

# PfSense

- [Un proxy Open Source avec PfSense](#)
  - [Introduction](#)
  - [Prérequis](#)
  - [Installation](#)
  - [Configuration de Squid](#)
  - [Configuration de SquidGuard](#)
  - [Configuration manuelle du proxy](#)
  - [Configuration automatique du proxy](#)
  - [Références](#)

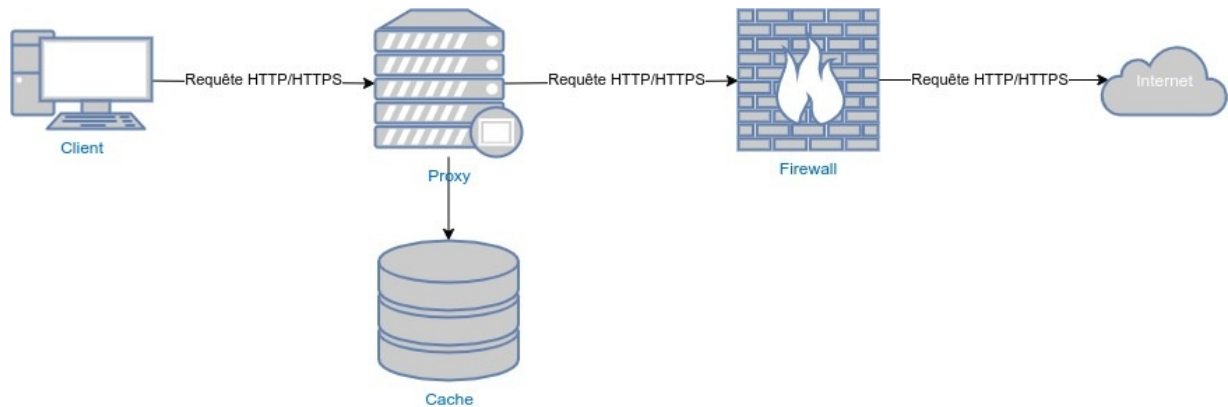
# Un proxy Open Source avec PfSense

# Introduction

Un **serveur mandataire** ou **proxy** (de l'anglais) est un serveur informatique qui a pour fonction de relayer des requêtes entre un poste client et un serveur. Les serveurs mandataires sont notamment utilisés pour assurer les fonctions suivantes :

- mémoire cache ;
- la journalisation des requêtes (« *logging* ») ;
- la sécurité du réseau local ;
- le filtrage et l'anonymat.

L'utilité des serveurs mandataires est importante, notamment dans le cadre de la sécurisation des systèmes d'information.



Ce tuto va vous permettre de créer un proxy avec filtrage et logging.

Nous allons utiliser [PfSense](#) comme base de travail.

A l'installation de base, nous allons ajouter les packages :

- Squid
- SquidGuard
- LightSquid

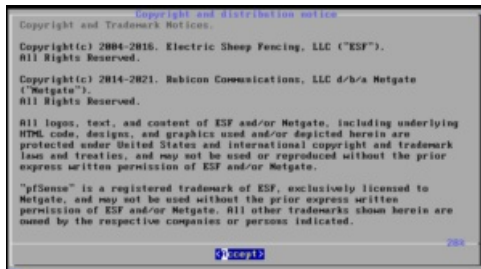
# Prérequis

- Une machine x86 physique ou virtuelle avec une interface réseau
- un serveur DNS
- un serveur DHCP
- un firewall

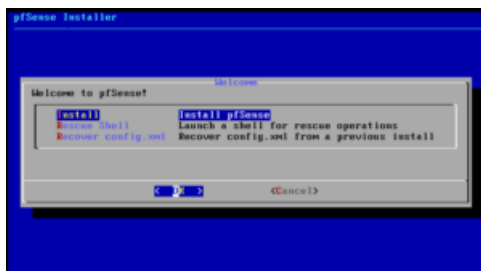
# Installation

Je vous invite à télécharger l'ISO de PfSense sur le site : <https://www.pfsense.org/download/>

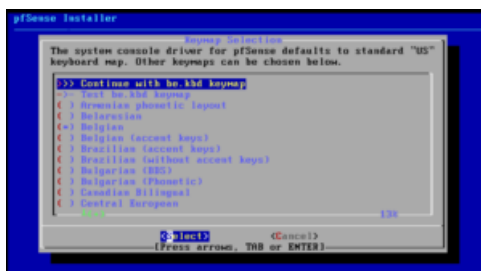
PfSense peut être installé sur une machine physique ou sur une machine virtuelle.  
Pour ma part, il sera installé sur VMMware ESXi 6.5.



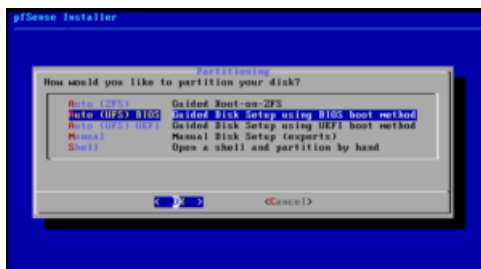
Le CLUF



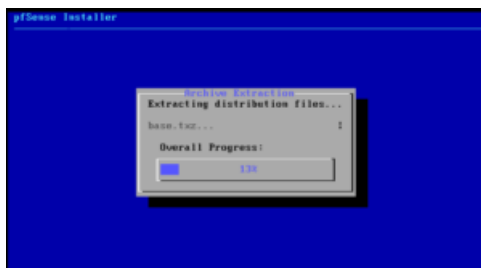
Sélectionner « Install »



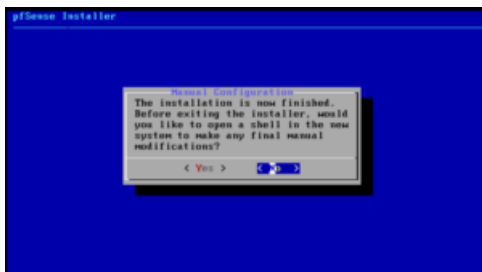
Choisir sa disposition de clavier



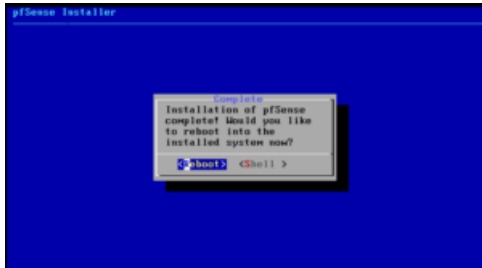
Choisir son type de système de fichiers



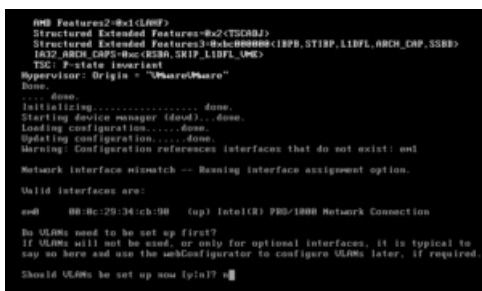
Patience...



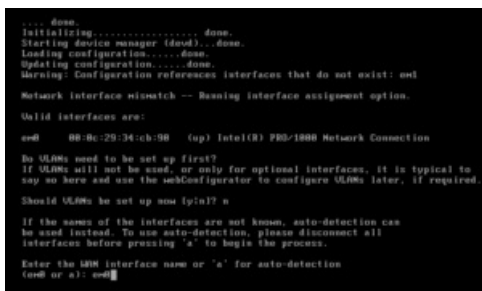
Sélectionner « No »



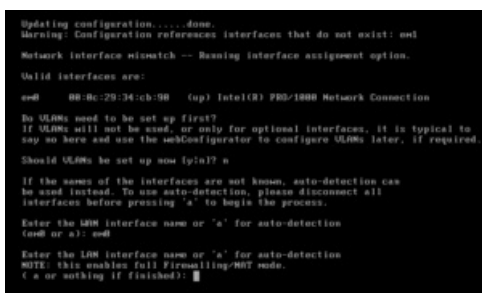
Sélectionner « Reboot »



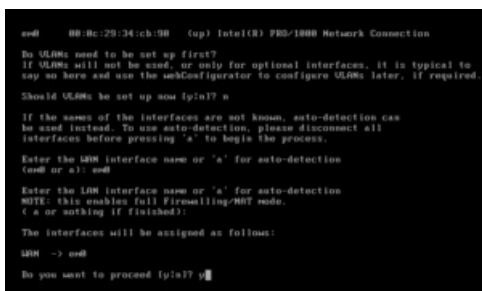
Ne pas configurer de Vlan



Introduire le nom de l'interface réseau



Presser « Enter »



Enter « Y »

```
Generating RRE graphs... done.
Starting syslogd... done.
Starting CRON... done.
pfSense 2.5.2-RELEASE amd64 Fri Jul 02 15:33:00 EDT 2021
Bootstrap complete

FreeBSD/amd64 (pfSense.hom.arp) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 73493e9476afad913055

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

M0N (mm) -> mm0 -> v4/DHCP4: 172.16.1.153/16

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 (ssh)
6) Halt system               15) Restore recent configuration
7) Ping host                 16) Restart PHP-FPM
8) Shell

Enter as option: 2
```

Sélectionner l'option 2 pour configurer l'adresse IP

```
VMware Virtual Machine - Netgate Device ID: 73493e9476afad913055

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

M0N (mm) -> mm0 -> v4/DHCP4: 172.16.1.153/16

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 (ssh)
6) Halt system               15) Restore recent configuration
7) Ping host                 16) Restart PHP-FPM
8) Shell

Enter as option: 2

Configure IPv4 address M0N interface via DHCP? (y/n) y
Configure IPv6 address M0N interface via DHCP? (y/n) n
Enter the new M0N IPv6 address. Press <ENTER> for none:
>
```

Je sélectionne l'option DHCP pour attribuer une IP

```
M0N (mm) -> mm0 -> v4/DHCP4: 172.16.1.153/16

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 (ssh)
6) Halt system               15) Restore recent configuration
7) Ping host                 16) Restart PHP-FPM
8) Shell

Enter as option: 2

Configure IPv4 address M0N interface via DHCP? (y/n) y
Configure IPv6 address M0N interface via DHCP? (y/n) n
Enter the new M0N IPv6 address. Press <ENTER> for none:
>
Disabling IPv4 DHCP...
Disabling IPv6 DHCP...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y
```

Introduire « Y »

```
Restarting webConfigurator...

The IPv4 M0N address has been set to dhcp
You can now access the webConfigurator by opening the following URL in your web browser:
      http://dhcp/

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 73493e9476afad913055

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

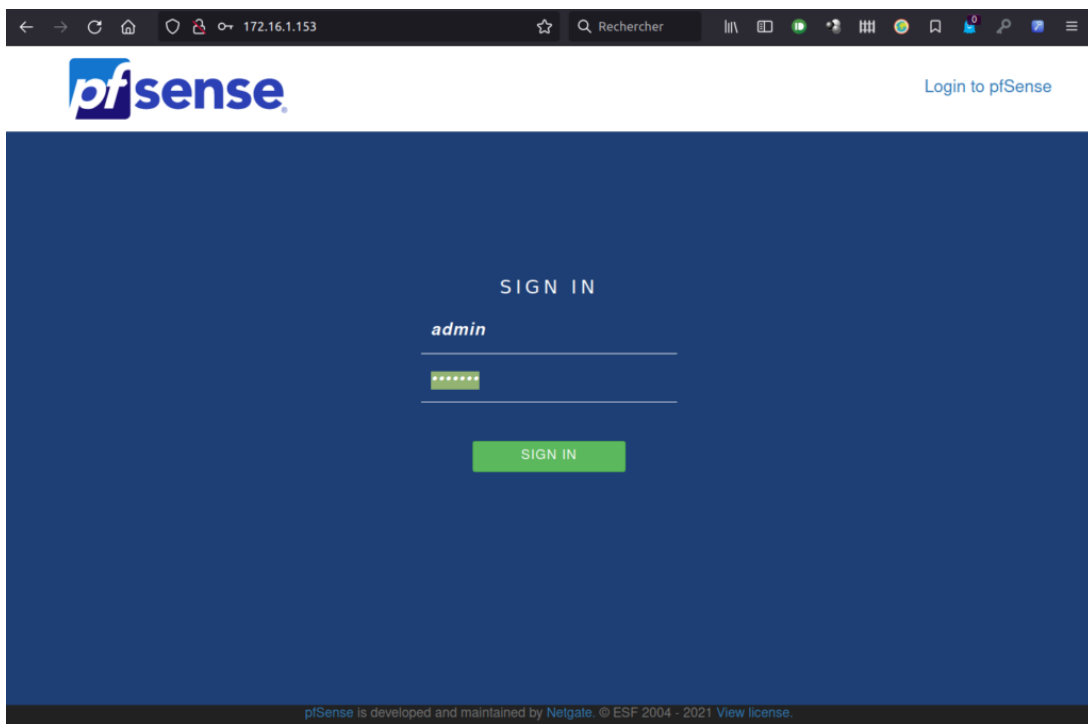
M0N (mm) -> mm0 -> v4/DHCP4: 172.16.1.153/16

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 (ssh)
6) Halt system               15) Restore recent configuration
7) Ping host                 16) Restart PHP-FPM
8) Shell

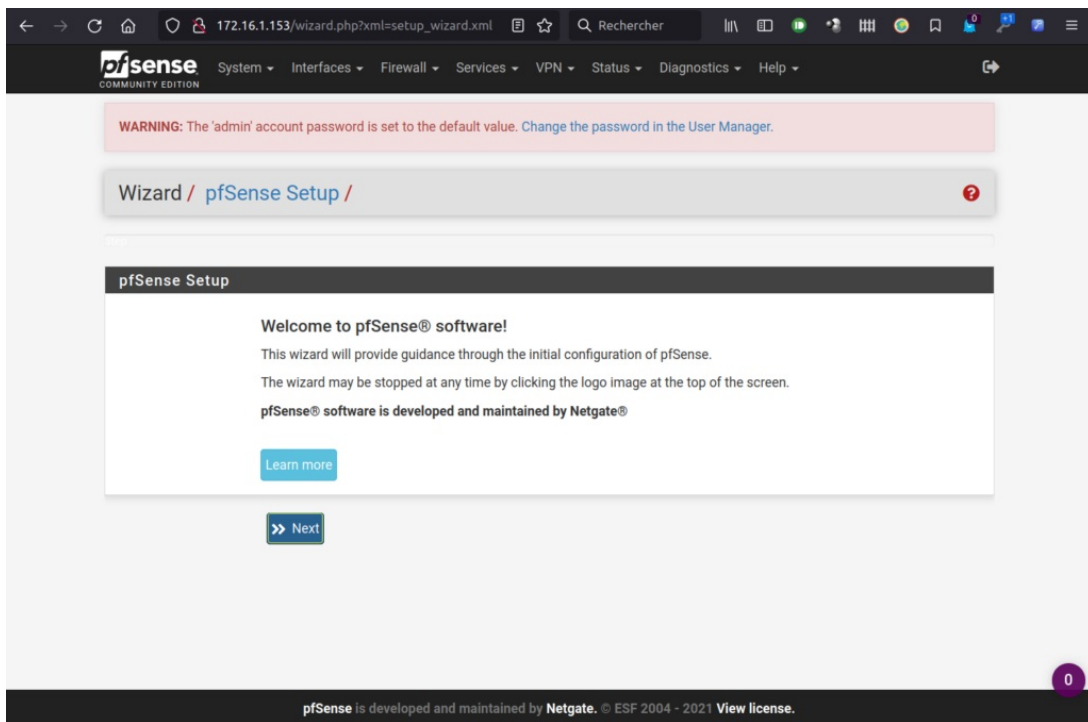
Enter as option: 
```

Et voilà

A présent, nous allons pouvoir passer via l'interface Web de management de PfSense via <http://<IP>> Pour Configurer PfSense et installer les packages nécessaires au fonctionnement du proxy.



Le login/password et admin/pfsense



« Next »



← → ↻ 172.16.1.153/wizard.php?xml=setup\_wizard.xml ⌘ ⌕ Rechercher

**pfSense** COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / **pfSense Setup** / Netgate® Global Support is available 24/7 ?

Step 1 of 9

**Netgate® Global Support is available 24/7**

Our 24/7 worldwide team of support engineers are the most qualified to diagnose your issue and resolve it quickly, from branch office to enterprise – on premises to cloud.

We offer several support subscription plans tailored to fit different environment sizes and requirements. Many companies around the world choose Netgate support because:

- Support is available 24 hours a day, seven days a week, including holidays.
- Support engineers are located around the world, ensuring that no support call is missed.
- Our support engineers hold many prestigious network engineer certificates and have years of hands-on experience with networking.

[Learn more](#)

[» Next](#)

pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 [View license.](#)

« Next »

← → ↻ 172.16.1.153/wizard.php?xml=setup\_wiz... 90 % ⌘ ⌕ Rechercher

**pfSense** COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / **pfSense Setup** / General Information ?

Step 2 of 9

**General Information**

On this screen the general pfSense parameters will be set.

**Hostname** proxy  
EXAMPLE: myserver

**Domain** home.local  
EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

**Primary DNS Server** 192.168.1.1

**Secondary DNS Server** 192.168.1.2

**Override DNS** ☒  
Allow DNS servers to be overridden by DHCP/PPP on WAN

[» Next](#)

pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 [View license.](#)

Introduire le hostname, le domainet et les ip's des DNS

← → ↻ 172.16.1.153/wizard.php?xml=setup\_wizard.xml 90% Rechercher

**pfSense** COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup / Time Server Information ?

Step 3 of 9

### Time Server Information

Please enter the time, date and time zone.

Time server hostname

Enter the hostname (FQDN) of the time server.

Timezone

>> Next

pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 [View license.](#)

Choisir son serveur NTP et la timezone

← → ↻ 172.16.1.153/wizard.php?xml=setup\_wizard.xml Rechercher

pptplocalsubnet

PPTP Remote IP Address

PPTP Dial on demand ☐ Enable Dial-On-Demand mode  
This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.

PPTP Idle timeout   
If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

### RFC1918 Networks

Block RFC1918 Private Networks ☐ Block private networks from entering via WAN  
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

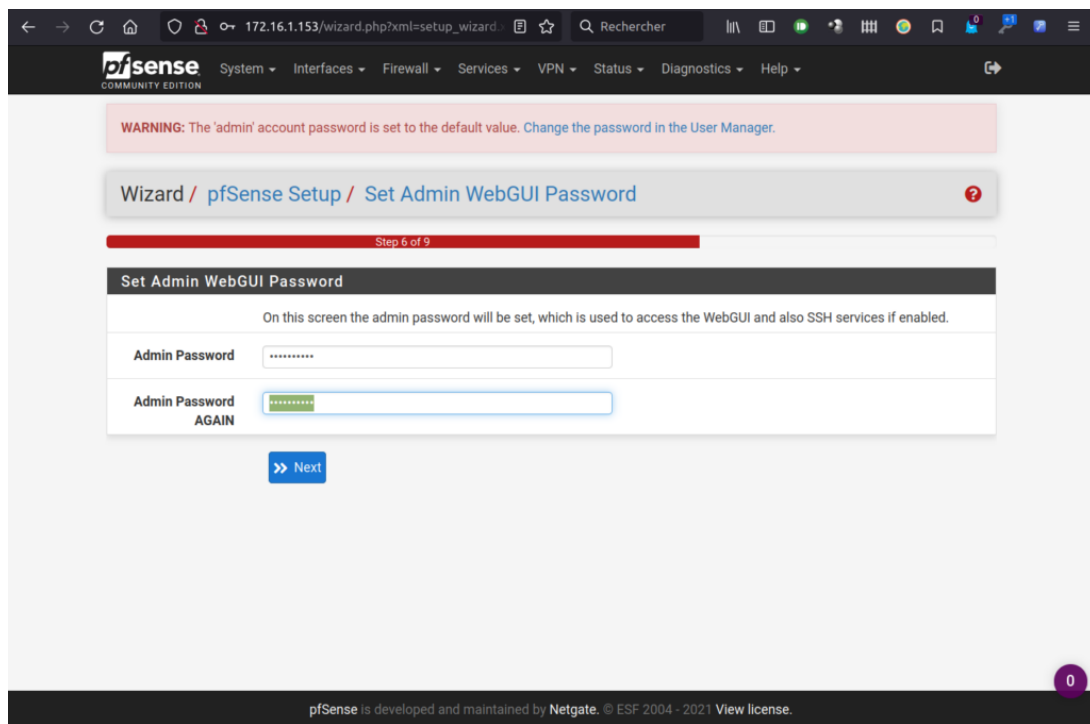
### Block bogon networks

Block bogon networks ☐ Block non-Internet routed networks from entering via WAN  
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

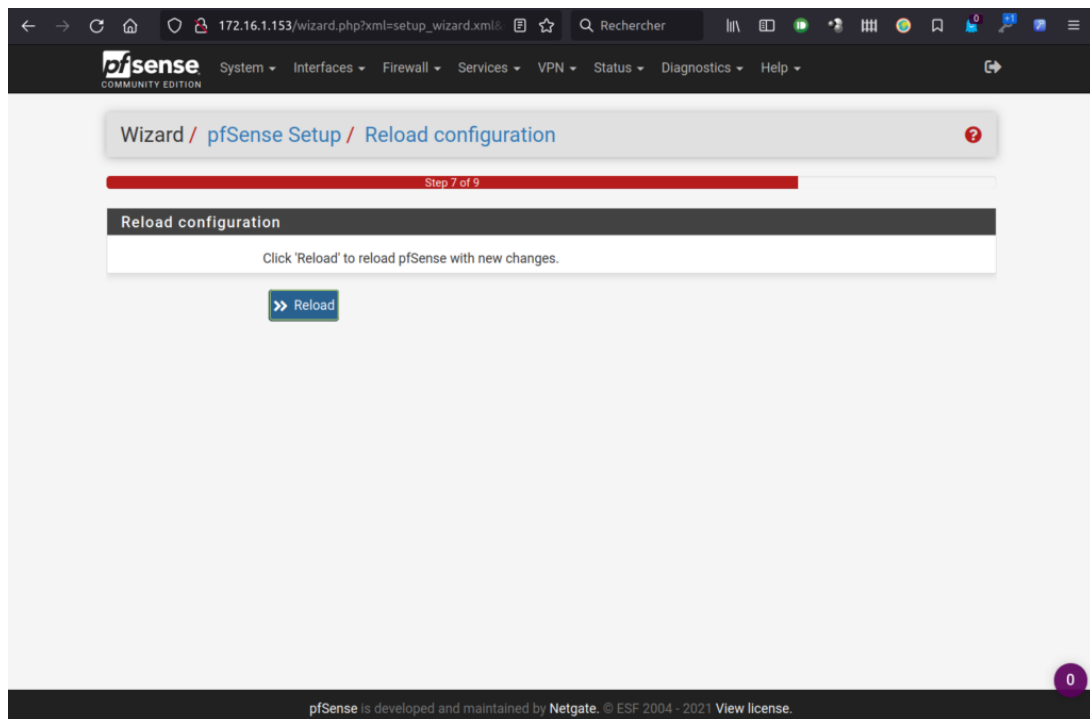
>> Next

pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 [View license.](#)

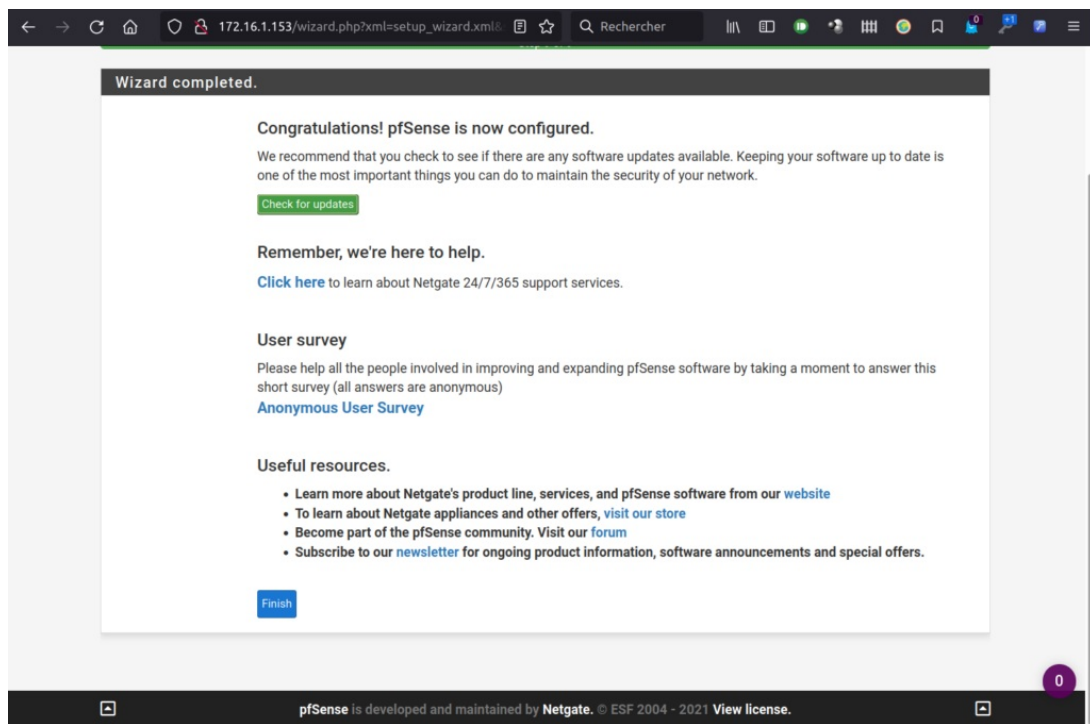
« Next »



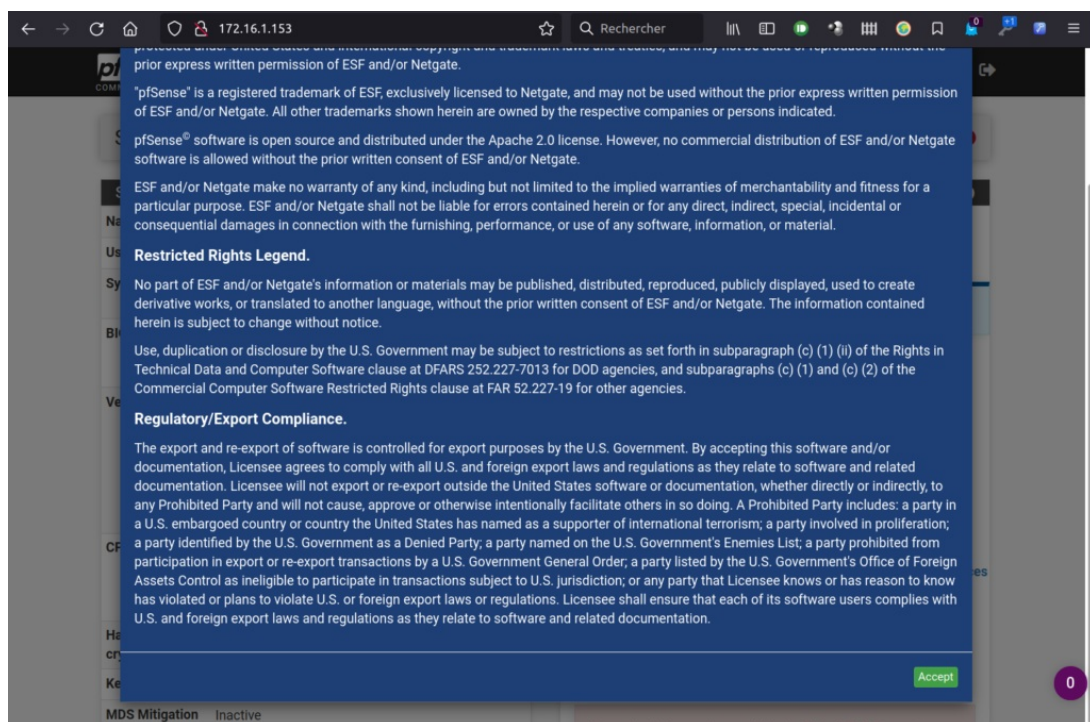
Introduire un nouveau mot de passe pour l'utilisateur « admin »



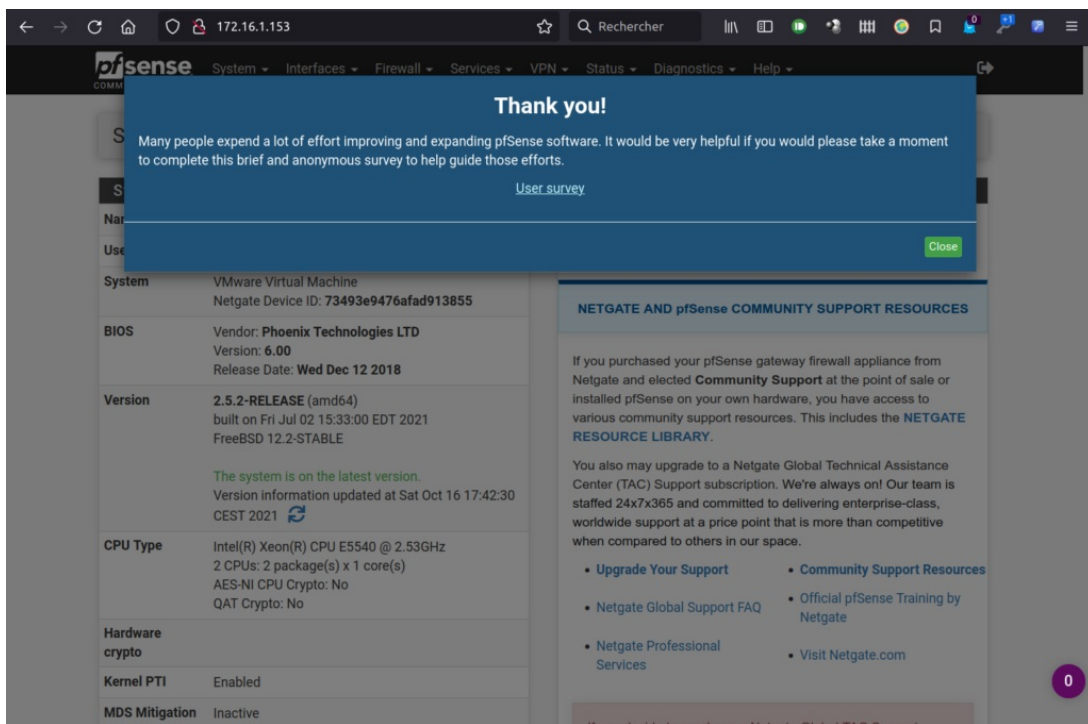
Cliquer sur « Reload »



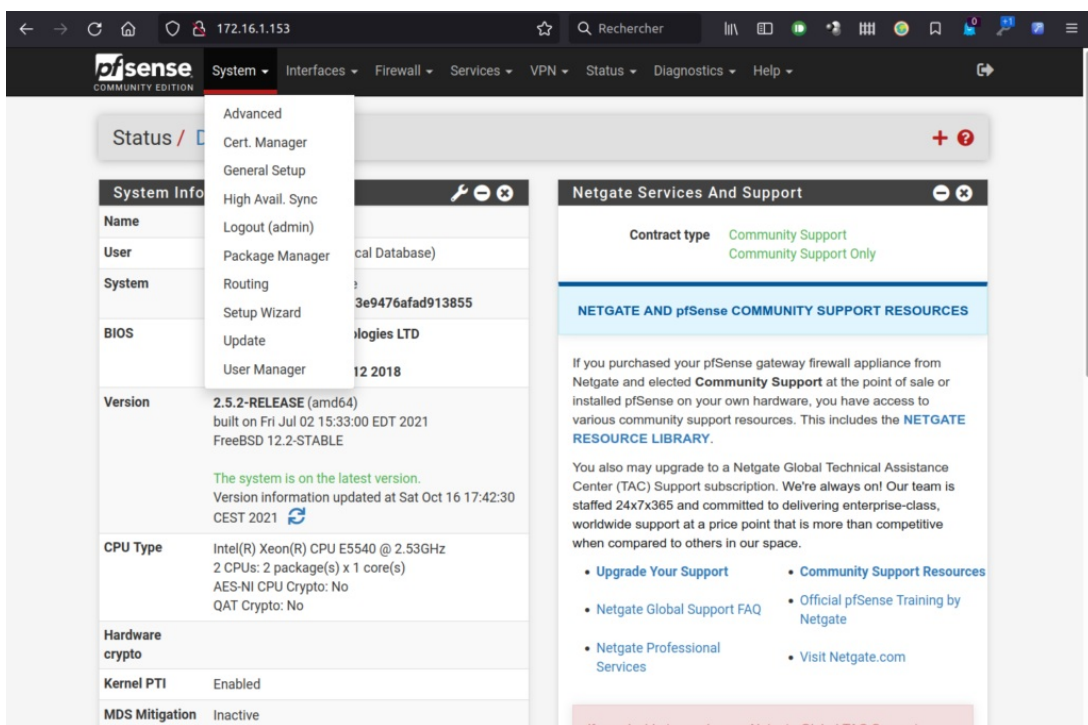
Cliquer sur « Finish »



« Accept »



« Close »



Sélectionner le « Package Manager »

← → ↻ 172.16.1.153/pkg\_mgr.php ☆ Rechercher

**pfSense** COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Package Manager / Available Packages ?

Installed Packages Available Packages

**Search**

Search term  Both Search Clear

Enter a search string or \*nix regular expression to search package names and descriptions.

**Packages**

Name	Version	Description	
Lightsquid	3.0.6_8	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package.	+ Install
Package Dependencies: <a href="#">lighttpd-1.4.59</a> <a href="#">lightsquid-1.8_5</a>			
squid	0.4.45_5	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.	+ Install
Package Dependencies: <a href="#">squidclamav-7.1</a> <a href="#">squid_radius_auth-1.10</a> <a href="#">squid-4.15</a> <a href="#">c-icap-modules-0.5.5</a>			
squidGuard	1.16.18_20	High performance web proxy URL filter.	+ Install
Package Dependencies: <a href="#">squidguard-1.4_15</a> <a href="#">pfSense-pkg-squid-0.4.45_5</a>			

Dans « Available Packages ». rechercher les packages liés à Squid

← → ↻ 172.16.1.153/pkg\_mgr\_install.php?pkg=pfSense-pkg-squid ☆ Rechercher

**pfSense** COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Package Manager / Package Installer ?

Installed Packages Available Packages Package Installer

**Confirmation Required to install package pfSense-pkg-squid.**

☒ Confirm

0

pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license.

Procéder à l'installation des packages



← → ↻ 172.16.1.153/pkg\_mgr\_install.php ☆ Rechercher

**pfSense** COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Package Manager / Package Installer ?

Please wait while the installation of **pfSense-pkg-squid** completes.  
This may take several minutes. Do not leave or refresh the page!

Installed Packages Available Packages **Package Installer**

**Package Installation**

```
(tmispack: 0.10.1 [pfSense]
pfSense-pkg-squid: 0.4.45_5 [pfSense]
squid: 4.15 [pfSense]
squid_radius_auth: 1.10 [pfSense]
squidclamav: 7.1 [pfSense]
unzoo: 4.4_2 [pfSense]

Number of packages to be installed: 14

The process will require 24 MiB more space.
6 MiB to be downloaded.
[1/14] Fetching pfSense-pkg-squid-0.4.45_5.txz: ..... done
[2/14] Fetching squidclamav-7.1.txz: ..... done
[3/14] Fetching c-icap-0.5.8,2.txz: ..... done
[4/14] Fetching cyrus-sasl-2.1.27.1.txz: ..... done
[5/14] Fetching brotli-1.0.9,1.txz: .....|
```

0

← → ↻ 172.16.1.153/pkg\_mgr\_install.php ☆ Rechercher

**pfSense** COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Package Manager / Package Installer ?

**pfSense-pkg-squid** installation successfully completed.

Installed Packages Available Packages **Package Installer**

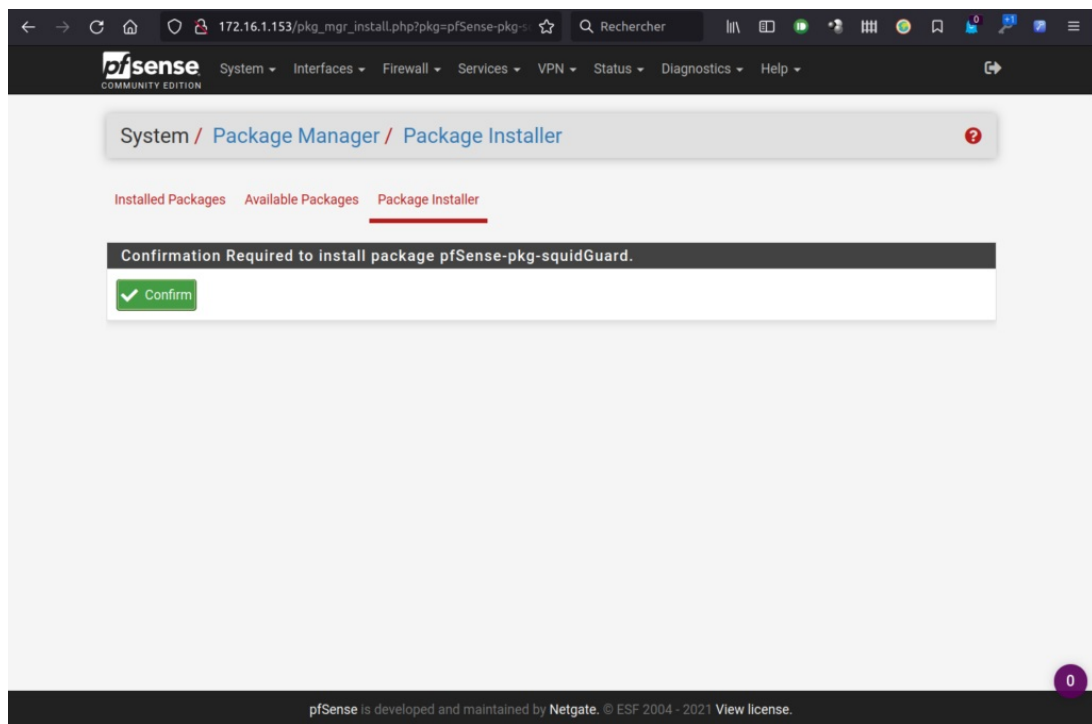
**Package Installation**

```
make sure to check your Squid configuration against the 3.4 default
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-0.4.45_5:

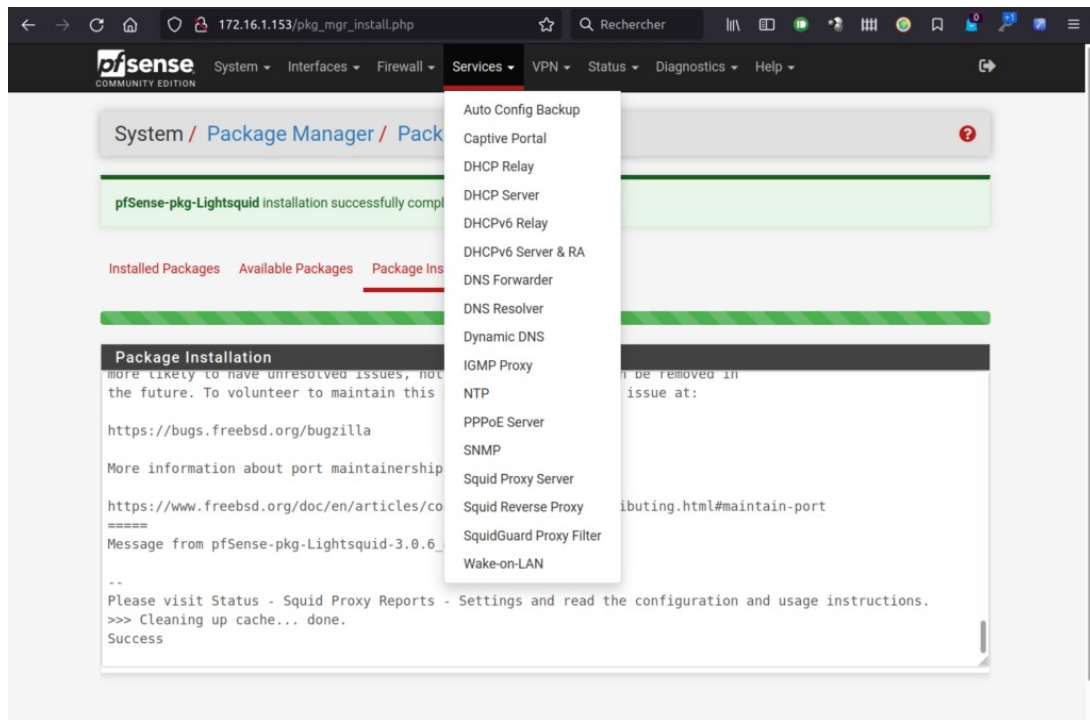
--
Please visit Services - Squid Proxy Server menu to configure the package and enable the proxy.
>>> Cleaning up cache... done.
Success
```



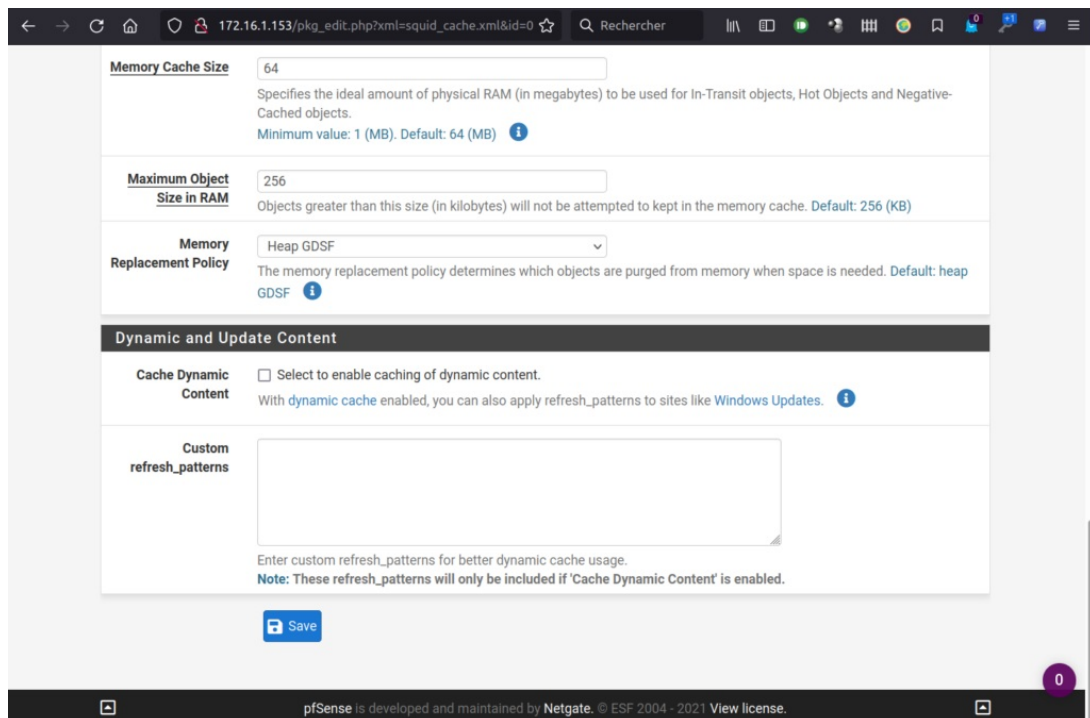
Et voilà...



# Configuration de Squid



Sélectionner « Squid Proxy Server »



Faire un « Save » dans l'option « LocalCache » pour l'initialiser

← → ↻ 172.16.1.153/pkg\_edit.php?xml=squid.xml&id=0 Rechercher

**pfSense** COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

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

**Outgoing Network** Default (auto)

Cocher « Check to enable the Squid proxy »

← → ↻ 172.16.1.153/pkg\_edit.php?xml=squid.xml&id=0 Rechercher

Certificate Adapt Sets the Not After (setValidAfter)  
Sets the "Not Before" (setValidBefore)  
Sets CN property (setCommonName)  
See `sslproxy_cert_adapt` directive documentation and Mimic original SSL server certificate wiki article for details.

### 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** 10  
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** 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** en  
Select the language in which the proxy server will display error messages to users.

**X-Forwarded Header Mode** (on)

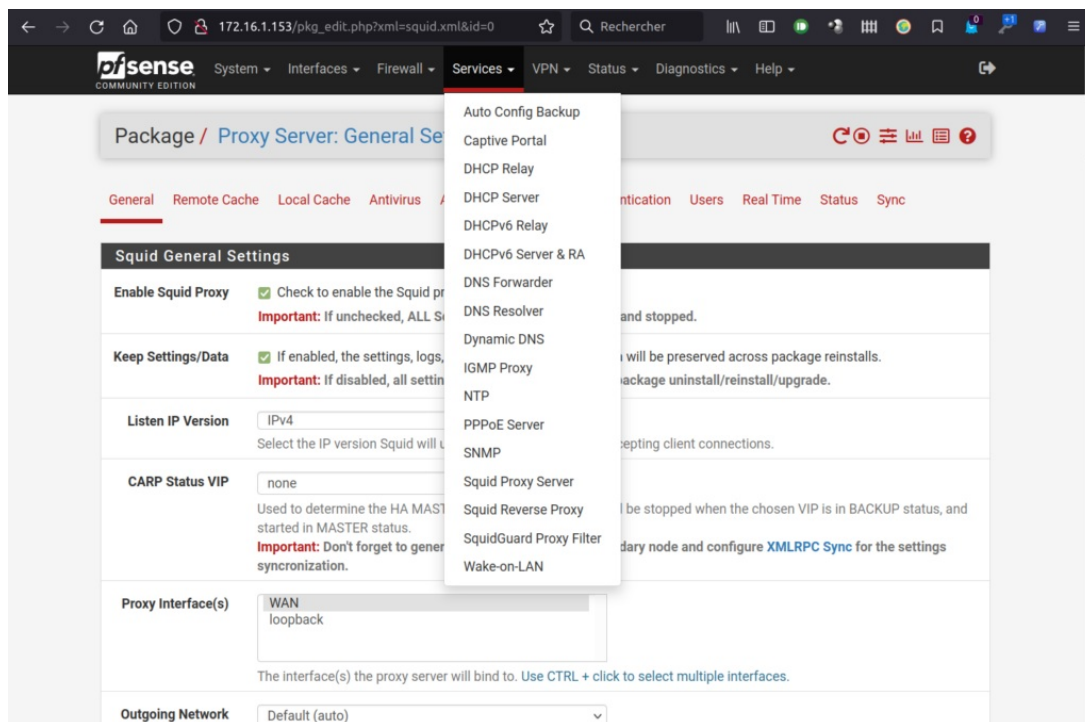
Coocher « This will enable the access log » et « Save »

# Configuration de SquidGuard

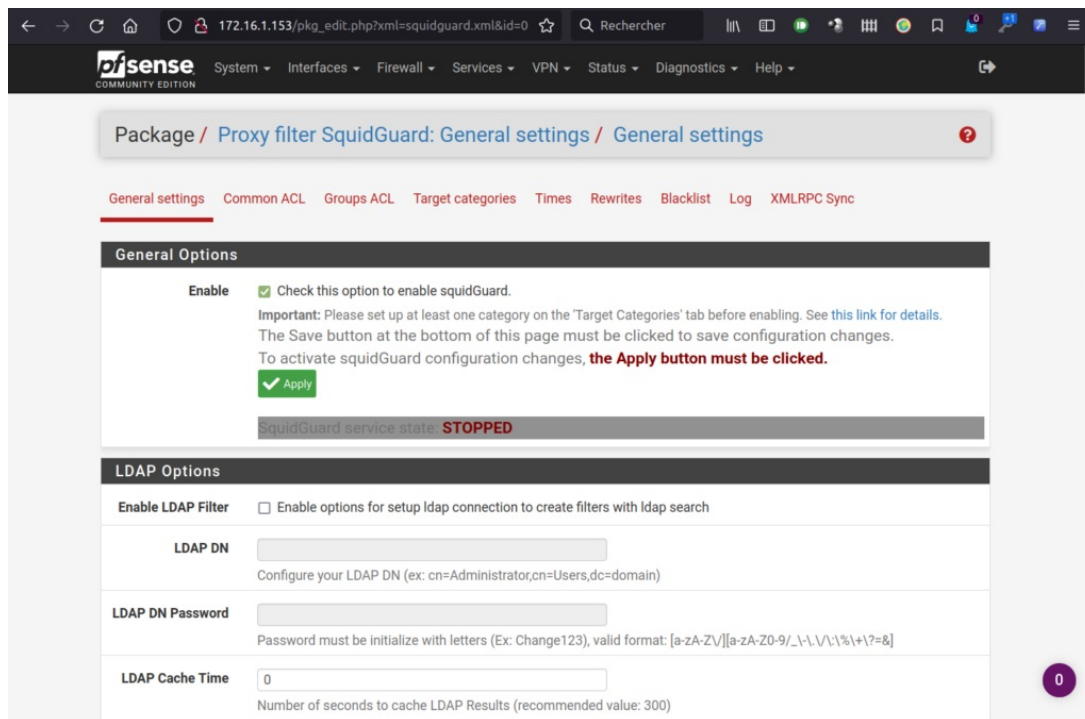
SquidGuard est un « add-on » pour Squid qui va vous permettre d'effectuer du filtrage basé sur des blacklists/whitelists.

J'utilise la blacklist de L'Université de Toulouse.

<https://dsi.ut-capitole.fr/blacklists/>



Sélectionner « SquiGuard Proxy Filter »



Cocher « Check this option to enable squidGuard »

172.16.1.153/pkg\_edit.php?xml=squidguard.xml&id=0

Rechercher

**Enable GUI log** ☐ Check this option to log the access to the Proxy Filter GUI.

**Enable log** ☐ Check this option to log the proxy filter settings like blocked websites in Common ACL, Group ACL and Target Categories. This option is usually used to check the filter settings.

**Enable log rotation** ☐ Check this option to rotate the logs every day. This is recommended if you enable any kind of logging to limit file size and do not run out of disk space.

**Miscellaneous**

**Clean Advertising** ☐ Check this option to display a blank gif image instead of the default block page. With this option the user gets a cleaner webpage.

**Blacklist options**

**Blacklist** ☒ Check this option to enable blacklist

**Blacklist proxy**

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'

**Blacklist URL**

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).

[Save](#)

pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license.

Cocher « Check this option to enable blacklist » et introduire l'URL de la blacklist

172.16.1.153/squidGuard/squidguard\_blacklist.php

Rechercher

System Interfaces Firewall Services VPN Status Diagnostics Help

Package / SquidGuard / Blacklists

General settings Common ACL Groups ACL Target categories Times Rewrites **Blacklist** Log XMLRPC Sync

**Blacklist Update**

Blacklist download progress

0%

[Download](#) [Cancel](#) [Restore Default](#)

Enter FTP or HTTP path to the blacklist archive here.

**Blacklist update Log**

```

Begin blacklist update
Start download.
Download archive ftp://ftp.ut-capitole.fr/pub/reseau/cache
/squidguard_contrib/blacklists.tar.gz

```

0

Effectuer le download de la blacklist

← → ↻ 172.16.1.153/pkg\_edit.php?xml=squidguard\_default... Rechercher

**pfSense** COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Package / Proxy filter SquidGuard: Common Access Control List (ACL) / Common ACL ?

General settings **Common ACL** Groups ACL Target categories Times Rewrites Blacklist Log XMLRPC Sync

**General Options**

Target Rules

**Target Rules List** + -

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

Target Categories	Access	Action
[blk_blacklists_ads]	access	---
[blk_blacklists_adult]	access	deny
[blk_blacklists_aggressive]	access	---
[blk_blacklists_gmail]	access	---
[blk_blacklists_associations_religieuses]	access	---
[blk_blacklists_astrology]	access	---
[blk_blacklists_audio-video]	access	---
[blk_blacklists_bank]	access	---
[blk_blacklists_bitcoin]	access	---
[blk_blacklists_blog]	access	---
[blk_blacklists_celebrity]	access	---
[blk_blacklists_chat]	access	---

Sélectionner les catégories que vous désirez filtrer

← → ↻ 172.16.1.153/pkg\_edit.php?xml=squidguard\_default... Rechercher

[blk_blacklists_special]	access	---
[blk_blacklists_sports]	access	---
[blk_blacklists_stalkerware]	access	---
[blk_blacklists_strict_redirector]	access	---
[blk_blacklists_strong_redirector]	access	---
[blk_blacklists_translation]	access	---
[blk_blacklists_tricheur]	access	---
[blk_blacklists_update]	access	---
[blk_blacklists_vpn]	access	---
[blk_blacklists_warez]	access	---
[blk_blacklists_webmail]	access	---
Default access [all]	access	allow

**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[product\_name] proxy"

**Redirect mode** int error page (enter error message)   
 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** ☐ Enable the protected mode of search engines to limit access to mature content.

Attention, le « all » est en deny par défaut, ce qui filtre tous les sites



172.16.1.153/pkg\_edit.php?xml=squidguard\_default

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 Sg[product\_name] proxy"

Redirect mode

int error page (enter error message)

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

safesearch

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

Log

☐ Check this option to enable logging for this ACL.

Save

pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license.

Activer le « safesearch » pour rendre votre moteur de recherche « safe »

System Interfaces Firewall Services VPN Status Diagnostics Help

Package / Proxy filter SquidGuard: General settings / General settings

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log XMLRPC Sync

General Options

Enable ☒ Check this option to enable squidGuard.  
Important: Please set up at least one category on the 'Target Categories' tab before enabling. See [this link](#) for details.  
The Save button at the bottom of this page must be clicked to save configuration changes.  
To activate squidGuard configuration changes, **the Apply button must be clicked.**

Apply

SquidGuard service state: **STARTED**

LDAP Options

Enable LDAP Filter ☐ Enable options for setup ldap connection to create filters with ldap search

LDAP DN

Configure your LDAP DN (ex: cn=Administrator,cn=Users,dc=domain)

LDAP DN Password

Password must be initialize with letters (Ex: Change123), valid format: [a-zA-ZV][a-zA-Z0-9/\_\.\:\%{+}?=&]

LDAP Cache Time

0

Number of seconds to cache LDAP Results (recommended value: 300)

Ne pas oublier de cliquer sur « Save » pour valider la configuration

# Configuration de LightSquid

LightSquid va vous permettre de faire du reporting sur les accès Squid.

pfSense  
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ **Status ▾** Diagnostics ▾ Help ▾

Package / Proxy Server: General Settings / General

General Remote Cache Local Cache Antivirus ACLs Traffic Mgmt

### Squid General Settings

**Enable Squid Proxy** ☒ Check to enable the Squid proxy.  
**Important:** If unchecked, ALL Squid services will be disabled.

**Keep Settings/Data** ☒ If enabled, the settings, logs, cache, AV defs and other data will be kept across package reinstalls.  
**Important:** If disabled, all settings and data will be wiped on install/upgrade.

**Listen IP Version**   
Select the IP version Squid will use to select addresses.

**CARP Status VIP**   
Used to determine the HA MASTER/BACKUP status. Squid will only start in MASTER status.  
**Important:** Don't forget to generate Local Cache on the backup node for synchronization.

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

**Outgoing Network**

Captive Portal  
CARP (failover)  
Dashboard  
DHCP Leases  
DHCPv6 Leases  
DNS Resolver  
Filter Reload  
Gateways  
Interfaces  
IPsec  
Monitoring  
NTP  
OpenVPN  
Queues  
Services  
Squid Proxy Reports  
System Logs  
Traffic Graph

Sélectionner « Squid Proxy Reports »

### 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](#)

### Report Template Settings

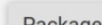
**Language**   
Select report language.

**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) ⓘ



System ▾
Interfaces ▾
Firewall ▾
Services ▾
VPN ▾
Status ▾
Diagnostics ▾
Help ▾

COMMUNITY EDITION

Package / Squid / Realtime Stats (SQStat)

Squid RealTime stat 1.20 for the proxy server [squid/4.15 \(127.0.0.1:3128\)](#).

Auto refresh:  sec.   Created at: 10:35:31 16/10/2021

URI	Curr. Speed	Avg. Speed	Size	Time
Total: 1 users and 31 connections @ 88.09/58.29 KB/s (CURR/AVG)				
192.168.1.64				
firebaseuserstoptics-pa.googleapis.com:443			0.99 KB/s	5 kb 6s
clients4.google.com:443	54.86 KB/s	28.64 KB/s	171 kb	6s
www.lesoir.be:443	0.04 KB/s	1.05 KB/s	7 kb	7s
www.googleapis.com:443		0.40 KB/s	2 kb	7s
widgets.outbrain.com:443		0.85 KB/s	5 kb	7s
ad.doubleclick.net:443	3.27 KB/s	2.44 KB/s	17 kb	7s
aswpsdkeu.com:443		0.14 KB/s	1 kb	7s
content-autofill.googleapis.com:443		0.74 KB/s	5 kb	8s
update.googleapis.com:443	0.04 KB/s	0.82 KB/s	7 kb	9s
stats.g.doubleclick.net:443		0.16 KB/s	1 kb	9s
www.lesoir.be:443		0.26 KB/s	2 kb	9s
clients2.google.com:443	0.37 KB/s	0.93 KB/s	8 kb	9s
rossel.emsecure.net:443		0.56 KB/s	5 kb	9s
offer.slgnt.eu:443		0.45 KB/s	4 kb	9s
mv.outbrain.com:443	7.29 KB/s	3.24 KB/s	29 kb	9s
dis.criteo.com:443		0.42 KB/s	3 kb	9s
www.google-analytics.com:443		0.15 KB/s	1 kb	9s
cs.emxdgt.com:443		0.29 KB/s	2 kb	9s
sync.hgrtb.com:443		0.67 KB/s	5 kb	9s
pixel-us-east.rubiconproject.com:443		0.36 KB/s	3 kb	9s
www.google.be:443		0.63 KB/s	5 kb	9s
www.facebook.com:443	14.30 KB/s	5.57 KB/s	50 kb	9s

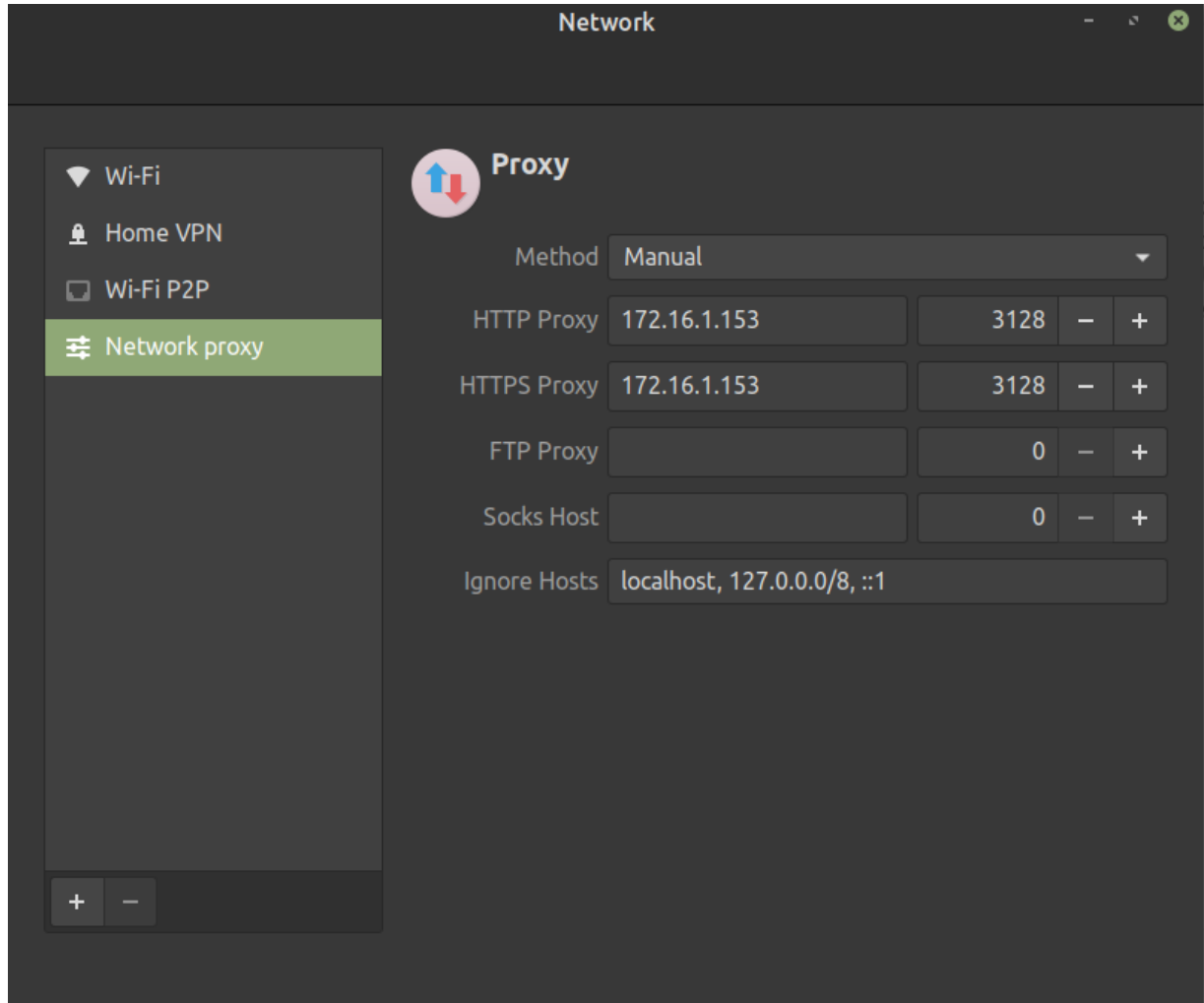


# Configuration manuelle du proxy

Les écrans ci-dessous sont propres à Linux

Vous avez 2 possibilités:

- La configuration manuelle du proxy



- par l'ajout de l'URL du serveur WEB hébergeant votre fichier de configuration

---

# Configuration automatique du proxy

## Fichier PAC et WPAD

### Introduction

Pour déployer automatiquement l'adresse de votre proxy, nous allons créer un fichier proxy.pac.

Extrait de Wikipédia

[https://fr.wikipedia.org/wiki/Fichier\\_.PAC](https://fr.wikipedia.org/wiki/Fichier_.PAC)

Le [navigateur](#) va chercher ce fichier PAC en priorité. Les URL qu'il contient peuvent être configurées manuellement, ou déterminées automatiquement par le WPAD ([Web Proxy Autodiscovery Protocol \(en\)<sup>1</sup>](#)).

Un fichier PAC contient une [fonction](#) en [JavaScript](#) appelée « FindProxyForURL(url, host) ». Cette [fonction](#) retourne une [chaîne de caractères](#) avec une ou plusieurs spécifications (règles) sur la façon d'y accéder. Ces règles amènent le [navigateur web](#) à utiliser un serveur [proxy](#) particulier ou à se connecter directement.

### Prérequis

Un fichier proxy.pac doit être déployé à travers un serveur web.

Perso, j'utilise un serveur Apache.

Voici un lien pour vous aider à installer un serveur Apache sous Ubuntu :

<https://www.digitalocean.com/community/tutorials/how-to-install-the-apache-web-server-on-ubuntu-20-04-quickstart-fr>

Pour l'extension .pac soit prise en charge par votre serveur Web Apache, il faut ajouter un fichier .htaccess contenant :

```
AddType application/x-ns-proxy-autoconfig .pac
```

Dans le répertoire contenant votre fichier proxy.pac

Créez, également, un symbolic link wpad.dat vers votre fichier proxy.pac. Exemple:

```
ln -s /var/www/html/proxy.pac /var/www/html/wpad.dat
```

## Exemple de fichier proxy.pac

```
function FindProxyForURL(url, host)
{
  //Les adresses privées n'utilisent pas le proxy
  if (isInNet(host, "192.168.0.0", "255.255.0.0")) {
    return "DIRECT";
  }
  if (isInNet(host, "10.0.0.0", "255.0.0.0")) {
    return "DIRECT";
  }
  // les urls suffixées domain.local n'utilisent pas le proxy
  if (shExpMatch(url, "/*.domain.local/*"))
    return "DIRECT";
  } else {
    // définition du proxy pour l'http et l'https
    if (shExpMatch(url, "http:*"))
      return "PROXY 172.16.1.153:3128" ;
    if (shExpMatch(url, "https:*"))
      return "PROXY 172.16.1.153:3128" ;
    return "DIRECT";
  }
}
```

## Propagation via DNS

**Remarque:** La propagation de la configuration wpad/pac via DNS/DHCP n'est valable que pour des machines

Windows.

Pour propager votre configuration proxy via un serveur DNS.

Vous devez créer une entrée wpad soit un A pointant vers l'IP du serveur web hébergeant le fichier wpad/pac ou un CNAME pointant vers le FQDN du serveur web hébergeant le fichier wpad/pac.

```
wpad.mle. IN A 172.16.1.1
```

ou

```
wpad.mle. IN CNAME pacserver.mle.
```

## Propagation par DHCP

La propagation par DHCP de la configuration WPAD est principalement supporté par Windows.

Vous devez configurer l'option 252 qui pointera vers l'URL de votre fichier wpad.dat. Exemple :  
<http://pacserver.mle/wpad.dat>

# Références

<http://findproxyforurl.com>

[https://fr.wikipedia.org/wiki/Fichier\\_.PAC](https://fr.wikipedia.org/wiki/Fichier_.PAC)

<https://www.pfsense.org/>