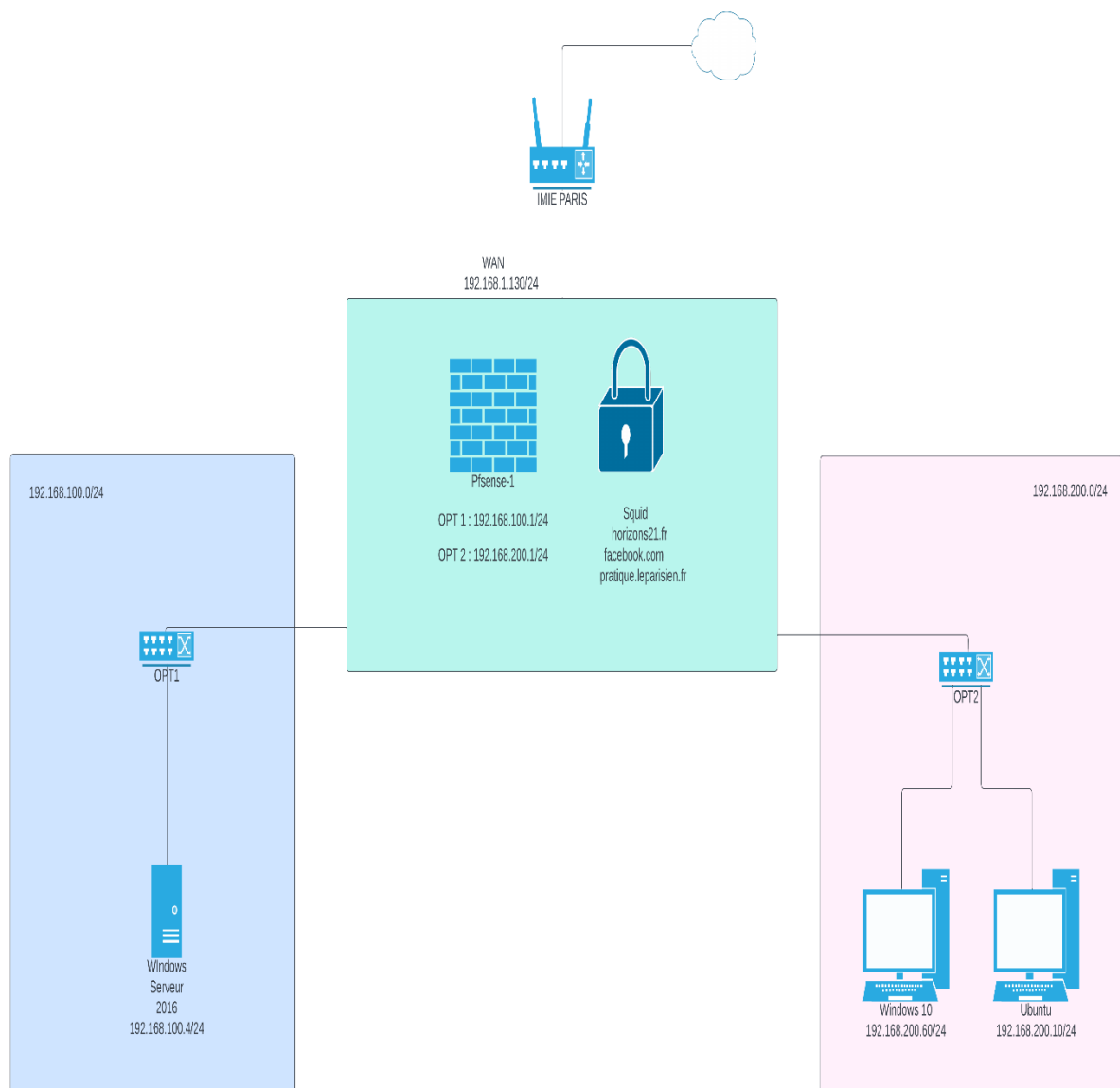


PROJET PERSONNEL ENCADRE n°1



MISE EN PLACE DE SQUID, SQUIDGUARD, LIGHTSQUID SUR PFSENSE

Schéma de l'infrastructure réseau



PPE n°1 : Mise en place de Squid sur Pfsense

Introduction :

Squid est un serveur proxy open-source populaire qui est couramment utilisé pour le cache et la filtration web.

Fonctionnement de SQUID

Lorsque Squid est installé sur pfSense, il peut être utilisé pour améliorer les performances de navigation web en mettant en cache le contenu web fréquemment consulté. Cela peut réduire la quantité de bande passante utilisée par les clients sur le réseau et accélérer les temps de chargement des pages. De plus, Squid peut être configuré pour bloquer l'accès à certains sites web ou catégories de contenu, offrant ainsi une couche supplémentaire de filtrage et de sécurité web.

Installation de SQUID

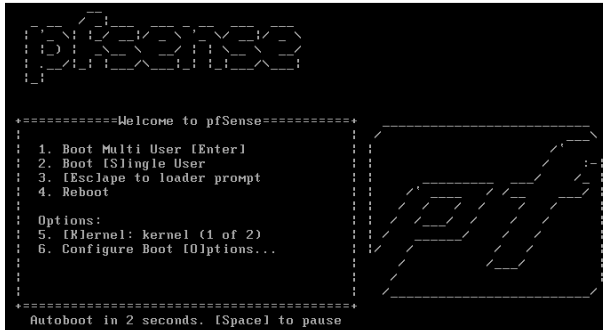
L'installation de Squid sur pfSense implique la configuration du paquet Squid dans l'interface de gestion basée sur le web de pfSense. Une fois installé, Squid peut être configuré pour répondre aux besoins spécifiques du réseau, notamment en définissant le contenu à mettre en cache et pendant combien de temps le conserver, en configurant les contrôles d'accès et les restrictions, ainsi qu'en configurant les journaux et la surveillance.

Avantages de SQUID

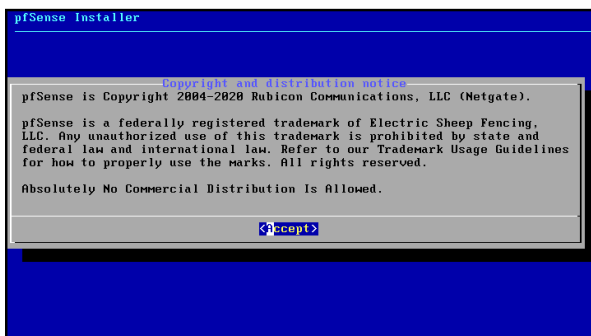
Dans l'ensemble, l'utilisation de Squid avec pfSense peut fournir des avantages significatifs pour les réseaux en termes de performances, de sécurité et de contrôle sur le contenu web.

Taches à effectuer :

1) Commençons tout de suite par **installer pfSense**. Après avoir insérer l'ISO de pfsense dans VM dédiée, vous pouvez démarrer la machine. Le setup va démarrer automatiquement après quelques secondes.



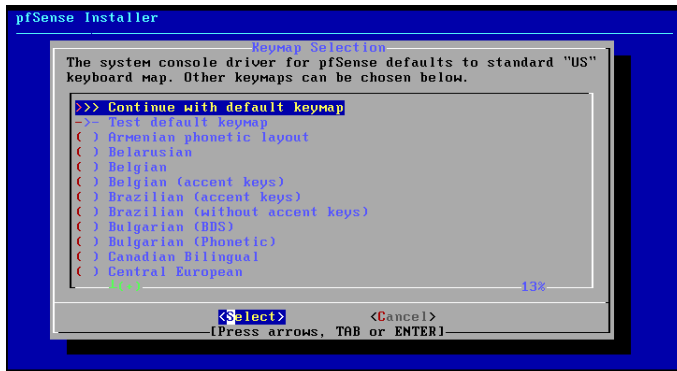
2) **L'installation va s'effectuer au clavier.** Appuyez sur la touche Entrée pour Accepter.



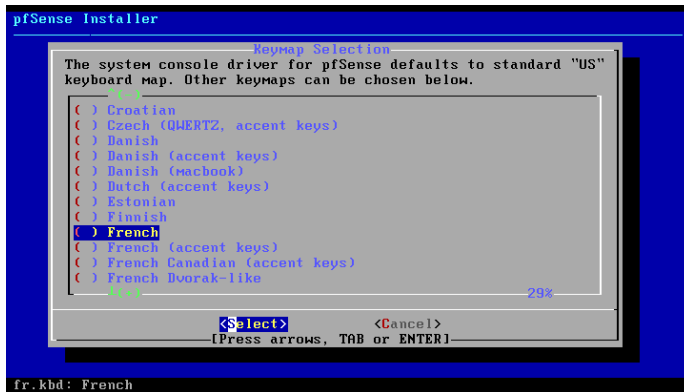
3) Vérifiez que vous êtes bien sur « **Install** » (*doit être sélectionné en bleu foncé comme dans l'image ci-dessous, sinon déplacez-vous avec les flèches de votre clavier*) et appuyez sur Entrée pour faire OK.



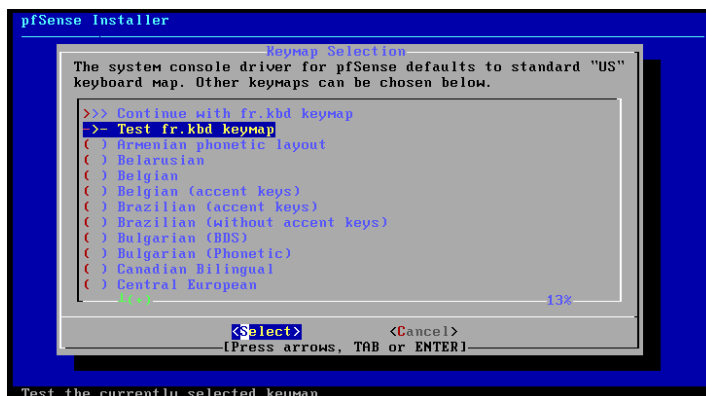
4) Il faut sélectionner le clavier



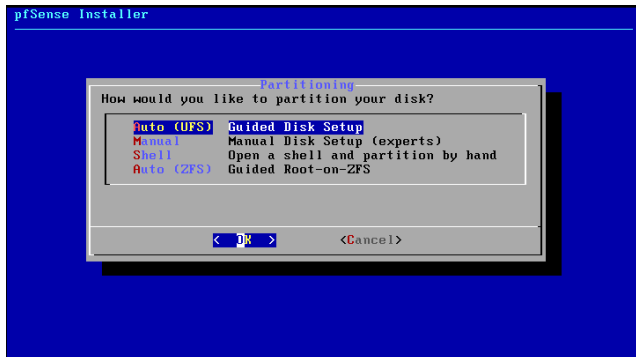
5) Descendez avec les flèches jusqu'à « French » et appuyez sur Entrée.



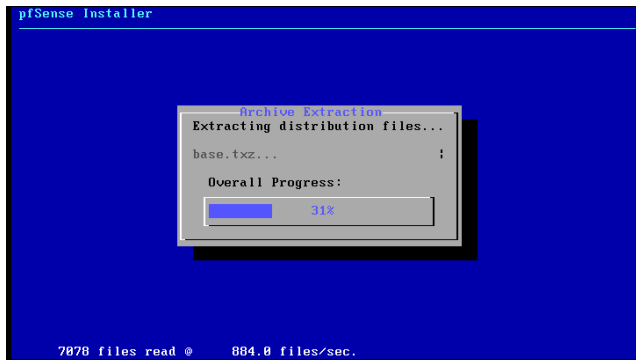
6) Vous verrez dans les 2 premières lignes que le clavier « fr.kdb » a été sélectionné. Vous pouvez le tester si besoin. Pour poursuivre, remontée sur la ligne « Continue with... » et appuyez sur Entrée.



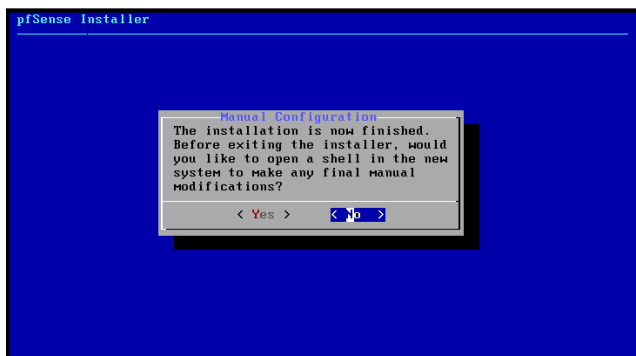
- 7) Le setup va vous demander de **partitionner le disque** de stockage de la machine. Sauf si vous avez besoin d'une configuration bien spécifique, **restez sur « Auto (UFS) »** et appuyez sur **Entrée**.



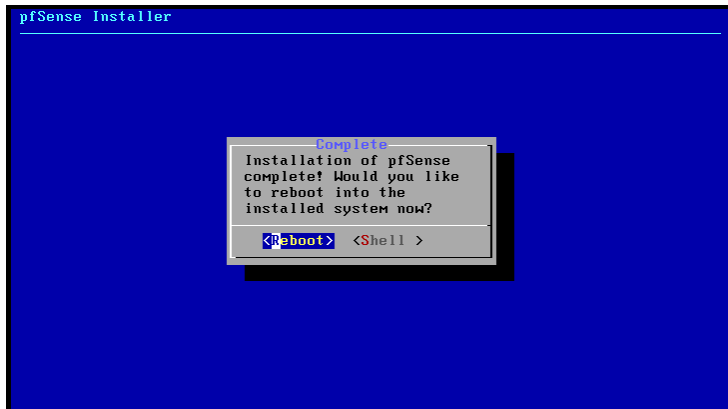
- 8) L'installation est désormais lancée. **Patiencez quelques secondes**, c'est très rapide.



- 9) Il vous sera ensuite proposer d'ouvrir un shell (*terminal*) si vous souhaitez apporter des modifications. Passez sur la case « **No** » et appuyez sur **Entrée**.



- 10) Et pour terminer cette installation du système, **appuyez une dernière fois sur Entrée pour rebooter et démarrer directement sur le nouveau pfsense fraîchement mis en place ;**



- 11) Au démarrage, **pfsense va se lancer, tester et configurer les services dont il a besoin.** Par exemples dans l'image ci-dessous, on peut voir que pfsense a tester la présence de l'interface WAN (*ligne Configuring WAN interface...done.*) et l'a configuré, idem pour l'interface LAN. Il a également lancé le service DNS pour la résolution de nom de domaine (*ligne Configuring DNS Resolver...*).

```
Updating configuration.....done.
Checking config backups consistency...done.
Setting up extended sysctls...done.
Setting timezone...done.
Configuring loopback interface...lo0: link state changed to UP
done.
Starting syslog...done.
Starting Secure Shell Services...done.
Setting up interfaces Microcode...done.
Configuring loopback interface...done.
Creating wireless clone interfaces...done.
Configuring LAGG interfaces...done.
Configuring VLAN interfaces...done.
Configuring QinQ interfaces...done.
Configuring IPsec UTI interfaces...done.
Configuring WAN interface...done.
Configuring LAN interface...done.
Configuring CARP settings...done.
Syncing OpenVPN settings...done.
Configuring firewall.....done.
Starting PFLOG...done.
Setting up gateway monitors...done.
Setting up static routes...done.
Setting up DNSs...
Starting DNS Resolver...█
```

- 12) Une fois que le démarrage est finalisé, vous aurez la vue suivante sur la machine :

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.4.5-RELEASE (Patch 1) amd64 Tue Jun 02 17:51:17 EDT 2020
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 20bc68d50f788aeb75b4

*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.200.131/24
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: █
```

- 13) On voit bien nos **deux interfaces réseaux** (WAN et LAN). On voit également que **l'interface WAN a bien récupéré une adresse IP automatiquement depuis un DHCP** (ce qui correspond à l'adresse IP publique). Nous devons aussi modifier l'adresse IP du WAN et la définir en statique. Concernant le LAN, il attribue une adresse statique par défaut que nous allons changer.

Vous avez **16 menus** qui vont permettre de faire différentes **actions et configurations**. Pour les utiliser, il faut **saisir leur numéro et appuyez sur Entrée**. Testons ensemble avec le menu **ping**. Saisissez au clavier le **chiffre 7** puis la touche **Entrée**.

```
Enter an option: 7
```

```
Enter a host name or IP address: █
```

Lançons un ping vers google.fr pour tester l'accès à internet et le bon fonctionnement de la résolution de nom.

Info ++ : Attention, malgré la configuration du clavier en français, celui-ci se retrouve par défaut en qwerty ! Pour saisir le point, il faut appuyez sur la touche « / ».

```
Enter a host name or IP address: google.fr
PING google.fr (172.217.18.195): 56 data bytes
64 bytes from 172.217.18.195: icmp_seq=0 ttl=128 time=45.646 ms
64 bytes from 172.217.18.195: icmp_seq=1 ttl=128 time=45.635 ms
^C
```

Vous pouvez **arrêter le ping** en appuyant **simultanément sur les touches Ctrl et C**. On voit que le ping passe sans problème, l'interface WAN est donc fonctionnelle.

Nous avons une dernière petite chose à faire avant de passer sur l'interface web de Pfsense pour la configuration finale. Il faut **assigner la bonne adresse IP à l'interface WAN**, c'est-à-dire celle qui correspond à notre réseau externe (pour moi dans le cadre de ce tuto, 192.168.1.130).

Pour cela, au choix des menus, **tapez 2 puis Entrée**.

```
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
```

```
Enter an option: 2█
```


On me demande **quelle interface je veux modifier**. L'interface WAN est ici vmx1, donc je tape 1 et j'appuie sur Entrée.

```
Available interfaces:
1 - WAN (vmx1 - static)
2 - LAN (vmx2 - static)
3 - OPT1 (vmx3 - static)
4 - OPT2 (vmx0 - static)

Enter the number of the interface you wish to configure: 1
```

Dans mon cas, je ne mets pas de DHCP sur le WAN alors j'appuie sur N :

```
Enter the number of the interface you wish to configure: 1
Configure IPv4 address WAN interface via DHCP? (y/n) n
```

Info + : le service DHCP peut être activé et configuré plus simplement par la suite via l'interface web.

Ensuite saisissez l'adresse IP que vous donnez à cette interface

```
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.1.130
```

Définissez le masque de sous-réseau du réseau local **en notation CIDR uniquement**, donc 24 pour moi.

```
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24
```

Pfsense demande ensuite si le réseau dispose d'une passerelle vers laquelle renvoyer les flux. Pour mon cas l'interface WAN doit avoir comme Gateway 192.168.1.1 (l'adresse du routeur de l'école)

```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

Répéter la même opération pour le LAN en lui mettant comme adresse ip 192.168.2.1/24

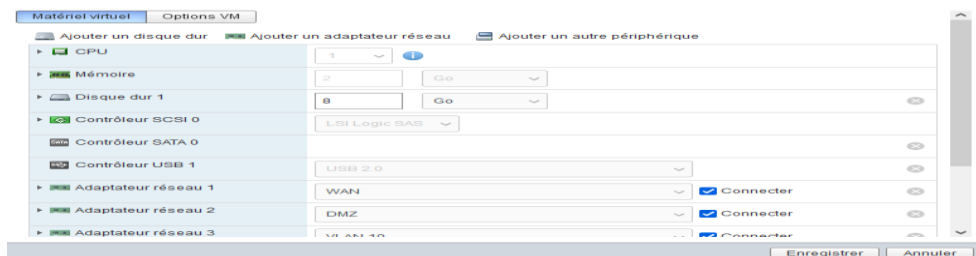
On n'active pas le dhcp sur le LAN

```
Do you want to enable the DHCP server on LAN? (y/n) n
```

Et enfin, la dernière question concerne le **protocole utilisé pour aller sur l'interface web**. Par défaut, il est en **HTTPS** donc sécurisé. Vous pouvez choisir de le passer en HTTP si vous le souhaitez en répondant « y » pour « Yes ». Personnellement je vais répondre « n ».

```
Disabling IPv4 DHCPD...Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n)
```

14) Ajouter des cartes réseaux qui se nommeront OPT1 et OPT2.



Faire la même configuration pour OPT1, en lui mettant comme adresse 192.168.100.1 et pareil pour OPT2 avec comme adresse 192.168.200.1 et OPT3 10.1.10.2/24 ce qui doit donner ça à la fin :

```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VMware Virtual Machine - Netgate Device ID: 596128dfe071b09d8ce5
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vmx1      -> v4: 192.168.1.130/24
LAN (lan)      -> vmx3      -> v4: 192.168.150.1/24
OPT1 (opt1)    -> vmx4      -> v4: 192.168.100.1/24
OPT2 (opt2)    -> vmx0      -> v4: 192.168.200.1/24
SYN0 (opt3)    -> vmx2      -> v4: 10.1.10.2/24

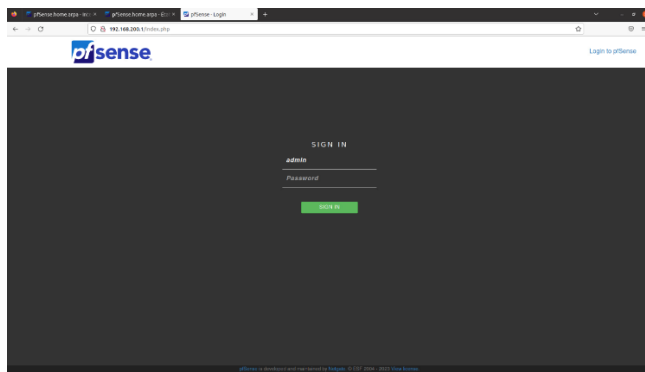
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system               14) Disable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

Enter an option:
```

La configuration de l'interface LAN est terminée. Je vois à l'écran l'**URL à utiliser pour aller sur pfsense qui est donc ici https://192.168.150.1/**, soit son adresse IP.

La configuration de pfsense en **lignes de commande** est maintenant terminée, passons sur l'interface web.

Depuis un PC sur le réseau local disposant d'une adresse IP fixe si le DHCP n'est pas actif, **ouvrez un navigateur internet et accédez à votre pfsense.**

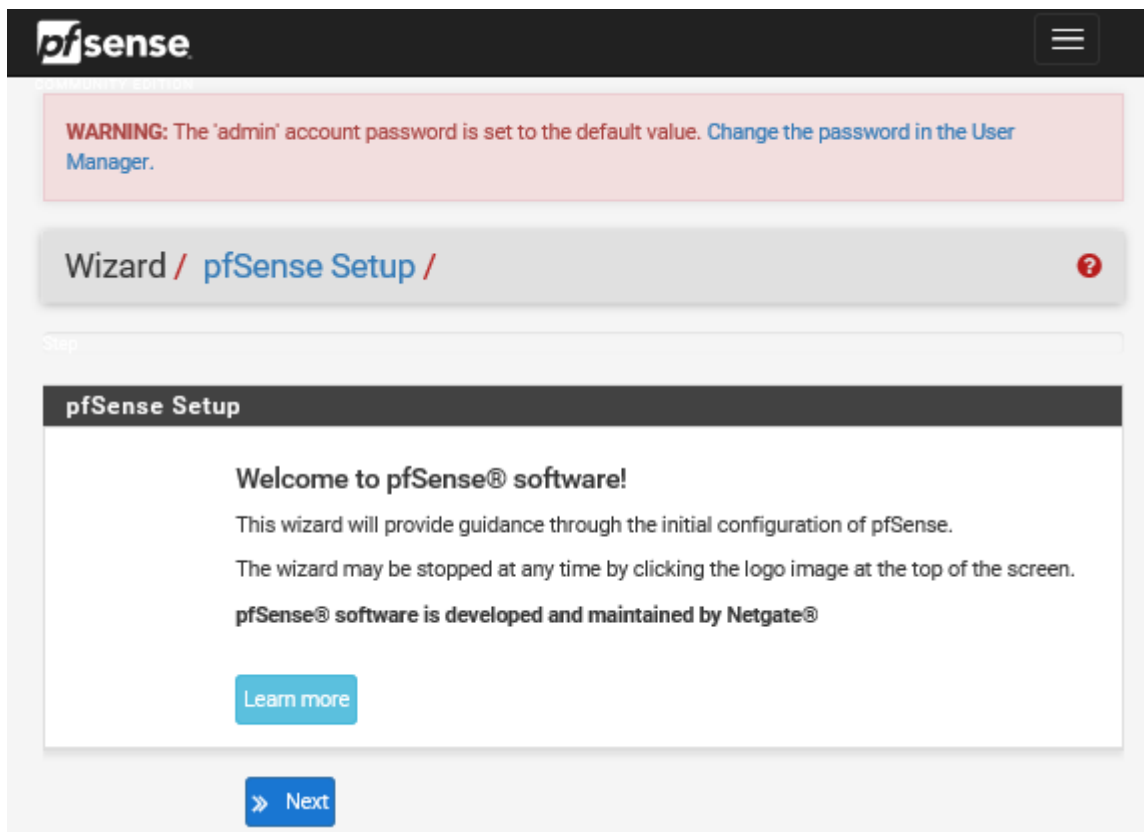


***Info ++** : Si vous avez laissé le protocole HTTPS, vous aurez une erreur de certificat qui est tout à fait normal. Le navigateur va vous prévenir qu'il y a un problème mais rien ne vous empêche de poursuivre votre navigation (méthode variable selon le navigateur) pour accéder à pfSense.*

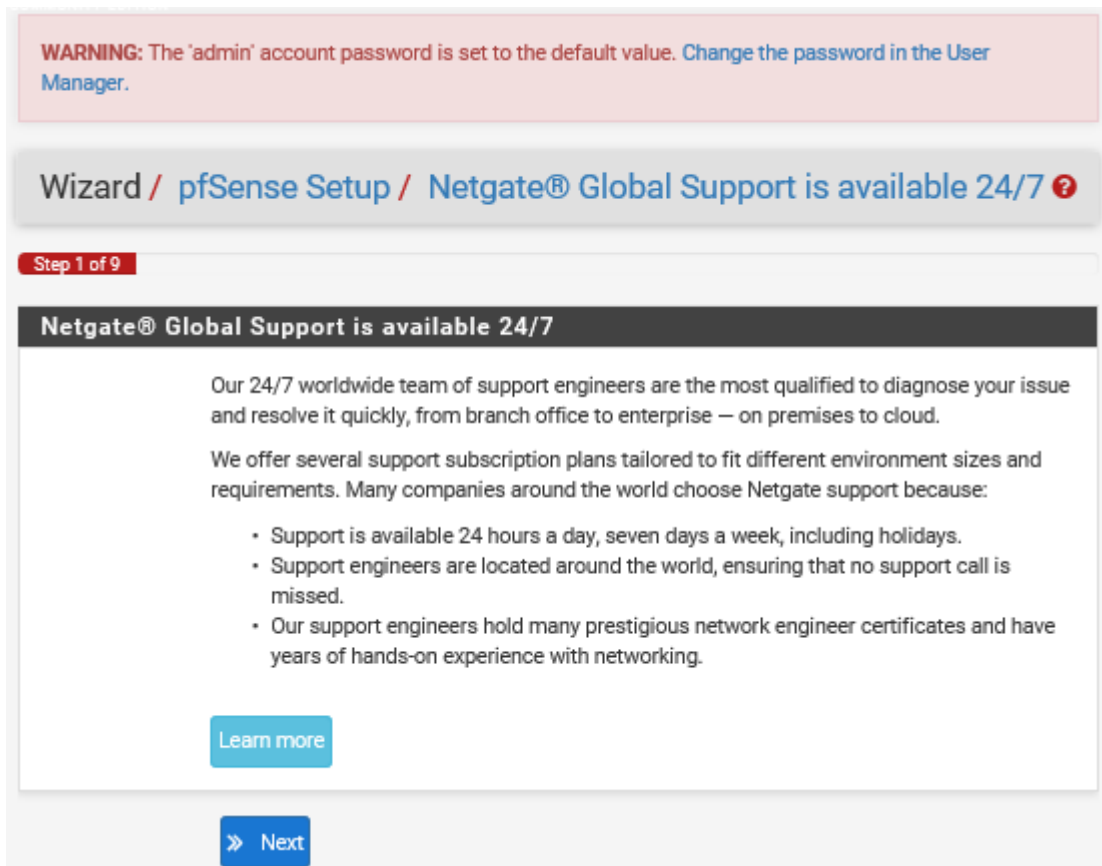
Les **identifiants par défaut de pfSense** sont les suivants :

- - **Login** : admin
 - **Mot de passe** : pfSense

Vous arrivez sur l'**assistant de configuration** de pfSense qui va nous permettre de finaliser l'installation de notre firewall. Cliquez sur le bouton « **Next** ».



L'assistant nous informe qu'il est possible d'avoir un **support technique sous condition de souscrire un contrat**. Cliquez de nouveau sur **Next**.



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

Au niveau de la partie des **informations générales**, vous pouvez modifier le **nom du firewall** et déclarer votre **nom de domaine si vous en avez un** dans votre réseau. Ici également vous pouvez **déclarer un serveur DNS local** (*ce n'est pas mon cas, j'utilise le DNS de mon AD pour ce tuto*). Je ne modifie ici aucun champ.

Wizard / pfSense Setup / General Information ?

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname
EXAMPLE: myserver

Domain
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

Secondary DNS Server

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

Choisissez « **Europe/Paris** » dans la **Timezone** et poursuivez.

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

Ensuite nous arrivons à la configuration de l'**interface WAN**. Elle est **configurée automatiquement par DHCP** donc **je ne vais le remettre en statique**.

Si vous avez besoin d'attribuer une IP fixe à cette interface, c'est dans cette partie que ça se définit.

Static IP Configuration	
IP Address	<input type="text"/>
Subnet Mask	<input type="text" value="32"/> ▼
Upstream Gateway	<input type="text"/>
DHCP client configuration	
DHCP Hostname	<input type="text"/> <p>The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).</p>

La partie « **PPPoE configuration** » sert en général à mettre les **identifiants fournis par votre FAI**. Ce sont ces identifiants qui sont définis dans votre box internet actuellement. Si vous souhaitez placer un firewall à la place de la box, il sera nécessaire de remplir cette partie.

PPPoE configuration	
PPPoE Username	<input type="text"/>
PPPoE Password	<input type="password"/>
Show PPPoE password	<input type="checkbox"/> Reveal password characters
PPPoE Service name	<input type="text"/> <p>Hint: this field can usually be left empty</p>
PPPoE Dial on demand	<input type="checkbox"/> Enable Dial-On-Demand mode <p>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.</p>
PPPoE Idle timeout	<input type="text"/> <p>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.</p>

La partie suivante « **PPTP configuration** » servira plutôt au **montage d'un VPN point à point** (*Protocole de tunnel point-à-point, à éviter car peu sécurisé, plutôt privilégier son petit frère IPSEC*).

PPTP configuration	
PPTP Username	<input type="text"/>
PPTP Password	<input type="password"/>
Show PPTP password	<input type="checkbox"/> Reveal password characters
PPTP Local IP Address	<input type="text"/>
pptplocalsubnet	<input type="text" value="32"/> <input type="button" value="v"/>
PPTP Remote IP Address	<input type="text"/>
PPTP Dial on demand	<input type="checkbox"/> 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	<input type="text"/> 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.

Les deux dernières options de cette page définissent que tout trafic entrant sur l'interface WAN et venant d'une classe d'adresse réseau privé est automatiquement bloqué. **Comme mon infra est ici virtuelle, je vais obligatoirement faire communiquer des réseaux privés, je n'utilise pas réellement une adresse publique.** Il est donc **nécessaire dans le cadre d'un labo de décocher ces 2 cases** sinon vous pourrez avoir des petits couacs.

RFC1918 Networks	
Block RFC1918 Private Networks	<input type="checkbox"/> 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	<input type="checkbox"/> 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.

Durant la phase de configuration, il est également **nécessaire de changer les identifiants par défaut du compte admin** de pfsense.

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password

Admin Password AGAIN

Next

La phase finale de l'installation de pfsense est terminée. Cliquez sur **Reload** pour recharger pfsense. A la fenêtre suivante, vous pourrez simplement cliquer sur le bouton **Finish**.

Wizard / pfSense Setup / Reload configuration

Step 7 of 9

Reload configuration

Click 'Reload' to reload pfSense with new changes.

Reload

Vous arrivez donc sur le **tableau de bord de votre pfsense**. Vous retrouvez ici des **infos sur l'utilisation des ressources de la machine** elle-même, ses **différentes adresses IP**, sa **version** et ses **mise à jour** si nécessaire etc...

pfSense Community Edition

État / Tableau de bord

Informations système

Non

Utilisateur: admin@192.168.200.1 (Local Database)

Système: VMware Virtual Machine
ID de l'agent Netgate: 7b489555ec0d74b03d

BIOS: Coreboot
Version: 6.00
Date de sortie: Thu Nov 12 2020

Version: 2.4.0-RELEASE (amd64)
Date au: Mon Jan 31 19:57:53 UTC 2022
FreeBSD 12.3-RELEASE

Le système est à jour.
Informations sur la version mises à jour à Mon Feb 20 19:16:11 CET 2022

Type de CPU: Intel(R) Xeon(R) CPU E5-4669 v3 @ 2.10GHz
AES-NI CPU Crypto: Yes (enabled)
QAT Crypto: No

Chiffrement matériel

Nouveau PTI: Active

MDS Mitigation: Inactive

Durée de fonctionnement: 01 Hour 12 Minutes 25 Seconds

Date/Heure actuelle: Mon Feb 20 20:26:27 CET 2022

Serveur(s) DNS: 127.0.0.1
192.168.100.4
192.168.100.1
8.8.8.8
192.168.200.1

Dernière modification de la configuration: Mon Feb 20 20:16:04 CET 2022

Taille de la table d'état: 0% (92/198000) Afficher ses états

Netgate Services And Support

Contract type: Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway/firewall appliances from Netgate, and elected Community Support as the point of sale or elected prior to on your own hardware, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always glad to have in-depth 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

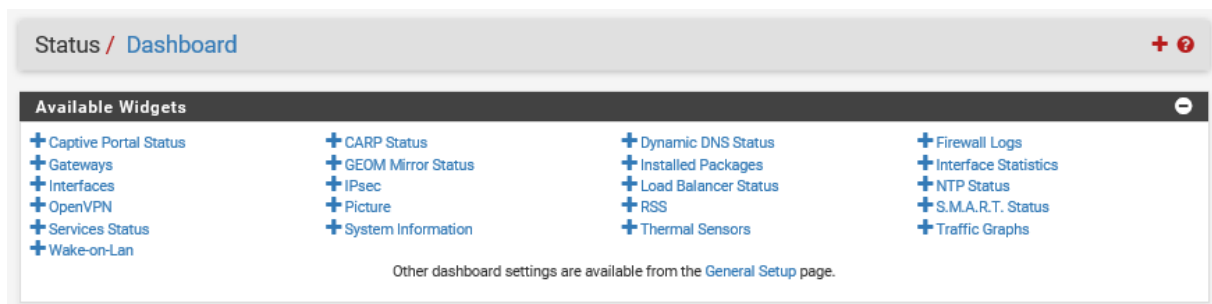
- Upgrade Your Support
- Netgate Global Support FAQ
- Netgate Professional Services
- Community Support Resources
- Official pfSense Training by Netgate
- Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, your MGR37 has your Netgate Device ID (NDID) from your firewall in order to validate support for this unit. Write down your NDID and store it in a safe place. You can purchase TAC support here.

Interfaces

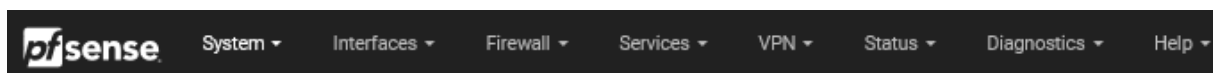
Interface	IP Address	Subnet	Netmask
WAN	192.168.1.130	192.168.1.0/24	255.255.255.0
LAN	192.168.2.1	192.168.2.0/24	255.255.255.0
DMZ	192.168.100.1	192.168.100.0/24	255.255.255.0
OPT1	192.168.200.1	192.168.200.0/24	255.255.255.0

Cette **vue est personnalisable** est cliquant sur le **petit + en haut à droite** dans la barre de titre.



Vous pouvez ajouter des graphiques, des infos sur les load balancer, le trafic, les logs, les VPN etc...

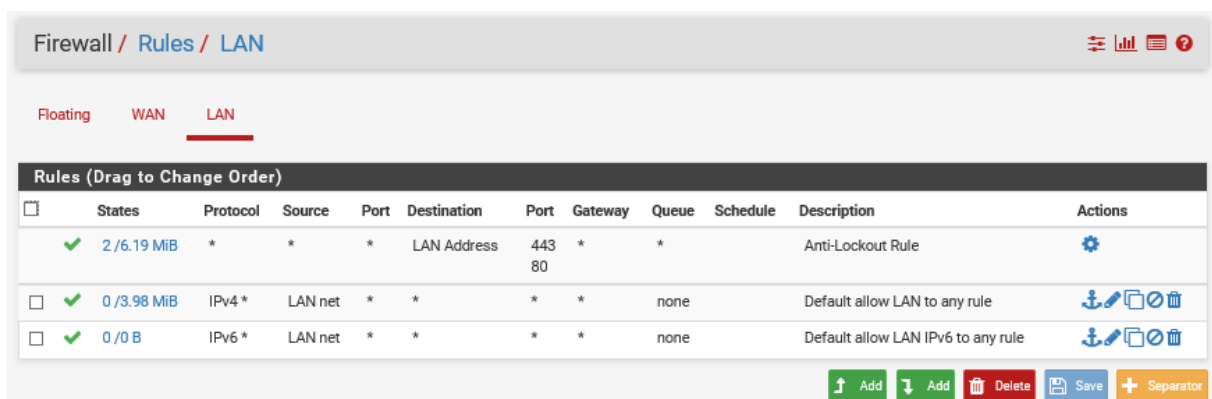
Les **différents menus** vont vous permettre de faire toutes sortes de choses sur votre firewall.



- - Mettre en place des VPN (*IPSEC, OpenVPN...*)
 - Activer des services (*DHCP, DNS, NLB, NTP, WOL...*)
 - Faire du NAT et du port forwarding
 - Ajouter des routes
 - Définir des règles pour le trafic entrant/sortant
 - Surveiller précisément ce même trafic
 - Ajouter des plugins qui vont apporter d'autres fonctionnalités (*filtrage Squidguard par exemple*)
 - ...

Info + : Pour modifier la langue de pfSense, allez dans le menu System et General Setup.

Par défaut lors de son installation, tout le trafic est ouvert. On peut voir ceci dans le menu « Firewall », sous-menu « Rules » et partie « LAN ».



Les règles présentes ici **définissent que tout le trafic IPv4 et IPv6, tout protocole confondu, venant sur réseau local (*LAN Net*) sur n'importe quel port et vers n'importe quelle destination est autorisé.**

D'ailleurs si vous avez correctement suivi ce tuto et que depuis le PC client vous faites un ping vers google.fr, le ping va bien aboutir, preuve en est que le trafic peut sortir sans intervention de votre part.

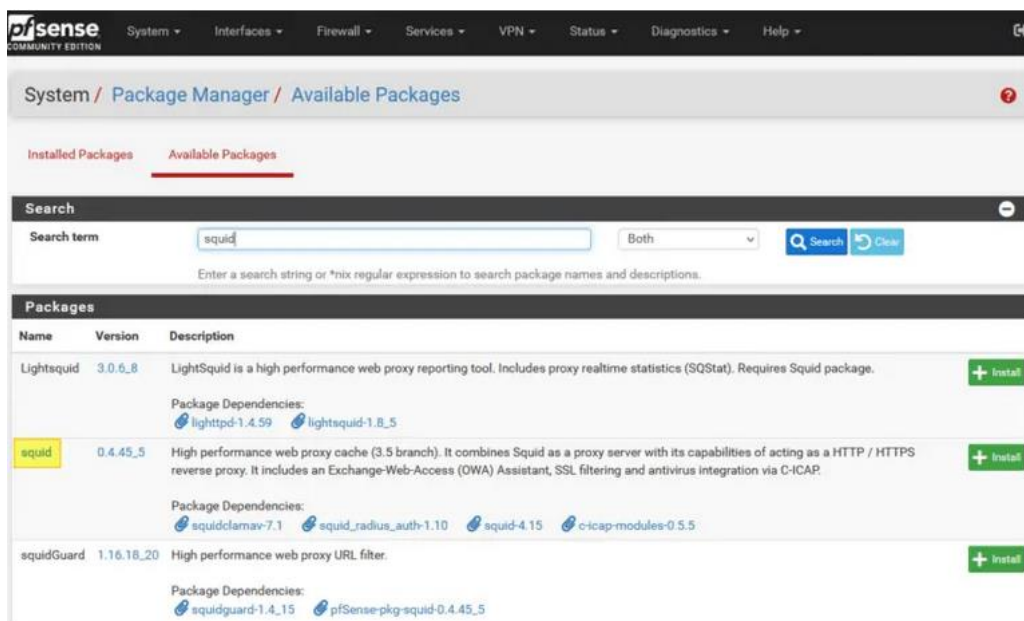
Il est plus que conseillé de brider ce trafic pour n'autoriser que les protocoles/port nécessaires. Le but d'un firewall étant de sécuriser ce qui entre et sort de son réseau, si c'est porte ouverte, il n'y a pas vraiment d'intérêt...

I.INSTALLATION DE SQUID

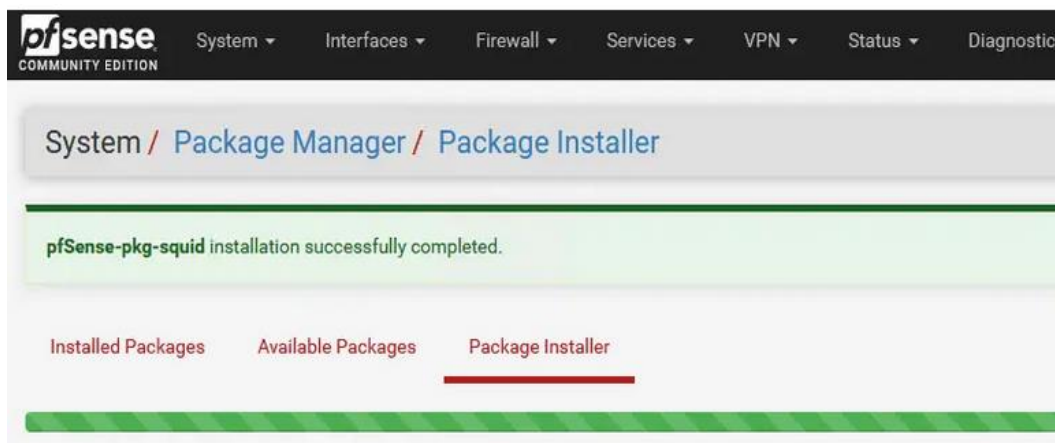
Connectez-vous sur l'interface d'administration de PfSense afin d'installer le paquet "*squid*". Pour cela, sous "**System**", cliquez sur "**Package Manager**" et ensuite sur l'onglet "**Available Packages**".

System > Package Manager > Available Packages

Recherchez "**squid**" et cliquez sur le bouton "**Install**" à droite, au niveau de la ligne correspondante.



À la fin de l'installation, le message "**pfSense-pkg-squid installation successfully completed**" doit s'afficher.



Le paquet étant installé, on peut passer à la configuration.

II.CONFIGURATION DE SQUID

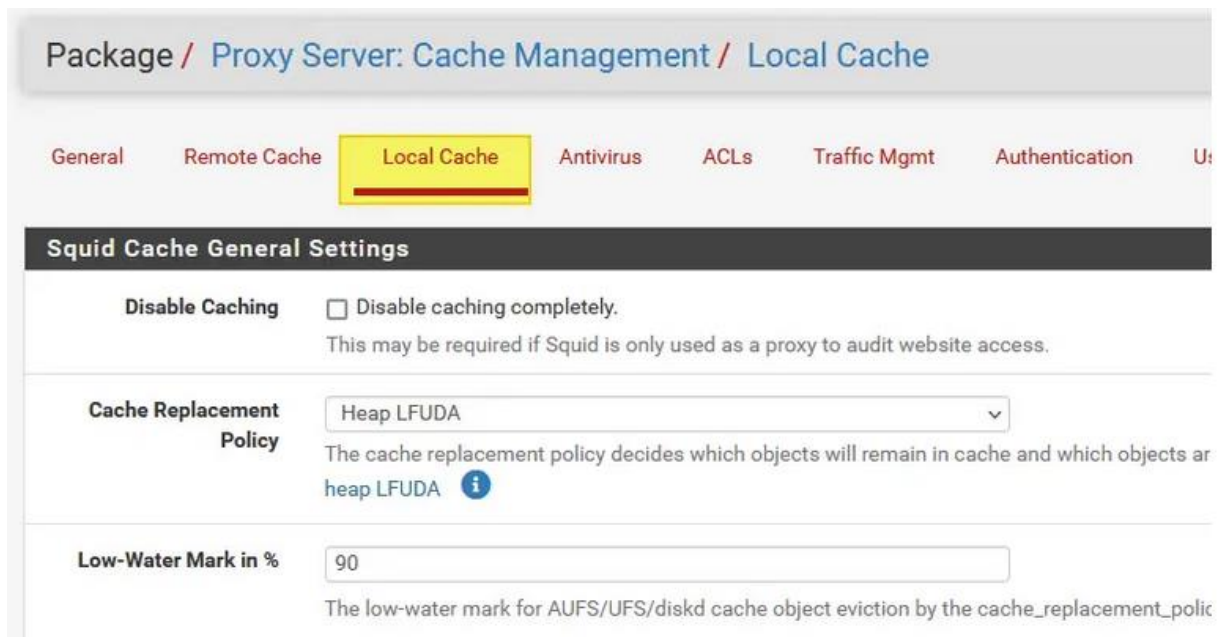
La configuration de Squid s'effectue via le menu "[Services](#)" :

Services > Squid Proxy Server

La configuration est découpée en plusieurs onglets. Afin de pouvoir activer Squid, il faut **configurer le cache local sinon le démarrage du processus Squid échouera**. Cliquez sur l'onglet "**Local Cache**". Comme pour chaque section, nous retrouvons de nombreux paramètres... Pour le cache, j'attire votre attention sur ces options :

- **Hard Disk Cache Size** : par défaut sur "100" pour 100 Mo, cette valeur correspond à la taille maximale du cache sur l'espace disque. Vous pouvez augmenter cette valeur à **1024 Mo** pour avoir 1 Go de cache.
- **Hard Disk Cache Location** : l'emplacement du cache, à savoir par défaut `"/var/squid/cache"`.

Que vous décidiez de modifier ou non l'un des paramètres de la section "**Local Cache**", vous devez cliquer sur le bouton "**Save**" en bas de la page.



Ensuite, cliquez sur l'onglet "**General**". Là encore, il y a de nombreuses options. Voici ce qu'il faut configurer à minima :

- **Enable Squid Proxy** : cochez la case pour activer Squid sur le pare-feu, ce qui signifie qu'il va démarrer
- *[facultatif]* **Listen IP Version** : écouter en IPv4, en IPv6 ou les deux
- **Proxy interface(s)** : sur quelle interface souhaitez-vous activer le proxy ? Ici, ce sera sur les interfaces "**OPT1**" et "**OPT2**" donc je les sélectionne. Vous pouvez en

sélectionner un seul si besoin, mais dans tous les cas le "WAN" ne sera pas sélectionné.

- **Proxy Port** : on laisse le port par défaut, à savoir 3128, mais il ne devra pas être déclaré sur les postes clients puisque l'on va configurer Squid en mode proxy transparent.
- **Allow Users on interface** : cochez cette case pour autoriser implicitement les utilisateurs connectés sur le réseau "OPT1" et "OPT2" à utiliser le proxy. Cela évite de déclarer le réseau dans un second temps.

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
Select the IP version Squid will use to select addressees for accepting client connections.

CARP Status VIP
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)
The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.

Outgoing Network Interface
The interface the proxy server will use for outgoing connections.

Port du mandataire (- proxy ->)
This is the port the proxy server will listen on. Default: 3128

ICP Port
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 ☒ 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 ☒ Enable this to force DNS IPv4 lookup first. This option is very useful if you have problems accessing HTTPS sites.

Descendez dans la page... et cochez l'option "**Transparent HTTP Proxy**" pour activer le mode proxy transparent pour le protocole HTTP. Pour l'activer pour le protocole HTTPS, il faudra cocher une autre option (nous en parlerons par la suite).

Dans le même esprit qu'au début de la configuration, sélectionnez "**OPT1**" et "**OPT2**" pour l'option "**Transparent Proxy Interface(s)**".

En configurant l'option "**Bypass Proxy for these Source IPs**", vous avez la possibilité de déclarer des adresses IP sources (ou un sous-réseau source) qui peuvent passer outre le proxy et accéder en direct à Internet, ici on va mettre les 2 AD's avec 192.168.100.4 et 192.168.100.5 car les salariés ne sont pas censés y avoir accès. Dans le même esprit, l'option "**Bypass Proxy for these Destination IPs**" permet d'outrepasser le proxy pour certaines destinations.

Transparent Proxy Settings

Transparent HTTP Proxy ☒ Enable transparent mode to forward all requests for destination port 80 to the proxy server.
Important: Transparent proxy mode works without any additional configuration being necessary on clients. Transparent proxy mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below.
Hint: In order to proxy both HTTP and HTTPS protocols **without intercepting SSL connections**, configure WPAD/PAC options on your DNS/DHCP servers.

Transparent Proxy Interface(s)
The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.

Bypass Proxy for Private Address Destination ☐ Do not forward traffic to Private Address Space (RFC 1918 and IPv6 ULA) destinations. Destinations in Private Address Space (RFC 1918 and IPv6 ULA) are passed directly through the firewall, not through the proxy server.

Bypass Proxy for These Source IPs
Do not forward traffic from these **source** IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall. **Applies only to transparent mode.** Separate entries by semi-colons (;)

Bypass Proxy for These Destination IPs
Do not proxy traffic going to these **destination** IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall. **Applies only to transparent mode.** Separate entries by semi-colons (;)

Pour le moment, laissez l'option "**Enable SSL filtering**" décochée.

SSL Man In the Middle Filtering	
HTTPS/SSL Interception	<input type="checkbox"/> Enable SSL filtering.
SSL/MITM Mode	<div>Splice All</div> <div>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. 📘</div>
SSL Intercept Interface(s)	<div> <div>WAN</div> <div>LAN</div> <div>OPT1</div> <div>OPT2</div> </div> <div>The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.</div>

Continuez de descendre dans la page... Activez les journaux comme ceci :

- **Enable Access Logging** : cochez l'option pour activer les journaux, ce qui va permettre de savoir qui fait quoi sur Internet.
- **Rotate Logs** : pendant combien de jours souhaitez-vous conserver les logs ? Pour les établissements scolaires, c'est pendant 365 jours qu'il faut conserver les logs (sauf erreur de ma part).

Logging Settings	
Enable Access Logging	<div><input checked="" type="checkbox"/> This will enable the access log.</div> <div>Warning: Do NOT enable if available disk space is low.</div>
Log Store Directory	<div>/var/squid/logs</div> <div>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.</div>
Rotate Logs	<div>365</div> <div>Defines how many days of logfiles will be kept. Rotation is disabled if left empty.</div>

Ensuite, la section "**Headers Handling, Language and Other Customizations**" permet de configurer les messages Squid. Le champ "**Visible Hostname**" correspond au nom d'hôte qui peut s'afficher côté client, notamment sur les pages de blocage Squid, tout comme l'e-mail spécifié pour l'option "**Administrator's Email**". Pour les messages d'erreurs justement, précisez la langue française au niveau de l'option "**Error Language**".

Pour des raisons de sécurité, on va masquer les informations sur Squid, notamment la version, en cochant l'option "**Suppress Squid Version**". Ce qui donne :

Headers Handling, Language and Other Customizations	
Visible Hostname	<div>BTS</div> <div>This is the hostname to be displayed in proxy server error messages.</div>
Administrator's Email	<div>korodaze@protonmail.com</div> <div>This is the email address displayed in error messages to the users.</div>
Error Language	<div>fr</div> <div>Select the language in which the proxy server will display error messages to users.</div>
X-Forwarded Header Mode	<div>(on)</div> <div>Choose how to handle X-Forwarded-For headers. Default: on 📘</div>
Disable VIA Header	<div><input type="checkbox"/> If not set, Squid will include a Via header in requests and replies as required by RFC2616.</div>
URI Whitespace Characters Handling	<div>strip</div> <div>Choose how to handle whitespace characters in URL. Default: strip 📘</div>
Suppress Squid Version	<div><input checked="" type="checkbox"/> Suppresses Squid version string info in HTTP headers and HTML error pages if enabled.</div>

Voilà, on est arrivé au bout de la page de configuration ! Cliquez sur "**Save**" pour appliquer cette nouvelle configuration.

IV. Tester le proxy transparent Squid

Pour tester le bon fonctionnement de notre proxy transparent HTTP, on peut tout simplement s'amuser à naviguer sur Internet. Pour que ce soit plus parlant, on va bloquer un nom de domaine.

Cliquez sur l'onglet "**ACLs**", toujours dans la configuration de Squid. C'est ici que vous pouvez déclarer les sous-réseaux autorisés à utiliser le proxy (**Allowed Subnets**) mais pour nous on renseignera le réseau 192.168.200.0/24 car on veut que tous les clients utilisent le proxy. Pour autoriser une ou plusieurs adresses IP (ou sous-réseau) à passer outre les restrictions, renseignez l'option "**Unrestricted IPs**" ici on va mettre les réseaux 192.168.100.4/24 et 192.168.100.5/24 car ce sont les 2 serveurs AD de notre infra et on ne veut pas qu'ils aient une restriction.

Squid Access Control Lists

Allowed Subnets 192.168.200.0/24

Enter subnets that are allowed to use the proxy in CIDR format. All the other subnets won't be able to use the proxy.
Put each entry on a separate line.
When 'Allow Users on Interface' is checked on 'General' tab, there is no need to add the 'Proxy Interface(s)' subnet(s) to this list.

Unrestricted IPs 192.168.100.4/24
192.168.100.5/24

Enter unrestricted IP address(es) / network(s) in CIDR format. Configured entries will NOT be filtered out by the other access control directives set in this page.
Put each entry on a separate line. ⓘ

Ce qui m'intéresse pour ce test, c'est l'option "**Blacklist**" puisqu'elle permet d'indiquer un ou plusieurs domaines à bloquer. Pour ce test, il nous faut un site en HTTP (ce qui est de plus en plus "rare", enfin surtout au niveau des sites connus). J'ai pris le site "*horizons21.fr*", au hasard, et je l'ai ajouté comme ceci :

Whitelist

Destination domains that will be accessible to the users that are allowed to use the proxy. Put each entry on a separate line. You can also use regular expressions.

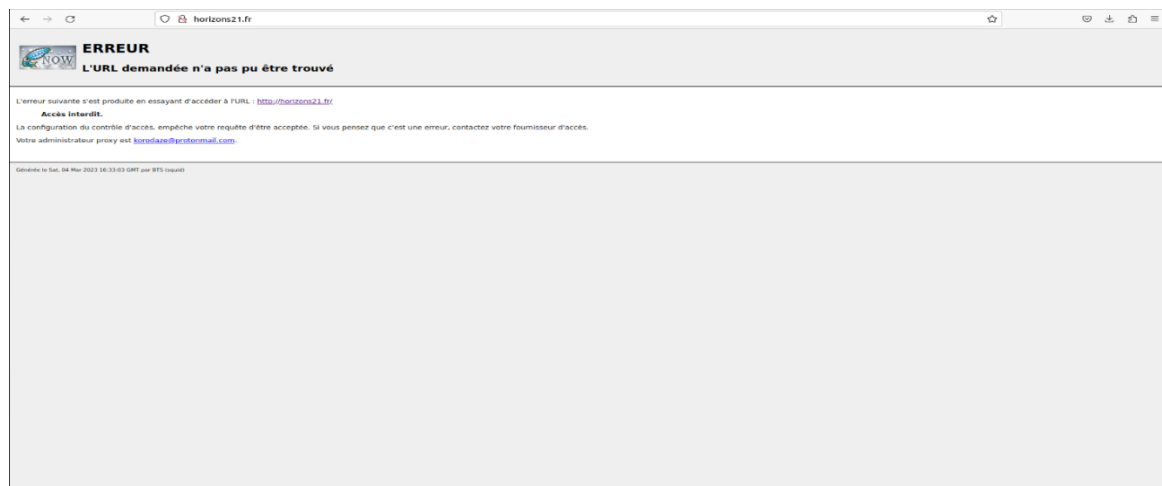
Blacklist

horizons21.fr

Destination domains that will be blocked for the users that are allowed to use the proxy. Put each entry on a separate line. You can also use regular expressions.

Block User Agents

Ensuite, on sauvegarde la configuration... Puis, à partir d'un poste de travail situé sur le réseau local, on tente d'accéder au site horizons21.fr. Et là, on peut voir que ça ne fonctionne pas ! On peut voir qu'une page "**Accès interdit**" renvoyée par Squid s'affiche !



On peut aussi suivre les logs en temps réel côté Squid, via l'onglet "**Real Time**". On voit très bien nos requêtes à destination du site "*horizons21.fr*" depuis l'hôte *192.168.200.150* : c'est la preuve irréfutable que notre PC passe bien par le proxy transparent !

Squid Access Table					
Squid - Access Logs					
Date	IP	État	Adresse	Utilisateur	Destination
05.03.2023 14:00:38	192.168.200.150	NONE/200	34.120.208.123:443	-	-
05.03.2023 14:00:38	192.168.200.150	NONE/200	35.241.9.150:443	-	-
05.03.2023 14:00:37	192.168.200.150	TCP_DENIED/403	http://horizons21.fr/favicon.ico	-	-
05.03.2023 14:00:36	192.168.200.150	TCP_DENIED/403	http://horizons21.fr/	-	-
05.03.2023 14:00:03	192.168.100.6	NONE/200	34.117.237.239:443	-	-
05.03.2023 13:59:59	192.168.100.60	NONE/000	error:transaction-end-before-headers	-	-
05.03.2023 13:59:59	192.168.100.60	NONE/409	v10.events.data.microsoft.com:443	-	-
05.03.2023 13:59:59	192.168.100.60	NONE/200	13.69.109.131:443	-	-
05.03.2023 13:58:26	192.168.100.61	NONE/000	error:transaction-end-before-headers	-	-
05.03.2023 13:58:26	192.168.100.61	NONE/409	v10.events.data.microsoft.com:443	-	-

V. Configurer Squid en proxy transparent HTTPS (SSL Inspection)

C'est bien beau notre configuration, mais notre proxy transparent fonctionne seulement sur le protocole HTTP. Depuis quelques années maintenant, la tendance est au HTTPS (et on ne va pas s'en plaindre) alors c'est indispensable que l'on permette à notre proxy transparent de travailler le HTTPS.




Cela est un peu plus complexe qu'une simple case à cocher dans les options du proxy, car il faut faire ce que l'on appelle du **SSL Inspection**. Puisqu'un flux HTTPS est chiffré, le proxy ne peut pas seulement regarder les trames passer. En effet, pour chaque connexion, il doit déchiffrer le flux, l'inspecter puis le chiffrer à nouveau afin de l'acheminer : une tâche d'envergure et gourmande en ressources.

A. Créer l'autorité de certification PfSense

Pour commencer, il faut créer une autorité de certification sur notre pare-feu PfSense. Rendez-vous dans le menu "**System**" puis "**Cert. Manager**" et dans l'onglet "**CAs**". Cliquez sur "**Add**" et renseignez les différents champs : c'est tout simple.

Note : si vous avez une autorité de certification Active Directory, il doit être possible d'ajouter un certificat existant directement.

Vous obtenez une autorité de certification, comme la mienne nommée "**BTS-PROXY**".

Autorités de certification						
Nom	Interne	Émetteur	Certificats	Nom distinctif	En cours d'utilisation	Actions
BTS-PROXY	✓	auto-signé	1	ST=Paris, OU=BTS SIO OPTION SISR, O=IMIE-PARIS, L=Paris, CN=BTS, C=FR  Valable depuis: Sat, 04 Mar 2023 15:58:04 +0000 Valable jusqu'à: Tue, 01 Mar 2023 15:58:04 +0000	Squid (2)	 

B. SSL Inspection avec Squid

Retournez dans la configuration de Squid, via le menu "**Services**". Cochez l'option "**Resolve DNS IPv4 First**" pour activer la résolution DNS en amont du filtrage, ce qui est recommandé lorsque l'on filtre le HTTPS (ce que l'on s'apprête à faire).

Resolve DNS IPv4 First☒ Enable this to force DNS IPv4 lookup first.

This option is very useful if you have problems accessing HTTPS sites.

Ensuite, activez l'option "**Enable SSL filtering**". Pour le mode "**SSL/MITM Mode**", choisissez le mode "**Splice All**" : c'est le mode le moins contraignant à mettre en œuvre, car il ne nécessite pas de déployer le certificat de l'autorité de certification sur l'ensemble des postes clients. C'est aussi le mode recommandé lorsque l'on prévoit de déployer Squid Guard, ce qui sera le cas dans la seconde partie de ce tutoriel.

Remarque : si vous prenez l'autre mode, il faut exporter le certificat de la CA créée précédemment et le déployer sur toutes les machines qui vont passer par le proxy transparent.

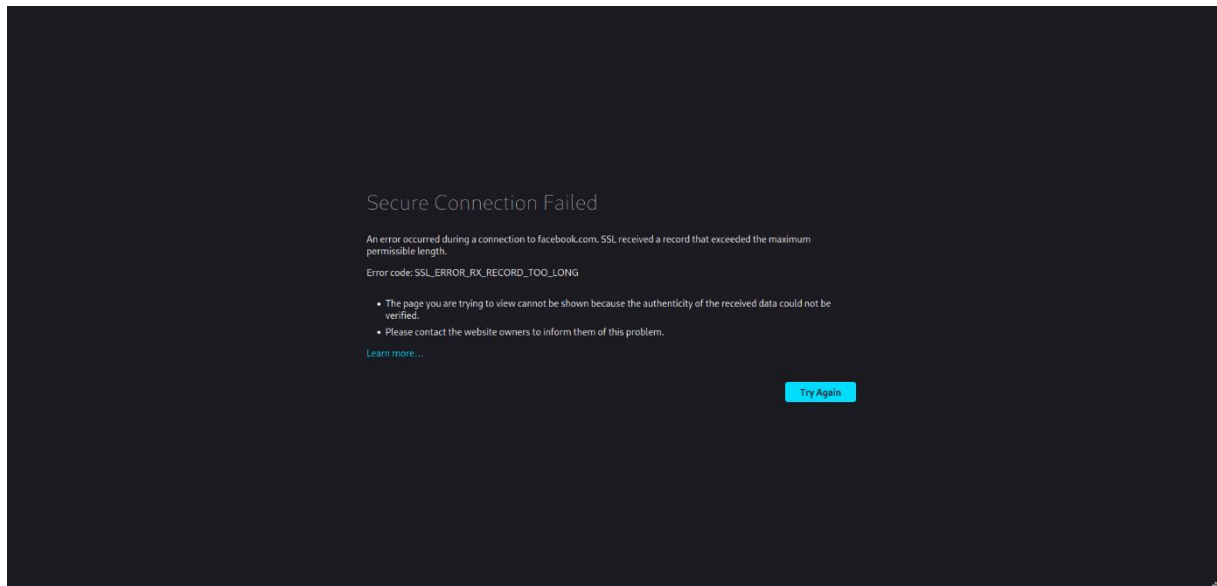
Sélectionnez l'autorité de certification créée précédemment au niveau de l'option "**CA**".

SSL Man In the Middle Filtering	
HTTPS/SSL Interception	<input checked="" type="checkbox"/> Enable SSL filtering.
SSL/MITM Mode	<div>Splice All</div> <div>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. ⓘ</div>
SSL Intercept Interface(s)	<div>WAN LAN OPT1 OPT2</div> <div>The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.</div>
SSL Proxy Port	<div>3129</div> <div>This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129</div>
SSL Proxy Compatibility Mode	<div>Modern</div> <div>The compatibility mode determines which cipher suites and TLS versions are supported. Default: Modern. Click Info for details. ⓘ</div>
DHParams Key Size	<div>2048 (default)</div> <div>DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.</div>
AC	<div>BTS-PROXY</div> <div>Select Certificate Authority to use when SSL interception is enabled. ⓘ</div>
SSL Certificate Deamon Children	<div></div> <div>This is the number of SSL certificate deamon children to start. May need to be increased in busy environments. Default: 5</div>
Remote Cert Checks	<div>Accept remote server certificate with errors Do not verify remote certificate</div> <div>Select remote SSL certificate checks to perform. Use CTRL + click to select multiple options.</div>
Certificate Adapt	<div>Sets the "Not After" (setValidAfter) Sets the "Not Before" (setValidBefore) Sets CN property (setCommonName)</div> <div>See sslproxy_cert_adapt directive documentation and Mimic original SSL server certificate wiki article for details.</div>

Sauvegardez via le bouton en bas de page.

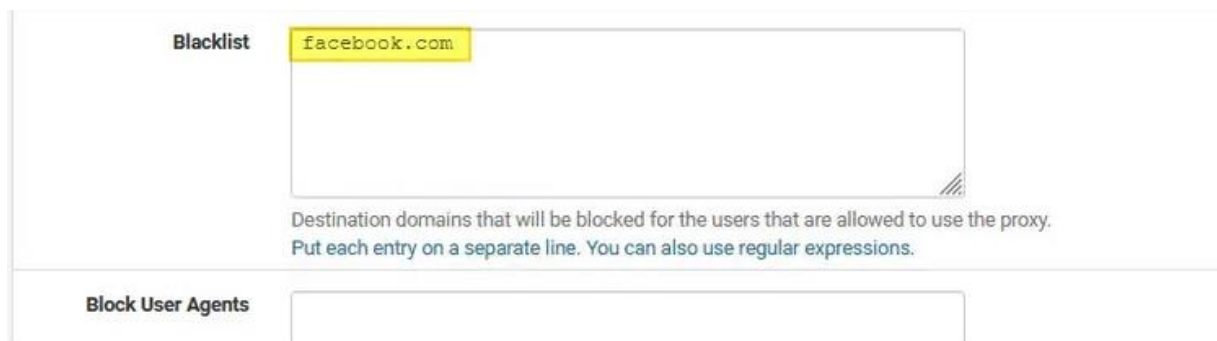
C. Tester l'accès à Internet

Maintenant, retournez sur votre poste de travail qui passe par le proxy puis tentez de naviguer sur un site en HTTPS. Vous allez très probablement obtenir le message d'erreur "**SSL_ERROR_RX_RECORD_TOO_LONG**". Ce qui confirme que le proxy fonctionne.



E. ACL : bloquer un site HTTPS dans Squid

Comme toute à l'heure, on va retourner dans l'onglet "**ACLs**" au niveau de la section "**Blacklist**". Cette fois-ci, on va bloquer un domaine où le site tourne en HTTPS : "*facebook.com*", à tout hasard. Ce qui donne :



On sauvegarde et on tente d'accéder à Facebook... Voici le message que l'on obtient :

Échec de la connexion sécurisée

Une erreur est survenue pendant une connexion à *www.ebay.fr*. 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

I. Présentation

Dans ce tutoriel, nous allons voir comment installer et configurer Squid Guard sur un [pare-feu PfSense](#) pour permettre à notre proxy Squid d'effectuer du filtrage de sites Web basé sur des catégories, via une blacklist.

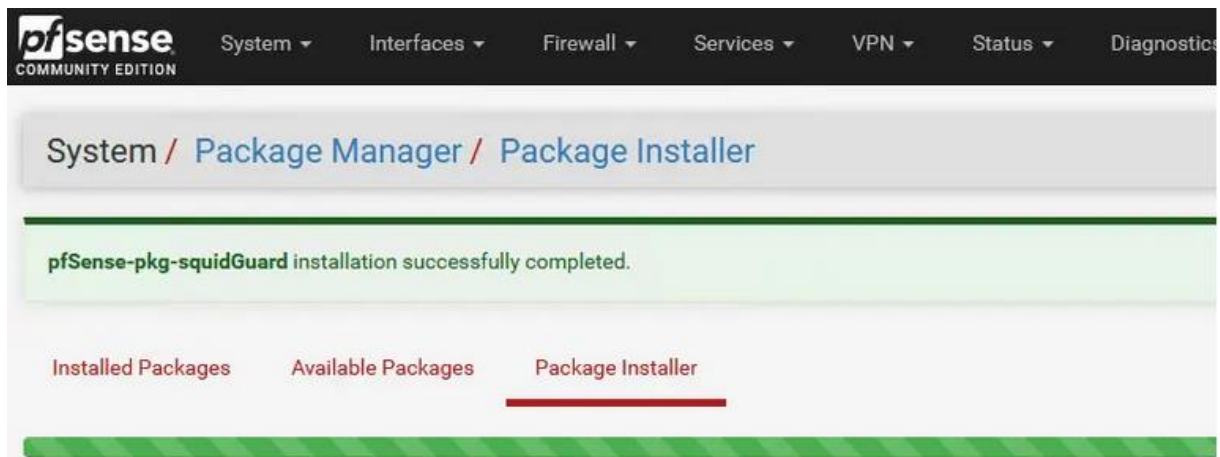
Au sein de Squid, sans Squid Guard donc, on peut mettre en place des ACLs et notamment bloquer des noms de domaine. Le problème, c'est que l'on ne peut pas créer de catégories pour regrouper plusieurs domaines, et on ne peut pas non plus créer des restrictions selon des plages horaires. Embêtant.

Grâce à Squid Guard, on va pouvoir utiliser une Blacklist existante, c'est-à-dire **une liste noire de domaines organisés par catégories**, afin d'affiner le filtrage au sein de notre proxy Squid. En complément, on pourra mettre en place des règles en fonction de plages horaires, de groupes utilisateurs, etc. De cette façon, vous allez pouvoir configurer votre proxy de manière à bloquer tous les sites liés à la pornographie.

La mise en place de Squid Guard nécessite au préalable d'avoir mis en place un proxy avec Squid puisque ce paquet vient en complément.

II. Installation de Squid Guard sur PfSense

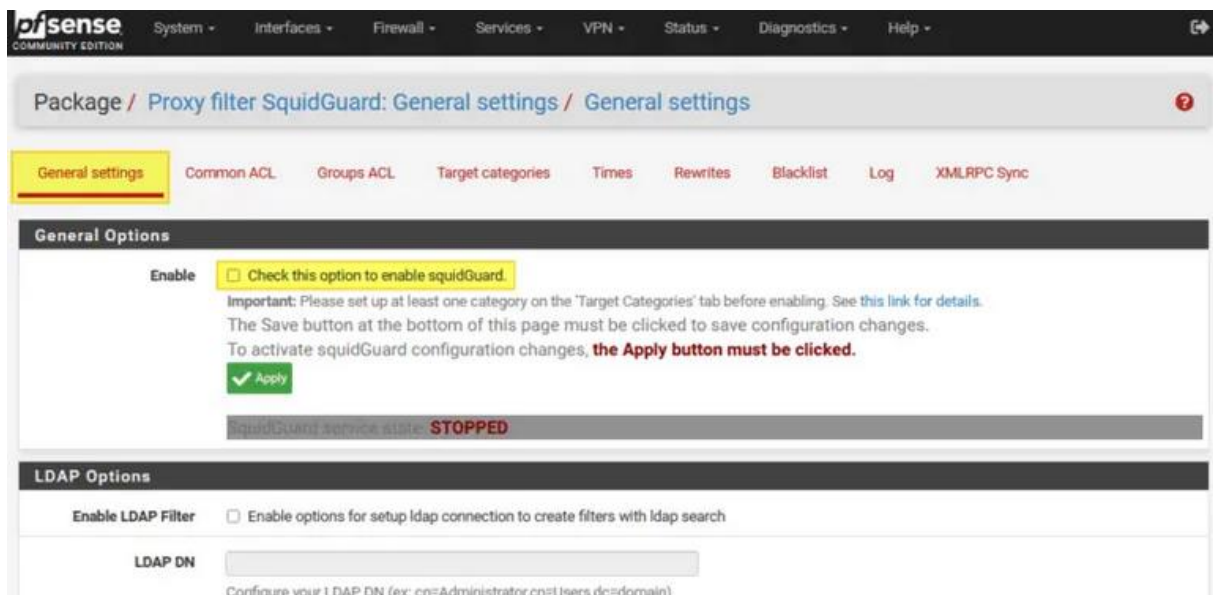
L'installation de ce paquet sur PfSense passe par le menu habituel sous "**System**", puis "**Package manager**". Dans la section "**Available Packages**", recherchez "*squid*" et vous devriez voir le paquet Squid Guard apparaître. Il ne reste plus qu'à cliquer sur le bouton "**Install**".



Une fois que c'est fait, nous pouvons passer à la configuration via le menu "[Services](#)" où se trouve une entrée "**SquidGuard Proxy Filter**".

III. Configuration de Squid Guard sur PfSense

Pour le moment, on va s'intéresser à l'onglet "**General Settings**". N'allez pas trop vite : **ne cochez pas l'option "Check this option to enable SquidGuard" pour le moment, car il faut le préconfigurer avant de l'activer.**



Cochez les deux options suivantes pour activer les logs : "**Enable GUI Log**" et "**Enable log**".

Service options	
Rewrite process children	<input type="text" value="16"/> <p>Maximum number of SquidGuard redirector processes that Squid may spawn. Using too few of these helper processes (a.k.a. "helpers") creates request queues. Using too many helpers wastes your system resources. (Default: 16)</p>
Rewrite process children startup	<input type="text" value="8"/> <p>Sets a minimum of how many SquidGuard processes are to be spawned when Squid starts or reconfigures. (Default: 8)</p>
Rewrite process children idle	<input type="text" value="4"/> <p>Sets a minimum of how many SquidGuard processes Squid is to try and keep available at all times. (Default: 4)</p>
Logging options	
Enable GUI log	<input checked="" type="checkbox"/> Check this option to log the access to the Proxy Filter GUI.
Enable log	<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.
Enable log rotation	<input 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	

Au sein de la section "**Blacklist**", cochez l'option "**Check this option to enable blacklist**" afin d'activer l'utilisation d'une blacklist, c'est-à-dire une liste noire. Nous allons utiliser **la liste noire de L'Université Toulouse Capitole**, car elle est française, fiable et elle existe depuis plusieurs années. **Elle contient de nombreuses catégories afin de répartir les sites et permettre un blocage ciblé selon certaines catégories.**

Ensuite, renseignez l'option "**Blacklist URL**" avec l'URL suivante :

`ftp://ftp.univ-tlse1.fr/blacklist/blacklists.tar.gz`

Enfin, cliquez sur le bouton "**Save**".

Blacklist options	
Blacklist	<input checked="" type="checkbox"/> Check this option to enable blacklist
Blacklist proxy	<input type="text"/> <p>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'</p>
Blacklist URL	<input type="text" value="ftp://ftp.univ-tlse1.fr/blacklist/blacklists.tar.gz"/> <p>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).</p>

Maintenant, basculez sur l'onglet "**Blacklist**" de SquidGuard. Cliquez sur le bouton "**Download**" pour télécharger la dernière version de la liste noire que nous avons renseignée dans les paramètres de SquidGuard.

Blacklist Update

0 %

ftp://ftp.univ-tlse1.fr/blacklist/blacklists.tar.gz

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.univ-tlse1.fr/blacklist/blacklists.tar.gz
Download complete
Unpack archive
Scan blacklist categories.
Found 63 items.
Start rebuild DB.
Copy DB to workdir.
Reconfigure Squid proxy.
Blacklist update complete.

```

Afin d'exploiter la liste noire, nous devons créer des règles sous la forme d'ACL. Cliquez sur **"Common ACL"** afin de créer une règle de base et commune au sein de Squid, tandis que la section **"Groups ACL"** permet de créer des ACL ciblées avec plusieurs critères (par exemple : *"bloquer une catégorie selon une plage horaire spécifique"* ou *"bloquer une catégorie à tous les membres d'un groupe Active Directory"*).

Au sein du champ **"Target Rules List"**, vous avez la liste de toutes les catégories récupérées à partir de la blacklist toulousaine.

Target Rules

all

Target Rules List + -

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

Target Categories

[blk_blacklists_ads]	access	---	▼
[blk_blacklists_adult]	access	---	▼
[blk_blacklists_aggressive]	access	---	▼
[blk_blacklists_arsj]	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	---	▼
[blk_blacklists_child]	access	---	▼
[blk_blacklists_cleaning]	access	---	▼
[blk_blacklists_cooking]	access	---	▼
[blk_blacklists_cryptolocking]	access	---	▼
[blk_blacklists_dangerous_material]	access	---	▼
[blk_blacklists_dating]	access	---	▼
[blk_blacklists_ddos]	access	---	▼
[blk_blacklists_dialer]	access	---	▼
[blk_blacklists_doh]	access	---	▼
[blk_blacklists_download]	access	---	▼
[blk_blacklists_drogue]	access	---	▼
[blk_blacklists_educational_games]	access	---	▼
[blk_blacklists_exam_pix]	access	---	▼
[blk_blacklists_exceptions_liste_bul]	access	---	▼
[blk_blacklists_filehosting]	access	---	▼
[blk_blacklists_financier]	access	---	▼
[blk_blacklists_forums]	access	---	▼

Je vous propose de bloquer la catégorie **"VPN"** correspondante à **"[blk_blacklists_vpn]"**, il faut donc modifier la valeur du champ **"access"** pour

préciser **"deny"**. En complément, pensez à configurer la valeur du champ **"Default access [all]"** sur **"allow"** pour autoriser toutes les autres catégories (par défaut).

[blk_blacklists_vpn]	access	deny
[blk_blacklists_warez]	access	---
[blk_blacklists_webmail]	access	---
Default access [all]	access	allow

Afin d'éviter qu'un petit malin contourne la restriction en précisant l'adresse IP du serveur distant à la place du nom de domaine, cochez l'option **"Do not allow IP-Addresses in URL"**. En complément, si vous souhaitez utiliser la fonction SafeSearch des moteurs de recherche, cochez la case **"Use SafeSearch Engine"**, tout en sachant que cela permet d'utiliser Google, Bing, DuckDuckGo, Qwant, etc.

Do not allow IP-Addresses in URL	<input checked="" type="checkbox"/> 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	<div><input type="text"/></div> <div>The first part of the error message displayed to clients when access was denied. Defaults to "Request denied by \$g[product_name] proxy"</div>
Redirect mode	<div>int error page (enter error message)</div> <div>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'.</div>
Redirect info	<div><input type="text"/></div> <div>Enter external redirection URL, error message or size (bytes) here.</div>
Use SafeSearch engine	<input checked="" type="checkbox"/> 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.

Enfin, activez les logs pour cette règle en cochant l'option **"Log"** tout en bas, puis cliquez sur **"Save"**.

Journalise	<input checked="" type="checkbox"/> Check this option to enable logging for this ACL.
-------------------	---

La configuration étant prête, retournez dans **"General Settings"**, cochez l'option **"Check this option to enable SquidGuard"** et cliquez sur **"Apply"**.

Package / Proxy filter SquidGuard: General settings / General settings

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log X

General Options

Enable

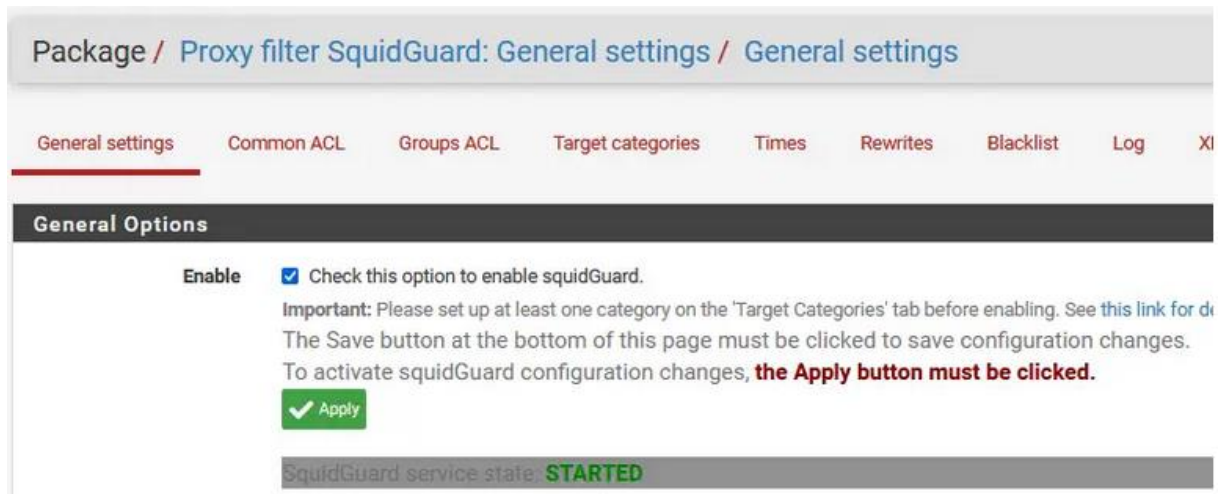
☒ Check this option to enable squidGuard.

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.**

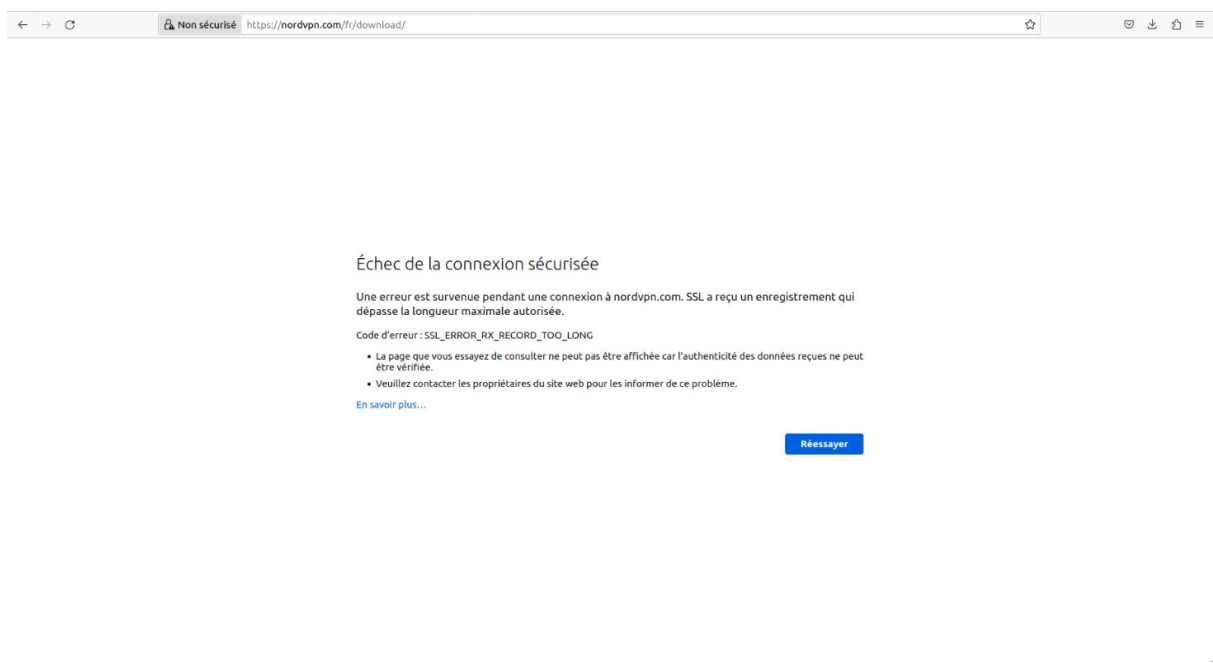
SquidGuard service state: **STOPPED**

Le statut du service SquidGuard doit changer et passer sur "**STARTED**". Si ce n'est pas le cas, vérifiez que Squid est bien démarré de son côté.

Remarque importante : à chaque fois que vous modifiez la configuration de Squid Guard (exemple : bloquer une catégorie supplémentaire), il faut impérativement venir dans l'onglet "**General Settings**" pour cliquer sur le bouton "**Apply**" sinon les modifications ne sont pas prises en compte !





À partir d'un poste client, tentez d'accéder à un site en rapport avec la thématique "**VPN**", comme le site de NordVPN et vous verrez que la connexion est en erreur. En réalité, c'est SquidGuard qui est intervenu pour bloquer la connexion à ce site, conformément à la politique de filtrage mise en place.



Pour aller plus loin, je vous invite à regarder deux onglets en particulier : "**Times**" pour créer des plages horaires" et "**Groups ACL**" pour créer des règles basées sur plusieurs critères. Sachez également que la section "**Target categories**" vous permet de créer des listes personnalisées.

IV. Installation et Configuration de LightSquid

Paquets installés				
Nom	Catégorie	Version	Description	Actions
✓ Lightsquid	www	3.0.6_9	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package. Dépendances du paquet: lighttpd-1.4.63 lightsquid-1.8_5	 

Tout d'abord installer le packet LightSquid.

Nous allons désormais configurer Lightsquid. Dans l'onglet « Status », cliquez sur « Squid Proxy Reports ».

pfSense
COMMUNITY EDITION

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

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term

Enter a search string or *nix regular expression to search

Packages

Name	Version	Description
acme	0.6.9_3	Automated Certificate Management E certificates. Package Dependencies: pecl-ssh2-1.1.2 socat-1.7.3.3 7.68.0
apcupsd	0.3.91_9	"apcupsd" can be used for controlling power and battery status, perform aut to power down other hosts on a LAN

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

Search

descriptions.

use of LetsEncrypt

php72-ftp-7.2.29

monitor and log the c
run in network mode

Vous pouvez ici changer les identifiants de connexion à la page Lightsquid. Par défaut, il s'agira des identifiants de PFSENSE.

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](#)

Vous pouvez ensuite changer la langue de l'interface.

Report Template Settings

Language French
Select report language.

Report Template Base
Select report template.

Bar Color Orange
Select bar color.

Indiquez ensuite une période de rafraîchissement des données dans l'interface dans « Refresh Scheduler ».

Reporting Settings and Scheduler

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

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 60min (+)
Select data refresh period. The reporting task will be executed every XX minutes/hours.
Legend: ⓘ(*) Use only with fast hardware (+) Recommended values

Manual Refresh Use these buttons to start a background refresh of the Lightsquid reports.

Refresh Will (re)parse today's entries only in Squid's current access.log.

Refresh Full Will (re)parse all entries in all Squid's access logs, including the rotated ones. This may take a long time to finish!

Cliquez enfin sur « save » et « refresh ».

Cliquez ensuite sur « Open Lightsquid ». Une page contenant les informations de Logs devrait s'afficher.

← → ↻ https://192.168.100.1:7445 ☆ ⓘ ⌵ ≡

[Squid, rapport d'accès utilisateur](#)
Période de travail: Mar 2023

Calendar									
2023									
01	02	03	04	05	06	07	08	09	10
11	12								

Top Sites	Total	Groups
ANNEE	ANNEE	ANNEE
MOIS	MOIS	MOIS

Date	Groupes Utilisateurs	Quota	Digant	Octets	Moyenne	Hit %
08 Mar 2023	88	9	2	93.8 M	10.4 M	2.93%
Total/Moyenne:		9	2	93.8 M	10.4 M	2.93%

Lightsquid v1.8 (c) Sergey Erokhin AKA ESL

Redémarrez ensuite PFSENSE. Dans l'onglet « Diagnostics », cliquez sur « Reboot ».