

Serveur proxy sur pfsense

Etape 1 : On se retrouve sur le dashboard de PfSense après l'installation classique, en accédant à l'interface Web avec l'ip du routeur. On clique sur System > Package Manager(Gestionnaire de paquet)

The screenshot shows the pfSense dashboard with the following sections:

- Informations système**:
 - Nom: pfSense.home.arpa
 - Utilisateur: admin@192.168.100.102 (Local Database)
 - Système: VMware Virtual Machine, ID de l'appareil Netgate: f8deee8da432a406e774
 - BIOS: Fournisseur: Phoenix Technologies LTD, Version: 6.00, Date de sortie: Thu Feb 27 2020
 - Version: 2.6.0-RELEASE (amd64), Base sur Mon: Jan 31 19:57:53 UTC 2022, FreeBSD 12.3-STABLE
 - Type de CPU: Intel(R) Core(TM) i7-9700 CPU @ 3.00GHz, AES-NI CPU Crypto: Yes (inactive), QAT Crypto: No
 - Encryption matérielle: Noyau PTI: Désactivé, MDS Mitigation: Inactive
 - Durée de fonctionnement: 00 Hour 31 Minutes 54 Seconds
 - Date/Heure actuels: Thu Apr 13 17:11:31 UTC 2023
 - Serveur(s) DNS: 127.0.0.1, 172.16.14.254
 - Dernière modification de la configuration: Thu Apr 6 9:49:48 UTC 2023
 - Taille de la table d'état: 0% (93/198000) [Afficher les états](#)
 - Utilisation MBUF: 0% (2396/1000000)
- Netgate Services And Support**:
 - Contract type: Community Support, Community Support Only
 - NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES
 - Text: If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.
 - Text: You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.
 - Links: Upgrade Your Support, Netgate Global Support FAQ, Netgate Professional Services, Community Support Resources, Official pfSense Training by Netgate, Visit Netgate.com
 - Text: If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC support [here](#).
- Interfaces**:
 - WAN: 1000baseT <full-duplex>, 172.16.14.90
 - LAN: 1000baseT <full-duplex>, 192.168.100.254

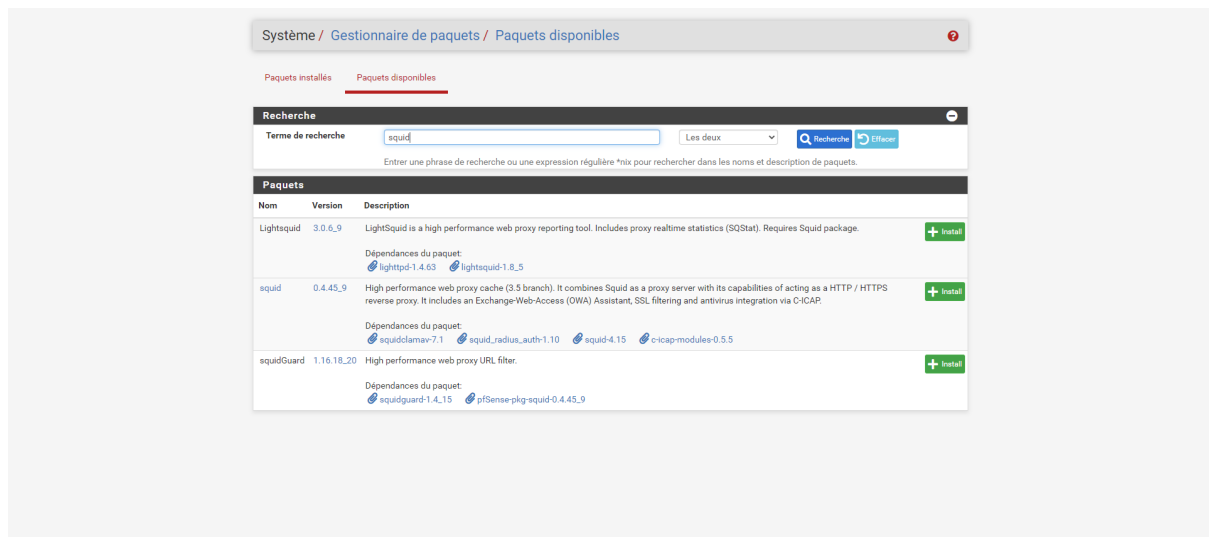
Etape 2 : Sur la page Package Manager, on recherche le paquet suivant : « Squid »

The screenshot shows the pfSense Package Manager interface. The 'Système' menu is open, displaying the following options:

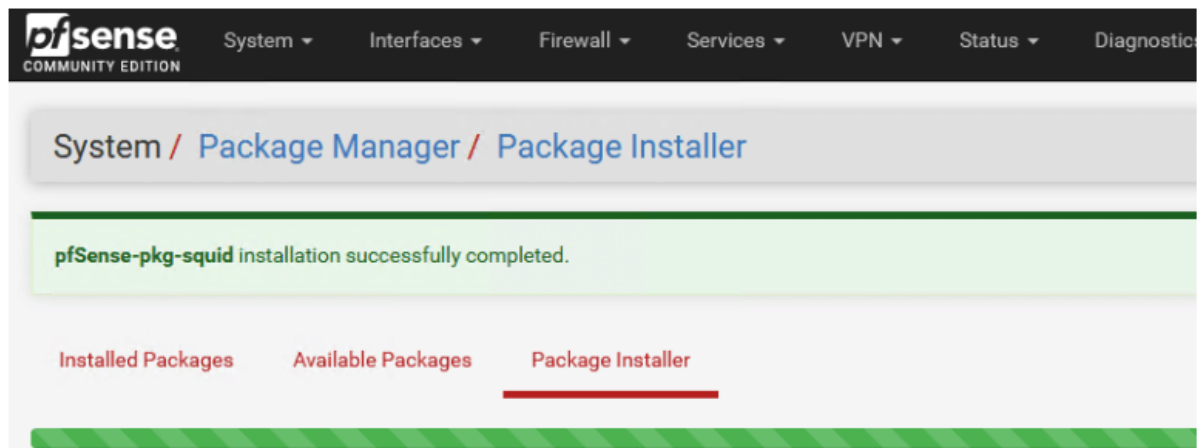
- Assistant de configuration
- Avancé
- Configuration générale
- Déconnexion (admin)
- Gestionnaire d'utilisateurs
- Gestionnaire de certificats
- Gestionnaire de paquets
- Mettre à jour
- Register
- Routing
- Synchronisation à haute disponibilité

The main content area shows 'Paquets installés' with a table containing two rows:

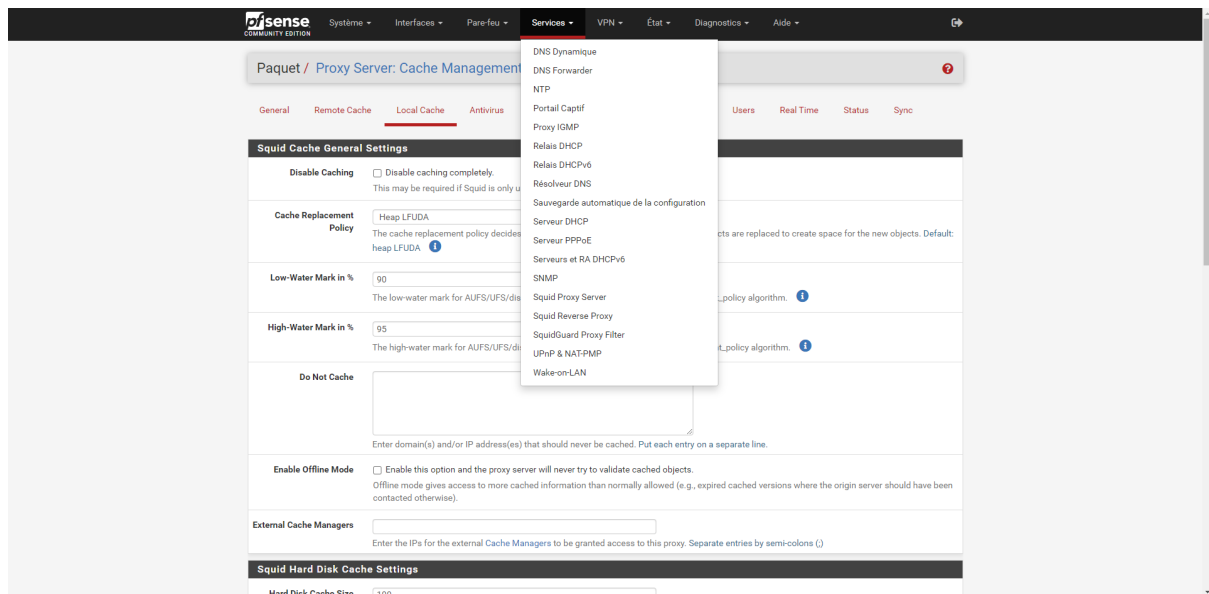
Paquet	Version	Statut
...	...	...
...	...	...



Etape 3: Installer le paquet squid



Etape 4: On navigue sur Services > Squid Proxy Server



Étape 5 : On navigue sur l'onglet Local Cache, puis pour le champ « Hard Disk Cache Size », on met 500 Mo. Puis on clique sur enregistrer

Squid Hard Disk Cache Settings	
Hard Disk Cache Size	500 Amount of disk space (in megabytes) to use for cached objects.
Hard Disk Cache System	ufs This specifies the kind of storage system to use.
Clear Disk Cache NOW	Hard Disk Cache is automatically managed by swapstate_check.php script which is scheduled to run daily via cron. If you wish to clear cache immediately , click this button once : <button>Clear Disk Cache NOW</button>
Level 1 Directories	16 Specifies the number of Level 1 directories for the hard disk cache.
Hard Disk Cache Location	/var/squid/cache This is the directory where the cache will be stored. Default: /var/squid/cache
Minimum Object Size	0 Objects smaller than the size specified (in kilobytes) will not be saved on disk. Default: 0 (meaning there is no minimum)
Maximum Object Size	4 Objects larger than the size specified (in megabytes) will not be saved on disk. Default: 4 (MB)

Étape 6 : On navigue sur l'onglet General. On coche Enable Squid Proxy. On sélectionne l'interface proxy « LAN », et on coche « Resolve IPv4 First ». Puis on

coche également « Trasnparent HTTP Proxy » avec l’interface « LAN » de nouveau.

Paquet / Proxy Server: General Settings / General

General

Remote Cache

Local Cache

Antivirus

ACLs

Traffic Mgmt

Authentication

Users

Real Time

Status

Sync

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

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

LAN

boeuf locale

The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.

Outgoing Network Interface

LAN
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

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.

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

Transparent Proxy Settings

Transparent HTTP Proxy

☒ Enable transparent mode to forward all requests for destination port 80 to the proxy server.

i

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 (,)

Pour le moment, laissez l'option "Enable SSL filtering" décochée.

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 LAN The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.
SSL Proxy Port	This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129

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

Logging Settings	
Enable Access Logging	☒ This will enable the access log. Warning: Do NOT enable if available disk space is low.
Log Store Directory	/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.

Dans « Error language », on sélectionne « fr », puis on coche également « Suppress Squid Version » puis appuyez sur enregistrer

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

Étape 7 : 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.

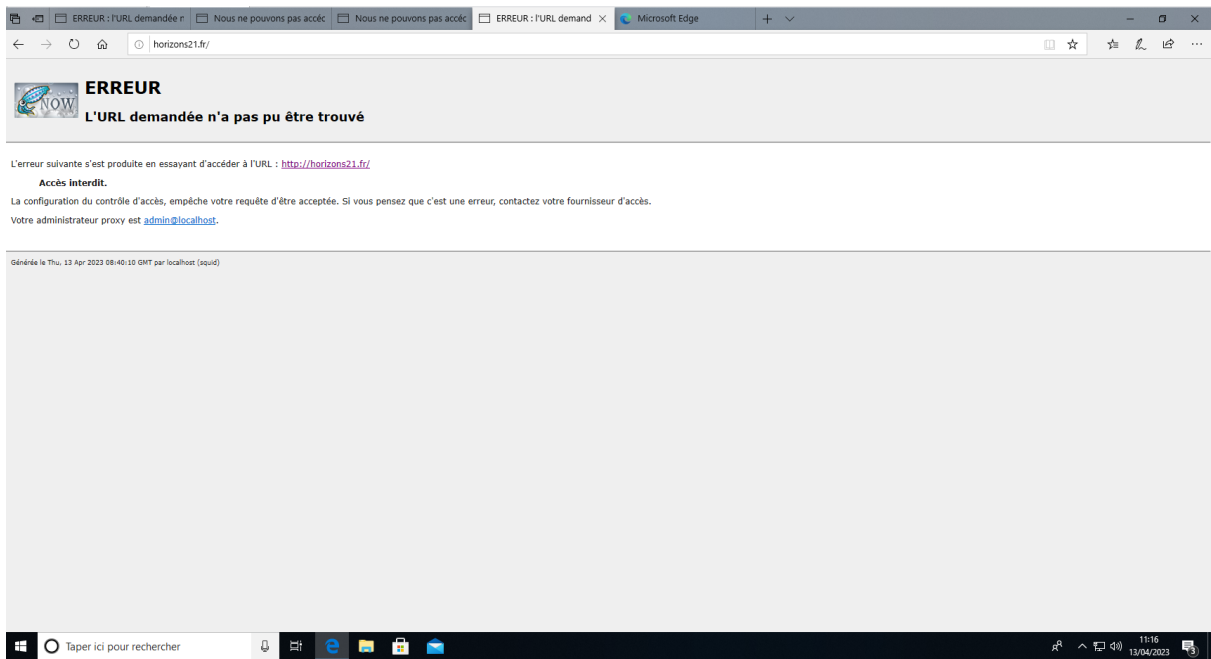
The screenshot shows the Pfsense web interface for configuring Squid Access Control Lists. The breadcrumb trail is "Paquet / Proxy Server: Access Control / ACLs". The "ACLs" tab is selected in the top navigation bar. The main section is titled "Squid Access Control Lists" and contains four input fields:

- Allowed Subnets:** A text area for entering subnets in CIDR format. Below it, instructions state: "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:** A text area for entering unrestricted IP addresses or networks in CIDR format. Below it, instructions state: "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."
- Banned Hosts Addresses:** A text area for entering IP addresses or networks in CIDR format. Below it, instructions state: "Enter IP address(es) / network(s) in CIDR format. Configured entries will NOT be allowed to use the proxy. Put each entry on a separate line."
- Whitelist:** An empty text area.

Puis dans blacklist nous mettons le site qu'on veut bloquer

The screenshot shows the "Blacklist" configuration section. It has a label "Blacklist" and a text area containing the domain "horizons21.fr". Below the text area, instructions state: "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."

Étape 8 : Allez sur un pc client et essayer le site horizons21.fr



Pour finir nous voyons bien qu'il met erreur donc le site a bien été bloqué