PFSense

Rapport d’un Serveur PFSense

Guillaume
BEAUPELLET

30 Janvier 2023

Table des matières

1. PRESENTATION 2
1. INSTALLATION 2
1.2 SCHEMA 4
1.3 CONFIGURATION 4
2. LES PACKAGES 5
3.1. SQUID 6
3.2. LIGHTSQUID 6
3.3. SQUIDGUARD 6
3. PROXY FILTER 7
4.1 BLACK LIST 7
4.2 LISTES PERSONNALISEES 8
4.3 VERIFICATION DU PROXY 8
4.4 RAPPORT D'ACTIVITE 10
..... 10
4. FIREWALL 11
5. ANTIVIRUS 12

PFSense

Rapport d'un Serveur PFSense bien configuré

1.Présentation

PFSense (Packet Filter Sense) est un Firewall / Routeur basé sur une distribution FreeBSD.
La solution PFSense a plusieurs concurrents, notamment la célèbre distribution « IPCop ».
Dans ce rapport d'installation, nous allons travailler sur la version 2.6 en 64 Bits de PFSense sortie en Février 2022.

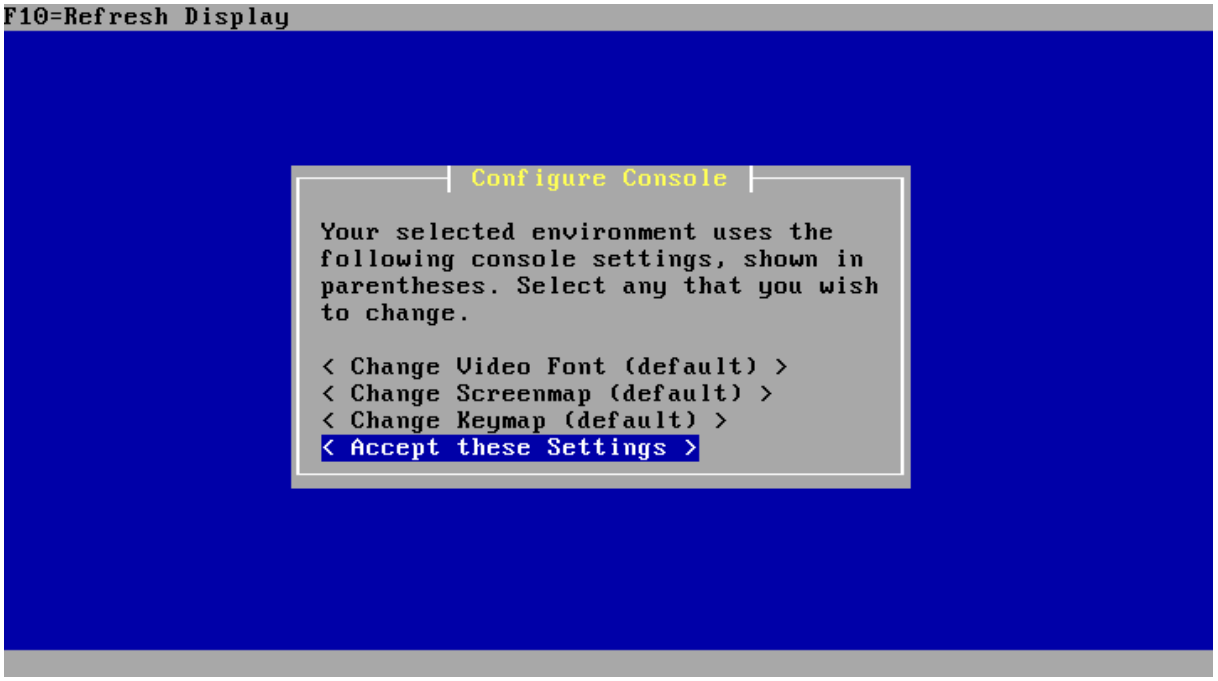
Nous allons l'utiliser en simulant le cas du groupe GEFOR ayant un budget serré et qui veut sécuriser son parc informatique et filtrer la navigation de ses employés et des élèves.

Après l'installation et les rudiments de configuration sur le serveur en lui-même, l'administration de PFSense se fera principalement via son interface de gestion WEB.

2. Installation

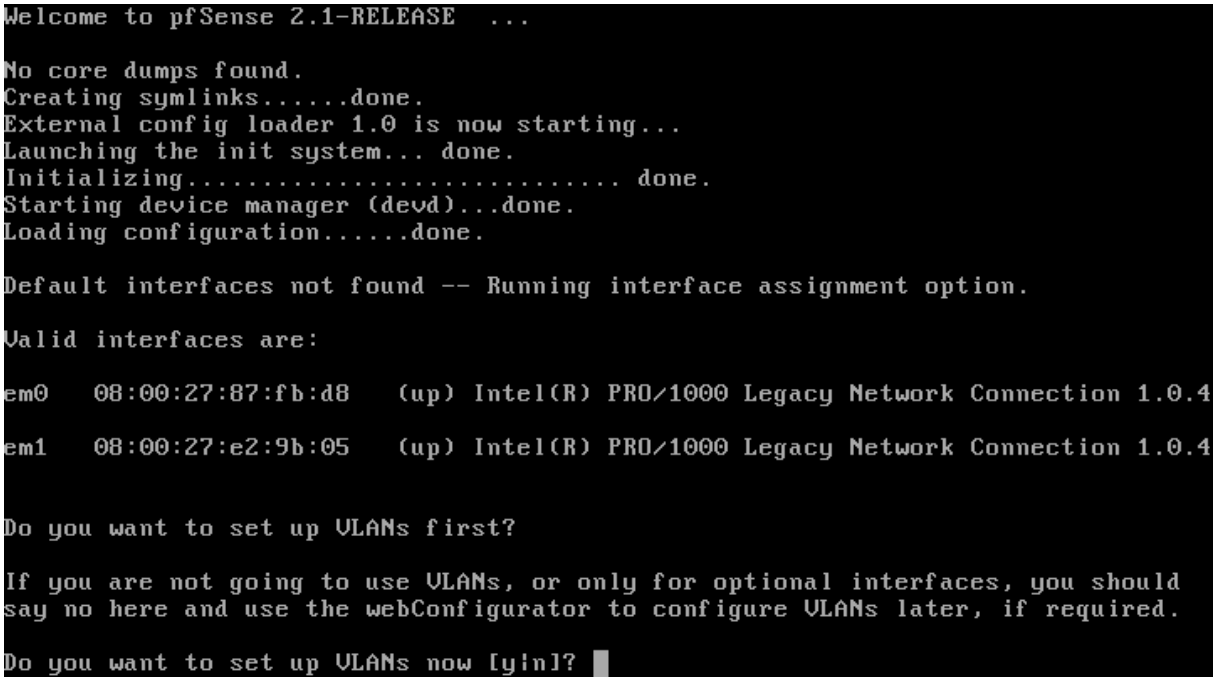
Comme dit plus haut, nous allons donc utiliser l'ISO (Image Disque) de PFSense 2.6 en x64.
Cela commence par la configuration des Cartes Réseaux, l'une en NAT pour le réseau extérieur et l'autre en Host Only pour communiquer avec l'interface Web.

Les attributions de RAM et d'espace disque minimum dépendent de la capacité de votre ordinateur. En revanche, la moyenne voudrait que la RAM soit entre 500Mo et 1Go, et qu'un espace de 2Go soit alloué pour des performances de travail optimales.



Pour peu de complications quant à l'installation, accepter les paramètres recommandés, et lancerl'installation en « quick launcher ».

Cette opération vous mènera à la détection de vos cartes réseaux. Si vous avez correctement configuré vos périphériques, elles seront nommées « eth0 » et « eth1 »



Accepter de gérer les cartes réseaux en assignant :

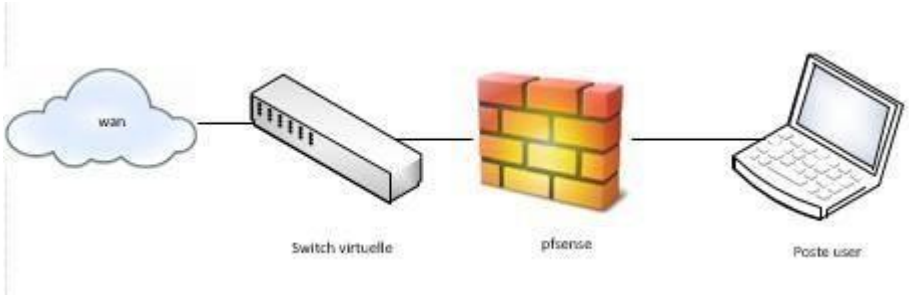
- WAN (NAT) sur eth0

- LAN (Host Only) sur eth1

```
WAN (wan)       -> em0        -> v4/DHCP4: 10.0.2.15/24
LAN (lan)       -> em1        -> v4: 192.168.1.1/24

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


Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.123.1
```

Ne pas oublier d'attribuer les adresses IP en fonction de votre réseau NAT (eth0) et Host Only (eth1).

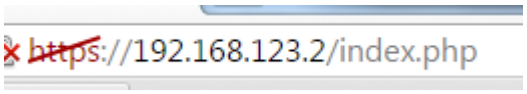
2.2 Schéma



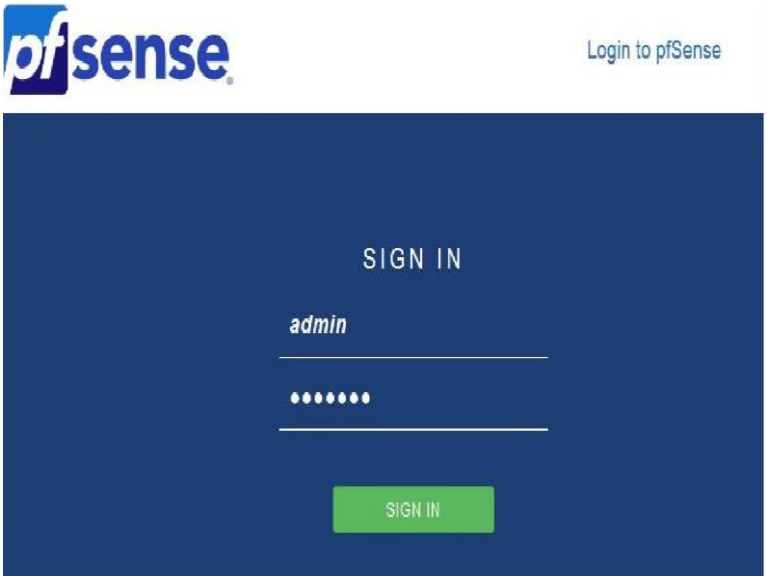
2.3 Configuration

Une fois l'installation finalisée, nous pouvons, en théorie, nous connecter en HTTP à l'interface graphique.

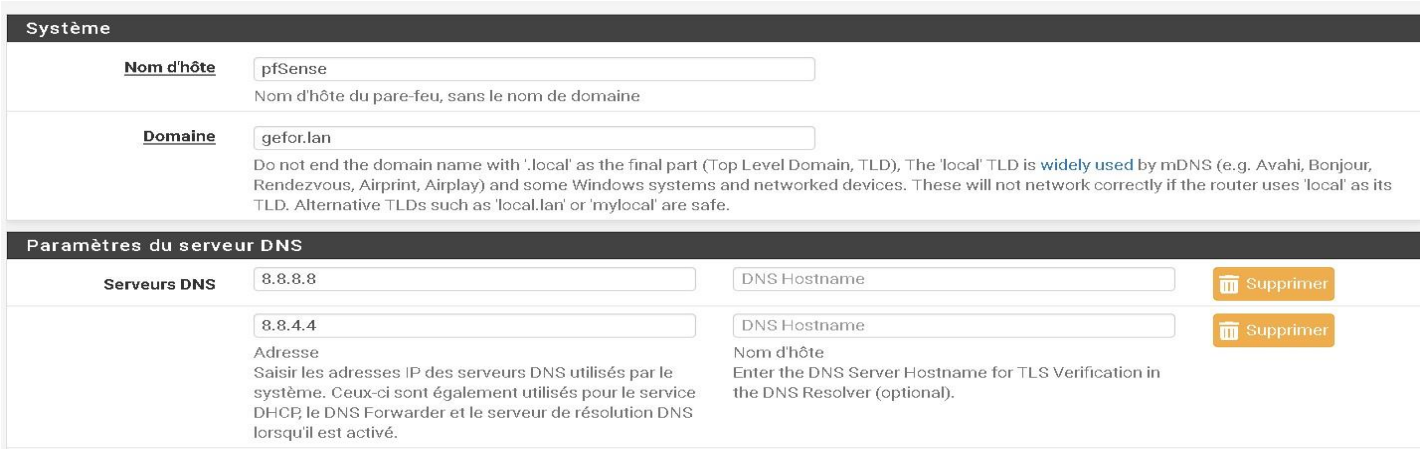
Pour ce faire, il suffit d'ouvrir un moteur de recherche et de rentrer dans l'URL l'adresse IP au préalablement inscrite dans eth1 (nous prendront 192.168.123.2 pour exemple).



Une fois cette étape effectuée, nous nous retrouvons devant la page de login de PFSense.
Le login par défaut est «admin » pour identifiant et « pfsense » pour mot de passe :



Dans menu « **System** », cliquez sur « **Setup Wizard** » et configurer les points suivants :Le nom d'hôte ;
Le domaine ;
Le serveur DNS ; **je conseille le primaire et secondaire de google** (8.8.8.8 et 8.8.4.4)
Le serveur NTP ;
Zone horaire : Europe /Paris ;
L'interface WAN sera configurée en DHCP ;
L'interface coté LAN est à choisir en fonction de votre configuration.
Ne pas oublier d'instaurer un mot de passe autre que celui par défaut !



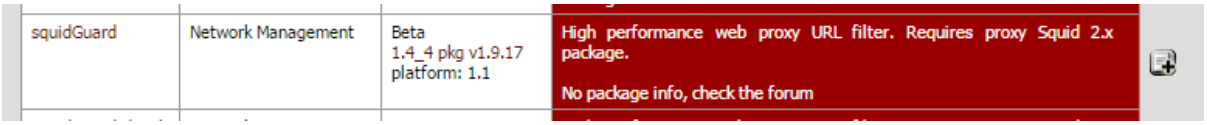
3. Les packages

PFSense est doté d'une multitude de packages. C'est ce qui fait sa force, il peut concentrer une vaste étendue de fonctionnalités dans une seule application.

Pour notre TP, la base de la sécurité en entreprise est d'installer un proxy, un historique de navigation et une base de données d'éléments à bloquer

3 packages seront donc à installer.

Dans « **System** » aller dans la rubrique « **packages** », et installer « **Squid** », « **LightSquid** » ainsi que « **SquidGuard** ».



3.1. Squid

Squid est un proxy, entièrement libre et très performant. Intégré dans PFSense, il est capable de gérer la plupart des protocoles utilisé en navigation web (FTP, http, HTTPS..) ;

Paramétrage de **Squid** dans le menu **« Services »**, cliquer sur **« Proxy server ».**
Dans l'onglet **« General »** réaliser la configuration:
Proxy Interface : LAN
Allow Users : OK
Transparent Proxy: OK
Log store directory: /var/squid/log
Proxy Port: 3128
Language: French (pour les pages d'erreurs)

3.2. LightSquid

LightSquid est un analyseur de Logs pour le proxy Squid. Il enregistre la navigation du parc sur lequel Squid est installé et génère des statistiques ainsi qu'un historique de navigation.

3.3. SquidGuard

SquidGuard est un **redirecteur** qui utilise la librairie Berkeley Database de SleepyCat.

Une fois avoir activé l'utilisation des Blacklist, vous pouvez (manuellement ou automatiquement) ajouter des fichiers comportant plusieurs adresses URL qui l'on souhaite bloquer.

Ces listes sont disponibles et acceptables par SquiGuard uniquement en fichiers **compressé** Linux / FreeBSD, le **tar.gz**

De nombreuses sources de téléchargement compatibles avec Squidguard / PFSense sont disponibles. Dans notre TP, nous utiliser la source ftp://ftp.univ_tlse1.fr/blacklist/blacklists_for_pfsense.tar.gz
Proposé par nos amis de l'université de Toulouse.

4. Proxy Filter

Comme mentionné plus haut, SquidGuard redirige les URL en function de sa base de données.

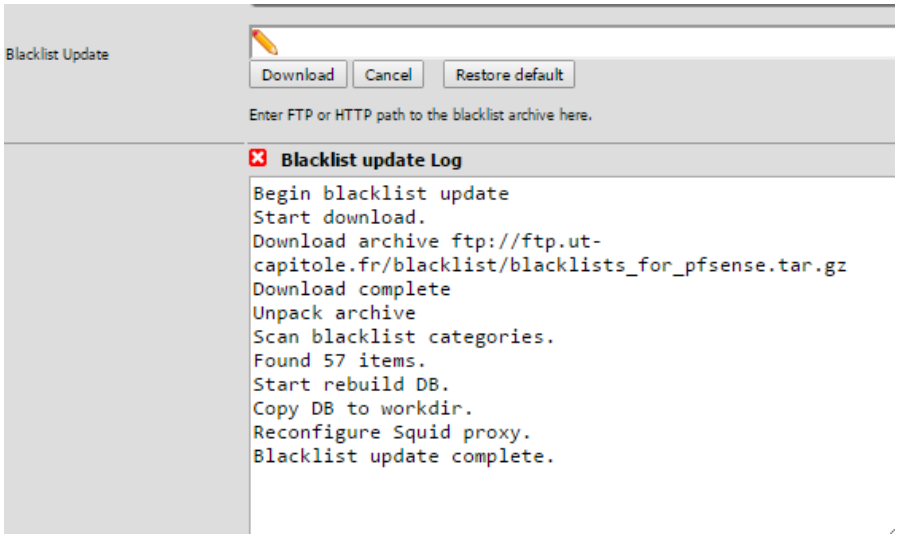
Il faut donc entrer ces listes dans les archives de SquiGuard.

4.1 Black List

Paramétrage de **Squidguard** dans le menu **« Services »**, cliquer sur **« Proxy filter ».**

Cocher la case « **Enable** » dans **General Settings.**

Configuration des listes :
Aller dans l'onglet « **General settings** » et cocher « **Blacklist** » dans la rubrique « **Blacklist options** ».



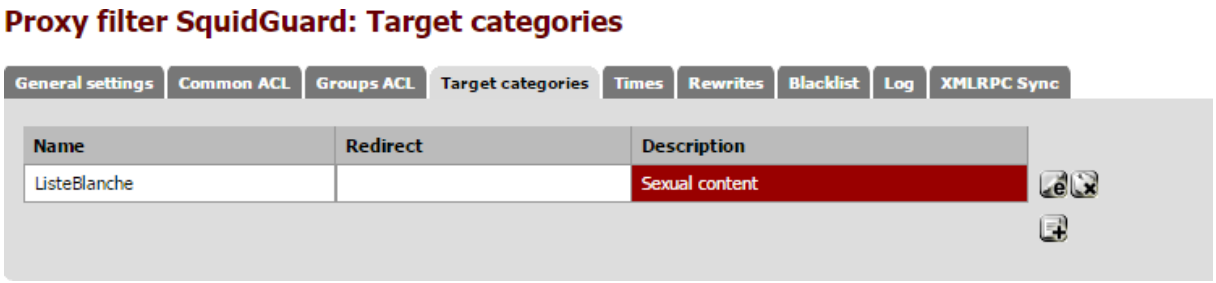
Ces listes sont acceptées en URL FTP ou HTTP.

Aller dans l'onglet « Common ACL » et cliquer sur l'icône comme indiqué ci-dessous :

La liste des listes configurées apparait et comme indiqué plus haut, tout est bloqué par défaut (dernière ligne : "Default access [all]" = deny).

4.2 Listes personnalisées

Afin de gérer plus finement les sites interdits, il est nécessaire, en plus des listes téléchargées de créer ses propres listes noires et liste blanche. Dans le menu « Services », cliquer sur « **Proxy filte**r », onglet « **Target categories** » pour ajouter des listes personnalisées.



Il est possible de bloquer un domaine entier comme 01net.com par exemple ou simplement une URL, il faut dans ce cas-là placer l'URL dans la catégorie « **URLs list** ».

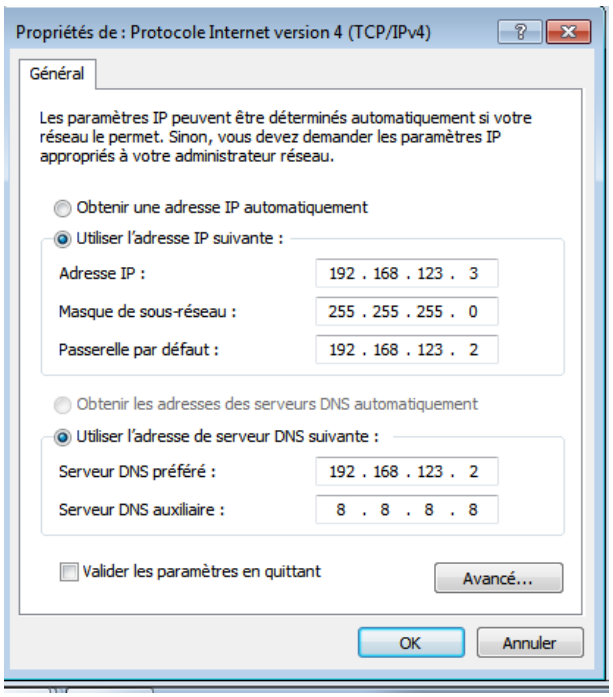
Il est également possible de filtrer par expressions, par exemple tous les sites dont l'URL contient « **jeux** », il faut à ce moment-là mettre « jeux » dans catégorie « **Expressions** ».

4.3 Vérification du proxy

Pour vérifier si nos configurations sont actives, nous allons virtualiser un **client** qui nous permettra, en lien avec le **serveur** PFSense, de simuler une navigation sous contrôle du Proxy.

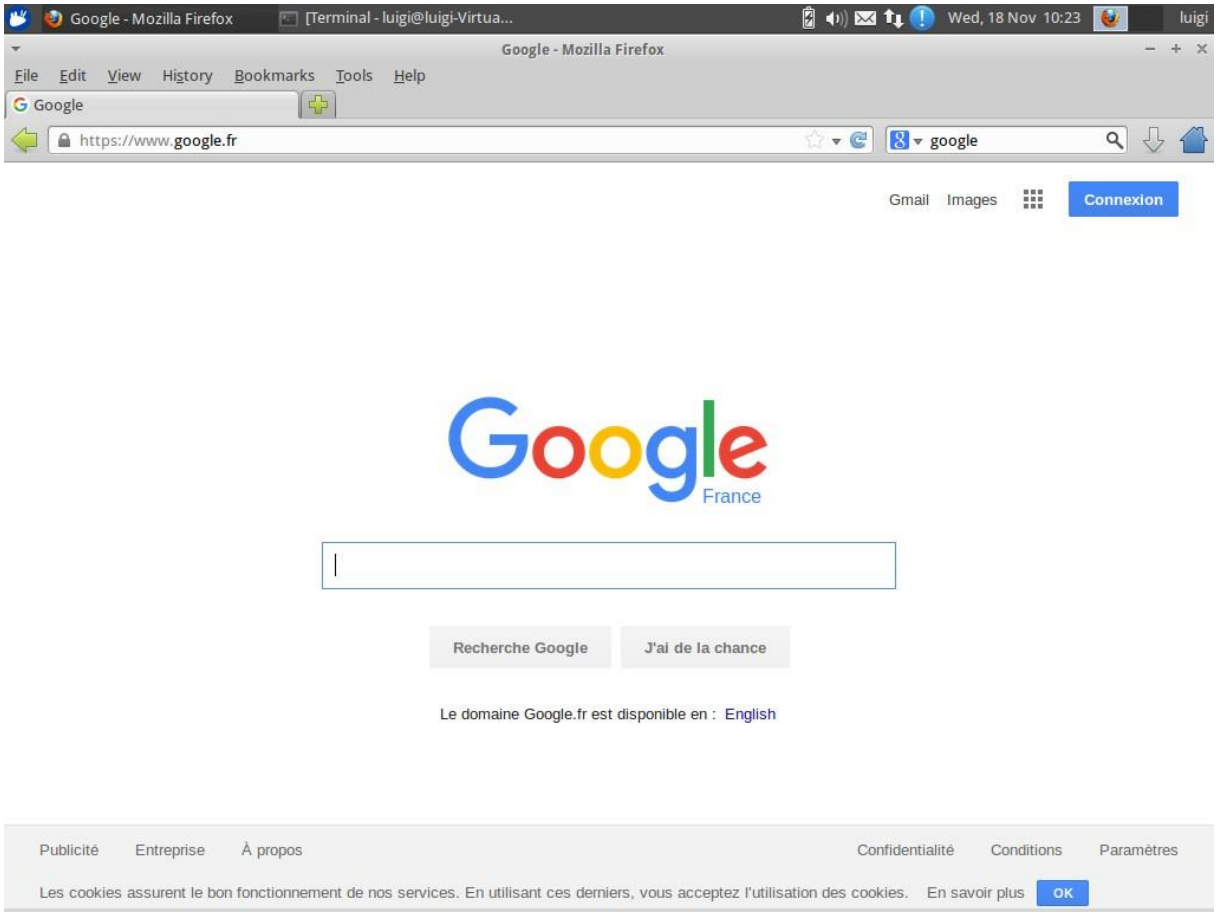
Pour se faire, nous allons utiliser une seule carte réseau, la même que la HostOnly du serveur PFSense pour simuler ces deux entités sur le même réseau. (em1 192.168.123.2)

Une fois votre client installé, mettre **l'IP fixe** du client sur la même plage réseau que la carte HostOnly, et changer les informations tel que suivit :

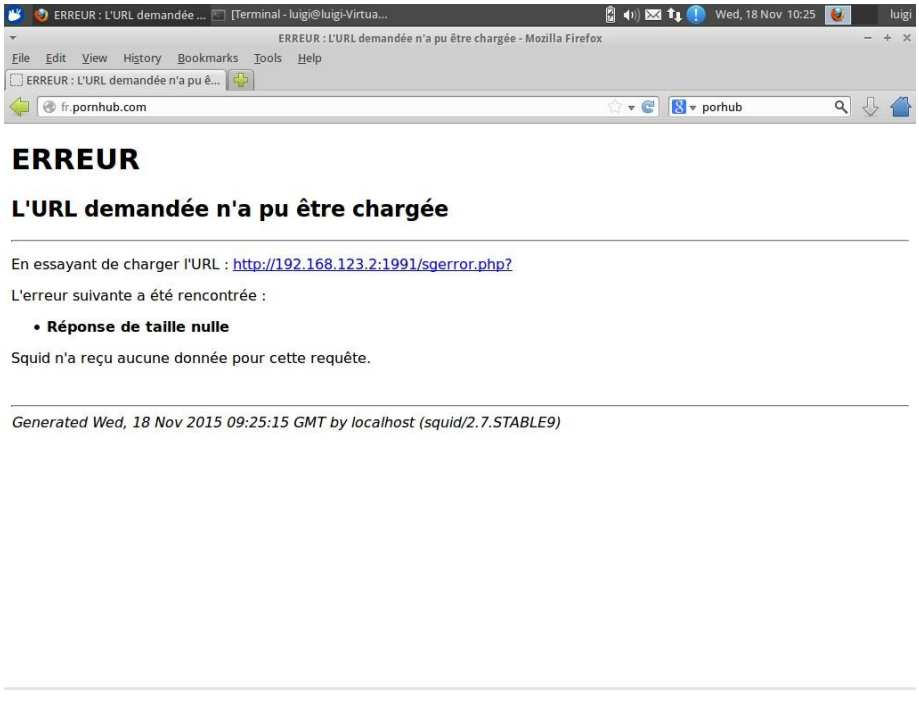


Cela nous permet donc d'avoir un accès internet en passant par le serveur PFSense.

Ouvrez une page de votre navigateur et voyons si la liaison avec internet se fait.

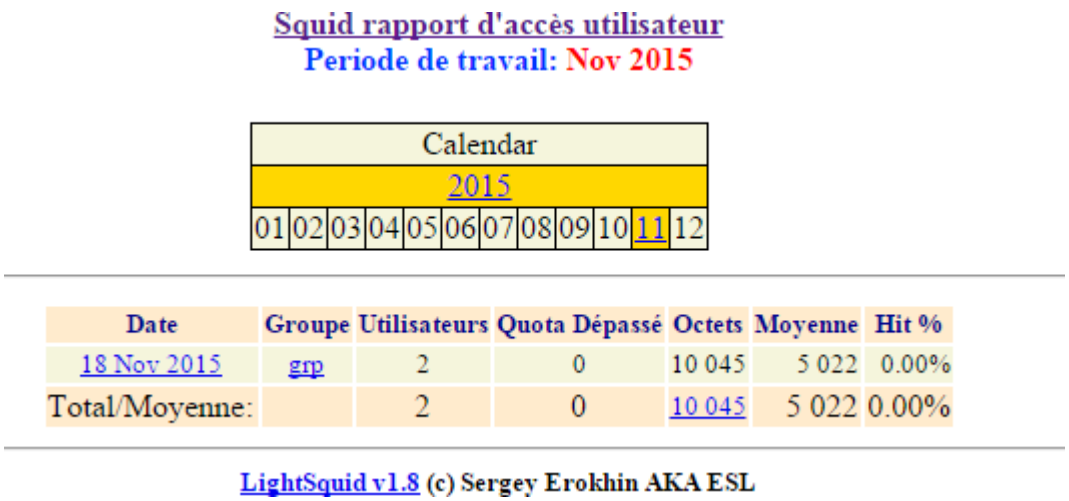


Bien ! Nous avons internet. Maintenant il nous faut aller sur un site blacklisté pour constater que notre proxy fonctionne bel et bien ; pour ma part, je vais aller sur un site avec du contenu interdit pour le vérifier.



4.4 Rapport d'activité

Le rapport d'activité, lié à **LightSquid**, permet d'instaurer un **rapport de navigation** sur chacun des postes du parc contrôlé par PFSense.



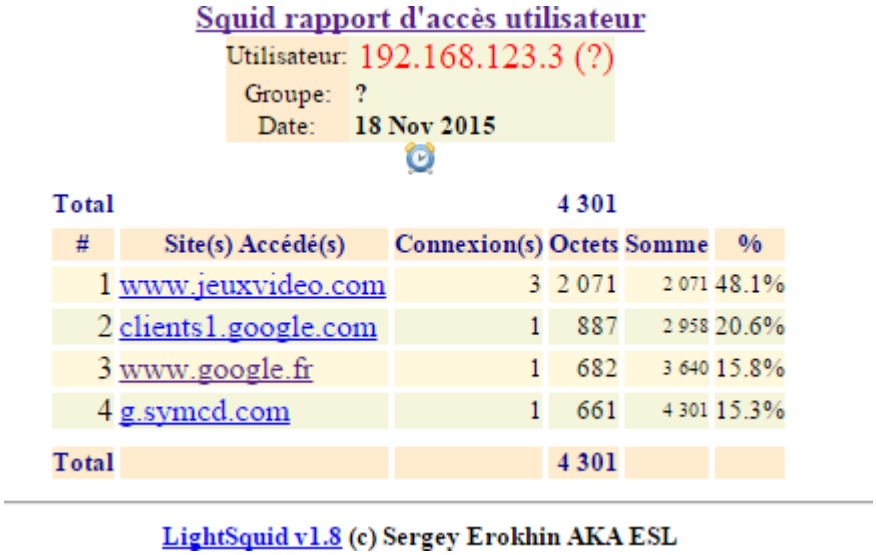
Squid rapport d'accès utilisateur
Periode de travail: Nov 2015

Calendar											
2015											
01	02	03	04	05	06	07	08	09	10	11	12

Date	Groupe	Utilisateurs	Quota Dépassé	Octets	Moyenne	Hit %
18 Nov 2015	grp	2	0	10 045	5 022	0.00%
Total/Moyenne:		2	0	10 045	5 022	0.00%

LightSquid v1.8 (c) Sergey Erokhin AKA ESL

Dans le menu « **Status** », cliquer sur « **Proxy report** » puis cliquer sur l'onglet « **Lightsquid Report** ». Cela affiche une fenêtre comme ci-dessus. Pour voir en détail chacun des historiques, cliquer sur le groupe de votre choix.



Squid rapport d'accès utilisateur
Utilisateur: 192.168.123.3 (?)
Groupe: ?
Date: 18 Nov 2015

Total 4 301

#	Site(s) Accédé(s)	Connexion(s)	Octets	Somme	%
1	www.jeuxvideo.com	3	2 071	2 071	48.1%
2	clients1.google.com	1	887	2 958	20.6%
3	www.google.fr	1	682	3 640	15.8%
4	g.symcd.com	1	661	4 301	15.3%
Total			4 301		

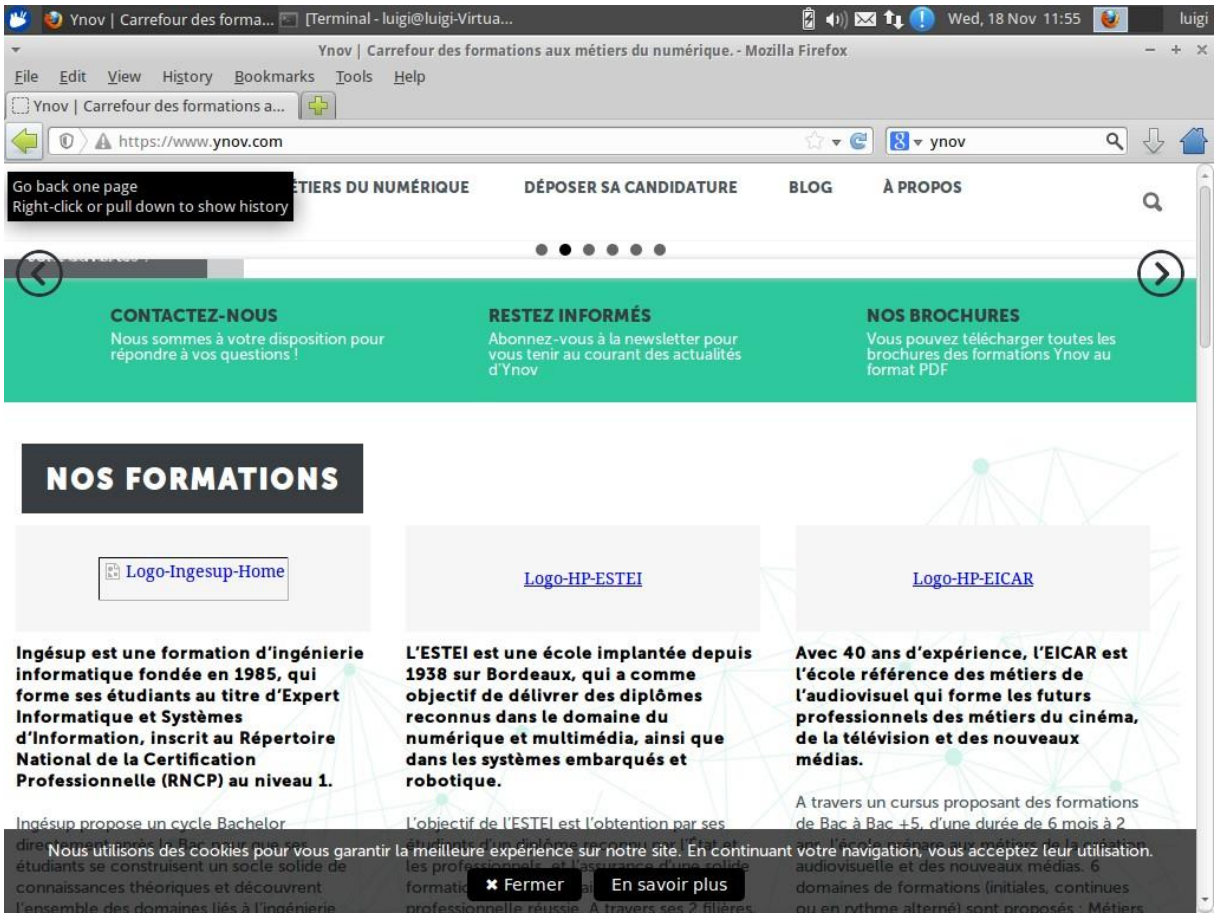
LightSquid v1.8 (c) Sergey Erokhin AKA ESL

L'administrateur dispose d'une pléiade d'information pour identifier l'utilisateur qui navigue sur cette multitude de site. Notamment son adresse IP (donc le poste) et le groupe auquel il appartient (donc le secteur d'activité).

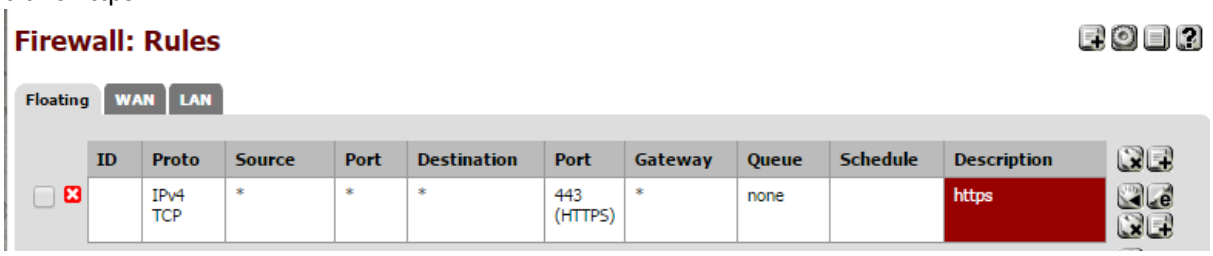
5. Firewall

Pour bien configurer le firewall, il est important de restreindre les accès en **HTTPS** (utilisant le protocole SSL) sur toutes les pages qui sont indiqués en **WhiteList**.

Nous allons donc procédé en plusieurs étapes. Pour ce faire, essayer de vous connecter en https sur une page de votre choix.



Bien. Nous pouvons donc voir que l'HTTPS est encore actif. Une fois cette vérification faite, dans le menu « **Firewall** », cliquer sur « **Rules** ». Dans l'onglet « **Floating** », créer une règle bloquant tout le trafic https.



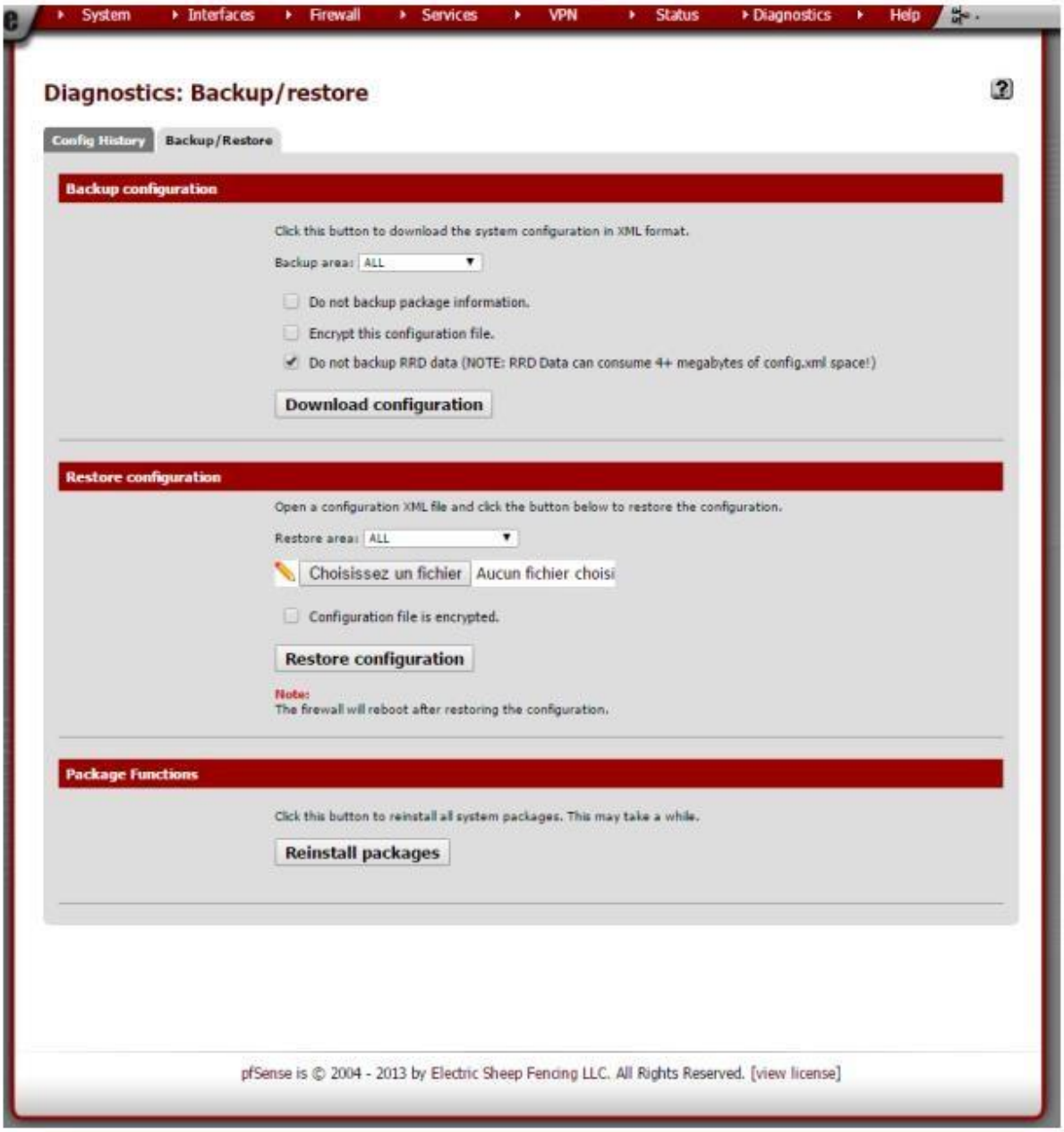
Attention, cette règle sera à répéter sur tous les onglets (WAN et LAN) des « **Rules** » du Firewall.

Mais certains sites en WhiteList ne peuvent fonctionner qu'en HTTPS, il faut donc créer des règles.

Pour créer une règle dans le pare-feu, il suffit, dans la section « **destination** » d'entrer l'IP du site voulu, et de choisir l'action « **allow** » au lieu de « **block** » comme utilisé précédemment.

6. Sauvegarde

PFSense fait automatiquement une sauvegarde de la configuration après chaque modification. Il est donc possible après une mauvaise manipulation de facilement revenir en arrière (un peu comme les points de restauration sous Windows). Pour voir les sauvegardes faites, aller dans « Diagnostics » puis « Backup/Restore » Onglet « Config History ».

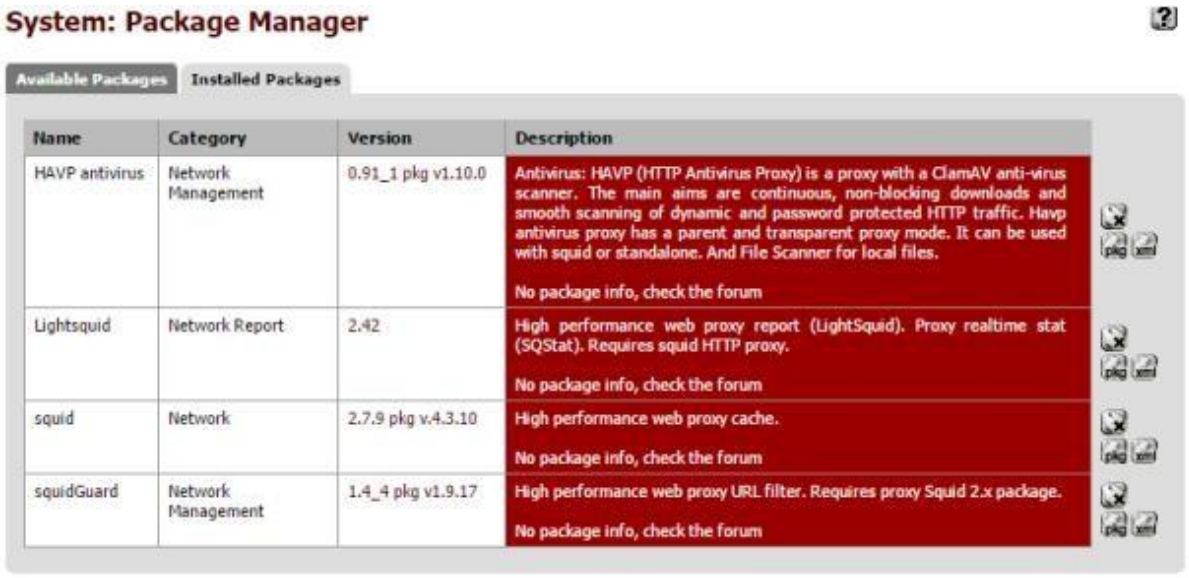


Cette configuration exporte la totalité des réglages en **XML**.

7. Antivirus

Tout parc informatique a besoin d'un **antivirus** pour se protéger de **logiciels malveillant**. PFSense propose donc ce service directement intégré à son interface.

Le package que nous allons installer en tant qu'antivirus s'appelle « HAVP antivirus »



Puis, dans l'onglet « settings », régler :

Mise à jour de la base de données toutes les 24 heures ;

Régler le **mirroir** sur « **Europe** » ;

Activer « **Log** » et « **Syslog** » ;