

Documentation technique

*27/02/2024
Installation de
SQUID sur PfSense*

Sommaire

- Définition
- Schéma réseau
- Installation de SQUID sur PfSense
- Configurer squid proxy sur PfSense
- Tester le proxy transparent
- Configurer squid en proxy transparent https

Définition

Serveur proxy

Les serveurs proxy permettent de sécuriser et d'améliorer l'accès à certaines pages Web en les stockant en cache (ou copie). Ainsi, lorsqu'un navigateur envoie une requête sur la demande d'une page Web qui a été précédemment stockée, la réponse et le temps d'affichage en sont améliorés. L'utilisateur accède plus rapidement au site et ne sature pas le proxy pour sortir. Les serveurs proxy renforcent également la sécurité en filtrant certains contenus Web et les logiciels malveillants.

Filtrage

Le filtrage est appliqué en fonction de la politique de sécurité en place sur le réseau. Cela permet de bloquer selon une liste noire, les sites considérés comme malveillants et/ou inutiles au contexte de travail de l'entreprise (armes, drogues, etc).

Authentification

Afin de limiter l'accès au réseau extérieur, et de renforcer ainsi la sécurité du réseau local, il peut être nécessaire de mettre en place un système d'authentification pour accéder aux ressources extérieures. Ceci est assez dissuasif pour les utilisateurs souhaitant visiter des sites contraires à la charte de leur système d'information. Ils se sentent suivis et restent sensés dans leurs recherches.

Stockage des logs

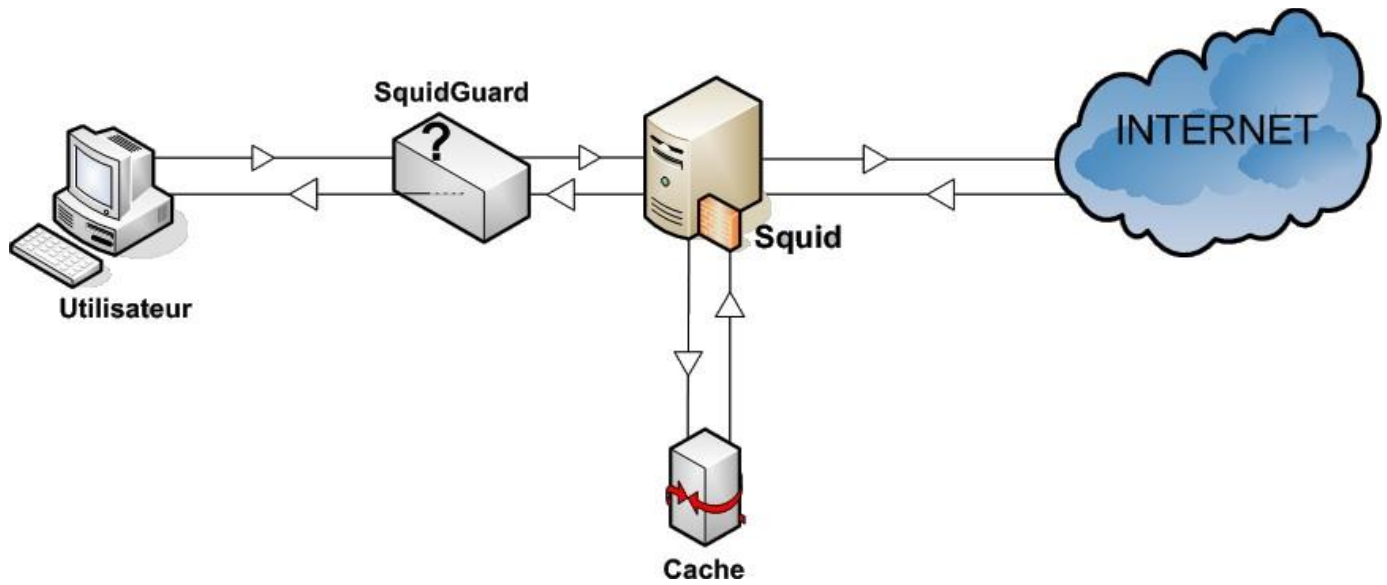
Le stockage des logs des sites visités et des pages vues, permet à l'administrateur du réseau de redéfinir la politique de sécurité du réseau et/ou d'intervenir auprès d'un utilisateur qui visite fréquemment des sites malveillants ou sans rapport avec l'activité de l'entreprise.

Squid

Squid est un serveur proxy-cache, c'est à dire, qu'il stocke les données fréquemment consultées sur les pages Web (notamment les images) sur un serveur cache du réseau local pour éviter de les télécharger à chaque connexion. De même, il peut mettre en mémoire cache les requêtes DNS. Il permet ainsi de réduire et d'optimiser l'usage de la bande passante vers Internet et du réseau en général, d'ouvrir Internet aux machines situées derrière un pare feu, de restreindre les ressources web utilisables et d'en contrôler l'utilisation.

Squid et Squidguard (filtre) sont disponibles sous forme de packages sur PfSense.

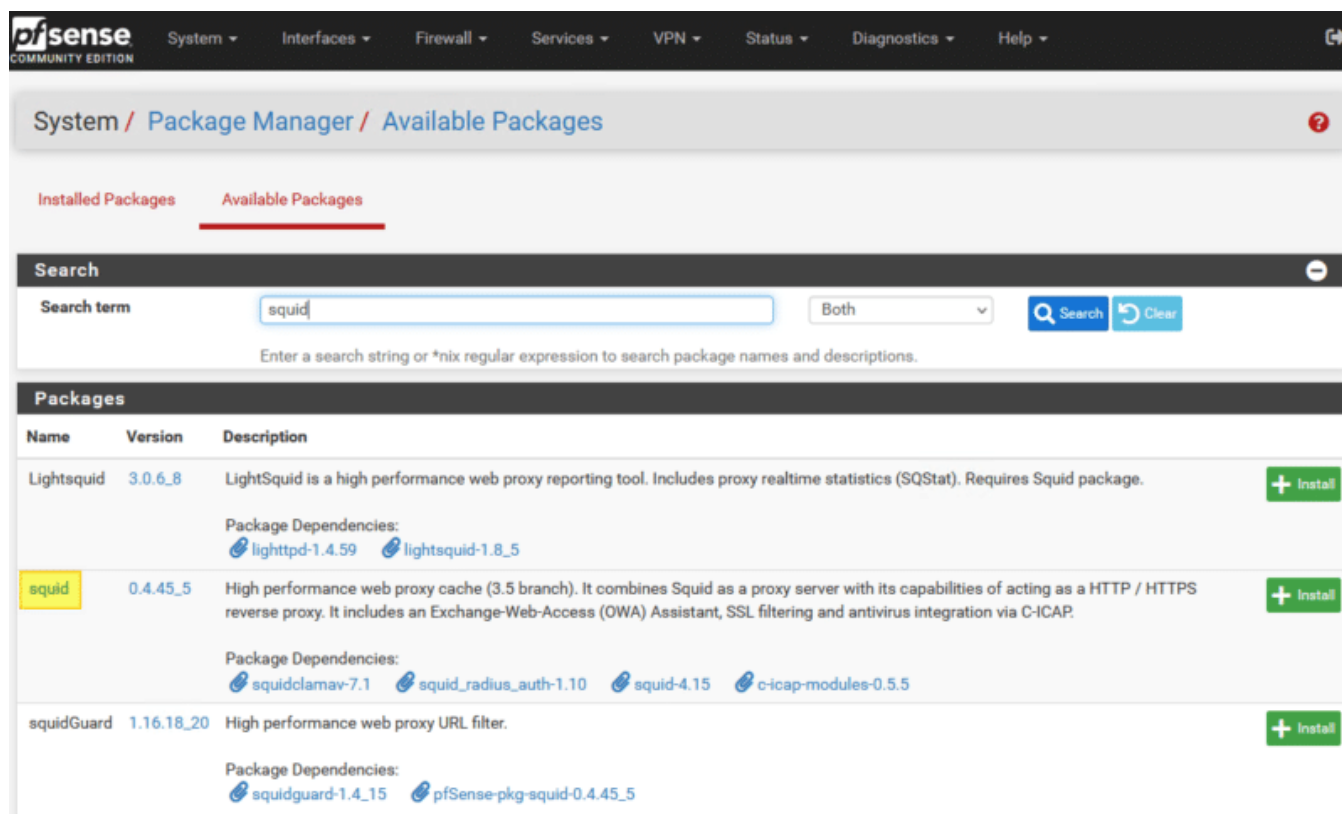
Schéma réseau



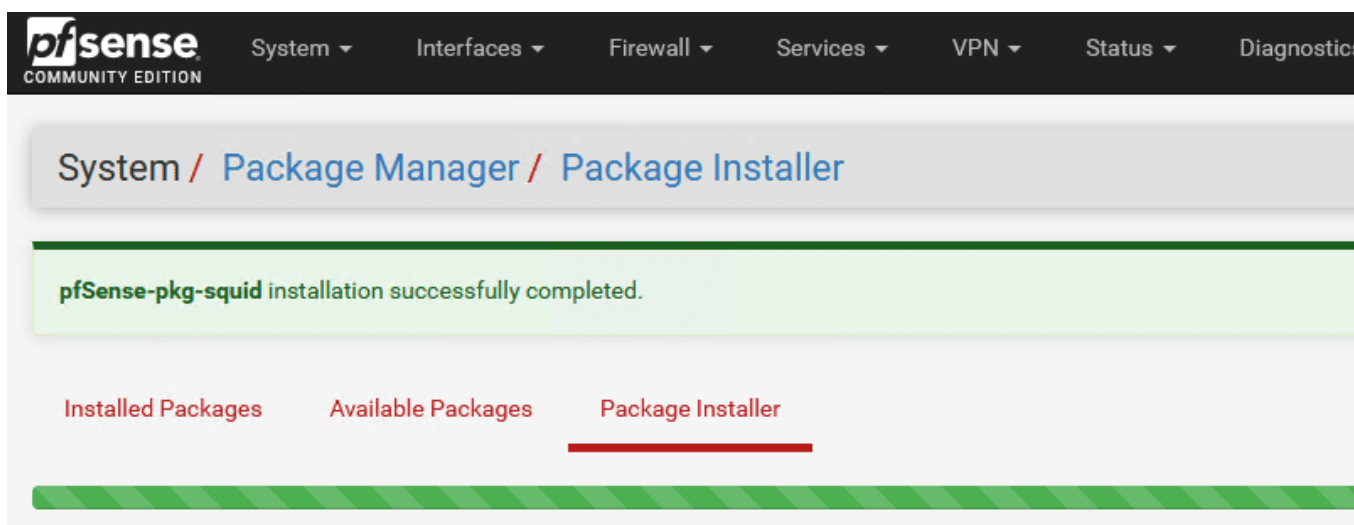
Installation de SQUID sur PfSense

Pour installer SQUID, connectez-vous sur l'interface d'administration de PfSense afin d'installer le paquet *squid*. Pour cela, sous « **System** », cliquez sur « **Package Manager** » et ensuite sur l'onglet « **Available Packages** ».

Recherchez « **squid** » et cliquez sur le bouton « **Install** » à droite, au niveau de la ligne correspondante.



À la fin de l'installation, le message « **pfSense-pkg-squid installation successfully completed** » doit s'afficher.



Une fois le paquet installé, on peut passer à la configuration.

Configurer squid proxy sur PfSense

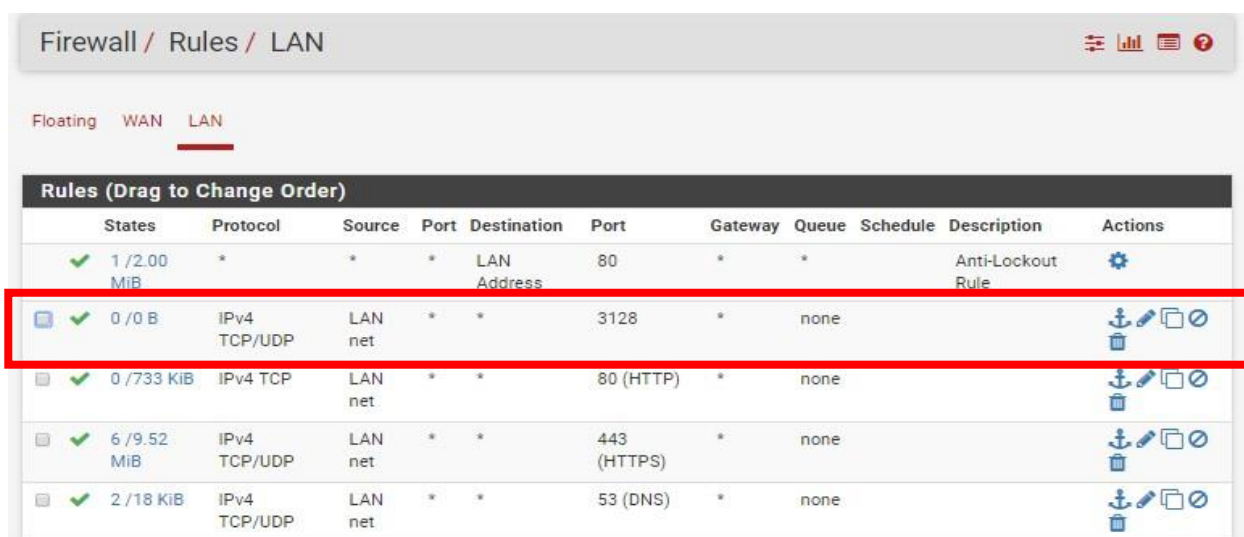
La configuration de Squid s'effectue via le menu « **Services** », puis « Squid Proxy Server ».

La configuration est découpée en plusieurs onglets. Afin de pouvoir activer Squid, **il faut configurer le cache local sinon le démarrage du processus Squid échouera**. Cliquez sur l'onglet « **Local Cache** ». Comme pour chaque section, nous retrouvons de nombreux paramètres... Pour le cache, j'attire votre attention sur ces options :

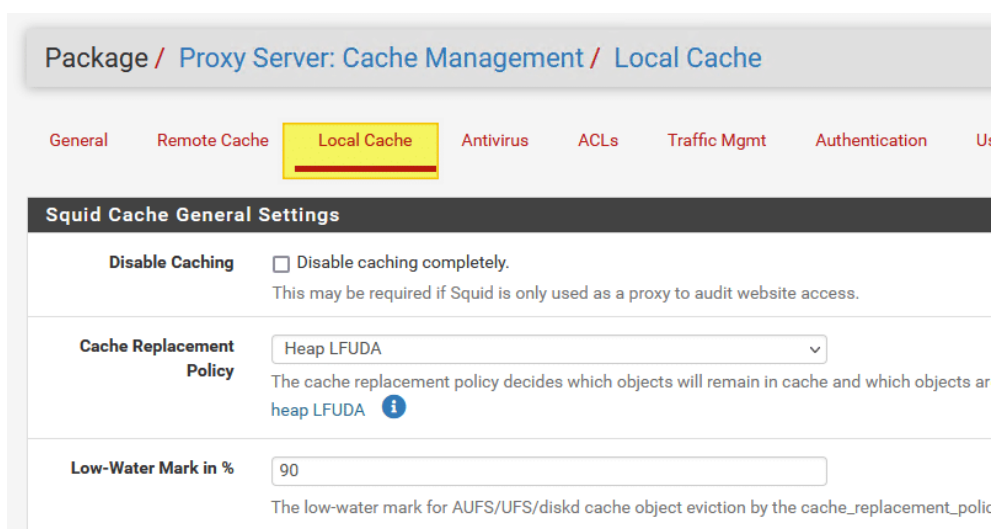
- **Hard Disk Cache Size** : par défaut sur « 100 » pour 100 Mo, cette valeur correspond à la taille maximale du cache sur l'espace disque. Vous pouvez augmenter cette valeur à **1024 Mo** pour avoir 1 Go de cache.
- **Hard Disk Cache Location** : l'emplacement du cache, à savoir par défaut « `/var/squid/cache` ».

Que vous décidiez de modifier ou non l'un des paramètres de la section « **Local Cache** », vous devez cliquer sur le bouton « **Save** » en bas de la page pour enregistrer.

Avant d'utiliser Squid il faut ouvrir le port 3128 (port utilisé par Squid) dans les règles du PfSense :



Pour configurer Squid, cliquez sur l'onglet Services, puis Squid Proxy Server :



Ensuite, cliquez sur l'onglet « **General** ». Là encore, il y a de nombreuses options. Voici ce qu'il faut configurer à minima :

- **Enable Squid Proxy** : cochez la case pour activer Squid sur le pare-feu, ce qui signifie qu'il va démarrer ;
- *[facultatif]* **Listen IP Version** : écouter en IPv4, en IPv6 ou les deux
- **Proxy interface(s)** : sur quelle interface souhaitez-vous activer le proxy ? Ici, ce sera seulement sur l'interface « **LAN** » donc je la sélectionne. Vous pouvez en sélectionner plusieurs si besoin, mais dans tous les cas le « **WAN** » ne sera pas sélectionné.
- **Proxy Port** : on laisse le port par défaut, à savoir 3128, mais il ne devra pas être déclaré sur les postes clients puisque l'on va configurer Squid en mode proxy transparent.
- **Allow Users on interface** : cochez cette case pour autoriser implicitement les utilisateurs connectés sur le réseau « **LAN** » à utiliser le proxy. Cela évite de déclarer le réseau dans un second temps.

The screenshot shows the 'Squid General Settings' page with the following configurations:

- 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 uninstall/reinstall/upgrade.
- Listen IP Version**: IPv4 (Selected). Select the IP version Squid will use to select addresses for accepting client connections.
- CARP Status VIP**: aucun. Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status. **Important:** Don't forget to generate Local Cache on the secondary node and configure XMLRPC Sync for the settings synchronization.
- Proxy Interface(s)**: WAN, VLAN10, VLAN20, VLAN30. The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.
- Outgoing Network Interface**: Default (auto). The interface the proxy server will use for outgoing connections.
- Port du mandataire (« proxy »)**: 3128. This is the port the proxy server will listen on. Default: 3128.

Descendez dans la page et cochez l'option « **Transparent HTTP Proxy** » pour activer le mode proxy transparent pour le protocole HTTP. Pour l'activer pour le protocole HTTPS, il faudra cocher une autre option (nous en parlerons par la suite).

Dans le même esprit qu'au début de la configuration, sélectionnez « **LAN** » pour l'option « **Transparent Proxy Interface(s)** ».

En configurant l'option « **Bypass Proxy for these Source IPs** », vous avez la possibilité de déclarer des adresses IP sources (ou un sous-réseau source) qui peuvent passer outre le proxy et accéder en direct à Internet. Dans le même esprit, l'option « **Bypass Proxy for these Destination IPs** » permet d'outrepasser le proxy pour certaines destinations.

The screenshot shows the 'Transparent Proxy Settings' page with the following configurations:

- Transparent HTTP Proxy**: ☒ Enable transparent mode to forward all requests for destination port 80 to the proxy server. **Important:** 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, VLAN10, VLAN20, VLAN30. 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.

Continuez de descendre dans la page et activez les journaux comme ceci :

- **Enable Access Logging** : cochez l'option pour activer les journaux, ce qui va permettre de savoir qui fait quoi sur Internet.
- **Rotate Logs** : pendant combien de jours souhaitez-vous conserver les logs ? Pour les établissements scolaires, c'est pendant 365 jours qu'il faut conserver les logs (sauf erreur de ma part).

Logging Settings

Enable Access Logging

☒ This will enable the access log.

Warning: Do NOT enable if available disk space is low.

Log Store Directory

The directory where the logs will be stored; also used for logs other than the Access Log above. **Default:** /var/squid/logs

Important: Do NOT include the trailing / when setting a custom location.

Rotate Logs

Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

Ensuite, la section « **Headers Handling, Language and Other Customizations** » permet de configurer les messages Squid. Le champ « **Visible Hostname** » correspond au nom d'hôte qui peut s'afficher côté client, notamment sur les pages de blocage Squid, tout comme l'e-mail spécifié pour l'option « **Administrator's Email** ». Pour les messages d'erreurs justement, précisez la langue française au niveau de l'option « **Error Language** ».

Pour des raisons de sécurité, on va masquer les informations sur Squid, notamment la version, en cochant l'option « **Suppress Squid Version** ». Ce qui donne :

Headers Handling, Language and Other Customizations

Visible Hostname
This is the hostname to be displayed in proxy server error messages.

Administrator's Email
This is the email address displayed in error messages to the users.

Error Language
Select the language in which the proxy server will display error messages to users.

X-Forwarded Header Mode
Choose how to handle X-Forwarded-For headers. Default: on ⓘ

Disable VIA Header ☐ If not set, Squid will include a Via header in requests and replies as required by RFC2616.

URI Whitespace Characters Handling
Choose how to handle whitespace characters in URL. Default: strip ⓘ

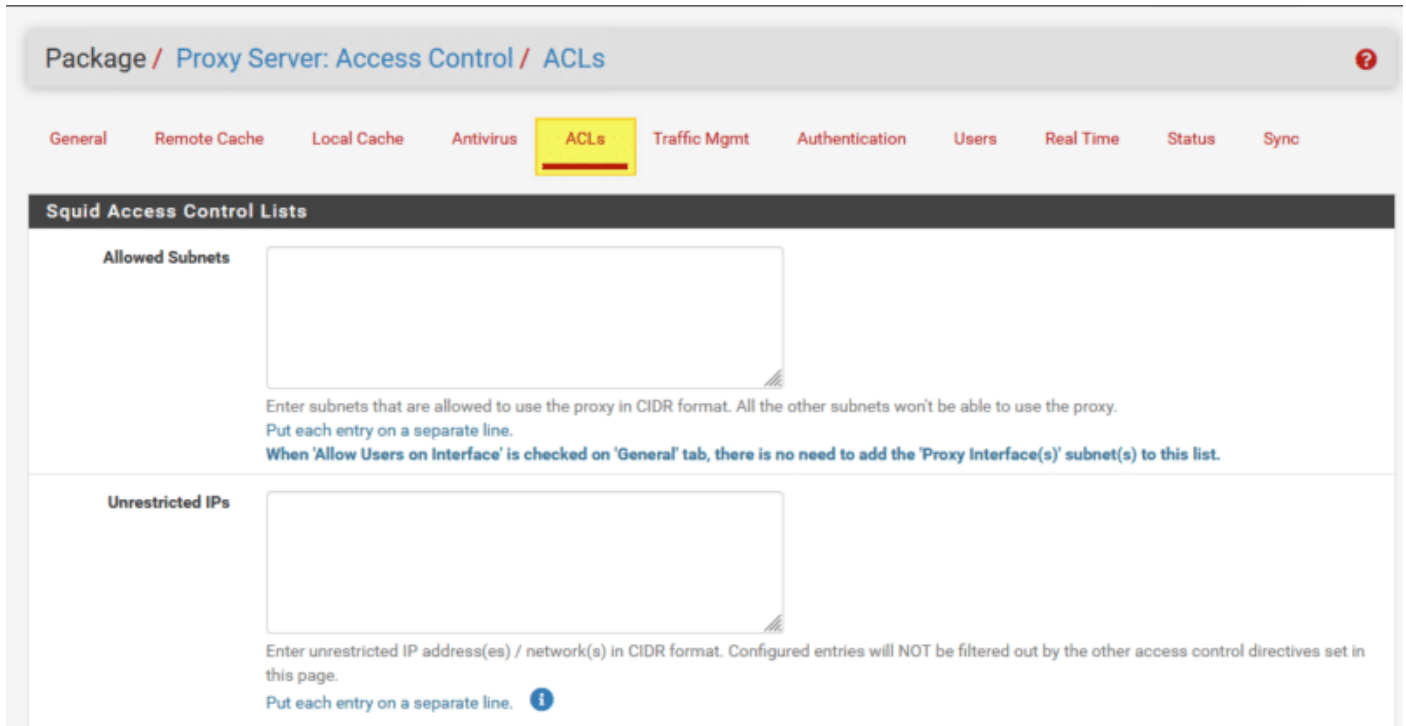
Suppress Squid Version ☒ Suppresses Squid version string info in HTTP headers and HTML error pages if enabled.

Voilà, on est arrivé au bout de la page de configuration ! Cliquez sur « **Save** » pour enregistrer et appliquer cette nouvelle configuration.

Tester le proxy transparent

Pour tester le bon fonctionnement de notre proxy transparent HTTP, on peut tout simplement s'amuser à naviguer sur Internet. Pour que ce soit plus parlant, on va bloquer un nom de domaine.

Cliquez sur l'onglet « **ACLs** », toujours dans la configuration de Squid. C'est ici que vous pouvez déclarer les sous-réseaux autorisés à utiliser le proxy (**Allowed Subnets**) mais pour nous c'est implicite (souvenez-vous de l'option cochée précédemment). Pour autoriser une ou plusieurs adresses IP (ou sous-réseau) à passer outre les restrictions, renseignez l'option « **Unrestricted IPs** ».



Package / Proxy Server: Access Control / ACLs

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

Squid Access Control Lists

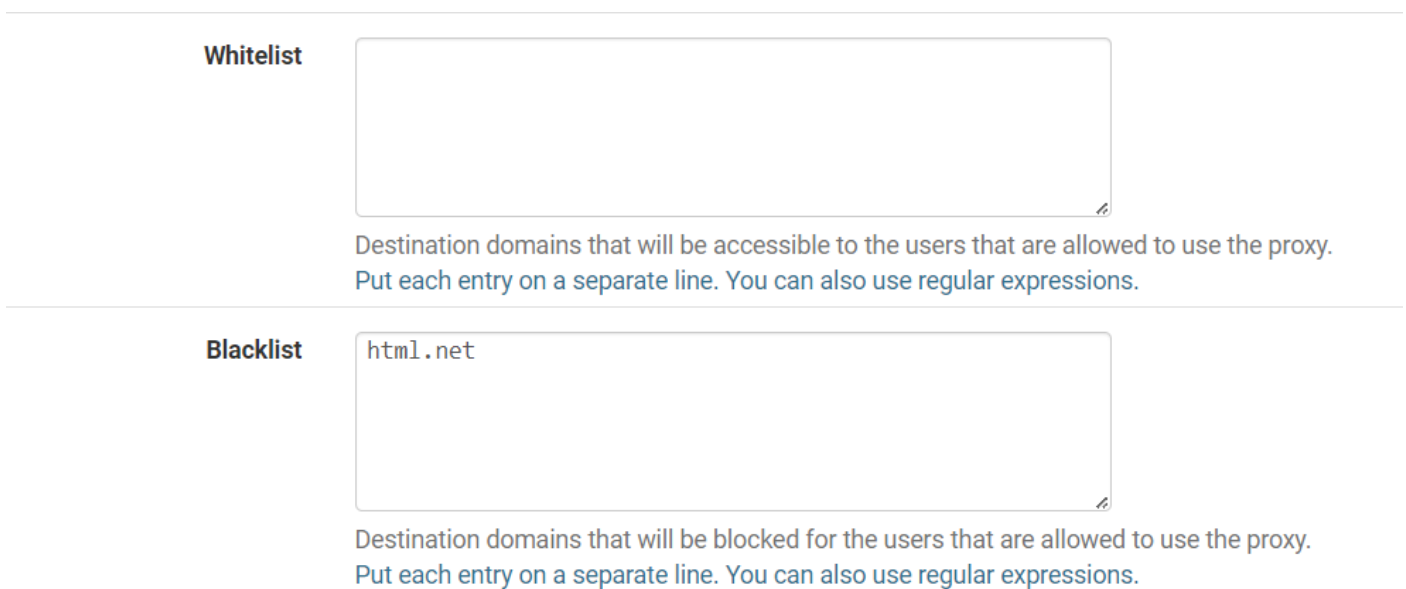
Allowed Subnets

Enter subnets that are allowed to use the proxy in CIDR format. All the other subnets won't be able to use the proxy. Put each entry on a separate line. When 'Allow Users on Interface' is checked on 'General' tab, there is no need to add the 'Proxy Interface(s)' subnet(s) to this list.

Unrestricted IPs

Enter unrestricted IP address(es) / network(s) in CIDR format. Configured entries will NOT be filtered out by the other access control directives set in this page. Put each entry on a separate line.

Ce qui nous faut pour ce test, c'est l'option « **Blacklist** » puisqu'elle permet d'indiquer un ou plusieurs domaines à bloquer. Pour ce test, il nous faut un site en HTTP (ce qui est de moins en moins fréquent, enfin surtout au niveau des sites connus). J'ai pris le site « *html.net* », au hasard, et je l'ai ajouté comme ceci :



Whitelist


Destination domains that will be accessible to the users that are allowed to use the proxy. Put each entry on a separate line. You can also use regular expressions.

Blacklist

html.net

Destination domains that will be blocked for the users that are allowed to use the proxy. Put each entry on a separate line. You can also use regular expressions.

Ensuite, on sauvegarde la configuration... Puis, à partir d'un poste de travail situé sur le réseau local, on tente d'accéder au site « *html.net* ». Et là, on peut voir que ça ne fonctionne pas ! On peut voir qu'une page « **Accès interdit** » renvoyée par Squid s'affiche !



ERROR
The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: <http://fr.html.net/>

Access Denied.

Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.

Your cache administrator is admin@m2l.fr.

Generated Fri, 01 Mar 2024 10:36:17 GMT by Proxy (squid)

On peut aussi suivre les logs en temps réel côté Squid, via l'onglet « **Real Time** ». On voit très bien nos requêtes à destination du site « *fr.html.net* » depuis l'hôte 172.30.0.5 : c'est la preuve irréfutable que notre PC passe bien par le proxy transparent !

Squid Access Table					
Date	IP	État	Squid - Access Logs		Utilisateur
			Adresse	Destination	
01.03.2024 10:38:19	172.30.0.5	TCP_DENIED/403	http://fr.html.net/	-	-
01.03.2024 10:38:19	172.30.0.5	TCP_DENIED/403	http://fr.html.net/	-	-
01.03.2024 10:38:19	172.30.0.5	TCP_DENIED/403	http://fr.html.net/	-	-
01.03.2024 10:38:18	172.30.0.5	TCP_DENIED/403	http://fr.html.net/	-	-

Configurer squid en proxy transparent https

Bien que la configuration de base soit faite, notre proxy transparent fonctionne seulement sur le protocole HTTP. Depuis quelques années maintenant, la tendance est au HTTPS (plus sécurisé) alors c'est indispensable que l'on permette à notre proxy transparent de travailler le HTTPS.

Cela est un peu plus complexe qu'une simple case à cocher dans les options du proxy, car il faut faire ce que l'on appelle du **SSL Inspection**. Puisqu'un flux HTTPS est chiffré, le proxy ne peut pas seulement regarder les trames passer. En effet, pour chaque connexion, il doit déchiffrer le flux, l'inspecter puis le chiffrer à nouveau afin de l'acheminer : une tâche d'envergure et gourmande en ressources.

1. Créer l'autorité de certification PfSense

Pour commencer, il faut créer une autorité de certification sur notre pare-feu PfSense. Rendez-vous dans le menu « **System** » puis « **Cert. Manager** » et dans l'onglet « **CAs** ». Cliquez sur « **Add** » et renseignez les différents champs.

Note : si vous avez une autorité de certification Active Directory, il doit être possible d'ajouter un certificat existant directement.

Vous obtenez une autorité de certification, comme la mienne nommée « CA-M2L ».

Authorities

Certificats

Revocation

Recherche

Terme de recherche

Les deux

Recherche

Effacer

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Autorités de certification

Nom	Interne	Émetteur	Certificats	Nom distinctif	En cours d'utilisation	Actions
m2l-vpn	✓	auto-signé	3	CN=m2l-ca, C=FR Valable depuis: Wed, 03 Jan 2024 16:35:52 +0000 Valide jusqu'au: Sat, 31 Dec 2033 16:35:52 +0000		
CA-M2L	✓	auto-signé	0	CN=internal-ca Valable depuis: Fri, 01 Mar 2024 10:41:34 +0000 Valide jusqu'au: Mon, 27 Feb 2034 10:41:34 +0000		

2. SSL Inspection avec Squid

Retournez dans la configuration de Squid, via le menu « **Services** ». Cochez l'option « **Resolve DNS IPv4 First** » pour activer la résolution DNS en amont du filtrage, ce qui est recommandé lorsque l'on filtre le HTTPS (ce que l'on s'apprête à faire).

Resolve DNS IPv4 First

☒ Enable this to force DNS IPv4 lookup first.

This option is very useful if you have problems accessing HTTPS sites.

Ensuite, activez l'option « **Enable SSL filtering** ». Pour le mode « **SSL/MITM Mode** », choisissez le mode « **Splice All** » : c'est le mode le moins contraignant à mettre en œuvre, car il ne nécessite pas de déployer le certificat de l'autorité de certification sur l'ensemble des postes clients. C'est aussi le mode recommandé lorsque l'on prévoit de déployer Squid Guard, ce qui sera le cas dans la seconde partie de cette documentation.

Remarque : si vous prenez l'autre mode, il faut exporter le certificat de la CA créée précédemment et le déployer sur toutes les machines qui vont passer par le proxy transparent.

Sélectionnez l'autorité de certification créée précédemment au niveau de l'option « **CA** ».

SSL Man In the Middle Filtering

HTTPS/SSL Interception

☒ Enable SSL filtering.

SSL/MITM Mode

Splice All

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
VLAN10
VLAN20
VLAN30

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

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.

AC

CA-M2L

Select Certificate Authority to use when SSL interception is enabled.

SSL Certificate Deamon Children

This is the number of SSL certificate deamon children to start. May need to be increased in busy environments. Default: 5

Remote Cert Checks

Accept remote server certificate with errors
Do not verify remote certificate

Select remote SSL certificate checks to perform. Use CTRL + click to select multiple options.

Sauvegardez via le bouton en bas de page.

3. ACL : bloquer un site HTTPS dans Squid

Comme vu plus haut, on va retourner dans l'onglet « **ACLs** » au niveau de la section « **Blacklist** ». Cette fois-ci, on va bloquer un domaine où le site tourne en HTTPS : « *youtube.com* ». Ce qui donne :

Whitelist

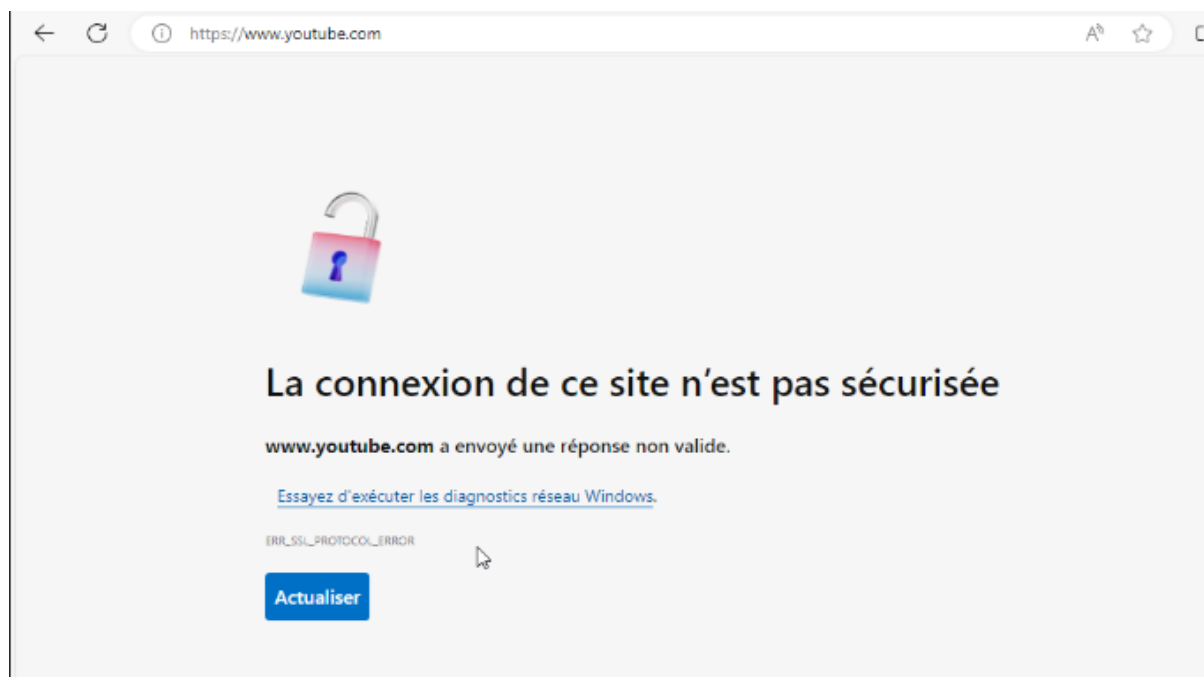
Destination domains that will be accessible to the users that are allowed to use the proxy.
Put each entry on a separate line. You can also use regular expressions.

Blacklist

youtube.com

Destination domains that will be blocked for the users that are allowed to use the proxy.
Put each entry on a separate line. You can also use regular expressions.

On sauvegarde et on tente d'accéder à YouTube. Voici le message que l'on obtient :



Même si ce message fait penser à une erreur, il empêche bien l'accès au site youtube.com. L'erreur de certificat qui s'affiche est liée à l'utilisation de notre certificat de CA locale pour filtrer « *youtube.com* », alors forcément la correspondance entre les deux ne peut paêtre effectuée.

Voilà, le proxy transparent HTTP/HTTPS avec Squid sur un pare-feu PfSense est en place !