

# GUIDE UTILISATEUR PFSENSE



protection analyse collecte reporting  
« **Command & Control** »  
confiance gestion sécurité

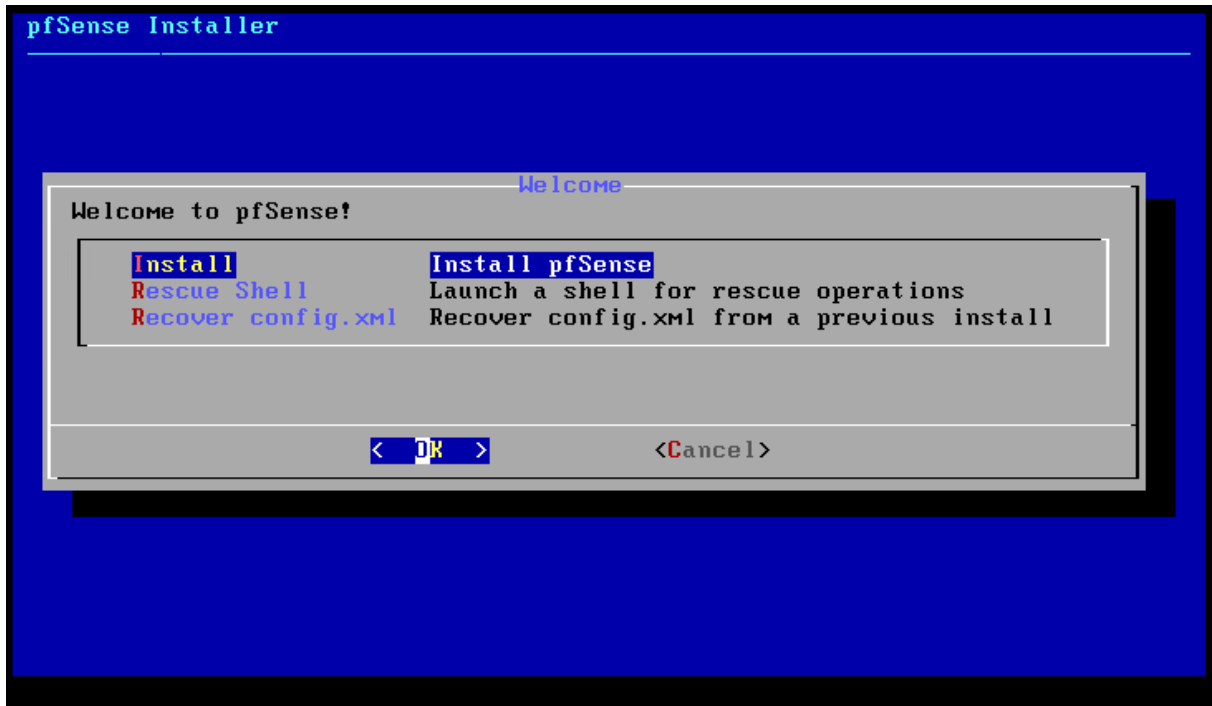


Votre centre de contrôle  
contre tous types d'attaques

## Tuto installation et configuration de pfsense

### I : Installation de pfsense

Sélectionner install



Une fois l'installation finit, il faudrat configuré le wan qui sera une ip qui aura accès à internet.

Et le lan qui sera pour vos autre machines.

```
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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

Enter an option: 1

Valid interfaces are:

em0      00:0c:29:df:cf:6f  (up) Intel(R) PRO/1000 Legacy Network Connection 1.
em1      00:0c:29:df:cf:79  (up) Intel(R) PRO/1000 Legacy Network Connection 1.

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n
```

Si vous souhaitez que votre pfsence distribue le dhcp activer le dhcp pour le lan.

## II : Configuration de pfsense

Pour se connecter à l'interface graphique, il faut utiliser l'ip wan ou lan.

Après la connection vous pourrez configurer le domain ainsi que les dns de votre routeur.  
EN cliquant sur next pour pourrez ensuite vérifié la configuration et changer le mot de passe du compte admin.

### General Information

On this screen the general pfSense parameters will be set.

<b>Hostname</b>	<input type="text" value="pfSense"/> EXAMPLE: myserver
<b>Domain</b>	<input type="text" value="localdomain"/> EXAMPLE: mydomain.com
<p>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 &gt; DNS Resolver and enable DNS Query Forwarding after completing the wizard.</p>	
<b>Primary DNS Server</b>	<input type="text" value="192.168.100.254"/>
<b>Secondary DNS Server</b>	<input type="text" value="8.8.8.8"/>
<b>Override DNS</b>	<input checked="" type="checkbox"/> Allow DNS servers to be overridden by DHCP/PPP on WAN

[> Next](#)

## III : Configuration du proxy

Pour le proxy nous utilisons squid qui est l'un des plus utilisé. Il permet de filtrer les requêtes.

Pour le filtrage des sites en https nous allons créer un certificat.

Installations des paquets :

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

System / Package Manager / Installed Packages

Installed Packages Available Packages

Name	Category	Version	Description	Actions
✓ Lightsquid	www	3.0.6_4	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package.  Package Dependencies: lighttpd-1.4.49 lightsquid-1.8_5	
✓ squid	www	0.4.44_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.  Package Dependencies: squidclamav-6.16 squid_radius_auth-1.10 squid-3.5.27_3 c-icap-modules-0.5.2	
✓ squidGuard	www	1.16.17_3	High performance web proxy URL filter.  Package Dependencies: squidguard-1.4.15	

= Update  = Current  
 = Remove = Information = Reinstall  
 Newer version available

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

System / Certificate Manager / CAs / Edit

CAs Certificates Certificate Revocation

Create / Edit CA

**Descriptive name**

**Method**

**Internal Certificate Authority**

**Key length (bits)**

**Digest Algorithm**   
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

**Lifetime (days)**

**Common Name**

The following certificate authority subject components are optional and may be left blank.

Ensuite, nous allons configurer squid

Rendez-vous dans service squid server et ensuite modifier le hard disk cache size sur 500 pour qu'il plus avoir plus de cache.

Squid Hard Disk Cache Settings	
<b>Hard Disk Cache Size</b>	<input type="text" value="500"/> Amount of disk space (in megabytes) to use for cached objects.
<b>Hard Disk Cache System</b>	<input type="text" value="ufs"/> This specifies the kind of storage system to use. <a href="#">i</a>
<b>Clear Disk Cache NOW</b>	Hard Disk Cache is automatically managed by swapstate_check.php script which is scheduled to run daily via cron. <a href="#">i</a> If you wish to clear cache <b>immediately</b> , click this button <b>once</b> : <input type="button" value="Clear Disk Cache NOW"/>
<b>Level 1 Directories</b>	<input type="text" value="16"/> Specifies the number of Level 1 directories for the hard disk cache. <a href="#">i</a>
<b>Hard Disk Cache Location</b>	<input type="text" value="/var/squid/cache"/> This is the directory where the cache will be stored. Default: /var/squid/cache <a href="#">i</a>
<b>Minimum Object Size</b>	<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)
<b>Maximum Object Size</b>	<input type="text" value="4"/> Objects larger than the size specified (in megabytes) will not be saved on disk. Default: 4 (MB) <a href="#">i</a>

## Activer « enable squid proxy »


Squid General Settings	
<b>Enable Squid Proxy</b>	<input checked="" type="checkbox"/> Check to enable the Squid proxy. <b>Important:</b> If unchecked, ALL Squid services will be disabled and stopped.
<b>Keep Settings/Data</b>	<input checked="" type="checkbox"/> If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls. <b>Important:</b> If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.
<b>Proxy Interface(s)</b>	<input type="text" value="LAN"/> WAN loopback The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.
<b>Proxy Port</b>	<input type="text" value="3128"/> This is the port the proxy server will listen on. Default: 3128
<b>ICP Port</b>	<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.

## Activer « resolve dns ipv4 first

«

<b>Allow Users on Interface</b>	<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.
<b>Patch Captive Portal</b>	<b>This feature was removed</b> - see Bug #5594 for details!
<b>Resolve DNS IPv4 First</b>	<input checked="" type="checkbox"/> Enable this to force DNS IPv4 lookup first. This option is very useful if you have problems accessing HTTPS sites.
<b>Disable ICMP</b>	<input type="checkbox"/> Check this to disable Squid ICMP pinger helper.
<b>Use Alternate DNS Servers for the Proxy Server</b>	<input type="text"/> To use DNS servers other than those configured in System > General Setup, enter the IP(s) here. Separate entries by semi-colons (;)

## Activer « Transparent http proxy »

Transparent Proxy Settings	
<b>Transparent HTTP Proxy</b>	<input checked="" type="checkbox"/> Enable transparent mode to forward all requests for destination port 80 to the proxy server.  Transparent proxy mode works without any additional configuration being necessary on clients. <b>Important:</b> Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below. <b>Hint:</b> In order to proxy both HTTP and HTTPS protocols <b>without intercepting SSL connections</b> , configure WPAD/PAC options on your DNS/DHCP servers.
<b>Transparent Proxy Interface(s)</b>	<div style="border: 1px solid #ccc; padding: 2px;"><div style="background-color: #007bff; color: white; padding: 2px;">LAN</div><div style="padding: 2px;">WAN</div></div> <p>The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.</p>
<b>Bypass Proxy for Private Address Destination</b>	<input type="checkbox"/> Do not forward traffic to Private Address Space (RFC 1918) destinations. Destinations in Private Address Space (RFC 1918) are passed directly through the firewall, not through the proxy server.
<b>Bypass Proxy for These Source IPs</b>	<input type="text"/> Do not forward traffic from these <b>source</b> IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall. <b>Applies only to transparent mode.</b> Separate entries by semi-colons (;)
<b>Bypass Proxy for These Destination IPs</b>	<input type="text"/> Do not proxy traffic going to these <b>destination</b> IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall. <b>Applies only to transparent mode.</b> Separate entries by semi-colons (;)

## Activer « https/ssl interception » et sélectionner votre certificat dand AC

## 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 '  
 Default: Splice Whitelist, Bump Otherwise. [Click Info for details.](#) **i**

**SSL Intercept Interface(s)**  ▲  
 WAN ▼  
 The interface(s) the proxy server will intercept SSL requests on. Use CTR

**SSL Proxy Port**   
 This is the port the proxy server will listen on to intercept SSL while using

**SSL Proxy Compatibility Mode**  ▼  
 The compatibility mode determines which cipher suites and TLS version details. **i**

**DHParams Key Size**  ▼  
 DH parameters are used for temporary/ephemeral DH key exchanges an ciphers.

**AC**  ▼

Il faut ensuite ce rendre sur proxy filter squidguard et l'activer

**pfSense** 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.**

SquidGuard service state: **STOPPED**

Activer les logs et les logs rotations pour avoir accès aux historiques.

Logging options	
<b>Enable GUI log</b>	<input type="checkbox"/> Check this option to log the access to the Proxy Filter GUI.
<b>Enable log</b>	<input checked="" type="checkbox"/> 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.
<b>Enable log rotation</b>	<input checked="" type="checkbox"/> 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	
<b>Clean Advertising</b>	<input type="checkbox"/> Check this option to display a blank gif image instead of the default block page. With this option the user gets a cleaner webpage.

Cocher la blacklist et insérer l'url pour avoir une liste pré fait de site bloquer.

Blacklist options	
<b>Blacklist</b>	<input checked="" type="checkbox"/> Check this option to enable blacklist Do NOT enable this on NanoBSD installs!
<b>Blacklist proxy</b>	<input type="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'
<b>Blacklist URL</b>	<input type="text" value="http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar"/> 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).
	

### III : Configuration de snort

Installer le packet snort comme vu ci-dessus .

Ensuite on active les règles et récupérer son snort oinkmaster sur la page web :

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

- Account
- Oinkcode**
- Subscription
- Receipts
- False Positive

Oinkcode

bd7f731a28869bf50e04e9e8d715a635da39f002

Regenerate

Documentation

[How to use your oinkcode](#)

## Services / Snort / Global Settings



- Snort Interfaces
- Global Settings**
- Mises à jour
- Alerts
- Blocked
- Pass Lists
- Suppress
- IP Lists
- SID Mgmt
- Log Mgmt
- Sync

### Snort Subscriber Rules

**Enable Snort VRT**  Click to enable download of Snort free Registered User or paid Subscriber rules

[Sign Up for a free Registered User Rules Account](#)  
[Sign Up for paid Snort Subscriber Rule Set \(by Talos\)](#)

**Snort Oinkmaster Code**

Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)

## Ensuite on update snort

- Snort Interfaces
- Global Settings
- Mises à jour**
- Alerts
- Blocked
- Pass Lists
- Suppress
- IP Lists
- SID Mgmt
- Log Mgmt
- Sync

### Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	e127347699636deae64bb71383d6ccc1	Monday, 08-Jul-19 13:35:25 UTC
Snort GPLv2 Community Rules	Not Enabled	Not Enabled
Emerging Threats Open Rules	Not Enabled	Not Enabled
Snort OpenAppID Detectors	Not Enabled	Not Enabled
Snort OpenAppID RULES Detectors	Not Enabled	Not Enabled

### Update Your Rule Set

**Last Update** Jul-08 2019 13:35 **Result:** Success

**Update Rules**

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

Par la suite on va créer une interface, lan ou wan selon nos besoins et ajouté des règles pour bloquer certaines choses pouvant causer des dégâts sur un poste.

Services / Snort / Edit Interface / WAN ?

[Snort Interfaces](#) [Global Settings](#) [Mises à jour](#) [Alerts](#) [Blocked](#) [Pass Lists](#) [Suppress](#) [IP Lists](#) [SID Mgmt](#) [Log Mgmt](#) [Sync](#)

[WAN Paramètres](#) [WAN Categories](#) [WAN Règles](#) [WAN Variables](#) [WAN Preprocs](#) [WAN Barnyard2](#) [WAN IP Rep](#) [WAN Journaux](#)

### Paramètres généraux

**Activer**  Activer interface

**Interface**  ▼  
Choose the interface where this Snort instance will inspect traffic.

**Description**   
Enter a meaningful description here for your reference.

**Snap Length**  max  
Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

<input type="checkbox"/>	<a href="#">snort_deleted.rules</a>	<input type="checkbox"/>	<a href="#">snort_netbios.so.rules</a>
<input type="checkbox"/>	<a href="#">snort_dns.rules</a>	<input type="checkbox"/>	<a href="#">snort_os-linux.so.rules</a>
<input type="checkbox"/>	<a href="#">snort_dos.rules</a>	<input type="checkbox"/>	<a href="#">snort_os-other.so.rules</a>
<input type="checkbox"/>	<a href="#">snort_experimental.rules</a>	<input type="checkbox"/>	<a href="#">snort_os-windows.so.rules</a>
<input checked="" type="checkbox"/>	<a href="#">snort_exploit-kit.rules</a>	<input type="checkbox"/>	<a href="#">snort_policy-other.so.rules</a>
<input type="checkbox"/>	<a href="#">snort_exploit.rules</a>	<input type="checkbox"/>	<a href="#">snort_policy-social.so.rules</a>
<input type="checkbox"/>	<a href="#">snort_file-executable.rules</a>	<input type="checkbox"/>	<a href="#">snort_protocol-dns.so.rules</a>
<input type="checkbox"/>	<a href="#">snort_file-flash.rules</a>	<input type="checkbox"/>	<a href="#">snort_protocol-nntp.so.rules</a>
<input type="checkbox"/>	<a href="#">snort_file-identify.rules</a>	<input type="checkbox"/>	<a href="#">snort_protocol-other.so.rules</a>
<input type="checkbox"/>	<a href="#">snort_file-image.rules</a>	<input type="checkbox"/>	<a href="#">snort_protocol-scada.so.rules</a>
<input type="checkbox"/>	<a href="#">snort_file-java.rules</a>	<input type="checkbox"/>	<a href="#">snort_protocol-snmp.so.rules</a>
<input type="checkbox"/>	<a href="#">snort_file-multimedia.rules</a>	<input type="checkbox"/>	<a href="#">snort_protocol-tftp.so.rules</a>
<input type="checkbox"/>	<a href="#">snort_file-office.rules</a>	<input type="checkbox"/>	<a href="#">snort_protocol-voip.so.rules</a>
<input type="checkbox"/>	<a href="#">snort_file-other.rules</a>	<input type="checkbox"/>	<a href="#">snort_pua-p2p.so.rules</a>
<input type="checkbox"/>	<a href="#">snort_file-pdf.rules</a>	<input type="checkbox"/>	<a href="#">snort_server-apache.so.rules</a>
<input type="checkbox"/>	<a href="#">snort_finger.rules</a>	<input type="checkbox"/>	<a href="#">snort_server-iis.so.rules</a>
<input type="checkbox"/>	<a href="#">snort_ftp.rules</a>	<input type="checkbox"/>	<a href="#">snort_server-mail.so.rules</a>
<input type="checkbox"/>	<a href="#">snort_icmp-info.rules</a>	<input type="checkbox"/>	<a href="#">snort_server-mysql.so.rules</a>

Vous pourrez ensuite visualiser les alerts du aux règles que vous avez appliquéés.