |
| Suppress Squid Version | <input checked="" type="checkbox"/> | Suppresses Squid version string info in HTTP headers and HTML error pages if enabled. |

Enregistrer **Afficher les options avancées**

Configuration de 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.

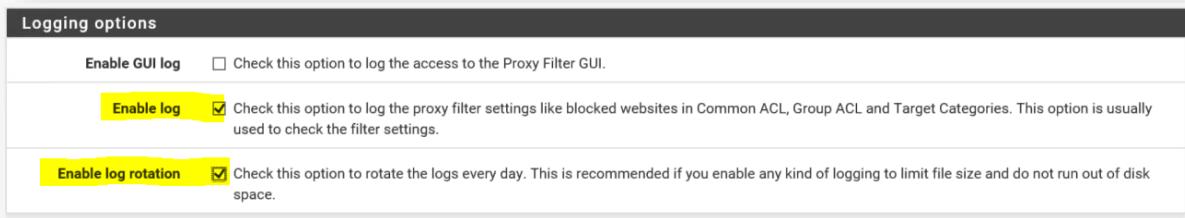
Pour configurer SquiGuard aller dans **Services** puis **SquidGuard Proxy Filter**



Dans **Général settings** cocher la case **check this option to enable squidguard**

The screenshot shows the 'General settings' tab of the SquidGuard configuration page. The 'Activer' checkbox is checked, with the instruction 'Check this option to enable squidGuard.' Below it, there is an 'Important' note: 'Please set up at least one category on the 'Target Categories' tab before enabling. See [this link for details.](#)' It also states: '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.**' A green 'Apply' button is visible. At the bottom, it says 'SquidGuard service state: STOPPED'.

Cocher **enable log** et **enable log rotation**

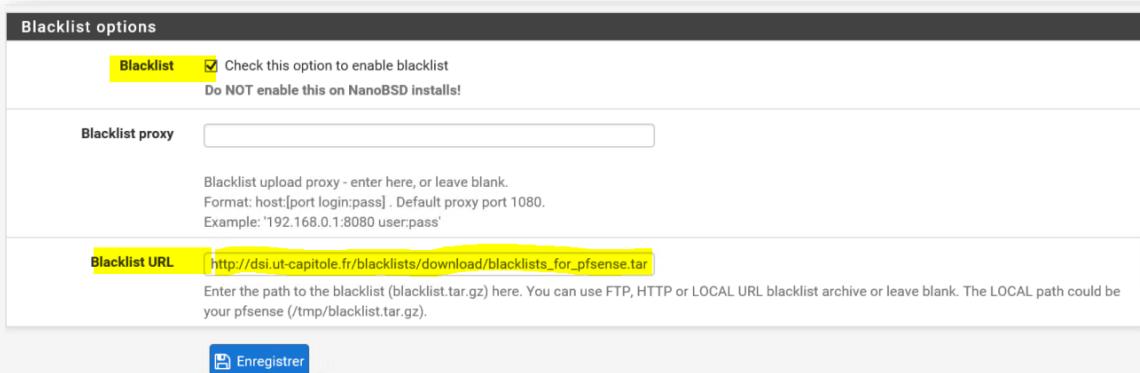


Cocher **check this option to enable**

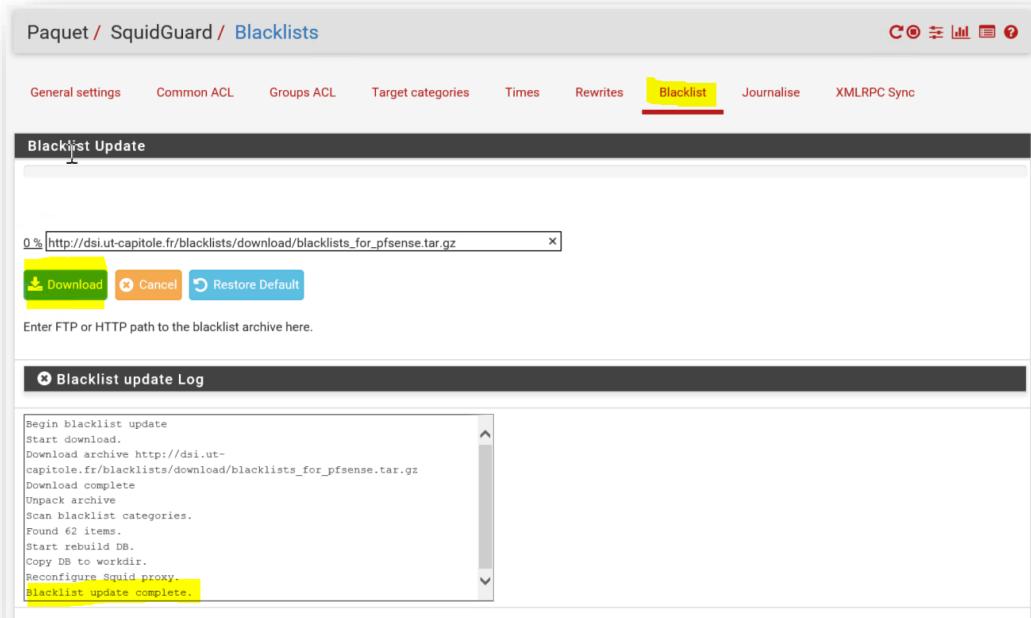
Dans **Blacklist URL** taper le site ci-dessous

http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz

Cliquer sur **Enregistrer** pour valider l'ensemble de la page



Aller dans l'onglet **Blacklist** et cliquer sur **Download** pour télécharger la liste de filtrage.



Aller dans l'onglet **Common ACL** puis cliquer dans **+ de Target Rules List**

Il est important dans default Access all en bas de la liste de sélectionner Allow

Cela permet d'activer toutes les règles et d'en suite bloquer par **deny** celle que l'on souhaite.

Dans cet exemple les règles pour le site adultes est appliquée ainsi que pour les réseaux sociaux.

The screenshot shows the 'Common ACL' tab selected in the top navigation bar. Below it, the 'Target Rules List' section is active, indicated by a yellow highlight. The list displays numerous target categories, each with an 'access' dropdown menu. Most categories have 'access' set to 'deny'. A specific category, 'blk_blacklists_adult', has its 'access' dropdown set to 'allow', which is highlighted with a yellow box. At the bottom of the list, there is a row for 'Default access [all]' with an 'access' dropdown set to 'allow'.

| Category | Access Rule |
|---|-------------|
| [blk_blacklists_adult] | allow |
| [blk_blacklists_agressif] | deny |
| [blk_blacklists_arjel] | deny |
| [blk_blacklists_associations_religieuses] | deny |
| [blk_blacklists_astrology] | deny |
| [blk_blacklists_audio-video] | deny |
| [blk_blacklists_bank] | deny |
| [blk_blacklists_bitcoin] | deny |
| [blk_blacklists_blog] | deny |
| [blk_blacklists_celebrity] | deny |
| [blk_blacklists_chat] | deny |
| [blk_blacklists_child] | deny |
| [blk_blacklists_cleaning] | deny |
| [blk_blacklists_cooking] | deny |
| [blk_blacklists_cryptojacking] | deny |
| [blk_blacklists_dangerous_material] | deny |
| [blk_blacklists_dating] | deny |
| [blk_blacklists_ddos] | deny |
| [blk_blacklists_dialer] | deny |
| [blk_blacklists_doh] | deny |
| [blk_blacklists_download] | deny |
| [blk_blacklists_drogue] | deny |
| [blk_blacklists_educational_games] | deny |
| [blk_blacklists_exceptions_liste_bu] | deny |
| [blk_blacklists_filehosting] | deny |
| [blk_blacklists_financial] | deny |
| [blk_blacklists_forums] | deny |
| [blk_blacklists_gambling] | deny |
| [blk_blacklists_games] | deny |
| [blk_blacklists_hacking] | deny |
| [blk_blacklists_jobsearch] | deny |
| [blk_blacklists_lingerie] | deny |
| [blk_blacklists_liste_blanche] | deny |
| [blk_blacklists_liste_bu] | deny |
| [blk_blacklists_malware] | deny |
| [blk_blacklists_manga] | deny |
| [blk_blacklists_marketingware] | deny |
| [blk_blacklists_mixed_adult] | deny |
| [blk_blacklists_mobile-phone] | deny |
| [blk_blacklists_phishing] | deny |
| [blk_blacklists_press] | deny |
| [blk_blacklists_publicode] | deny |
| [blk_blacklists_radio] | deny |
| [blk_blacklists_reaffected] | deny |
| [blk_blacklists_redirector] | deny |
| [blk_blacklists_remote-control] | deny |
| [blk_blacklists_sect] | deny |
| [blk_blacklists_sexual_education] | deny |
| [blk_blacklists_shopping] | deny |
| [blk_blacklists_shortener] | deny |
| [blk_blacklists_social_networks] | deny |
| [blk_blacklists_special] | deny |
| [blk_blacklists_sports] | deny |
| [blk_blacklists_stalkerware] | deny |
| [blk_blacklists_strict_redirector] | deny |
| [blk_blacklists_strong_redirector] | deny |
| [blk_blacklists_translation] | deny |
| [blk_blacklists_tricheur] | deny |
| [blk_blacklists_update] | deny |
| [blk_blacklists_vpn] | deny |
| [blk_blacklists_warez] | deny |
| [blk_blacklists_webmail] | deny |
| Default access [all] | allow |

Cocher do not **allowIP adresses in URL** et **Use SafeSearch engine**
 Cliquer ensuite sur **enregistrer**.

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

The first part of the error message displayed to clients when access was denied. Defaults to "Request denied by \$g[product_name] proxy"

Redirect mode

Select redirect mode here.
 Note: if you use 'transparent proxy', then 'int' redirect mode will not accessible.
 Options: ext url err page , ext url redirect , ext url as 'move' , ext url as 'found'.

Redirect info

Enter external redirection URL, error message or size (bytes) here.

Use SafeSearch engine 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.
 Note: This option overrides 'Rewrite' setting.

Rewrite

Enter the rewrite condition name for this rule or leave it blank.

Journalise Check this option to enable logging for this ACL.

Enregistrer

La validation définitive des paramètres doit se faire depuis l'onglet **General Setting** en cliquant sur **Apply**

A chaque modification dans SquiGard il faut cliquer sur apply dans General Setting

Paquet / Proxy filter SquidGuard: General settings / General settings

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

Options générales

Activer 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**.

Apply

SquidGuard service state: **STARTED**

Voici l'erreur depuis le site Facebook du aux blocages des réseaux sociaux depuis les filtres



Configuration de LightSquid

LightSquid est un outil de reporting et d'analyse des accès depuis SquidProxy Server. Il permet de suivre les connexions des stations de travail depuis un réseau local vers internet en interceptant les url HTTP ou HTTPS depuis un log exploitable à partir d'une page web utilisant le port 7445.

Le paramétrage se fait à partir de **Etat** puis **Squid Proxy Reports**

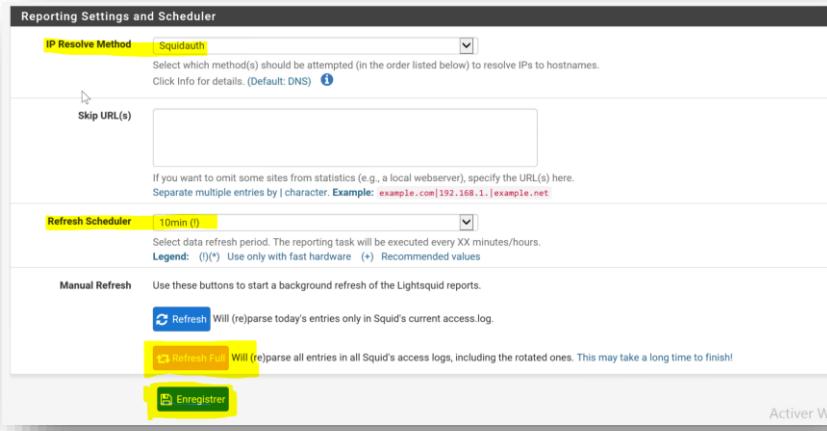


Décocher **Lightsquid Web SSL** pour effectuer une connexion en http **puis définir un mot de passe admin**

Changer le language en **Français**

The screenshot shows the Lightsquid configuration interface. In the 'Web Service Settings' section, the 'Lightsquid Web Port' is set to 7445. The 'Lightsquid Web SSL' checkbox is unchecked. The 'Lightsquid Web User' is set to 'admin' and the 'Lightsquid Web Password' is set to '*****'. In the 'Links' section, there are buttons for 'Open Lightsquid' and 'Open sqstat'. In the 'Report Template Settings' section, the 'Language' is set to 'Français', 'Report Template' is set to 'Base', and 'Bar Color' is set to 'Orange'.

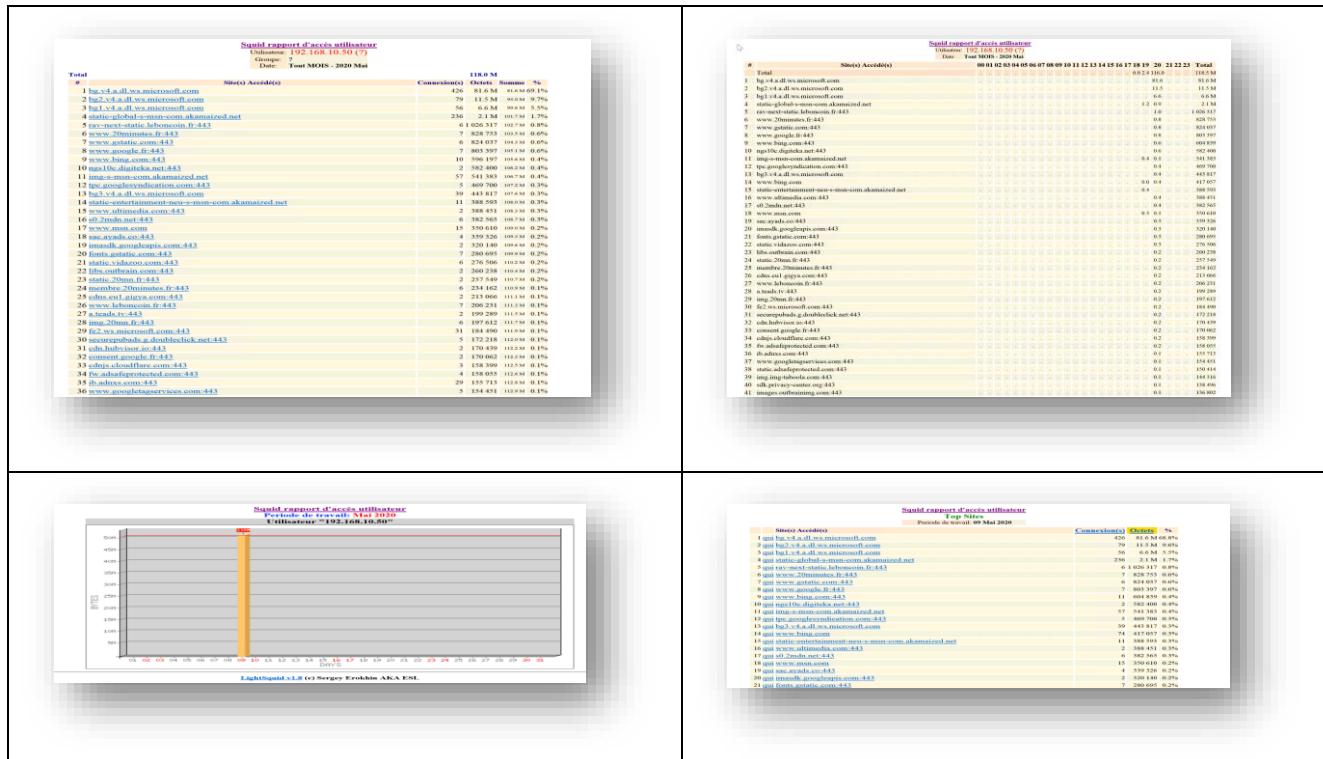
Sélectionner dans **IP resolve Method Squidauth** définir dans **refresh scheduler 10mn** cocher ensuite **Enregister** puis **Refresh Full**



Pour se connecter taper dans le navigateur <http://192.168.10.254:7445>



On peut même avoir un détail des connexions selon la date et la machine, des graphiques, des tops sites, du temps passé etc...

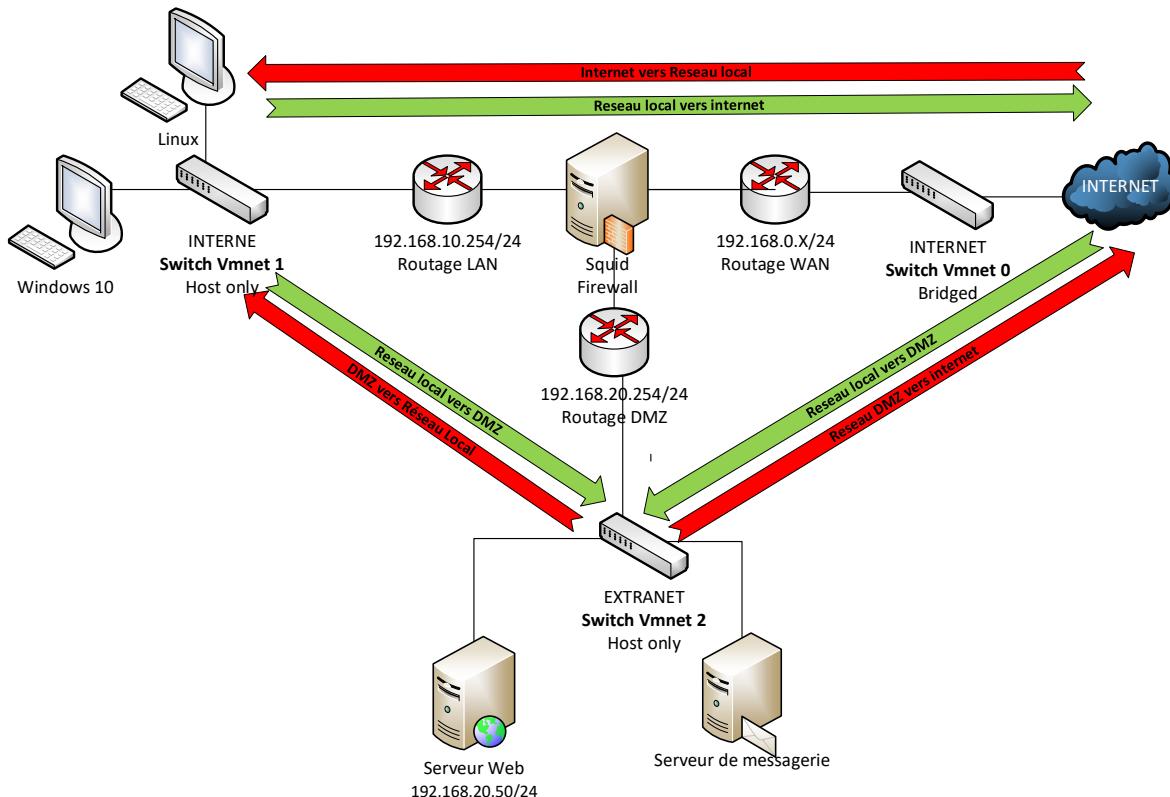


Configuration du NAT pour un serveur WEB en DMZ

Le but d'une DMZ est de protéger son réseau local contre les attaques provenant du réseau internet, la DMZ est une zone intermédiaire placée sur un autre réseau local protégé par des pare-feu et un routage spécifique.

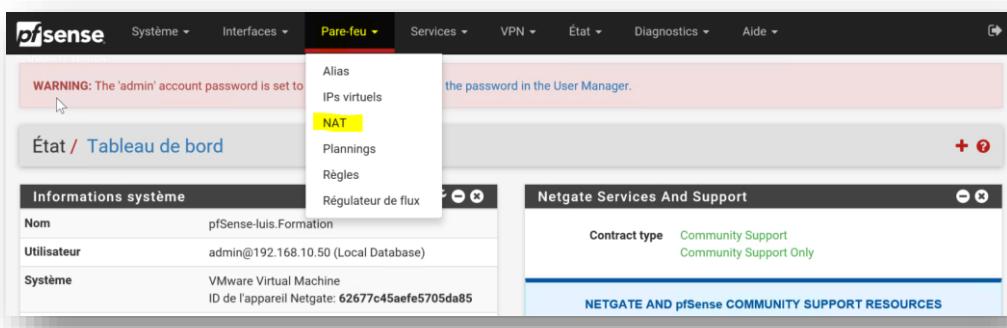
Sur cette zone se trouve le plus souvent des serveurs auxquels les machines du réseau local peuvent accéder et aussi le réseau internet.

En rouge les interdictions d'un réseau vers un autre en NAT, en vert ce qui est autorisé en NAT



Dans cette exemple il va falloir faire du NAT et utiliser le pare-feu pour permettre au station venant d'internet d'accéder au site web dans la DMZ.

Pour configurer la redirection de port aller dans **Pare-feu** puis **NAT**



Cliquer sur **ajouter** pour créer une nouvelle règle.

Pare-feu / NAT / Transfert de port

Transfert de port 1:1 Sortant NPT

Règles

| Interface | Protocole | Adresse source | Ports source | Adresse de destination | Ports dest. | IP NAT | Ports NAT | Description | Actions |
|-----------|-----------|----------------|--------------|------------------------|-------------|--------|-----------|-------------|--|
| | | | | | | | | | <input type="button" value="Ajouter"/> <input type="button" value="Supprimer"/> <input type="button" value="Enregistrer"/> <input type="button" value="Séparateur"/> |

Dans **plage de port de destination** définir **HTTP** et **HTTP, IP de redirection** correspond au serveur WEB ici **192.168.20.50** **port de redirection cible HTTP, description** du serveur, et **autoriser association de règles de filtre**.

Cliquer sur **Enregistrer**

Pare-feu / NAT / Transfert de port / Modifier

Modifier l'entrée de redirection

Désactivé Désactiver cette règle

Pas de RDR (NOT) Désactiver la redirection pour le trafic vérifié par cette règle
Cette option est rarement nécessaire. Ne pas l'utiliser sans avoir connaissance des implications.

Interface: WAN

Protocole: TCP

Source:

Destination: Inverser les critères. Type:
Plage de port de destination: Du port: Au port: Personnalisé(e)
Spécifier le port ou le groupe de port pour la destination du paquet pour ce mapping. Le champ "tous" est laissé vide seulement si un seul port est mappé.

IP de redirection cible:
Entrez l'adresse IP interne du serveur sur lequel les ports doivent être mappés.
ex : 192.168.1.12

Port de redirection cible:
Port: Personnalisé(e)
Spécifiez le port sur la machine qui a l'adresse IP entrée ci-dessous. Dans le cas d'un groupe de port, spécifiez le port de début du groupe (le port de fin sera calculé automatiquement). Ceci est habituellement identique avec la partie "Depuis le port" spécifiée ci-dessus.

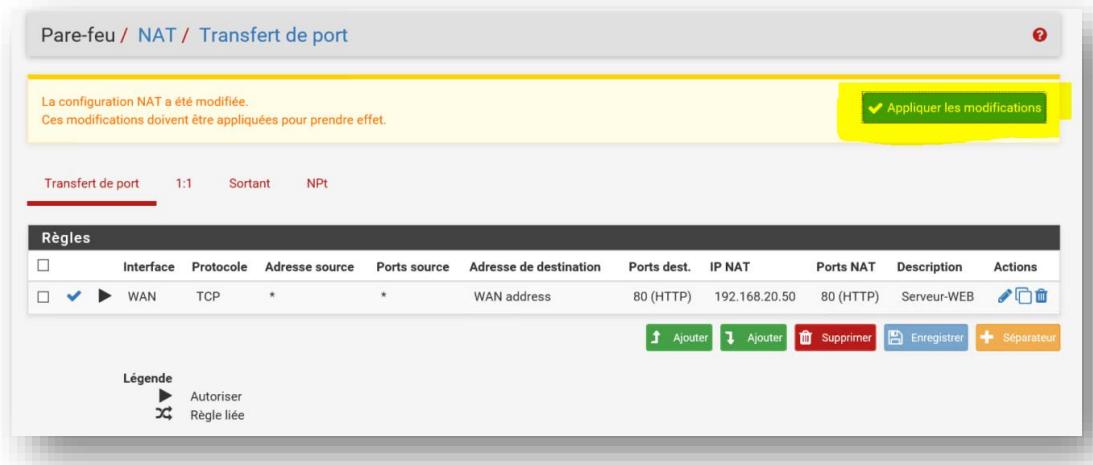
Description: Serveur-WEB
Une description peut être saisie ici à des fins de référence administrative (non analysée).

Pas de synchronisation XMRPC: Ne pas synchroniser automatiquement avec les autres membres CRAP
Ceci empêche la règle sur Maitre de se synchroniser automatiquement avec les autres membres CARP. Cela n'empêche PAS que la règle soit écrasée sur l'Esclave.

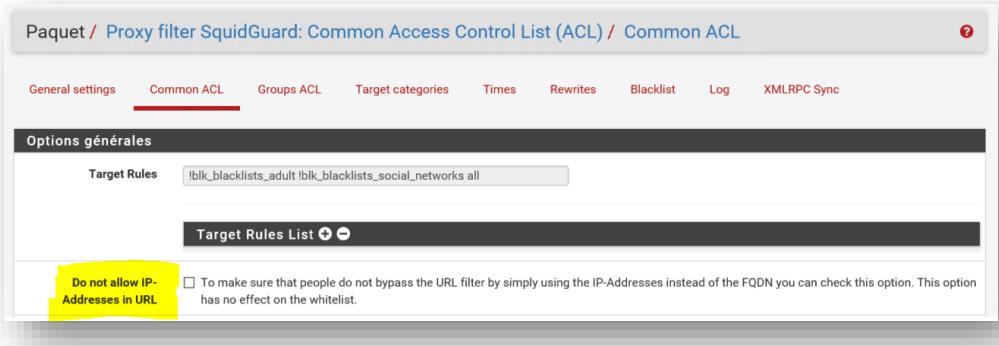
Réflexion NAT: Utiliser les paramètres par défaut du système

Association des Règle de filtre:
La sélection de "pass" ne fonctionne pas correctement avec plusieurs WAN. Cela fonctionnera uniquement sur une interface ayant la passerelle par défaut.

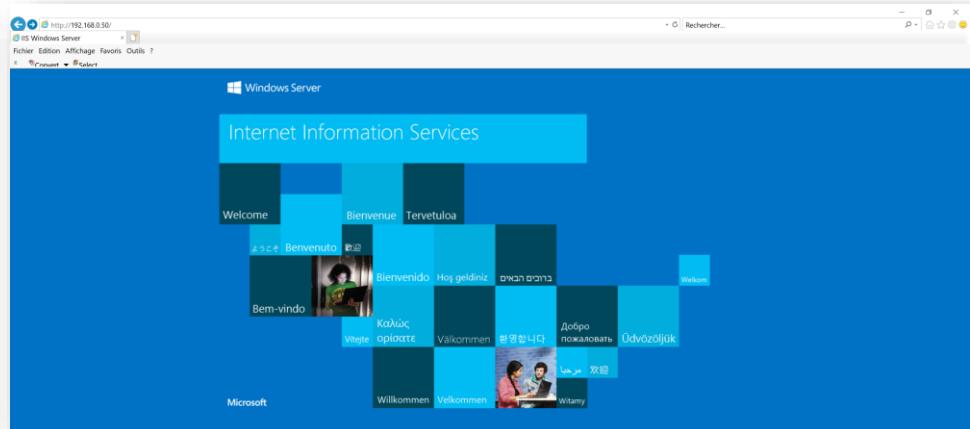
Cliquer ensuite sur **Appliquer les modifications**



Au cas où on ne pourrait pas accéder depuis l'extérieur on peut décocher dans **proxy filter squidguard do not allow ip-adresses in url**
Cela devrait fonctionner après.



L'accès se fait depuis une machine extérieure avec une adresse publique rediriger vers le serveur en zone DMZ



Configuration de ClamAV Anti-virus

Pfsense ne dispose pas d'Anti-virus, c'est à l'installation de Squid Server que ClamAV est installé. Il faut simplement le configurer pour qu'il télécharge sa base anti-virus à jour.

Pour configurer ClamAV, retourner sur **Services** puis **Squid Proxy Server**



Puis sélectionner **Anti-virus**



Cocher **Enable AV** puis **Google safe Brownsing** (Attention demande plus de ressources RAM 4 Go Minimum) Exclure **la video et l'audio**, choisir un **site miroir** puis cliquer **sur update AV** et **Enregistrer**

ClamAV Anti-Virus Integration Using C-ICAP

Enable AV Enable Squid antivirus check using ClamAV.

Client Forward Options Send both client username and IP info (Default)

Enable Manual Configuration désactivé

Redirect URL

Google Safe Browsing Enables Google Safe Browsing support.

Exclude Audio/Video Streams This option disables antivirus scanning of streamed video and audio.

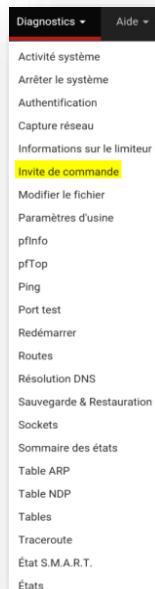
ClamAV Database Update every 24 hours

Regional ClamAV Database Update Mirror Europe

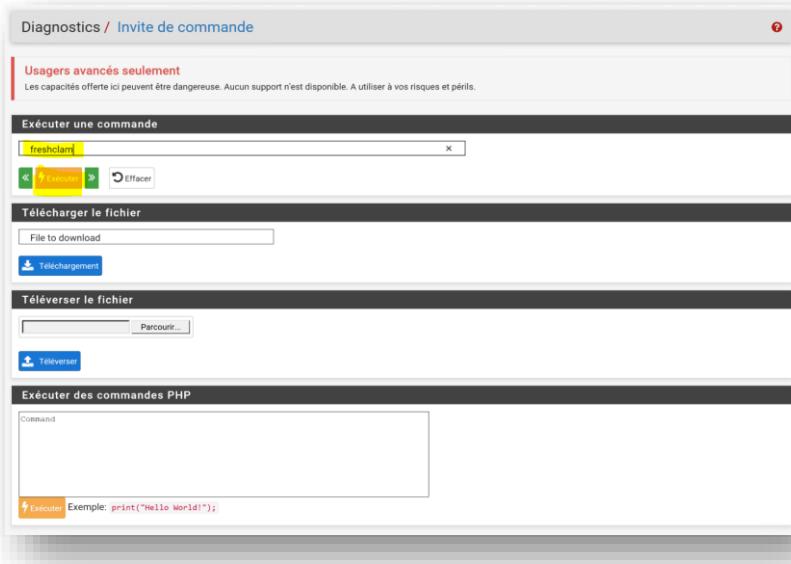
Optional ClamAV Database Update Servers Enter ClamAV update servers here, or leave empty. Separate entries by semi-colons (:) Note: For official update mirrors, use db.XY.clamav.net format. (Replace XY with your country code.)

Enregistrer **Afficher les options avancées**

Pour rafraîchir, il faut se rendre dans **Diagnostics** puis **invite de commande**



Puis lancer la commande **freshclam** et exécuter



Voici le résultat

```
Sortie Console - freshclam
ClamAV update process started at Thu May 28 21:49:10 2020
WARNING: Your ClamAV installation is OUTDATED!
WARNING: Local version: 0.102.2 Recommended version: 0.102.3
DON'T PANIC! Read https://www.clamav.net/documents/upgrading-clamav
daily.cvd database is up to date (version: 25827, sigs: 2516600, f-level: 63, builder: rayman)
main.cvd database is up to date (version: 59, sigs: 4564902, f-level: 60, builder: sigmgr)
bytecode.cvd database is up to date (version: 331, sigs: 94, f-level: 63, builder: anvilleg)
safebrowsing.cvd database is up to date (version: 49191, sigs: 2213119, f-level: 63, builder: google)
```

Aller ensuite dans le menu **Etat** puis **Services** si ClamAV Antivirus n'est pas actif il suffit de le démarrer.

| Service | Description | État | Actions |
|----------------|---|------|---|
| c-icap | ICAP Interface for Squid and ClamAV integration | ✓ | C R |
| clamd | ClamAV Antivirus | ✓ | C R |
| dhcpcd | Service DHCP | ✓ | C R I H M |
| dpinger | Démon de surveillance des passerelles | ✓ | C R I H M |
| lightsquid_web | Lightsquid Web Server | ✓ | C R |
| ntpd | Synchronisation horloge NTP | ✓ | C R I H M |
| openvpn | OpenVPN server: VPN-Formation | ✓ | C R I H M |
| squid | Squid Proxy Server Service | ✓ | C R I H M |
| squidGuard | Proxy server filter Service | ✓ | C R |
| syslogd | Le Démone de la journalisation système | ✓ | C R I |
| unbound | Résolveur DNS | ✓ | C R I H M |

Vérification sur un site de test eicar.org et on clique sur un fichier de test pour voir.

The screenshot shows the eicar.org website's download section. It includes a purple 'MEMBERS AREA' sidebar with login fields for 'Loginname' and 'Password'. The main content area has a 'DOWNLOAD' button and a 'DOWNLOADED' section containing four files:

- eicar.com (68 Bytes)
- eicar.com.txt (68 Bytes)
- eicar_com.zip (184 Bytes)
- eicarcom2.zip (308 Bytes)

ClamAV Antivirus a fait son travail

The screenshot shows the SquidClamav 7.1 interface with the message "SquidClamav 7.1 : Virus detected!". It details the following information:

- The requested URL <http://2016.eicar.org/download/eicar.com.txt> contains a virus
- Virus name: Win.Test.EICAR.HDB-1
- This file cannot be downloaded.
- Origin: 192.168.10.54 / -
- Powered by SquidClamav 7.1

Notes Personnel