

## Installation d'un Pare-Feu Pfsense

1. Objectif.....	2
2. Configuration des interfaces réseau.....	2
3. Installation des paquets Squid et SquidGuard.....	3
4. Création d'une autorité de certification (CA).....	5
5. Création d'un certificat pour Squid.....	7
6. Configuration du proxy Squid.....	9
7. Configuration de SquidGuard (Filtrage).....	12
8. Configuration du poste client.....	15
9. Test final.....	17

# 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

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0          -> v4/DHCP4: 192.168.1.164/24
LAN (lan)      -> em1          -> v4: 192.168.100.100/24
```

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

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0          -> v4/DHCP4: 192.168.1.164/24
LAN (lan)      -> em1          -> v4: 192.168.100.100/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system             14) Enable Secure Shell (sshd)
6) Halt system               15) Restore recent configuration
7) Ping host                 16) Restart PHP-FPM
8) Shell
```

Puis agissez sur les deux interfaces en fonction de la demande ( DHCP, Statique)

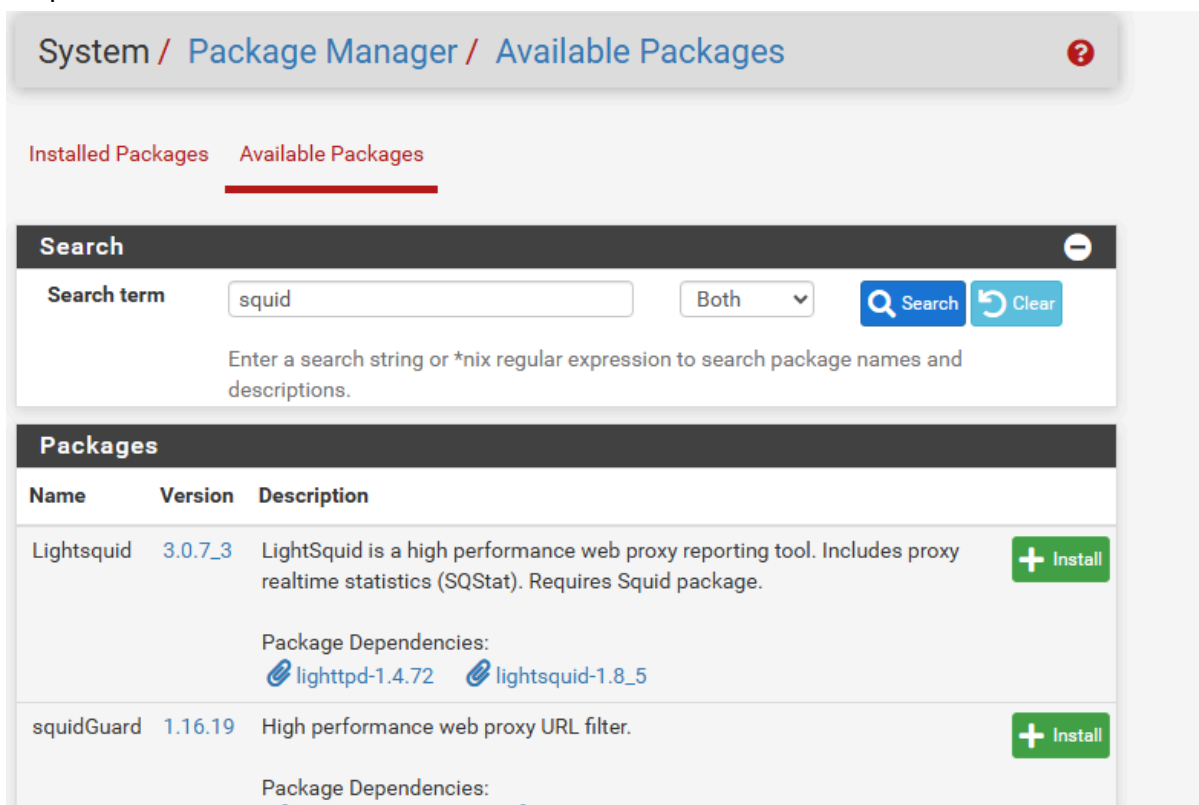
ATTENTION si le WAN est en statique il risque de ne pas être connecté à internet sauf cas exceptionnelle

# COMPTE-RENDU DÉTAILLÉ : CONFIGURATION PFSENSE

## 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 exceptionnelle



The screenshot shows the PfSense Package Manager interface. At the top, there is a breadcrumb trail: System / Package Manager / Available Packages. Below this, there are two tabs: 'Installed Packages' and 'Available Packages', with the latter being selected and underlined in red. A search bar is present with the search term 'squid' and a dropdown menu set to 'Both'. There are 'Search' and 'Clear' buttons. Below the search bar, there is a table of packages. The table has columns for Name, Version, and Description. Two packages are listed: 'Lightsquid' (version 3.0.7\_3) and 'squidGuard' (version 1.16.19). Both packages have a green '+ Install' button. The 'Lightsquid' package description mentions it requires the 'Squid' package and lists dependencies: 'lighttpd-1.4.72' and 'lightsquid-1.8\_5'. The 'squidGuard' package description mentions it is a high performance web proxy URL filter and lists dependencies.

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: <a href="#">lighttpd-1.4.72</a> <a href="#">lightsquid-1.8_5</a>	+ Install
squidGuard	1.16.19	High performance web proxy URL filter. Package Dependencies:	+ Install

# COMPTE-RENDU DÉTAILLÉ : CONFIGURATION PFSENSE

Répéter pour le paquet SquidGuard

```
Package Installation

http://www.squidguard.org/Doc/

To activate the changes do a /usr/local/sbin/squid -k reconfigure
=====
Message from pfSense-pkg-squidGuard-1.16.19:

--
Please visit Services - SquidGuard Proxy Filter - Target Categories and set up at least
one category there before enabling SquidGuard. See
https://docs.netgate.com/pfsense/en/latest/packages/cache-proxy/squidguard.html for
details.
>>> Cleaning up cache... done.
Success
```

Vérifiez qu'ils apparaissent bien dans Installed Packages

Installed Packages Available Packages

Installed Packages					
Name	Category	Version	Description	Actions	
✓ squid	www	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	🗑️ 🔄 ⓘ	
✓ squidGuard	www	1.16.19	High performance web proxy URL filter.  Package Dependencies: 🔗 squidguard-1.4_15 🔗 pfSense-pkg-squid-0.4.46	🗑️ 🔄	

🔄 = Update ✓ = Current  
🗑️ = Remove ⓘ = Information 🔄 = Reinstall

# COMPTE-RENDU DÉTAILLÉ : CONFIGURATION PFSENSE

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

Menu : System / Certificate / Authorities

System / Certificate / Authorities

Authorities Certificates Revocation

**Search**

Search term  Both

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

**Certificate Authorities**

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
------	----------	--------	--------------	--------------------	--------	---------

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 certificats créés, vous devez les importer pour le faire.

Menu : System / Certificate / Authorities

Cliquez sur l'étoile pour exporter le CA.

System / Certificate / Authorities

Authorities Certificates Revocation

**Search**

Search term  Both

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

**Certificate Authorities**

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
pf-sense-SSL-Proxy-CA	✓	self-signed	1	ST=France, O=Recharge+, L=Frejus, CN=pfsense-ssl-ca, C=FR	Squid (1)	<input type="button" value="Export CA"/>

Valid From: Wed, 28 May 2025 13:39:26 +0000  
Valid Until: Sat, 26 May 2035 13:39:26 +0000

Un fichier en .crt sera alors téléchargé.

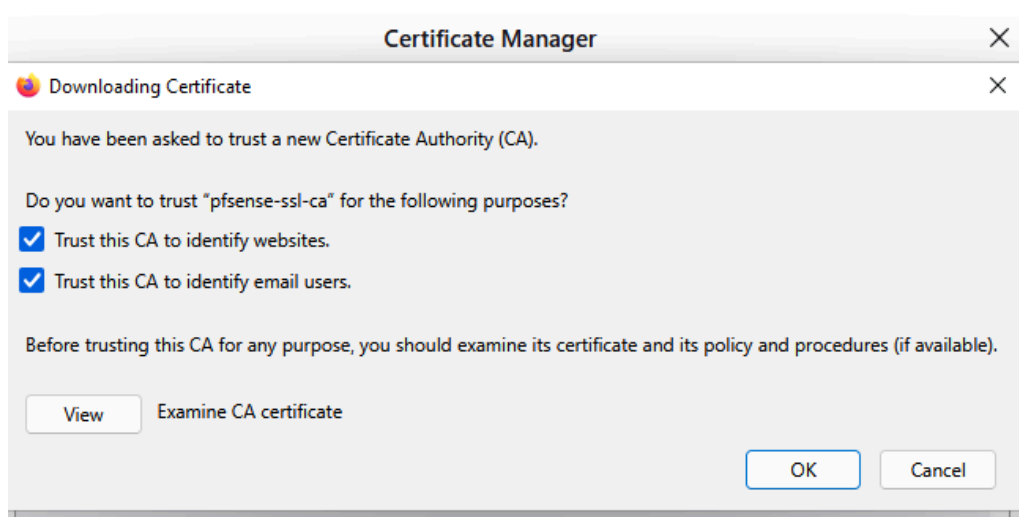


## Ajouter le certificat dans votre navigateur

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"**.

# COMPTE-RENDU DÉTAILLÉ : CONFIGURATION PFSENSE

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

System / Certificates / Certificates

Authorities Certificates Certificate Revocation

**Search**

Search term  Both

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

**Certificates**

Name	Issuer	Distinguished Name	In Use	Actions
GUI default (68370d24b806d) Server Certificate	self- signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-68370d24b806d		

CA: No  
Server: Yes

Valid From: Wed, 28 May 2025 13:18:28 +0000  
Valid Until: Tue, 30 Jun 2026 13:18:28 +0000

## 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'être 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	<input checked="" type="checkbox"/> Coche ( <b>Recommandé</b> )
Disable TCP segmentation offload	<input checked="" type="checkbox"/> Coche ( <b>Recommandé</b> )
Disable large receive offload	<input checked="" type="checkbox"/> Coche ( <b>Recommandé</b> )
hn ALTQ support	<input checked="" type="checkbox"/> Laisse décoché (sauf si Hyper-V)
Suppress ARP logs	<input type="radio"/> Optionnel
Reset all states on WAN IP change	<input type="radio"/> À activer si IP WAN est dynamique

Pour vérifier "nslookup [rechargeplus.fr](http://rechargeplus.fr)" il doit 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	<input type="checkbox"/> 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	<input type="checkbox"/> 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
<b>Squid General Settings</b>	Enable Squid Proxy	<input checked="" type="checkbox"/> activé
	Keep Settings/Data	<input checked="" type="checkbox"/> 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	<input checked="" type="checkbox"/> activé (autorise tous les utilisateurs des interfaces sélectionnées à utiliser le proxy)
	Resolve DNS IPv4 First	<input checked="" type="checkbox"/> activé (utile pour résoudre problèmes HTTPS)
	Disable ICMP	<input type="checkbox"/> 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)
<b>Transparent Proxy Settings</b>	Transparent HTTP Proxy	<input checked="" type="checkbox"/> activé
	Transparent Proxy Interface(s)	WAN, LAN (éviter d'autres interfaces non nécessaires)
	Bypass Proxy for Private Address Destination	<input checked="" type="checkbox"/> activé (ne pas proxy les IP privées RFC1918/ULA)

# COMPTE-RENDU DÉTAILLÉ : CONFIGURATION PFSENSE

	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)
<b>SSL Man In the Middle Filtering</b>	HTTPS/SSL Interception	<input checked="" type="checkbox"/> 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)
<b>Logging Settings</b>	Enable Access Logging	<input checked="" type="checkbox"/> activé (attention espace disque)
	Log Store Directory	/var/squid/logs
	Rotate Logs	7 (conserver 7 jours de logs)
	Log Pages Denied by SquidGuard	<input checked="" type="checkbox"/> activé (si SquidGuard utilisé pour filtrage)
<b>Headers, Language &amp; Custom</b>	Visible Hostname	localhost (ou nom du proxy personnalisé)
	Administrator's Email	admin@localhost (adresse email pour messages d'erreur)

# COMPTE-RENDU DÉTAILLÉ : CONFIGURATION PFSENSE

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 cliquer 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).

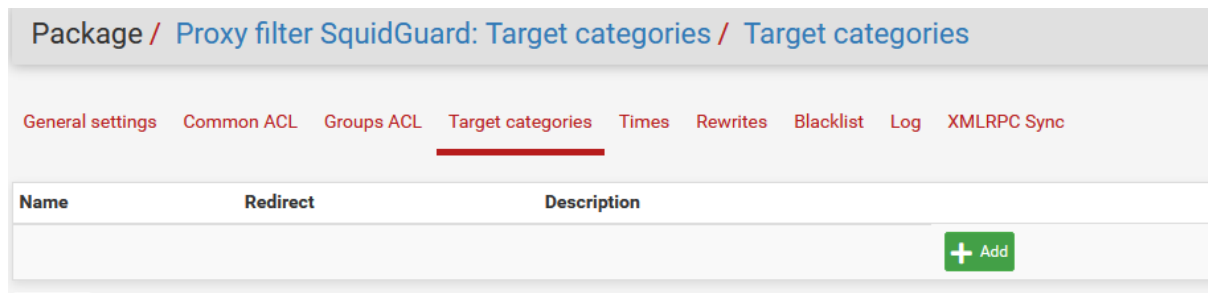
## Blacklist options :

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](http://recharplus.fr) (n'oublie pas les API)

Cliquez sur **Save**.

# COMPTE-RENDU DÉTAILLÉ : CONFIGURATION PFSENSE

Ensuite dans le même menu Allez sur "Commun ACLs"

## Target Rules List

ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.



## Target Categories

[SITE_AUTORISER]	access	allow	▼
Default access [all]	access	deny	▼

## General Options

**Target Rules**

---

**Target Rules List**  

---

**Do not allow IP-Addresses in URL**  To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.

---

**Proxy Denied Error**

The first part of the error message displayed to clients when access was denied. Defaults to `Request denied by g_get('product_name') proxy`.

---

**Redirect mode**

Select redirect mode here.  
Note: if you use 'transparent proxy', then 'int' redirect mode will not be accessible.  
Options: [ext url err page](#), [ext url redirect](#), [ext url as 'move'](#), [ext url as 'found'](#).

---

**Redirect info**

Enter external redirection URL, error message or size (bytes) here.

---

**Use SafeSearch engine**  Enable the protected mode of search engines to limit access to mature content.  
At the moment it is supported by Google, Yandex, Yahoo, MSN, Live Search, Bing, DuckDuckGo, OneSearch, Rambler, Ecosia and Qwant. Make sure that the search engines can be accessed. It is recommended to prohibit access to others.  
**Note:** This option overrides 'Rewrite' setting.

---

**Rewrite**

Enter the rewrite condition name for this rule or leave it blank.

---

**Log**  Check this option to enable logging for this ACL.

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

## Réseau et Internet > Proxy

Utilisez un serveur proxy pour les connexions Ethernet ou Wi-Fi. Ces paramètres ne s'appliquent pas aux connexions VPN.


### Configuration automatique du proxy


Détecter automatiquement les paramètres Activé

Utiliser un script d'installation Désactivé

### Configuration manuelle du proxy

Utiliser un serveur proxy Désactivé

 [Obtenir de l'aide](#)

 [Envoyer des commentaires](#)

Utiliser L'adresse ip LAN de l'étape une

# COMPTE-RENDU DÉTAILLÉ : CONFIGURATION PFSENSE

## 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

# COMPTE-RENDU DÉTAILLÉ : CONFIGURATION PFSENSE

## 9. Test final

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

**ERROR**

**The requested URL could not be retrieved**

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

**Unable to determine IP address from host name «http»**

The DNS server returned:

Name Error: The domain name does not exist.

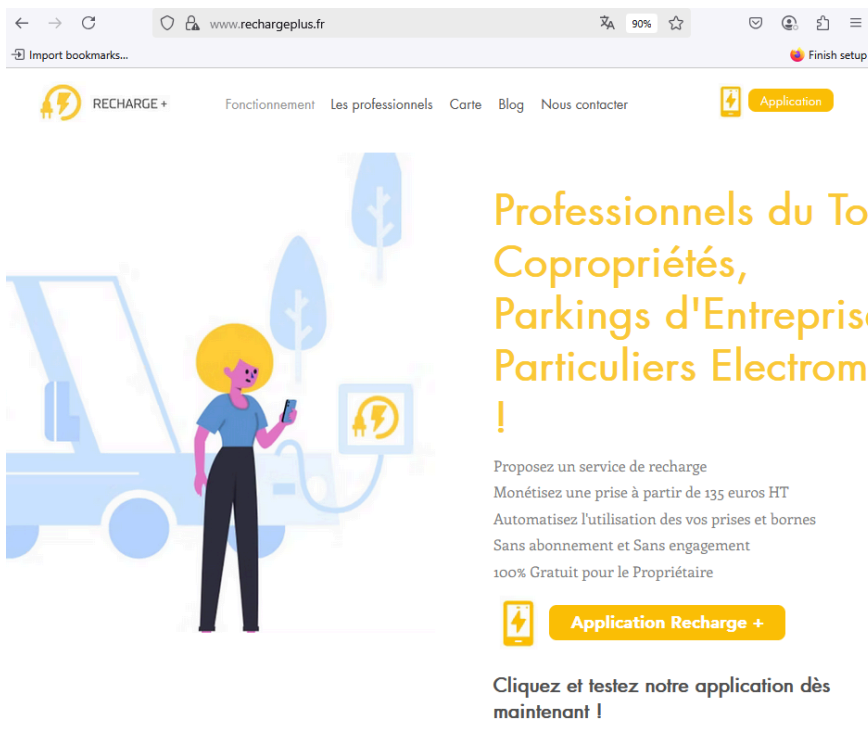
This means that the cache was not able to resolve the hostname presented in the URL. Check if the address is correct.

Your cache administrator is [admin@localhost](mailto:admin@localhost).

Generated Tue, 03 Jun 2025 11:31:41 GMT by localhost (squid/6.3)

Accéder à rechargeplus.fr : doit fonctionner normalement.

Cliquez sur Advanced



The screenshot shows a web browser displaying the website [www.rechargeplus.fr](http://www.rechargeplus.fr). The browser's address bar shows the URL and a 90% zoom level. The website's navigation menu includes: RECHARGE +, Fonctionnement, Les professionnels, Carte, Blog, Nous contacter, and Application. The main content area features a large illustration of a person with a yellow head and a blue shirt standing next to a blue electric vehicle. To the right of the illustration, the text reads: "Professionnels du Tou Copropriétés, Parkings d'Entreprise Particuliers Electrom !". Below this, a list of features is provided: "Proposez un service de recharge", "Monétisez une prise à partir de 135 euros HT", "Automatisez l'utilisation des vos prises et bornes", "Sans abonnement et Sans engagement", and "100% Gratuit pour le Propriétaire". A yellow button labeled "Application Recharge +" is prominently displayed. At the bottom, the text says "Cliquez et testez notre application dès maintenant !".