

2025

MISE EN PLACE D'UN PROXY SUR FIRWALL

TECHNICIEN SYSTEME ET RESEAU
MARC VOUA



EXPERIS FRANCE

Table des matières

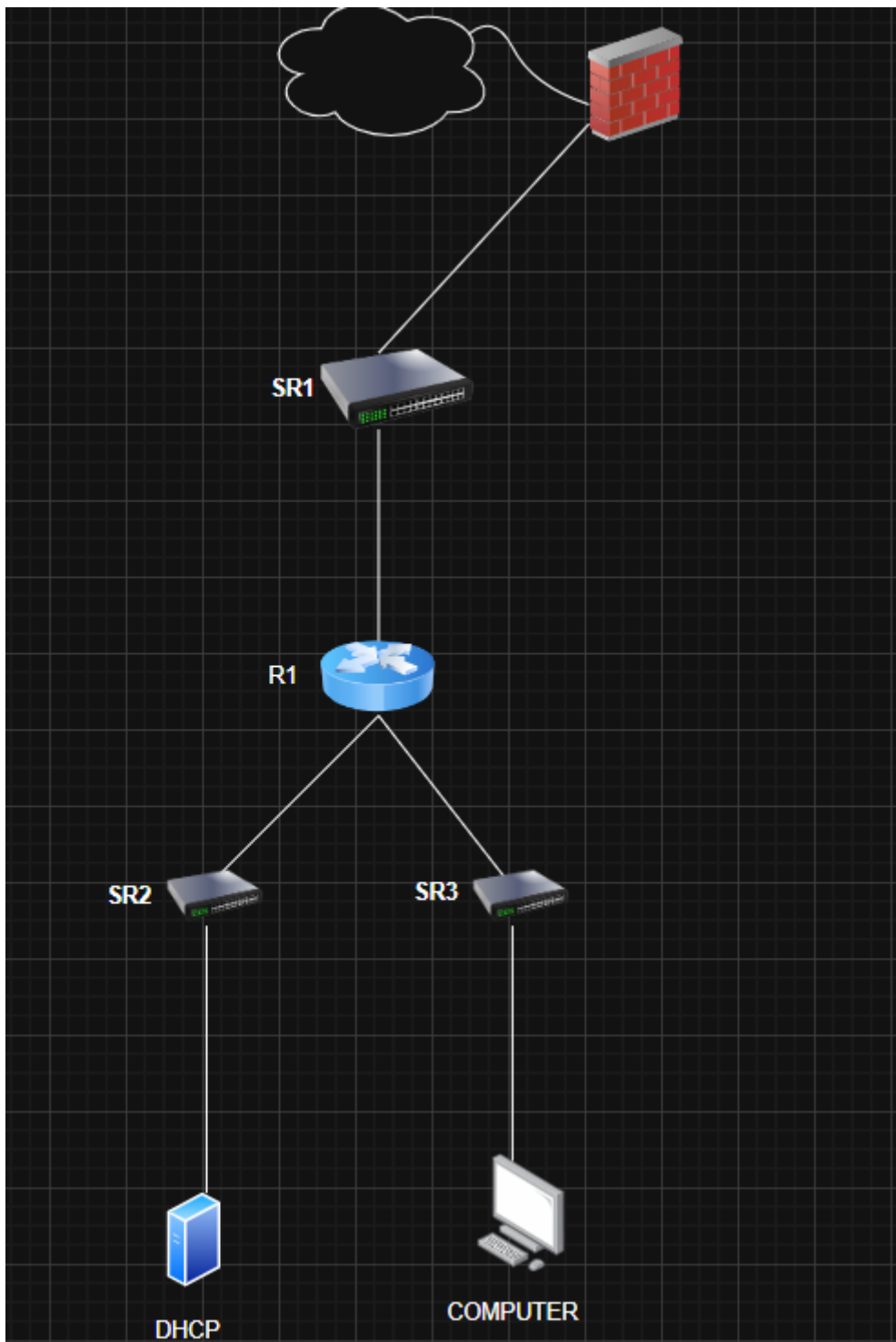
I-	Cahier des charges – Expression des besoins.....	2
1)	Descriptif de l'existant	2
a)	SCHEMA.....	2
2)	Besoin	3
II-	Analyse	3
1)	Descriptifs des solutions et choix des solutions	3
2)	Prévisions des tests de validation.....	3
III-	Mise en place	4
1)	Schéma, Tableau d'adressage.....	4
2)	Méthodologie	5

I- Cahier des charges – Expression des besoins

1) Descriptif de l'existant

a) SCHEMA

Le client possédant déjà une infrastructure réseau fonctionnelle, il nous présente...



Un schéma avec les différentes machines ainsi que leurs noms

2) Besoin

Le service informatique d'une entreprise constate une utilisation non contrôlée d'Internet et un manque de filtrage des accès web, ce qui entraîne des risques de sécurité et une consommation excessive de bande passante. De plus, aucune solution centralisée ne permet de surveiller ou de limiter les sites consultés par les utilisateurs. Pour améliorer la sécurité du réseau et mieux contrôler les accès Internet, l'entreprise décide de trouver une solution pouvant répondre à ses besoins..

II- Analyse

1) Descriptifs des solutions et choix des solutions

Après une analyse des besoins de l'entreprise et des problématiques liées à la sécurité et à l'utilisation d'Internet, plusieurs solutions ont été étudiées afin d'améliorer le contrôle et la supervision des accès web. Au regard du manque de filtrage des sites consultés, de l'absence de traçabilité des connexions et de la nécessité de sécuriser la navigation des utilisateurs, le choix s'est orienté vers la mise en place d'un serveur proxy.

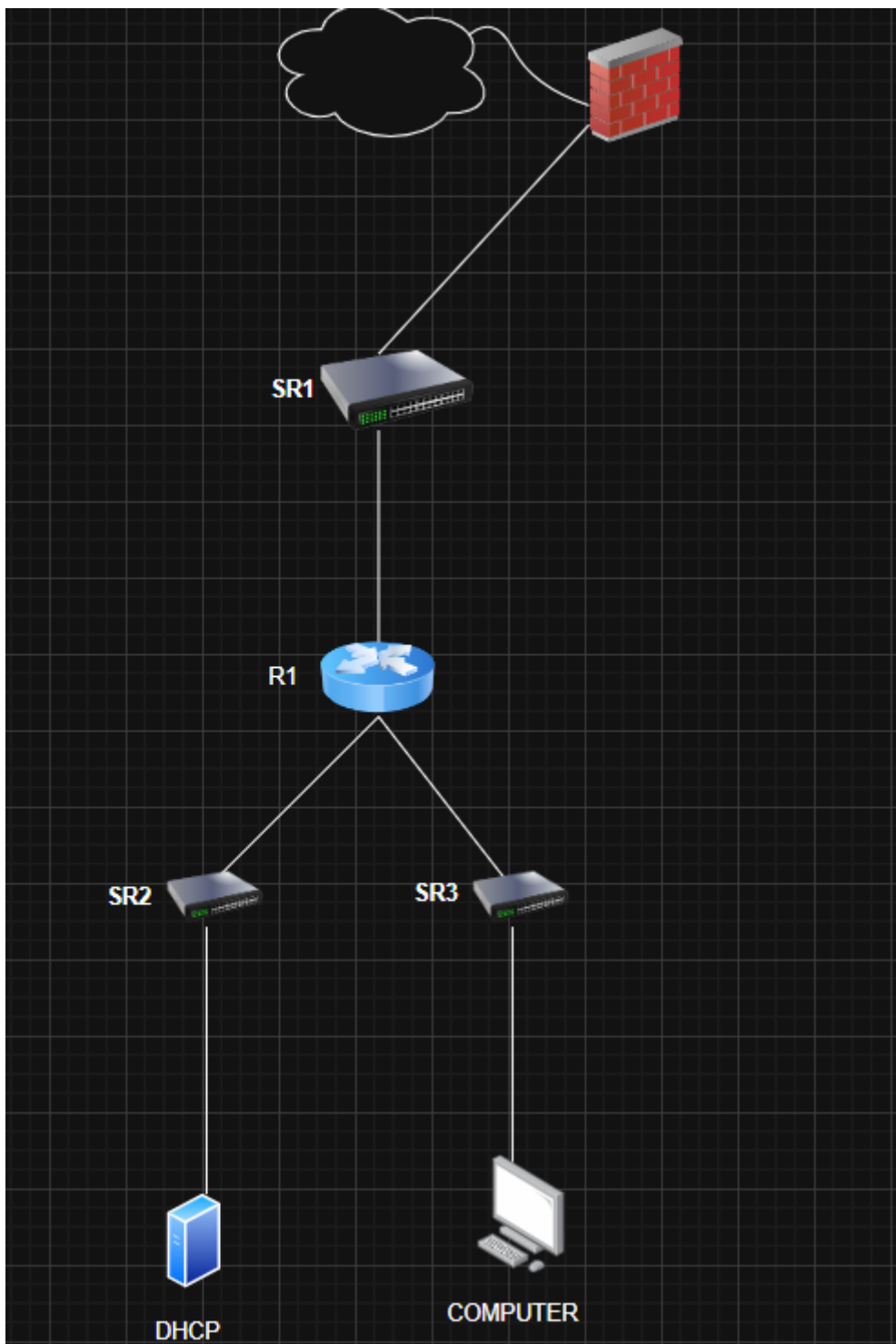
En retenant cette solution, l'entreprise adopte un dispositif permettant d'intermédiaire l'ensemble des requêtes Internet des utilisateurs. Le serveur proxy assure le filtrage des contenus, la journalisation des connexions et le contrôle des accès aux sites web selon des règles définies par l'administration. Ce choix améliore la sécurité du réseau, réduit les risques liés à la navigation, optimise l'utilisation de la bande passante et constitue une solution fiable, évolutive et adaptée aux besoins de supervision et de protection du système d'information.

2) Prévisions des tests de validation

Les tests seront réalisés après la mise en place du serveur proxy afin de vérifier le bon fonctionnement du filtrage et du contrôle des accès Internet. Elle consistera à accéder à différents sites web depuis des postes utilisateurs afin de s'assurer que les règles de filtrage sont correctement appliquées.

III- Mise en place

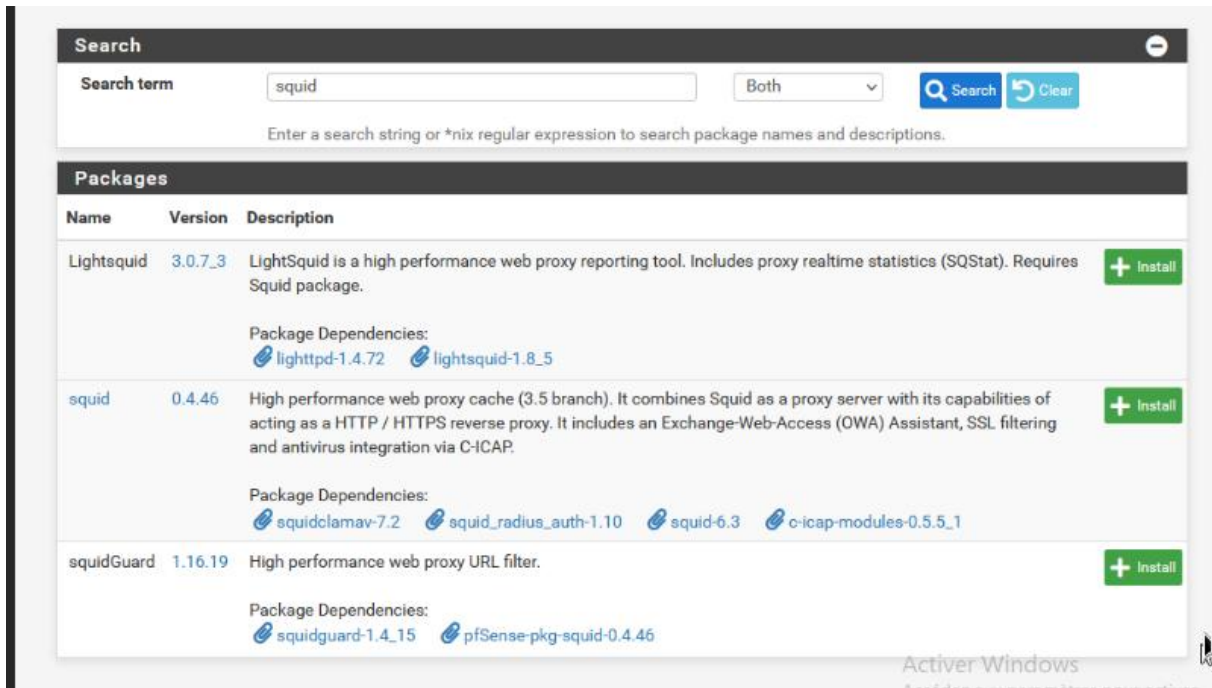
1) Schéma, Tableau d'adressage



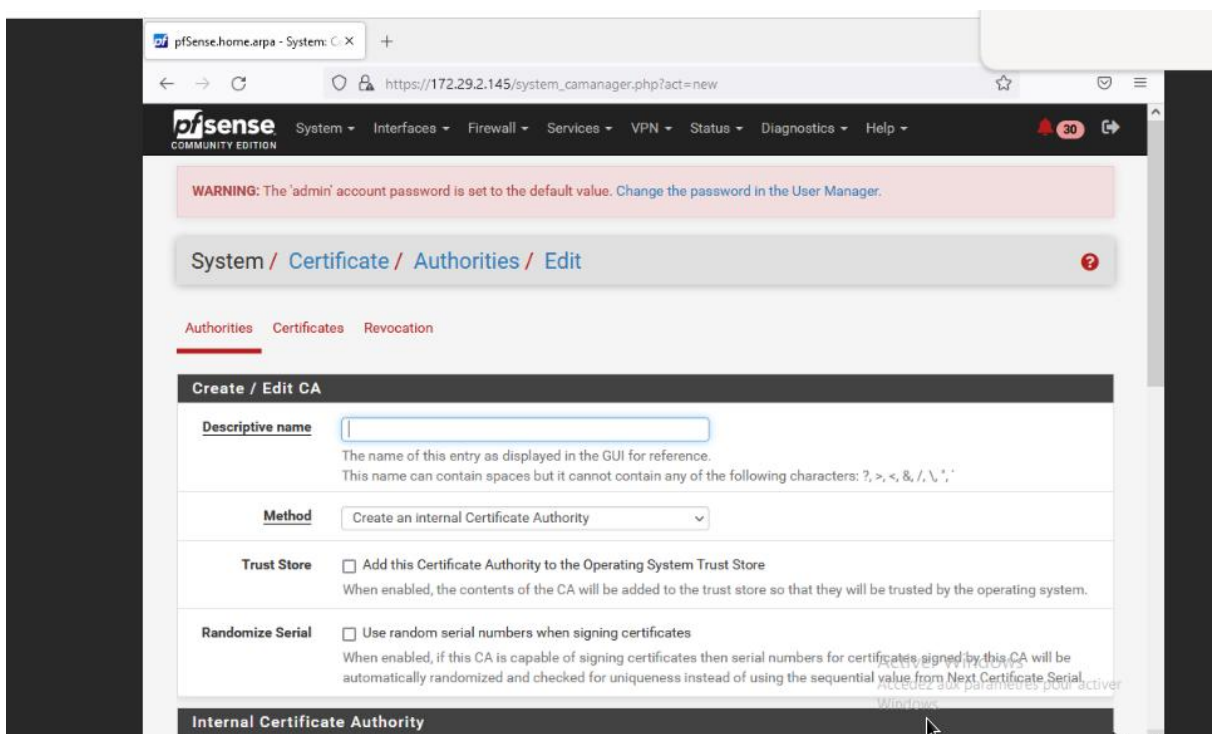
Les informations restent inchangées

2) Méthodologie

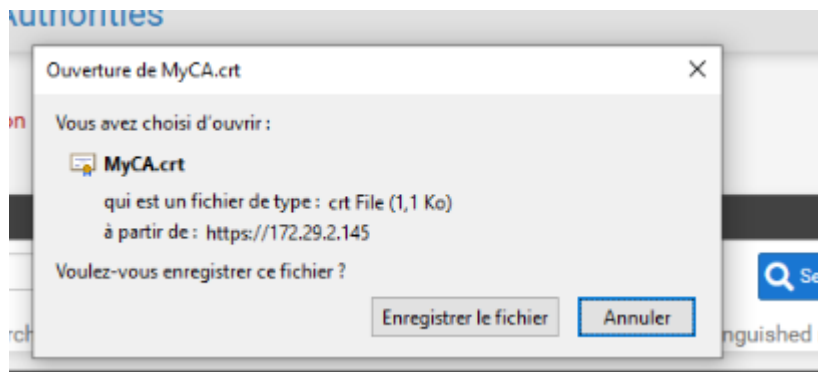
Installation des packages



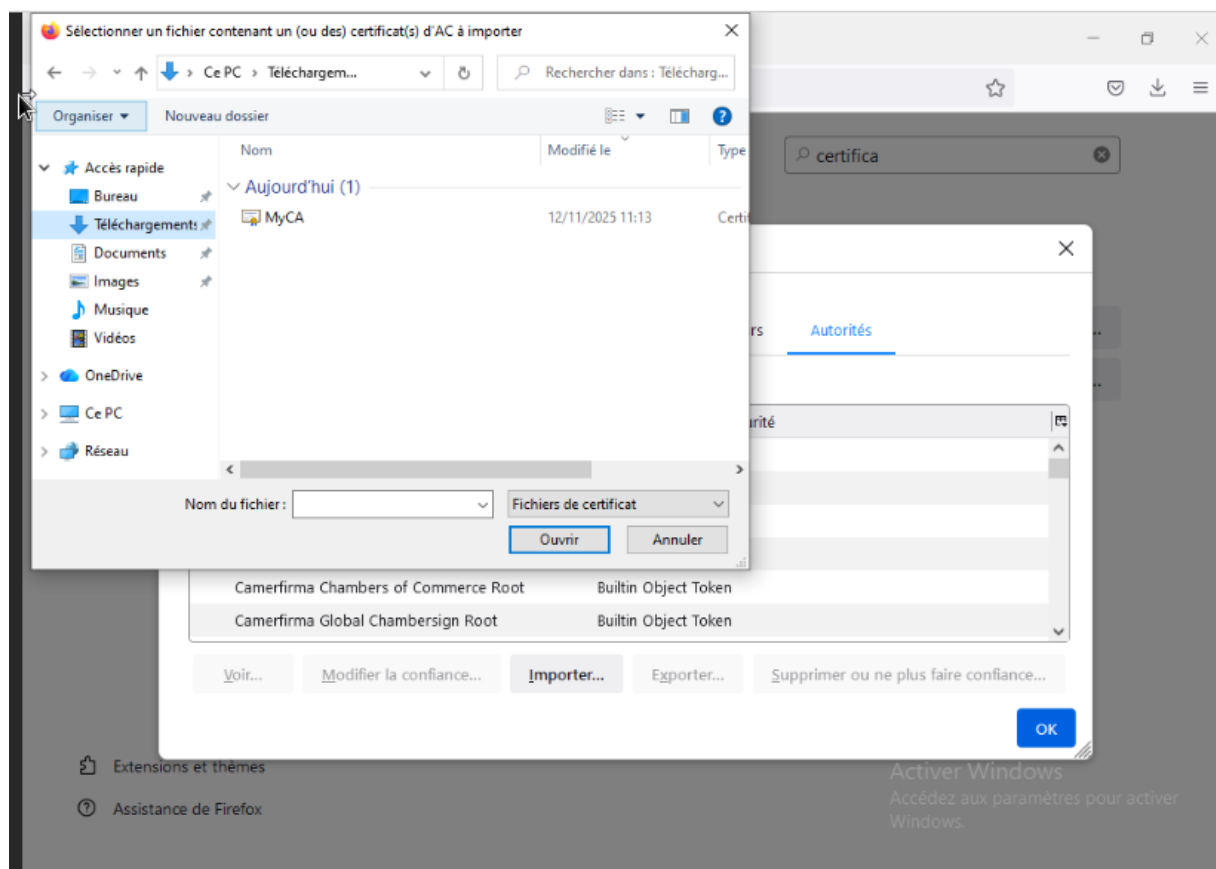
Création d'un certificat pour le filtrage



Export du certificat



Import du certificat dans le navigateur



Configuration du squid

SSL Man In the Middle Filtering

HTTPS/SSL Interception Enable SSL filtering.

SSL/MITM Mode
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)

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

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

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

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

Activer Windows

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.

Log Pages Denied by SquidGuard Makes it possible for SquidGuard denied log to be included on Squid logs.
[Click Info for detailed instructions.](#) ⓘ

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.

Activer Windows
Accédez aux paramètres pour active Windows.

Squid Hard Disk Cache Settings

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

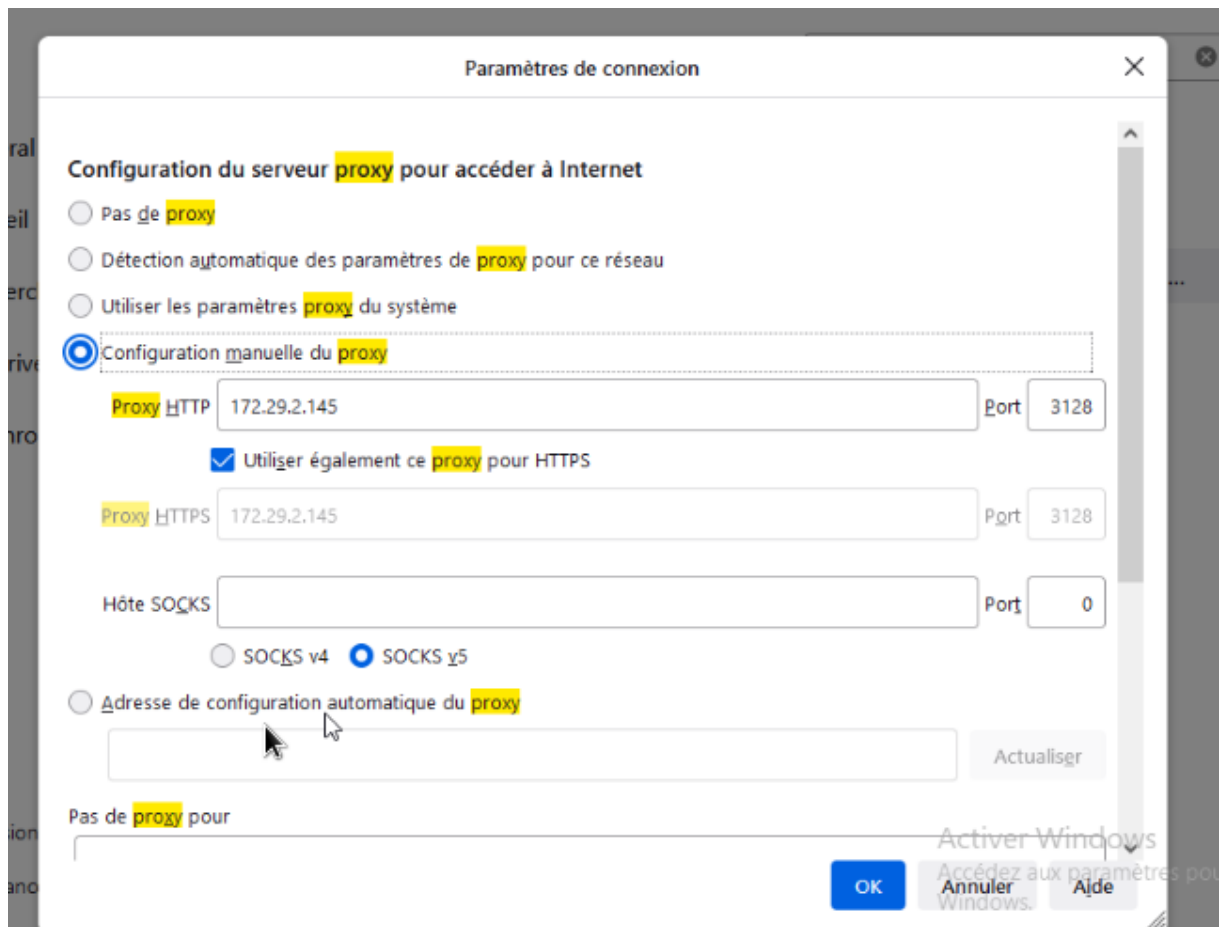
Activer Windows
Accédez aux paramètres pour activer Windows.

Taper ici pour rechercher

Proxy Interface(s)	<input type="text" value="WAN, LAN, loopback"/>	The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.
Outgoing Network Interface	<input type="text" value="Default (auto)"/>	The interface the proxy server will use for outgoing connections.
Proxy Port	<input type="text" value="3128"/>	This is the port the proxy server will listen on. Default: 3128
ICP Port	<input type="text"/>	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	<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	Enable this to force DNS IPv4 lookup first. This option is very useful if you have problems accessing HTTPS sites.
Disable ICMP	<input type="checkbox"/>	Check this to disable Squid ICMP pinger helper.

Activer Windows
Accédez aux paramètres pour activer Windows.

Configuration proxy pour le navigateur



Obligation aux clients de passer par le proxy

The screenshot shows the Windows Firewall Rules list. The rules are as follows:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/1.31 MiB	*	*	*	LAN Address	443, 80	*	*		Anti-Lockout Rule	⚙️
□ ✓ 16/532 KiB	IPv4 TCP	*	*	LAN address	3128	*	none		Autoriser l'accès au proxy	📌 🛠️ 🗑️ 🔄
□ ✗ 0/6 KiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		bloquer https direct	📌 🛠️ 🗑️ 🔄
□ ✗ 0/0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none		bloquer http direct	📌 🛠️ 🗑️ 🔄
□ ✓ 5/2.69 GiB	IPv4 *	*	*	*	*	*	none		Default allow LAN to any rule	📌 🛠️ 🗑️ 🔄
□ ✓ 0/0 B	IPv6 *	*	*	*	*	*	none		Default allow LAN IPv6 to any rule	📌 🛠️ 🗑️ 🔄

A watermark 'Activer Windows' is visible in the bottom right corner.

Configuration du service SQUIDGUARD

The image shows two identical screenshots of the SquidGuard configuration interface. The top section is titled "Logging options" and contains three settings: "Enable GUI log" (unchecked), "Enable log" (checked), and "Enable log rotation" (checked). The bottom section is titled "Blacklist options" and contains three settings: "Blacklist" (checked), "Blacklist proxy" (empty text box), and "Blacklist URL" (text box containing "itole.fr/blacklists/download/blacklists_for_pfsense.tar.gz"). Below the "Blacklist proxy" and "Blacklist URL" fields, there is explanatory text: "Blacklist upload proxy - enter here, or leave blank. Format: host:[port login:pass] . Default proxy port 1080. Example: '192.168.0.1:8080 user:pass'" and "Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL blacklist archive or leave blank. The LOCAL path could be your pfsense (/tmp/blacklist.tar.gz)."

Téléchargement de la liste de filtrage

The image shows the "Blacklist Update" interface. At the top, there is a red progress bar labeled "Blacklist download progress" which is at 100%. Below the progress bar, the URL "http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz" is displayed in a text box. There are three buttons: "Download" (green), "Cancel" (orange), and "Restore Default" (blue). Below the buttons, there is a text input field for "Enter FTP or HTTP path to the blacklist archive here." At the bottom, there is a "Blacklist update Log" section with a scrollable log area containing the following text: "Begin blacklist update", "Start download.", "Download archive http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz", "Download complete", "Unpack archive", "Scan blacklist categories.", "Found 66 items".

Échec de la connexion sécurisée


Une erreur est survenue pendant une connexion à www.pornhub.com. SSL a reçu un enregistrement qui dépasse la longueur maximale autorisée.

Code d'erreur : `SSL_ERROR_RX_RECORD_TOO_LONG`

- La page que vous essayez de consulter ne peut pas être affichée car l'authenticité des données reçues ne peut être vérifiée.
- Veuillez contacter les propriétaires du site web pour les informer de ce problème.

[En savoir plus...](#)

Réessayer

Activer Windows
Accédez aux paramètres pour activer Windows. 

Configuration du LightSQUID

Report Template Settings

Language Select report language.

Report Template Select report template.

Bar Color Select bar color.

Reporting Settings and Scheduler

IP Resolve Method Select which method(s) should be attempted (in the order listed below) to resolve IPs to hostnames. Click info for details. (Default: DNS) [i](#)

Skip URL(s)
If you want to omit some sites from statistics (e.g., a local webserver), specify the URL(s) here. Separate multiple entries by | character. **Example:** example.com|192.168.1.|example.net

Refresh Scheduler Select data refresh period. The reporting task will be executed every XX minutes/hours. Legend: (!)(*) Use only with fast hardware (+) Recommended values

Activer Windows
Accédez aux paramètres pour activer Windows.

Package / Squid Proxy Reports: Settings [↶](#) [⌵](#) [⌶](#) [⌵](#) [?](#)

Instructions

Perform these steps after install **IMPORTANT: Click Info and follow the instructions below if this is initial install!** [i](#)

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](#)

Activer Windows
Accédez aux paramètres pour activer Windows.

Report Template Settings

Accès LightSQUID

LighSquid diagnostic.

Error : report folder '/var/lightsquid/report' not contain any valid data! Please run lightparser.pl (and check 'report' folder content)

Please check config file !

Variable	value
\$tplpath	/usr/local/www/lightsquid/tpl
\$templatename	base
\$langpath	/usr/local/share/lightsquid/lang
\$langname	fr
\$reportpath	/var/lightsquid/report
Access to '/var/lightsquid/report' folder	yes
\$graphreport	1

folder content:

Test service proxy

ERROR

The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: <http://pornhub.com/>

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@localhost.

Generated Wed, 12 Nov 2025 13:44:06 GMT by localhost (squid)