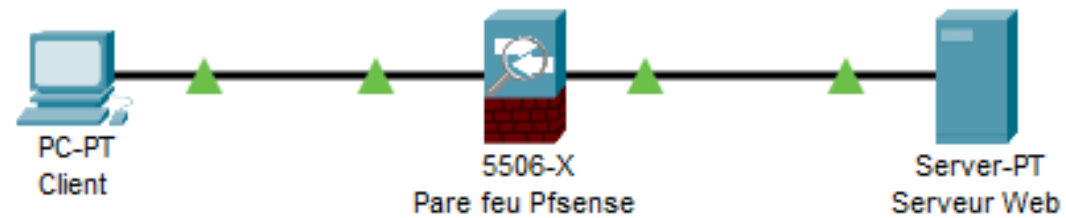




TP SQUID

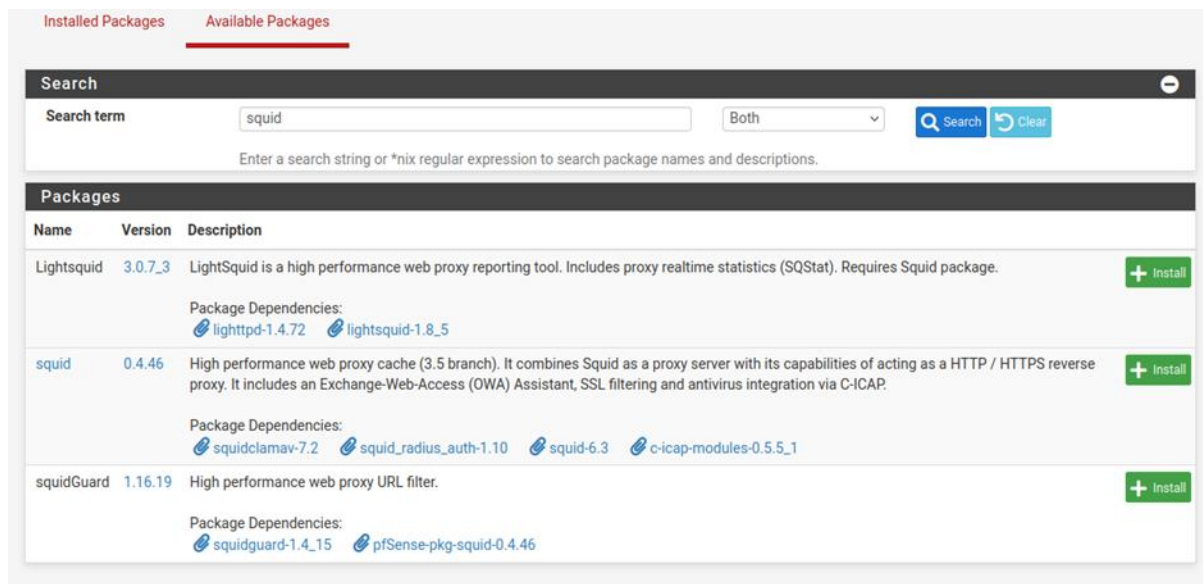
FLORENTIN BRACQ- -FLABAT, BTS 2 SIO

Schéma réseau



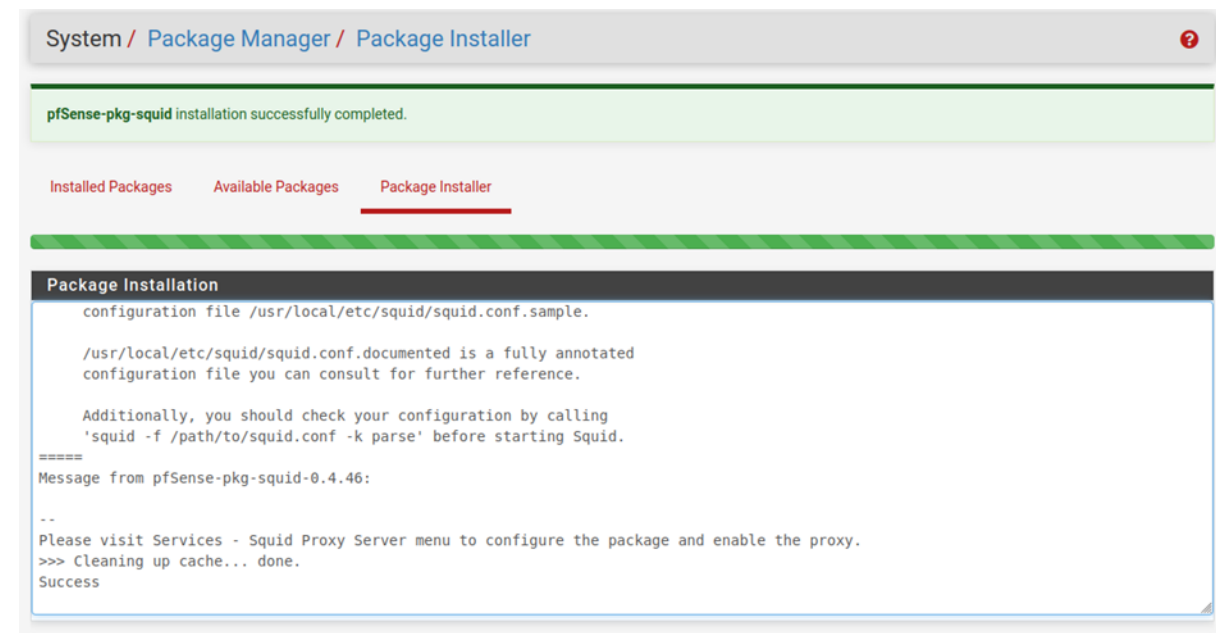
Installation de Squid sur Pfsense

Pour installer Squid sur un pare feu Pfsense, se rendre dans le **gestionnaire de paquets** et rechercher **squid** pour l'installer



The screenshot shows the 'Available Packages' tab in the Pfsense Package Manager. A search for 'squid' has been performed, resulting in three packages being listed:

Name	Version	Description	Action
Lightsquid	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	+ Install
squid	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	+ Install
squidGuard	1.16.19	High performance web proxy URL filter. Package Dependencies: squidguard-1.4.15 pfSense-pkg-squid-0.4.46	+ Install

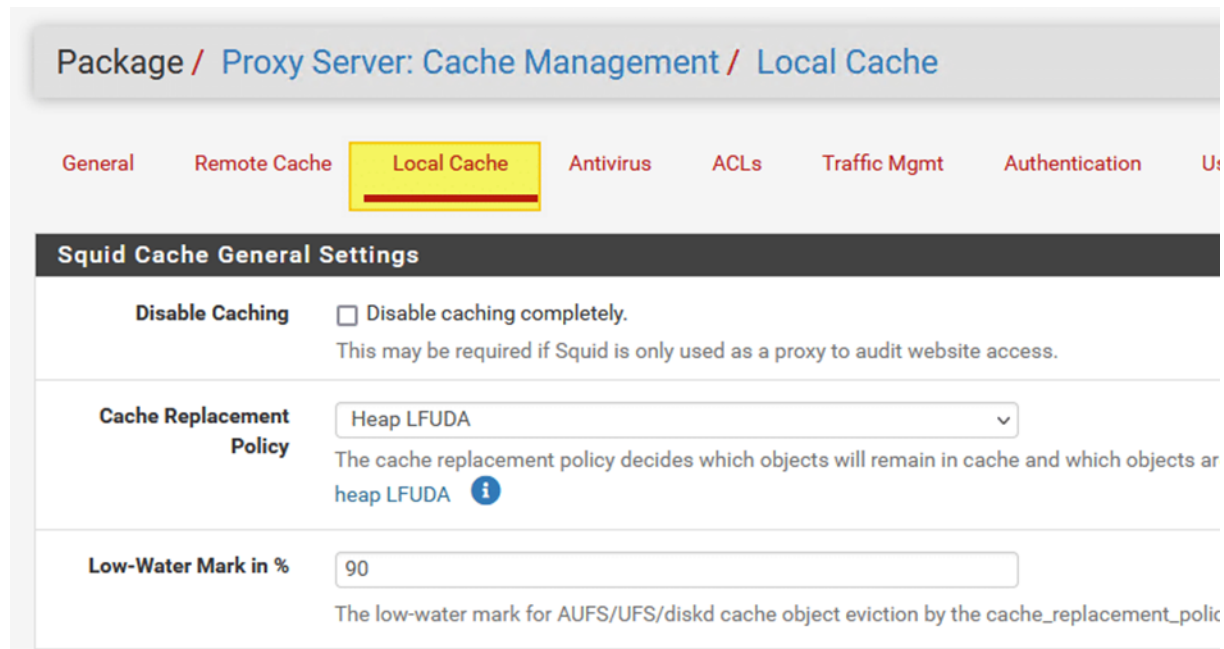


The screenshot shows the 'Package Installer' tab in the Pfsense Package Manager. A green banner at the top indicates that the installation of 'pfSense-pkg-squid' was successful. Below this, the 'Package Installation' section displays the following information:

```
configuration file /usr/local/etc/squid/squid.conf.sample.  
  
/usr/local/etc/squid/squid.conf.documented is a fully annotated  
configuration file you can consult for further reference.  
  
Additionally, you should check your configuration by calling  
'squid -f /path/to/squid.conf -k parse' before starting Squid.  
=====  
Message from pfSense-pkg-squid-0.4.46:  
  
--  
Please visit Services - Squid Proxy Server menu to configure the package and enable the proxy.  
>>> Cleaning up cache... done.  
Success
```

Configuration du Squid

Dans le menu **Services** de Pfsense, cliquer sur **Squid Proxy Server**, aller ensuite dans **Local Cache** et cliquer sur **save** en bas de la page même si vous n'apportez pas de modifications



The screenshot shows the 'Local Cache' configuration page for the Squid Proxy Server in Pfsense. The breadcrumb trail at the top reads 'Package / Proxy Server: Cache Management / Local Cache'. Below this, a horizontal menu contains several tabs: 'General', 'Remote Cache', 'Local Cache' (which is highlighted with a yellow background and a red underline), 'Antivirus', 'ACLs', 'Traffic Mgmt', 'Authentication', and 'User'. The main content area is titled 'Squid Cache General Settings' and contains three configuration sections:

- Disable Caching:** A checkbox labeled 'Disable caching completely.' is currently unchecked. Below it, a note states: 'This may be required if Squid is only used as a proxy to audit website access.'
- Cache Replacement Policy:** A dropdown menu is set to 'Heap LFUDA'. Below the dropdown, a note explains: 'The cache replacement policy decides which objects will remain in cache and which objects are evicted.' followed by 'heap LFUDA' and an information icon.
- Low-Water Mark in %:** A text input field contains the value '90'. Below it, a note states: 'The low-water mark for AUFS/UFS/diskd cache object eviction by the cache_replacement_policy.'

Configuration du Squid

Cliquer ensuite sur l'onglet **Général**, cocher la case pour **Enable Squid Proxy**, sélectionner l'interface **LAN** dans **Proxy Interface(s)** et définir le **Proxy Port** sur **3128**

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 uninstall/reinstall/upgrade.
Listen IP Version	IPv4 Select the IP version Squid will use to select addresses for accepting client connections.
CARP Status VIP	none 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 LAN DMZ loopback 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.
Proxy Port	3128 This is the port the proxy server will listen on. Default: 3128

Configuration du Squid

Pour la partie Transparent Proxy Settings :

Activer mode transparent http

Sélectionner l'interface LAN

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 DMZ 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 (;)

Configuration du Squid

Activer les logs et choix du nombre de jours que l'on conserve

Logging Settings	
Enable Access Logging	☒ This will enable the access log. Warning: Do NOT enable if available disk space is low.
<u>Log Store Directory</u>	/var/squid/logs 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	365 Defines how many days of logfiles will be kept. Rotation is disabled if left empty.
Log Pages Denied by SquidGuard	☐ Makes it possible for SquidGuard denied log to be included on Squid logs. Click Info for detailed instructions: 

Configuration du Squid

Pour la partie **Headers Handling, Language and Other Customizations**, remplir les différentes informations demandées, **Visible Hostname**, **Administrator's Email**, **Error Language** et **Suppress Squid Version**. Ce qui permettra de configurer les messages de Squid. Penser à cliquer sur save pour enregistrer les modifications

Headers Handling, Language and Other Customizations	
Visible Hostname	Proxy Florentin This is the hostname to be displayed in proxy server error messages.
Administrator's Email	contact@florentinbracqflabat.fr 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	☐ 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	☒ Suppresses Squid version string info in HTTP headers and HTML error pages if enabled.

Tester le proxy

Pour tester le proxy on peut se rendre dans l'onglet **ACLs**, dans la catégorie **Blacklist**, on peut ajouter un site web, par exemple florentinbracqflabat.fr

On clique sur **save** pour enregistrer les modifications et on peut tester à partir d'un poste client dans le réseau local

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.

Blacklist

florentinbracqflabat.fr

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.

Test du proxy à partir d'un client

Test en HTTP



The screenshot shows a web browser window with the address bar displaying "Non sécurisé florentinbracqflabat.fr". The main content area features a large "ERROR" message with a "NOW" logo, stating "The requested URL could not be retrieved". Below this, a detailed error message reads: "The following error was encountered while trying to retrieve the URL: <http://florentinbracqflabat.fr/>
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 contact@florentinbracqflabat.fr."

Generated Sat, 29 Mar 2025 08:51:35 GMT by Proxy (squid)

Vérification dans les logs

Si on se rend dans l'onglet **RealTime** il est possible de suivre les logs en temps réel

Package / Squid / Monitor

General

Remote Cache

Local Cache

Antivirus

ACLs

Traffic Mgmt

Authentication

Users

Real Time

Status

Sync

Filtering

Max lines:

10 lines

Max. lines to be displayed.

String filter:

Enter a grep-like string/pattern to filter the log entries.
E.g.: username, IP address, URL.
Use ! to invert the sense of matching (to select non-matching lines).

Squid Access Table

Squid - Access Logs

Date	IP	Status	Address	User	Destination
29.03.2025 08:59:58	192.168.1.109	TCP_MISS/204	http://connectivity-check.ubuntu.com/	-	91.189.91.96
29.03.2025 08:59:32	192.168.1.109	TCP_DENIED/403	http://florentinbracqflabat.fr/	-	-
29.03.2025 08:54:58	192.168.1.109	TCP_MISS/204	http://connectivity-check.ubuntu.com/	-	185.125.190.17
29.03.2025 08:51:36	192.168.1.109	TCP_DENIED/403	http://florentinbracqflabat.fr/favicon.ico	-	-
29.03.2025 08:51:36	192.168.1.109	TCP_HIT/200	http://proxy:3128/squid-internal-static/icons/SN.png	-	-
29.03.2025 08:51:35	192.168.1.109	TCP_DENIED/403	http://florentinbracqflabat.fr/	-	-
29.03.2025 08:51:20	192.168.1.109	TCP_MISS/200	http://detectportal.firefox.com/success.txt?	-	34.107.221.82
29.03.2025 08:51:20	192.168.1.109	TCP_MISS/200	http://detectportal.firefox.com/canonical.html	-	34.107.221.82
29.03.2025 08:49:58	192.168.1.109	TCP_MISS/204	http://connectivity-check.ubuntu.com/	-	91.189.91.96
29.03.2025 08:48:21	192.168.1.109	TCP_MISS/200	http://detectportal.firefox.com/success.txt?	-	34.107.221.82

Source

<https://www.it-connect.fr/proxy-transparent-mise-en-place-de-squid-sur-pfsense/>