COMPTE-RENDU DÉTAILLÉ :CONFIGURATION PFSENSE

Installation d’un Pare-Feu Pfsense

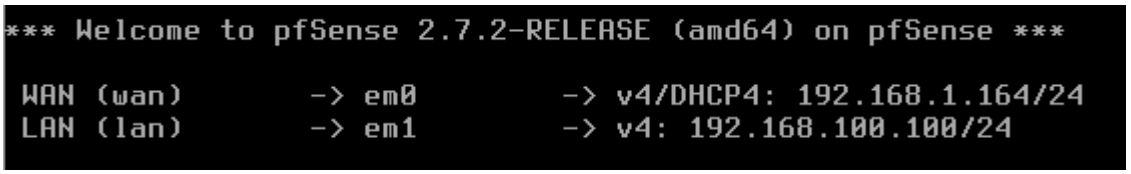
COMPTE-RENDU DÉTAILLÉ :CONFIGURATION PFSENSE

1.Objectif

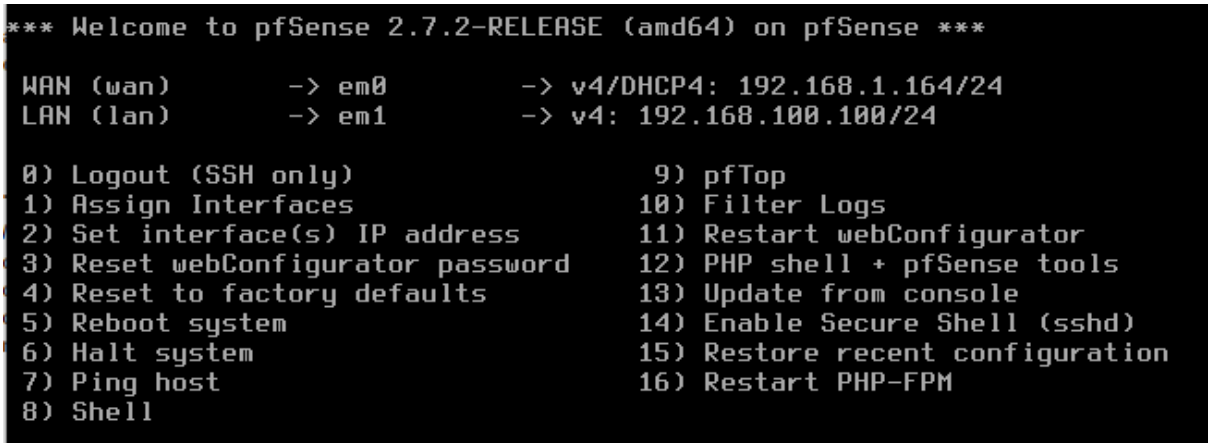
Bloquer tous les sites sauf rechargeplus.fr via un serveur pfSense, utilisé comme proxy filtrant dans le cadre d'une installation de bornes de recharge.

2. Configuration des interfaces réseau

WAN : Interface qui reçoit Internet. Choisir DHCP si vous êtes derrière une box ou un routeur.
LAN : Interface interne. Exemple : IP fixe 192.168.100.100



Si vous devez le mettre en place Allez dans l'option "Set interface IP address" ici 2

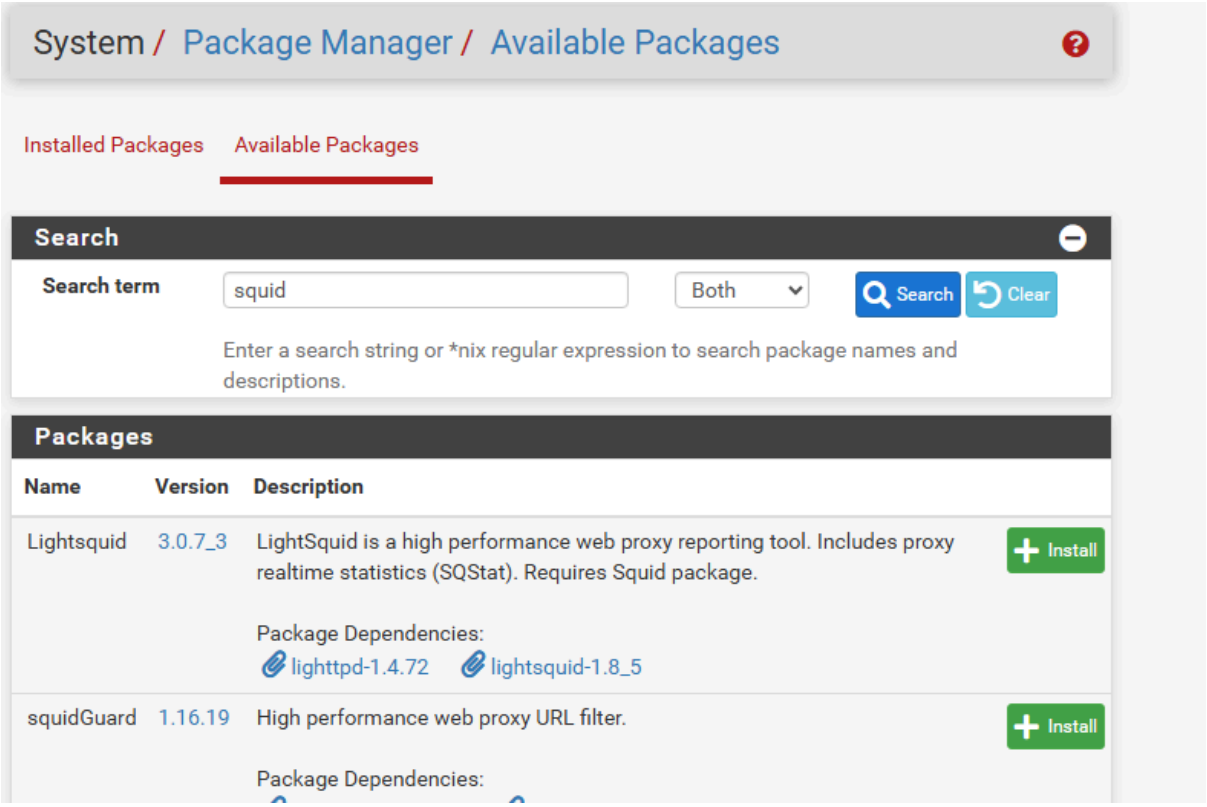


Puis agissez sur les deux interfaces en fonction de la demande (DHCP, Statique)
ATTENTION si le WAN est en statique il risque de ne pas être connecté à internet sauf cas exceptionnelle

3.Installation des paquets Squid et SquidGuard

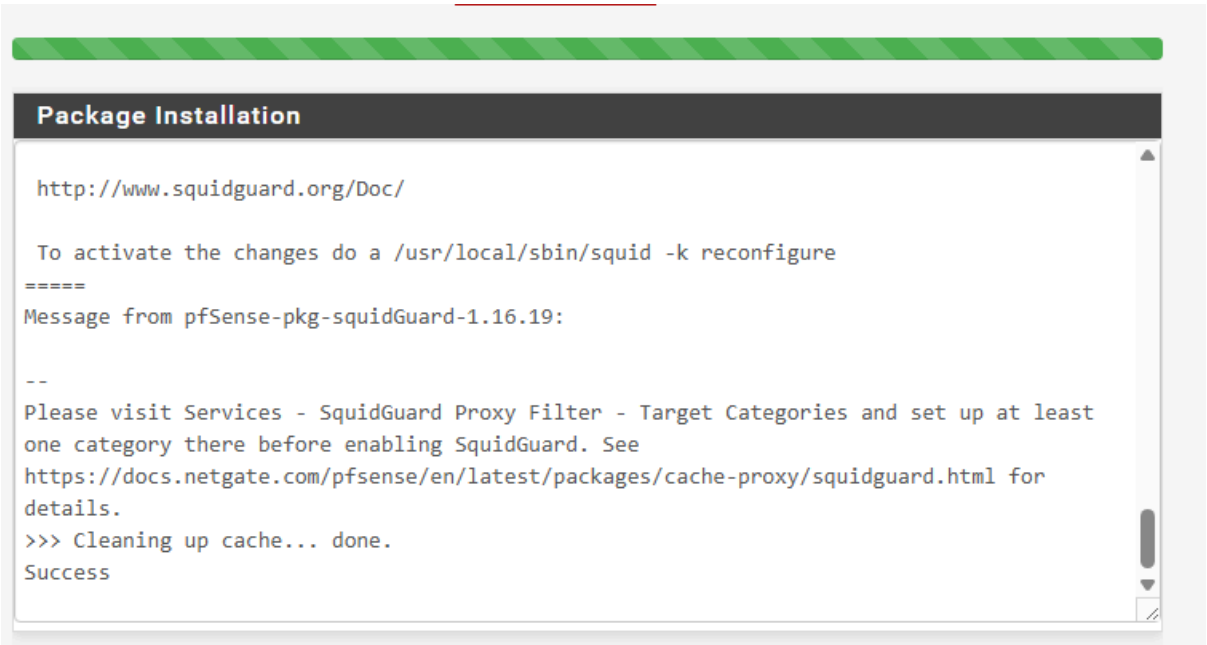
Aller dans System > Package Manager > Available Packages
Rechercher "Squid" puis cliquer sur Install > Confirm

Puis agissez sur les deux interfaces en fonction de la demande (DHCP, Statique)
ATTENTION si le WAN est en statique il risque de ne pas être connecté à internet sauf cas exeptionelle

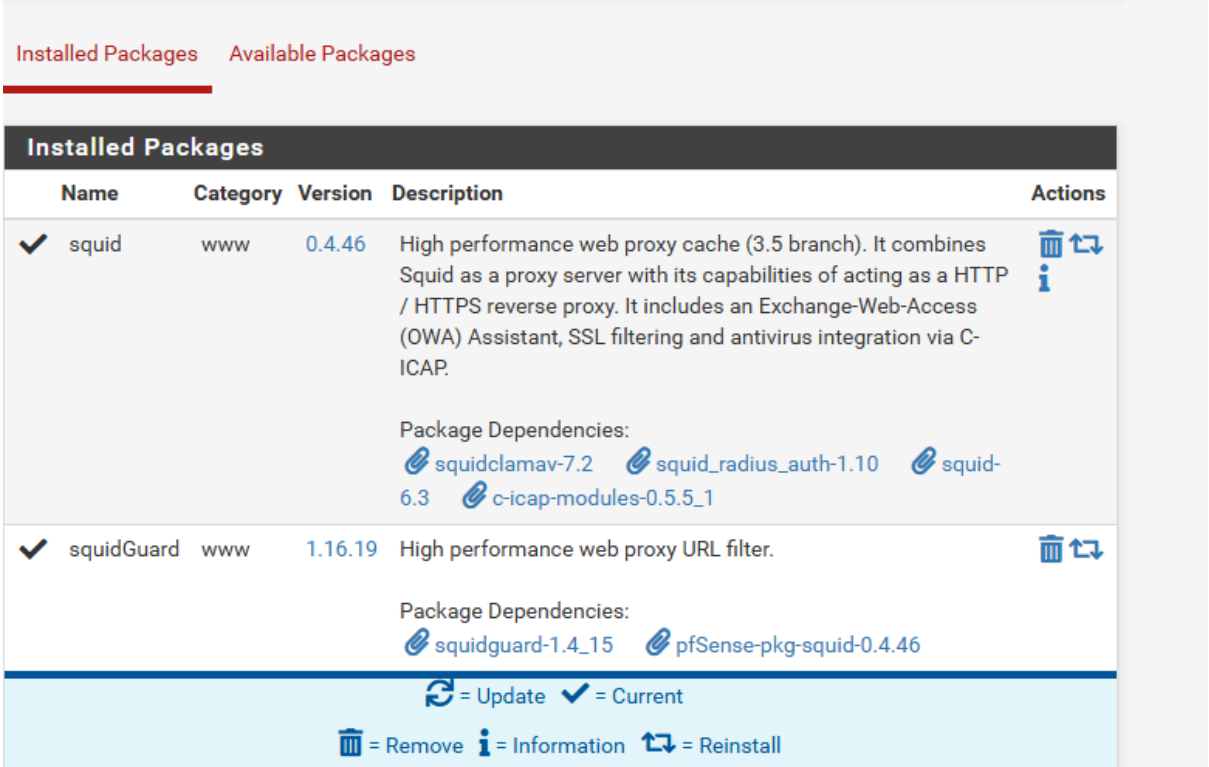


COMPTE-RENDU DÉTAILLÉ :CONFIGURATION PFSENSE

Répéter pour le paquet SquidGuard

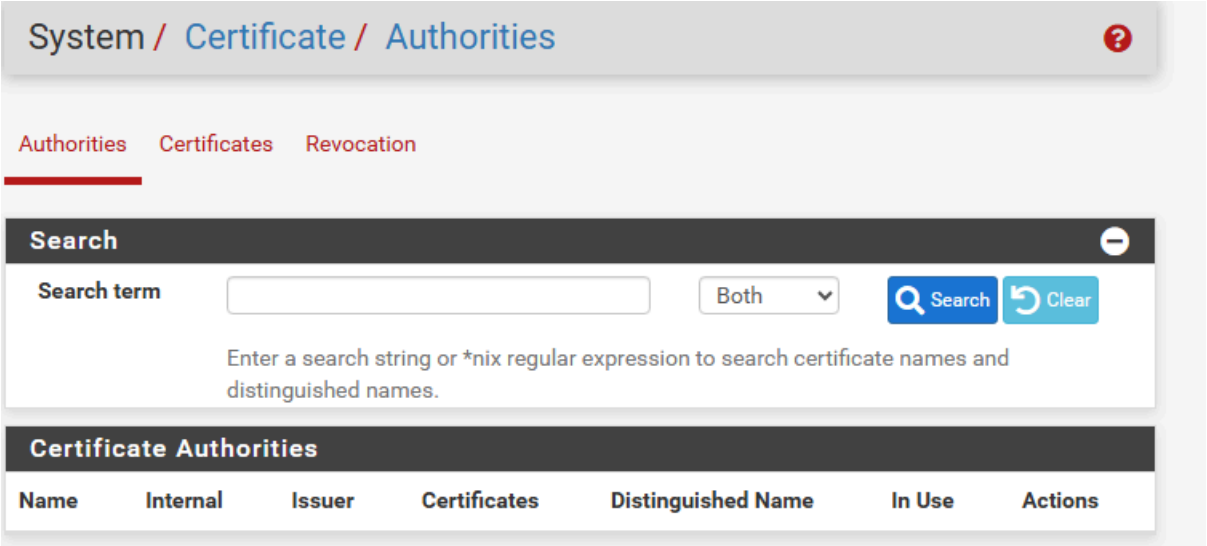


Vérifiez qu'ils apparaissent bien dans Installed Packages



4. Création d'une autorité de certification (CA)

Menu : System / Certificate / Authorities



Puis cliquez sur [+Add]

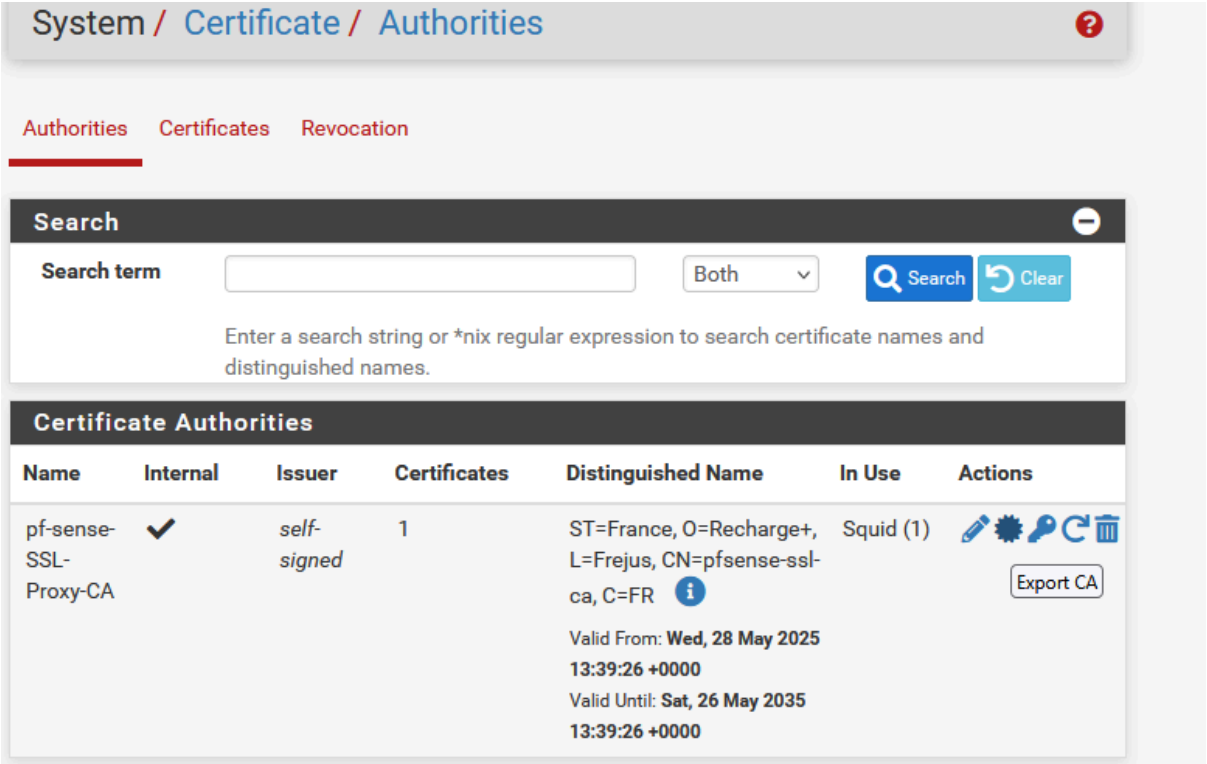
Champ	Valeur par défaut / Exemple
Descriptive Name	`pfSense-SSL-Proxy-CA`
Method	Create an internal Certificate Authority
Key length	2048 bits
Digest Algorithm	sha256
Lifetime	3650 (jours = 10 ans)
Country Code	FR
State	France
City	frejus
Organization	MonEntreprise

Ensuite Cliquez Save

COMPTE-RENDU DÉTAILLÉ :CONFIGURATION PFSENSE

Une fois les deux certificat créé vous devez les importés pour le faire

Menu : System / Certificate / Authorities
Cliquez sur l'étoile pour exportez le CA



Un fichier en .crt sera alors téléchargez

📌 Ajouter le certificat dans votre navigateur

1. **Ouvrez votre navigateur Internet** (ex. Firefox).
2. **Accédez aux paramètres** : cliquez sur les trois barres en haut à droite, puis choisissez **Paramètres**.
3. Dans le menu à gauche, cliquez sur **"Vie privée et sécurité"**.

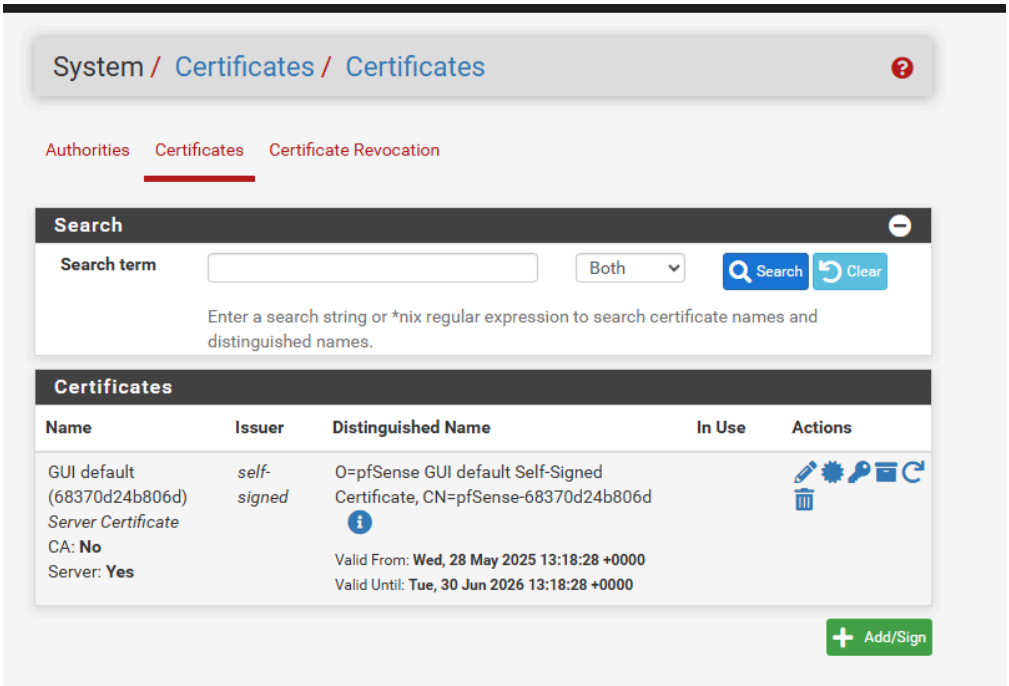
4. Descendez jusqu'à la section **"Certificats"**.
5. Cliquez sur le bouton **"Voir les certificats..."**.
6. Dans la fenêtre qui s'ouvre, cliquez sur **"Importer"**.
7. Sélectionnez le fichier du certificat que vous avez reçu ou téléchargé.
8. ⚠️ **Ne cochez pas la case pour "faire confiance à cette autorité pour identifier des sites de messagerie"**, car cela ne fonctionne pas ici.
9. ✅ **Cochez uniquement la case "Faire confiance à cette autorité pour identifier des sites web"**, puis cliquez sur **OK**.

Ne pas oublier de valider

5. Création d'un certificat pour Squid

Menu : System /Certificate / Certificates
Puis cliquez sur Add/Sign

COMPTE-RENDU DÉTAILLÉ :CONFIGURATION PFSENSE



Paramètres :

Champ	Valeur par défaut / Exemple
Descriptive Name	`Squid-SSL-Proxy-Cert`
Method	Create an internal Certificate
Certificate authority	`pfSense-SSL-Proxy-CA` (celle créée)
Key Type	RSA
Key length	2048 bits
Lifetime	3650 (jours = 10 ans)
Common Name	`Squid Proxy`
Country Code	FR
State	France
City	Frejus
Organization	Recharge+

Ensuite Save

ATTENTION BIEN VéRIFIER d'etre en KEA DHCP
Si NON voici la config a faire lors de l'activation de ce Backend DHCP :
Menu: System / advanced / networking

COMPTE-RENDU DÉTAILLÉ :CONFIGURATION PFSENSE

Option	Action recommandée
Disable hardware checksum offload	✅ Coche **(Recommandé)**
Disable TCP segmentation offload	✅ Coche **(Recommandé)**
Disable large receive offload	✅ Coche **(Recommandé)**
hn ALTQ support	❌ Laisse décoché (sauf si Hyper-V)
Suppress ARP logs	🔘 Optionnel
Reset all states on WAN IP change	🔘 À activer si IP WAN est dynamique

Pour vérifier “nslookup rechargeplus.fr” il dois pouvoir récupérer les Adresse IP

Sinon retour au début ou appel d’un Administrateur (numéro : 06 50 47 32 73)

6. Configuration du proxy Squid

Menu : Service / Squid Proxy Serveur / Local cache

Paramètre	Valeur / Description
Disable Caching	⬜ décoché (ne pas désactiver le cache, sauf besoin spécifique)
Cache Replacement Policy	`Heap LFUDA` (algorithme de remplacement de cache recommandé par défaut)
Low-Water Mark in %	`90` (seuil bas pour commencer à purger le cache disque)
High-Water Mark in %	`95` (seuil haut pour purger agressivement le cache disque)
Do Not Cache	Vide (liste des domaines ou IP à ne jamais cacher, si besoin)
Enable Offline Mode	⬜ décoché (le proxy vérifie toujours les objets expirés)
External Cache Managers	Vide (IP autorisées à gérer ce cache, si applicable)

Cliquez ensuite sur Save

COMPTE-RENDU DÉTAILLÉ :CONFIGURATION PFSENSE

Menu : Services / Squid Proxy Serveur / General

Section	Paramètre	Valeur / Description
Squid General Settings	Enable Squid Proxy	✅ activé
	Keep Settings/Data	✅ activé (pour préserver config, logs, cache)
	Listen IP Version	`IPv4`
	CARP Status VIP	`none`
	Proxy Interface(s)	`WAN`, `LAN`, `loopback` (sélectionne au moins `LAN`)
	Outgoing Network Interface	`Default (auto)`
	Proxy Port	`3128`
	ICP Port	vide (ne pas activer si pas besoin de neighbour caches)
	Allow Users on Interface	✅ activé (autorise tous les utilisateurs des interfaces sélectionnées à utiliser le proxy)
	Resolve DNS IPv4 First	✅ activé (utile pour résoudre problèmes HTTPS)
	Disable ICMP	❌ décoché (garde ICMP pinger helper)
	Use Alternate DNS Servers	vide (sauf besoin DNS spécifique)
	Extra Trusted CA	`none` (sauf si upstream proxy SSL/MITM spécifique)
Transparent Proxy Settings	Transparent HTTP Proxy	✅ activé
	Transparent Proxy Interface(s)	`WAN`, `LAN` (éviter d'autres interfaces non nécessaires)
	Bypass Proxy for Private Address Destination	✅ activé (ne pas proxy les IP privées RFC1918/ULA)

	Bypass Proxy for These Source IPs	vide (ajouter IP si besoin d'exclure du proxy)
	Bypass Proxy for These Destination IPs	vide (ajouter IP/domaines si besoin d'exclure du proxy)
SSL Man In the Middle Filtering	HTTPS/SSL Interception	✅ activé
	SSL/MITM Mode	`Splice Whitelist, Bump Otherwise` (mode recommandé)
	SSL Intercept Interface(s)	`WAN`, `LAN`
	SSL Proxy Port	`3129`
	SSL Proxy Compatibility Mode	`Modern`
	DHParams Key Size	`2048`
	CA	`pf-sense-SSL-Proxy-CA` (ton CA perso créé dans pfSense)
	SSL Certificate Daemon Children	`5` (ajuster selon charge CPU)
	Remote Cert Checks	sélectionner `Accept remote server certificate with errors` (pour éviter certains blocages)
	Certificate Adapt	laisser vide (optionnel, avancé)
Logging Settings	Enable Access Logging	✅ activé (attention espace disque)
	Log Store Directory	`/var/squid/logs`
	Rotate Logs	`7` (conserver 7 jours de logs)
	Log Pages Denied by SquidGuard	✅ activé (si SquidGuard utilisé pour filtrage)
Headers, Language & Custom	Visible Hostname	`localhost` (ou nom du proxy personnalisé)
	Administrator's Email	`admin@localhost` (adresse email pour messages d'erreur)

Error Language	`en` ou `fr` selon préférence
X-Forwarded Header Mode	`on` (garde les headers X-Forwarded-For)
Disable VIA Header	décoché (laisse le header Via pour conformité RFC)
URI Whitespace Characters Handling	`strip` (supprime les espaces dans URL pour sécurité)
Suppress Squid Version	optionnel (activer pour masquer version Squid dans erreurs/headers)

Ensuite n'oubliez pas de cliquez sur Save

7. Configuration de SquidGuard (Filtrage)

Menu : Services / SquidGuard Proxy Filter / General settings

LDAP Options :

Option	État recommandé	Commentaire
Enable LDAP Filter	❌ Non	LDAP non utilisé.
LDAP DN / Password / Cache Time	❌ Ignorer	Non applicable dans ton contexte.
Strip NT domain name	❌ Non	Inutile sans authentification.
Strip Kerberos Realm	❌ Non	Idem.
LDAP Version	Laisser par défaut	Version 3 est la valeur par défaut.

COMPTE-RENDU DÉTAILLÉ :CONFIGURATION PFSENSE

Logging Options – SquidGuard :

Option	État recommandé	Commentaire
Rewrite process children	✅ Oui (16)	Nombre maximal de processus redirecteurs SquidGuard.
Rewrite process children startup	✅ Oui (8)	Nombre minimal lancé au démarrage.
Rewrite process children idle	✅ Oui (4)	Nombre de processus disponibles en permanence.

Miscellaneous

Option	État recommandé	Commentaire
Clean Advertising	❌ Non	Permet d'afficher une vraie page de blocage (pas juste une image vide).

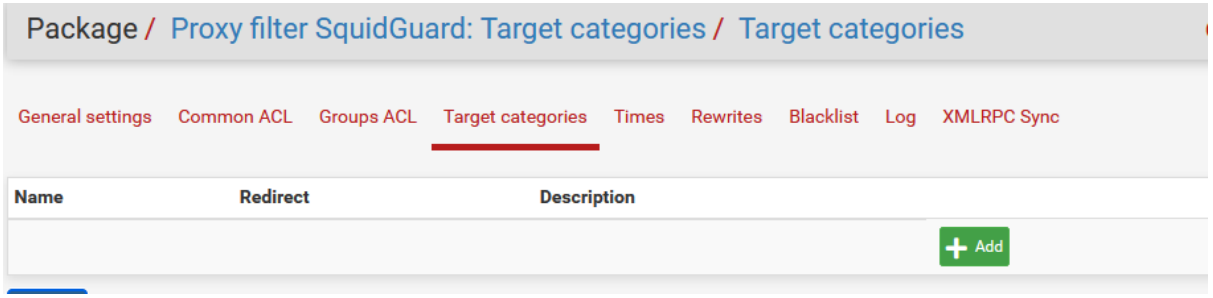
Blacklist options :

Option	État recommandé	Commentaire
Blacklist	❌ Non	Pas de blacklist externe, tu filtres manuellement par domaine.
Blacklist proxy	❌ Vide	Aucun proxy requis pour télécharger une blacklist.
Blacklist URL	❌ Vide	Aucune URL ou chemin local de blacklist utilisé.

Ensuite Save et en Haut de page cliquez sur Apply

COMPTE-RENDU DÉTAILLÉ :CONFIGURATION PFSENSE

Menu : Services / SquidGuard Proxy filter / Target Categories



Ensuite appuie sur [+Add]

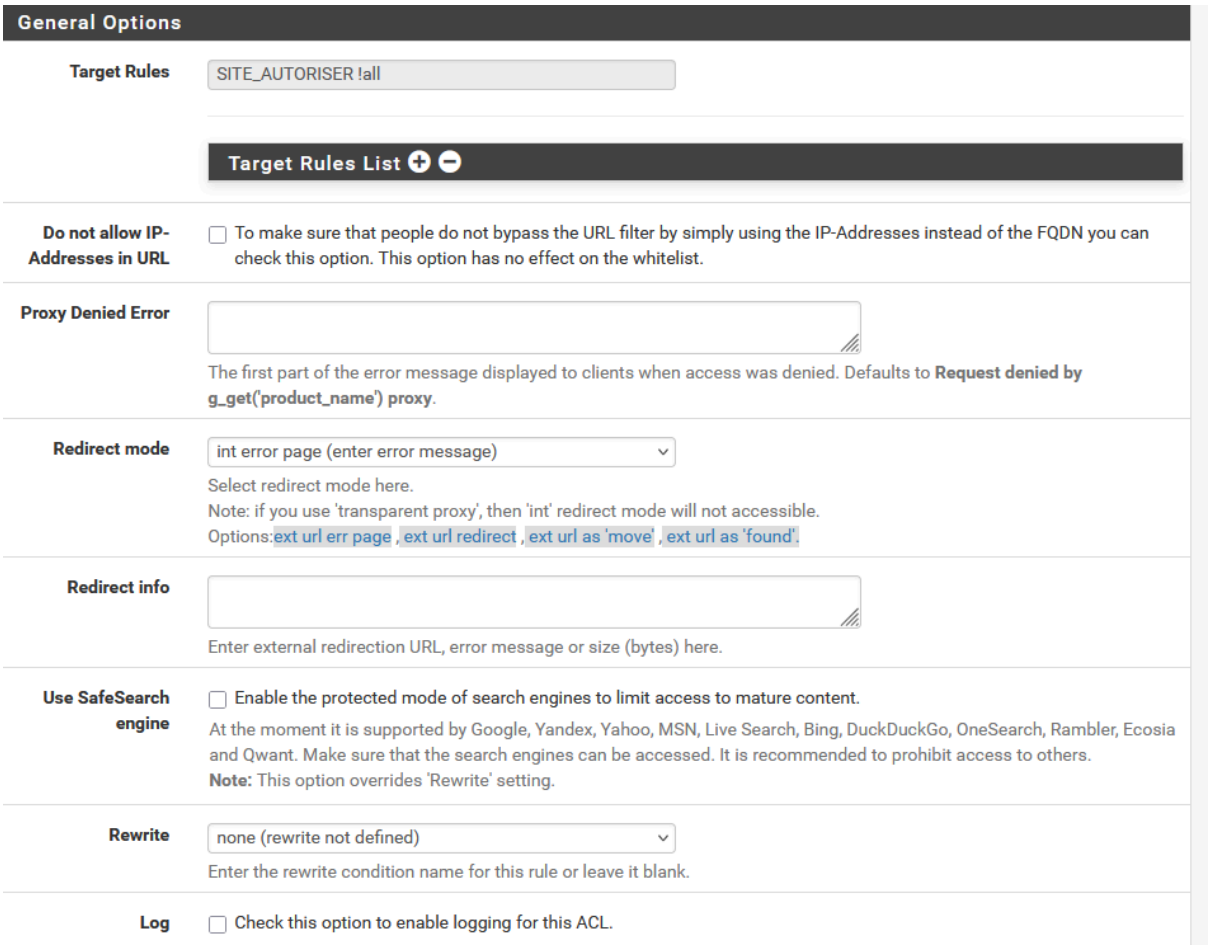
Remplis les champs :

Name : `allowed_sites`
Domain List : ajoute uniquement : recharplus.fr (n'oublie pas les API)

Cliquez sur **Save**.

COMPTE-RENDU DÉTAILLÉ :CONFIGURATION PFSENSE

Ensuite dans le même menu Allez sur “Commun ACLs”

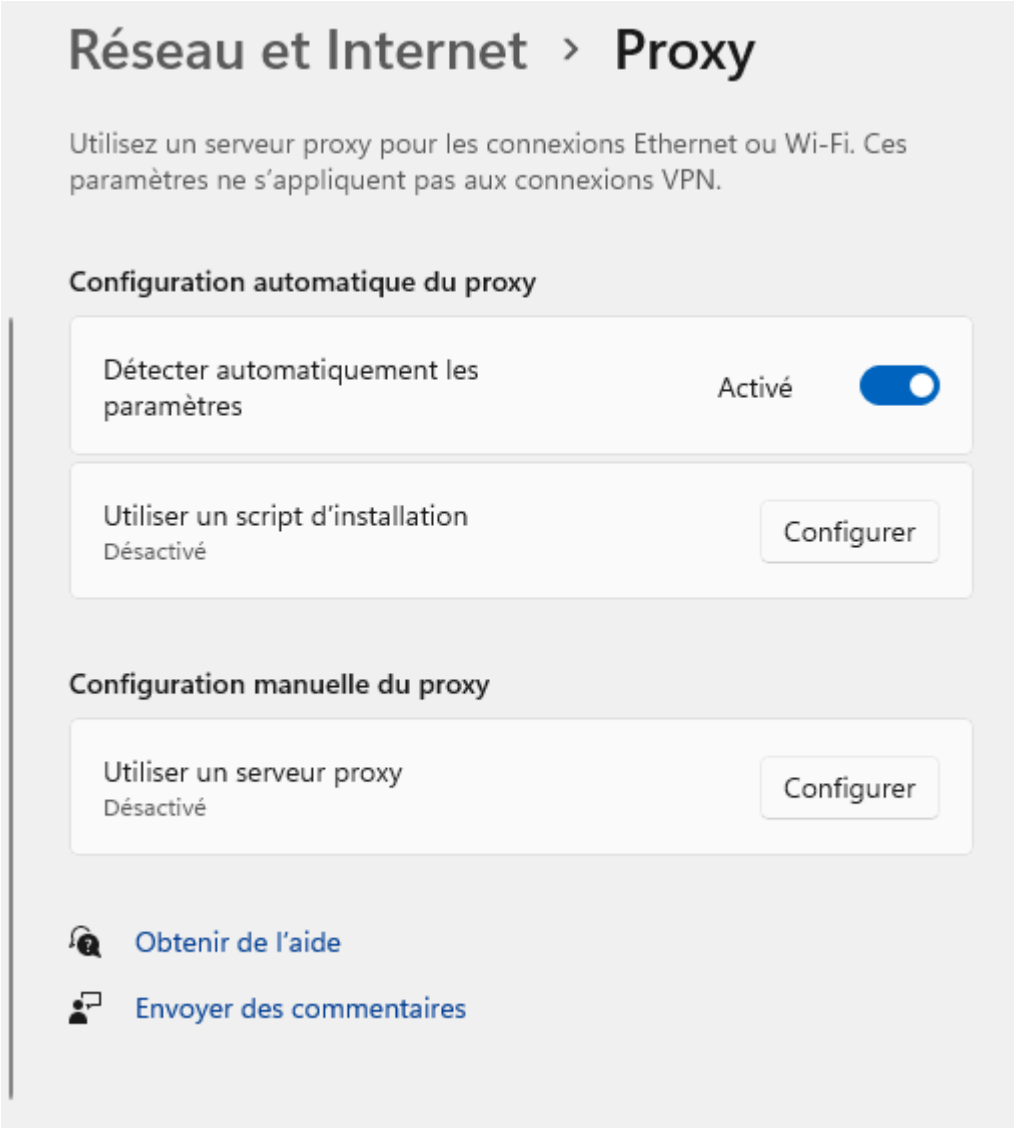


Après allez dans services/ SquidGuard : puis cliquez sur le bouton Apply afin de relancer le service.
Ensuite Services / Squid Proxy puis sur la flèche qui tourne afin de relancer le service.

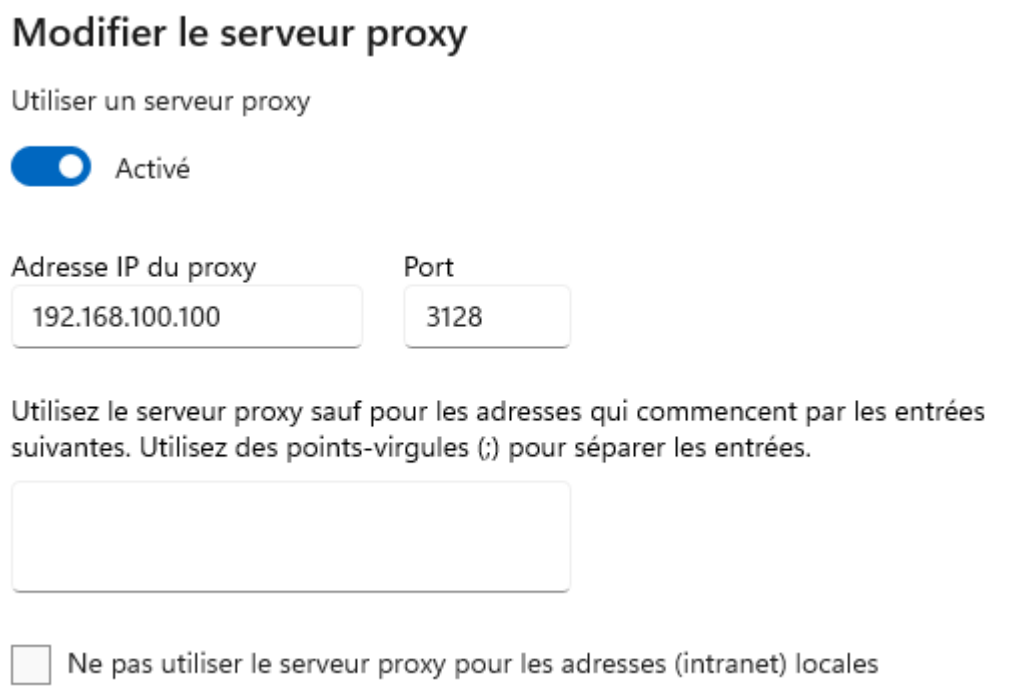
8. Configuration du poste client

Windows > Paramètres / Réseau & Internet / Proxy Activer "Utiliser un serveur proxy"
Adresse : IP du pfSense (ex. 192.168.100.100)
Port : 3128
Enregistrer

COMPTE-RENDU DÉTAILLÉ :CONFIGURATION PFSENSE

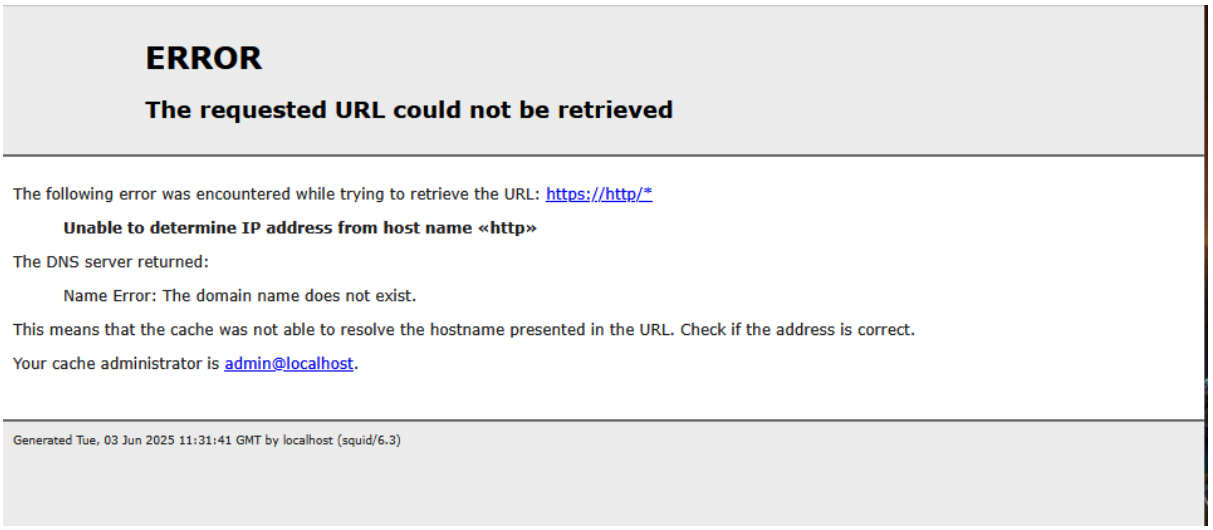


Utiliser L'adresse ip LAN de l'étape une


Modifier le serveur proxy
Utiliser un serveur proxy
Activé
Adresse IP du proxy
192.168.100.100
Port
3128
Utilisez le serveur proxy sauf pour les adresses qui commencent par les entrées suivantes. Utilisez des points-virgules (;) pour séparer les entrées.
Ne pas utiliser le serveur proxy pour les adresses (intranet) locales

9. Test final

Accéder à un site autre que rechargeplus.fr : doit être bloqué



Accéder à rechargeplus.fr : doit fonctionner normalement.

Cliquez sur Advanced