



Projet Personnalisé Encadré 4 (PPE4)

MISE EN PLACE D'UN FILTRAGE AVEC PFSENSE (FILTRAGE HTTPS)

Réalisé par Lacroix Werley

Table des matières

I-INTRODUCTION.....	6
a) Qu'est ce que Pfsense ?.....	7
b) Avantages et inconvénients.....	8
II-INSTALLATION ET CONFIGURATION DE PFSENSE.....	8
a) Paramétrage de Pfsense sous virtualbox.....	8
b) Installation de Pfsense.....	15
c) Configuration des IP.....	19
d) Configuration de l'interface web.....	21
III- INSTALLATION ET CONFIGURATION -FILTRE HTTP(S) AVEC SQUIDGARD. .	23
a) Création du certificat.....	24
b) Téléchargement du package Squid et squidgard.....	33
c) Configuration du proxy transparent pour HTTP.....	36
d) Activation de SquidGuard.....	38
e) Configuration de la liste noire.....	39
IV- TEST DU BON FONCTIONNEMENT DU PROJET.....	43
V- CONCLUSION.....	44

Index des images

Image 1: Schéma réseau.....	6
Image 2: Virtualbox.....	8
Image 3: Nom et système d'exploitation.....	9
Image 4: Taille de la mémoire.....	9
Image 5: Disque dur virtuel.....	10
Image 6: Type de fichier de disque dur.....	10
Image 7: Stockage sur disque dur physique.....	11
Image 8: Emplacement du fichier et taille.....	11
Image 9: Configuration VM.....	12
Image 10: Paramètre système VM.....	12
Image 11: Stockage VM.....	13
Image 12: Paramètre réseau VM.....	14
Image 13: Paramètre réseau carte 2.....	14
Image 14: Welcome to pfsense.....	15
Image 15: Information sur pfsense.....	15
Image 16: Install pfsense.....	16
Image 17: Sélection de Keymap.....	16
Image 18: UFS pfsense.....	17
Image 19: Copie des fichiers pfsense.....	17
Image 20: Manual configuration.....	18
Image 21: Installation complète.....	18
Image 22: Menu textuel pfsense.....	20
Image 23: Page de connexion pfsense.....	21
Image 24: Identifiant pfsense.....	21
Image 25: Page d'accueil pfsense.....	22
Image 26: Configuration interface WAN.....	23
Image 27: IPV6 Configuration type.....	24
Image 28: Cert.Manager.....	25
Image 29: Ajouter un nouveau certificat.....	25
Image 30: Create an internal Certificate Authority.....	26
Image 31: Information certificat.....	27
Image 32: Importation certificat.....	29
Image 33: Ouvrir certificat.....	29
Image 34: Installation certificat.....	29
Image 35: "Bienvenue" certificat.....	30
Image 36: Magasin certificat.....	30
Image 37: Fin de l'installation Importation de certificat.....	31
Image 38: Importation terminée.....	31
Image 39: Invite de commande .certmgr.....	32
Image 40: Utilisation du certificat créé.....	32
Image 41: Pfsense sécurisé.....	33

Image 42: Package manager.....	34
Image 43: Available packages.....	34
Image 44: Installation de squid.....	35
Image 45: Progression installation squid.....	35
Image 46: Installation terminée.....	35
Image 47: Activation du proxy squid.....	36
Image 48: Interface proxy LAN.....	37
Image 49: Activation filtre SSL.....	37
Image 50: CA-Pfsense.....	37
Image 51: Local Cache.....	38
Image 52: Activation Squidguard.....	39
Image 53: URL Blacklist.....	39
Image 54: Catégories blacklist.....	41
Image 55: Information blacklist.....	42
Image 56: Page web.....	43
Image 57: Page web non autorisée.....	43

Contexte : Une connexion wifi est proposée pour le personnel de l'agglomération d'Albi et des communes. Dans le cadre de ce PPE en organisation, nous souhaitons mettre en place un filtrage sur certains sites internet.

Objectif : Mise en place d'un filtrage d'URL via catégories (réseaux sociaux, sport...)

Matériels, logiciels : Un ordinateur Windows 10
Logiciel de virtualisation (Virtualbox)
2 machines virtuelles (Serveur Pfsense, machine Windows 7)

Difficultés rencontrées : Utilisation et compréhension de PFSense

Durée de la réalisation : Une semaine

Solutions possibles : Plusieurs solutions sont possibles pour le filtrage internet :

- La première solution consiste à se procurer un routeur sur lequel la distribution est déjà installée. Pfsense possède un store et propose à ses clients l'achat de ce type de matériel. Les prix, quant à eux, varient de 299€ à 2500€
- La deuxième solution, dans le cas où l'entreprise posséderait un ordinateur avec un logiciel de virtualisation, consiste à créer une machine virtuelle sur lequel serait hébergé Pfsense. L'avantage de ce cas de figure réside surtout dans le fait que le système est évolutif. En effet, les contraintes matérielles sont quasiment inexistantes puisqu'il est possible de changer "à la volée" les paramètres (processeur, RAM, espace disque) de la VM

Solution retenue : Utiliser un ordinateur avec un logiciel de virtualisation sur lequel pfsense est hébergé . Filtrage par HTTP.

Conditions initiales: Installation de VirtualBox prêt à l'emploi
Installation machine virtuelle windows 7 déjà installé et configuré.

Outils utilisés : Un ordinateur Windows 10
Un logiciel de virtualisation (VirtualBox)
Une machine virtuelle Windows 7
Une machine virtuelle (Serveur Pfsense)
Du réseaux

Résultat final : Un serveur Pfsense installé, Filtrage internet réussi

COMPÉTENCES MISES EN ŒUVRE

A1.1.1 Analyse du cahier des charges d'un service à produire
A1.1.3 Étude des exigences liées à la qualité attendue d'un service
A1.2.5 Définition des niveaux d'habilitation associés à un service
A1.3.1 Test d'intégration et d'acceptation d'un service
A1.3.4 Déploiement d'un service
A1.4.1 Participation à un projet
A2.1.2 Évaluation et maintien de la qualité d'un service
A3.1.1 Proposition d'une solution d'infrastructure
A3.2.1 Installation et configuration d'éléments d'infrastructure
A3.3.1 Administration sur site ou à distance des éléments d'un réseau, de serveurs, de services et d'équipements terminaux
A3.3.3 Gestion des identités et des habilitations
A5.2.3 Repérage des compléments de formation ou d'auto-formation utiles à l'acquisition de nouvelles compétences
A5.2.4 Étude d'une technologie, d'un composant, d'un outil ou d'une méthode

I-INTRODUCTION

Pfsense est un pare-feu open source que nous utilisons dans les écoles. Avec l'aide de Squid (un serveur proxy) et de SquidGuard (le filtre web actuel), nous voulons filtrer les connexions HTTP et HTTPS.

Pour réaliser ce projet, il me faut une machine physique équipée de Virtualbox et 2 machines virtuelles qui comprendront un serveur Pfsense et une machine Windows 7.

Schéma réseau

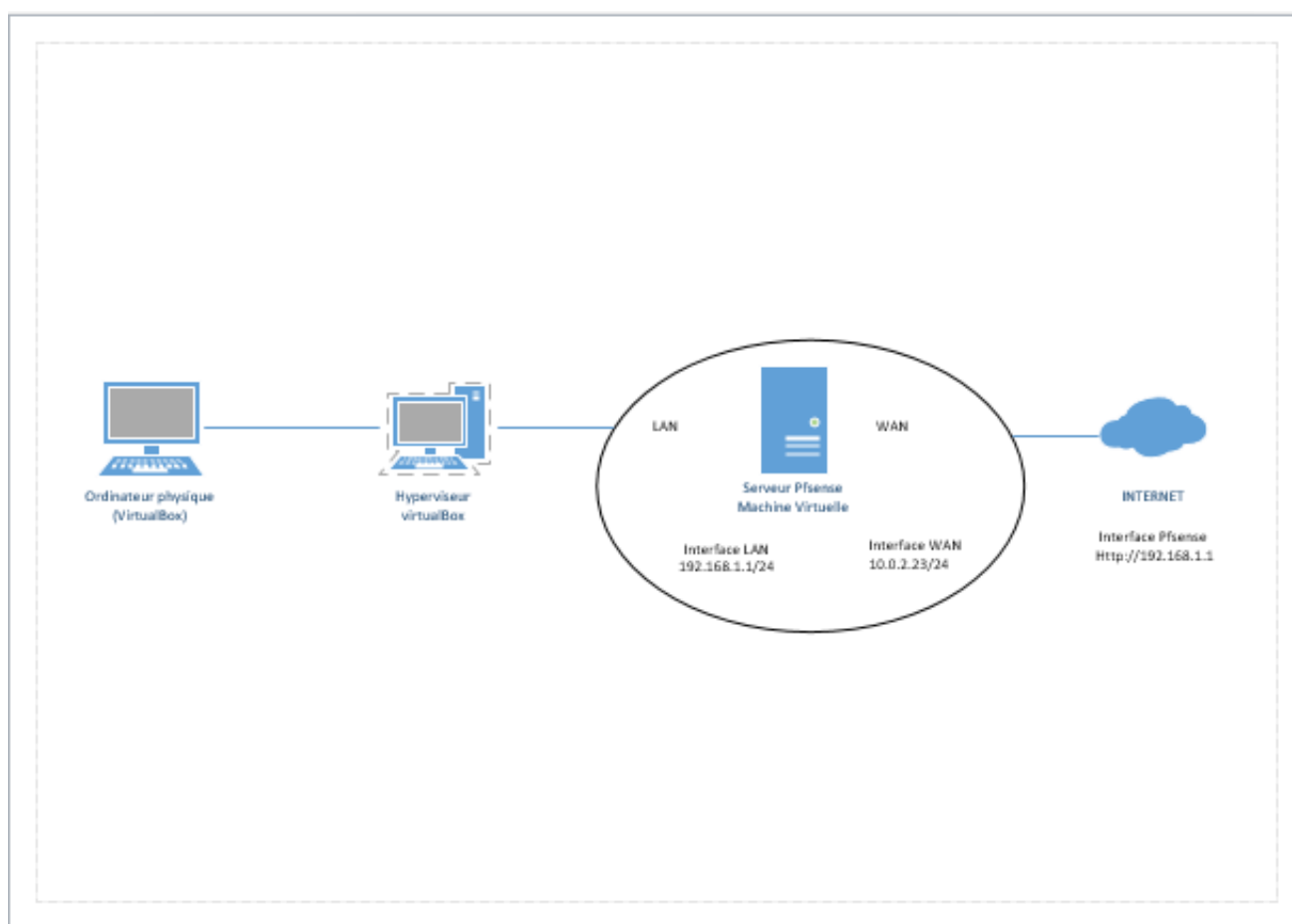


Image 1: Schéma réseau

a) Qu'est ce que Pfsense ?

PfSense est une distribution logicielle permettant de réaliser une passerelle réseau à partir d'un serveur x86. Il date de 2004 à partir d'un fork de m0n0wall par Chris Buechler et Scott Ullrich.

Très fréquemment rencontré dans les PME et les petites structures, pfSense offre une solution complète de routage, filtrage, VPN et partage de connexion et intègre un grand nombre de composants tiers : serveur DHCP/DNS, serveur de temps, proxy web, monitoring... La configuration se fait entièrement via une interface web.

pfSense est disponible sous licence BSD. Un support officiel est proposé par la société BSD Perimeter.

Il offre une solution de firewall complète pour les entreprises :

- **Filtrage**
- **NAT** (Network Address Translation ; Mécanisme de conversion d'adresses IP non routables (internes ou privées) en adresses IP routables (sur internet), mis en place pour pallier la carence d'adresses IPv4.)
- **VPN (IPSEC, SSL, ...)** *virtual Private Network* ». Traduit en français, « Réseau Privé Virtuel ».
- **Qualité de Service**
- **Gestion des VLAN** (Grace au Vlan un administrateur réseau pourra ainsi intervenir sur un secteur précis de l'entreprise. Ces propriétés apportent en fait une grande facilité de gestion.)
- **Serveur DHCP** (Un serveur DHCP (ou service DHCP) est un serveur (ou service) qui délivre des adresses IP aux ordinateurs qui se connectent sur le réseau)
- **Serveur DNS** (Le serveur DNS va permettre de faire la relation entre nom d'ordinateur et adresse IP)
- **Portail Captif**
- **Solution proxy**
- **Filtrage d'urls**
- **Antivirus sur certains flux**

b) Avantages et inconvénients

Comme toute solution de routeur/pare-feu, Pfsense possède son lot d'avantages et d'inconvénients. Mais sa polyvalence et le nombre conséquent de fonctionnalités font de cet outil une solution fiable pour les entreprises, et ce, quelles que soient la taille et l'activité de ces dernières.

Pfsense est très peu gourmand en termes de ressources. En effet, la configuration minimale requiert un processeur équivalent ou supérieur à 500Mhz quand la mémoire exigée est de 256Mo.

En revanche, et malgré les nombreux avantages de cette solution, il faudra s'assurer que la personne en charge de gérer le parc informatique ait les connaissances nécessaires pour déployer cette solution. Il faut du matériel parfaitement compatible avec FreeBSD notamment la carte réseau. PfSense a peu d'inconvénients sinon l'ergonomie qui peut toujours être améliorée, beaucoup de menus.

II-INSTALLATION ET CONFIGURATION DE PFSENSE

a) Paramétrage de Pfsense sous virtualbox

Le projet est réalisé à l'aide de machine virtuelle . Pour ma part j'utilise Virtualbox. Ne pas oublier de télécharger L'ISO de Pfsense

VirtualBox propose de virtualiser vos systèmes d'exploitation (OS) invités sur une machine hôte. Appelée hyperviseur, l'application supporte les systèmes Windows, Linux, Mac OS X, Solaris, Free BSD, etc.

Lien de téléchargement :
<https://www.virtualbox.org/>



Image 2: Virtualbox

Après l'installation vous pouvez démarrer Virtualbox. Une fenêtre s'ouvre. Cliquez sur le bouton « **Nouvelle** » en haut de la fenêtre du gestionnaire Virtualbox.

Sur l'écran vous verrez l'assistant qui vous demandera le minimum d'information dont il a besoin pour créer une VM, en particulier

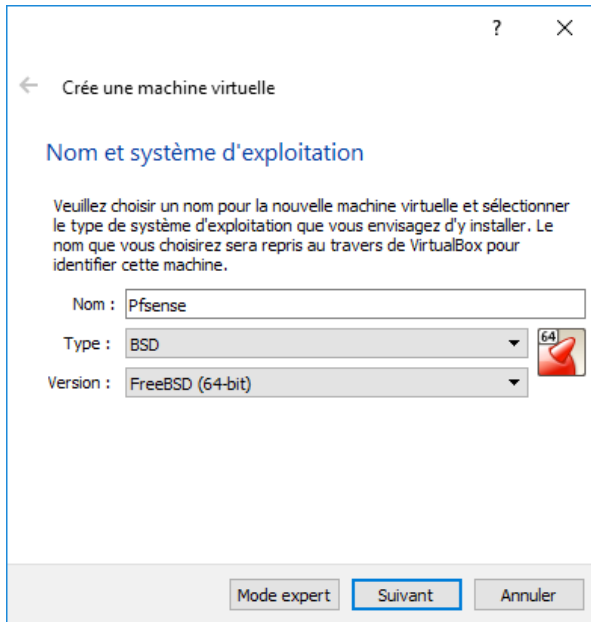


Image 3: Nom et système d'exploitation

1. **Le nom** de la Vm : Pfsense
2. **Le type** de système d'exploitation que vous voulez installer plus tard : BSD
3. **Version**: FreeBSD

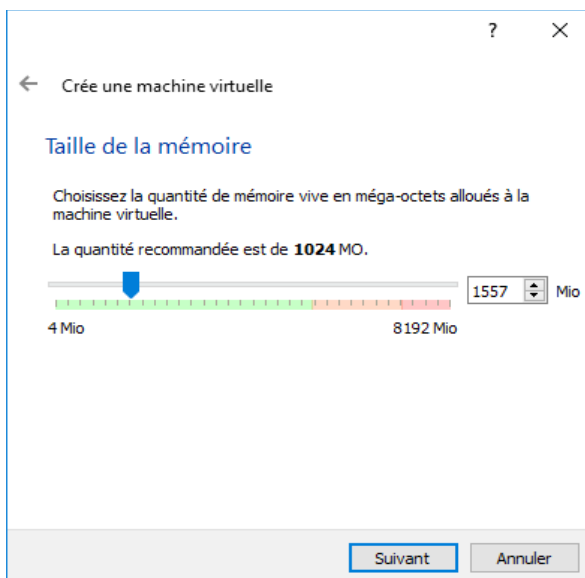


Image 4: Taille de la mémoire

Attribuer une certaine quantité de mémoire vive à la machine virtuelle.

Suivre les étapes sélectionnées

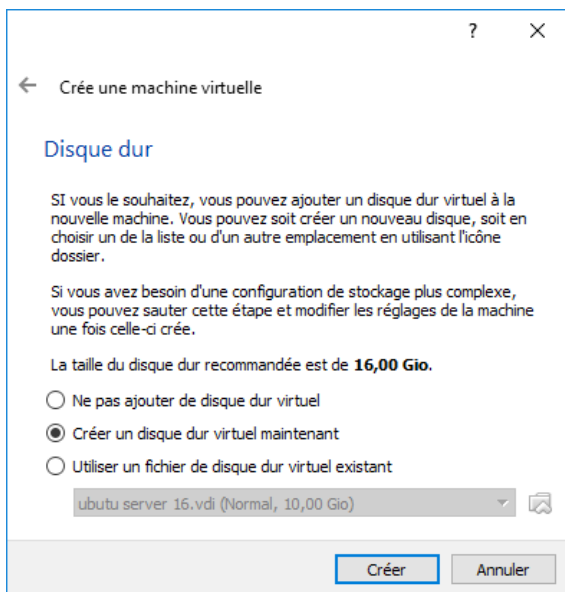


Image 5: Disque dur virtuel

Cochez VDI (cela permet non seulement d'éviter la mise à niveau matérielle des postes de travail, mais laisse aussi à l'utilisateur la possibilité de faire des va et vient entre des environnements systèmes différents)

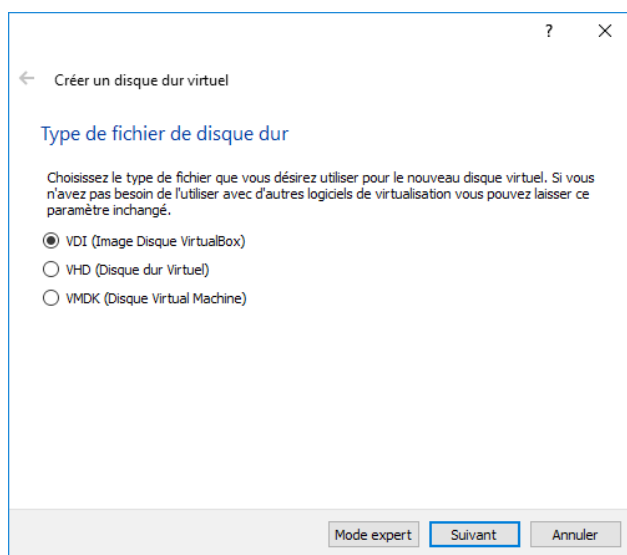


Image 6: Type de fichier de disque dur

VirtualBox propose deux modes pour la gestion de la taille des images disques : allocation dynamique ou taille fixe. Dans le premier cas, le fichier image est initialement créé avec une taille minimale et grossit au fur et à mesure que des données sont écrites jusqu'à atteindre la taille maximale configurée. En revanche, une image fixe, comme son nom l'indique, est créée dès le départ avec la taille demandée et occupe donc immédiatement sa capacité maximale sur le disque physique de l'hôte.

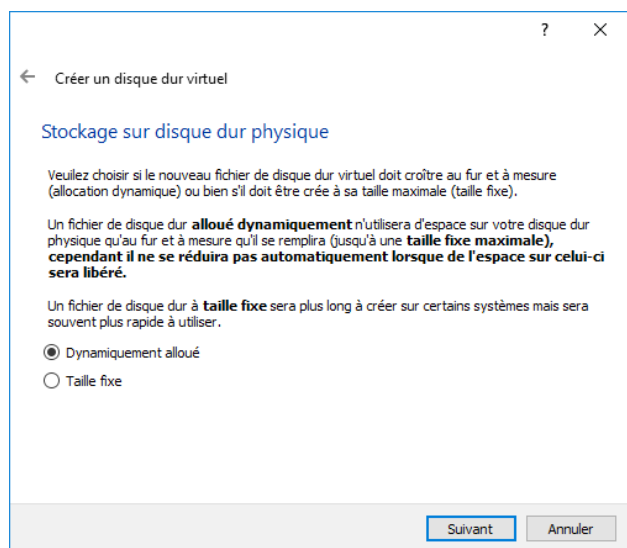


Image 7: Stockage sur disque dur physique

Choisir la taille du disque , lui attribuer un nom
Cliquer sur créer.

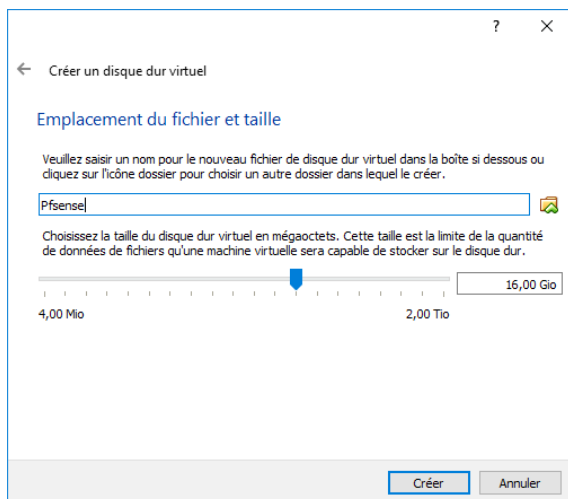


Image 8: Emplacement du fichier et taille

Cliquer sur la machine virtuelle et cliquer sur **Configuration**

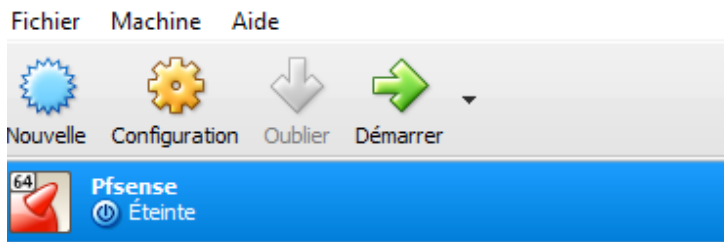


Image 9: Configuration VM

Dans processeur , mettez le nombre que vous voulez utiliser selon la capacité de votre machine. Pour une machine virtuelle ; deux processeurs sont suffisants.

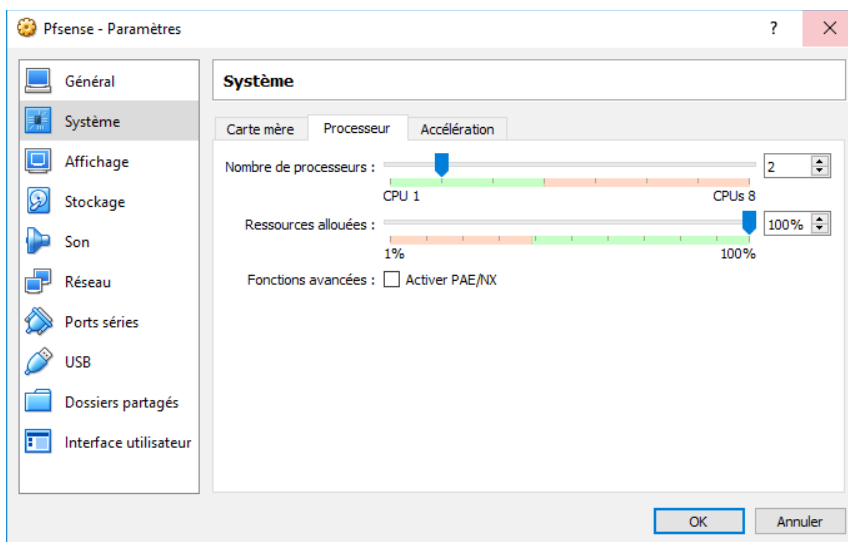


Image 10: Paramètre système VM

Dans stockage cliquer sur vide ensuite sur le petit cd à droite et sélectionner l'ISO télécharger et cliquer sur OK pour valider les modifications.

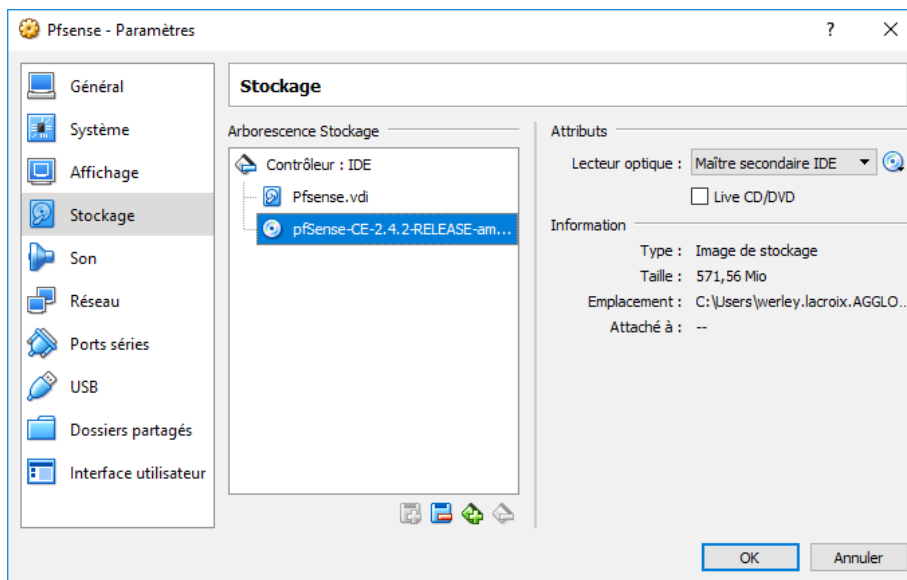


Image 11: Stockage VM

Un serveur Pfsense possèdent deux interfaces réseaux :

- Un interface LAN :il sera connecté en wifi au pc utilisateur
- Un interface WAN:il sera conecté au serveur web

interface réseau :partie qui assure la connexion entre un terminal utilisateur et un réseau public ou privé.

Configurer les deux cartes réseaux et appuyer sur OK pour terminer l'installation.

Dans ce mode, la carte réseau virtuelle est « pontée » à une carte réseau physique de l'hôte. La VM communiquera avec les autres machines du réseau de la même façon qu'une machine réelle, aussi bien avec l'hôte qu'avec les autres machines du réseau.

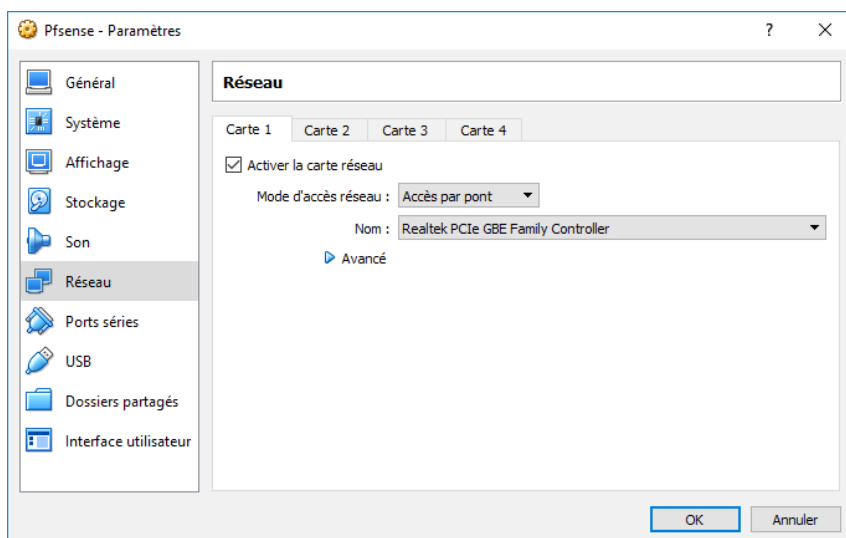


Image 12: Paramètre réseau VM

En mode NAT, la VM va utiliser la translation d'adresse, la machine hôte servant de passerelle et effectuant la translation d'adresse.

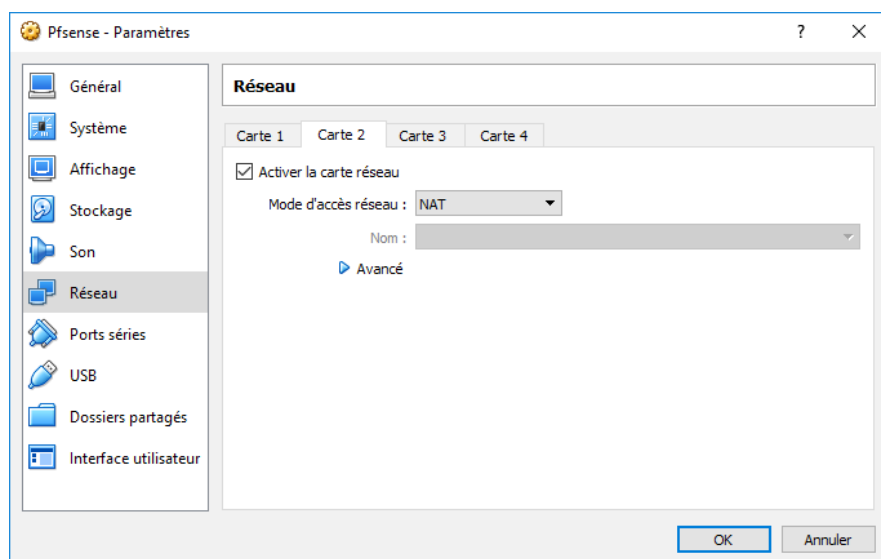


Image 13: Paramètre réseau carte 2

b) Installation de Pfsense

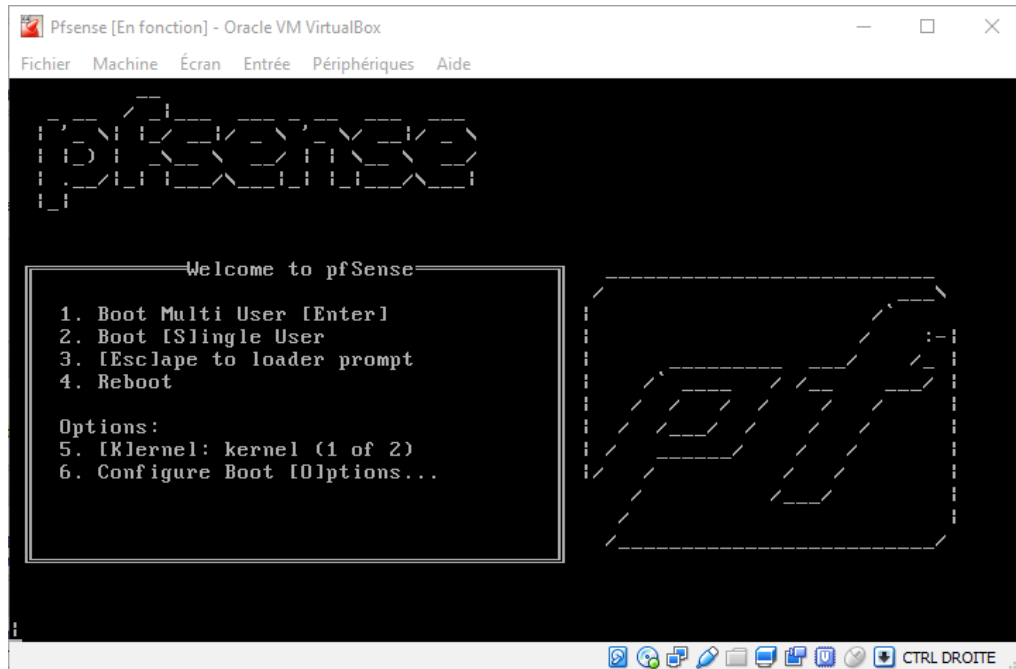


Image 14: Welcome to pfsense

Appuyer sur « **accept** »

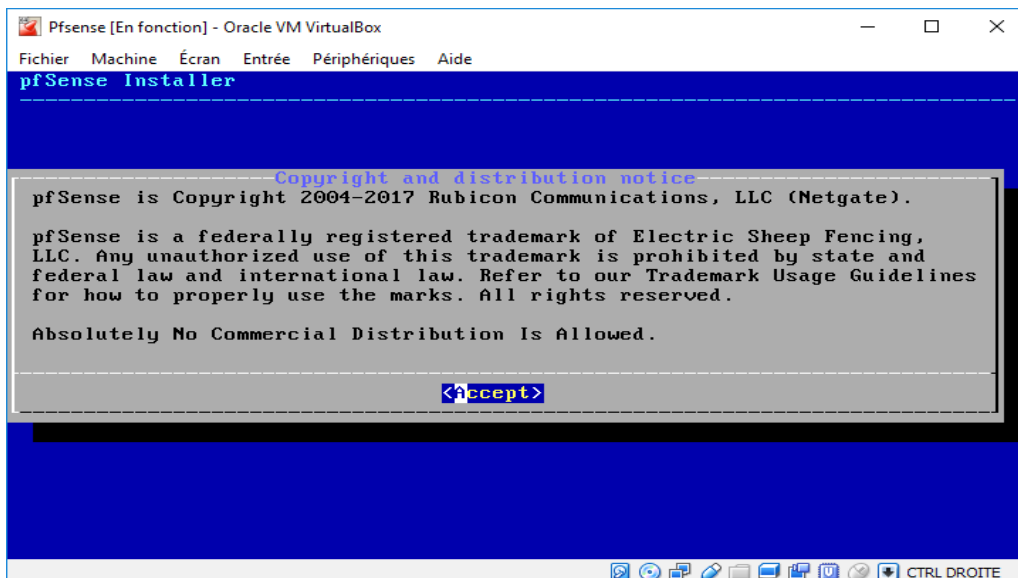


Image 15: Information sur pfsense

Pour la première installation cliquer sur « **install** »

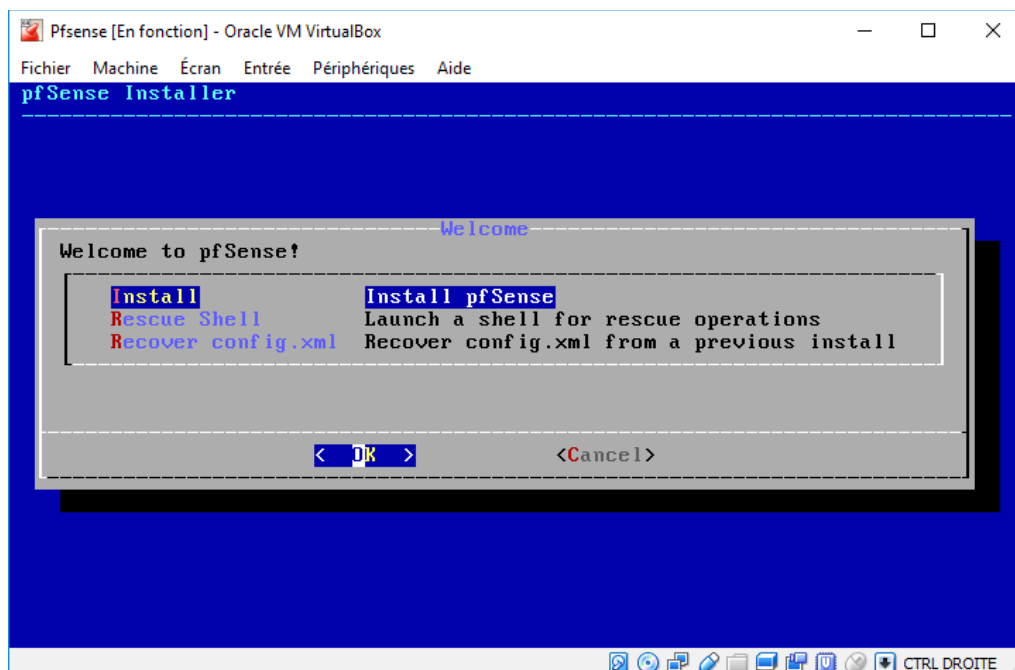


Image 16: Install pfSense

L'étape suivante permet la **sélection de Keymap** . Standard **US** est par défaut. Passez à l'étape suivante avec **Select** .

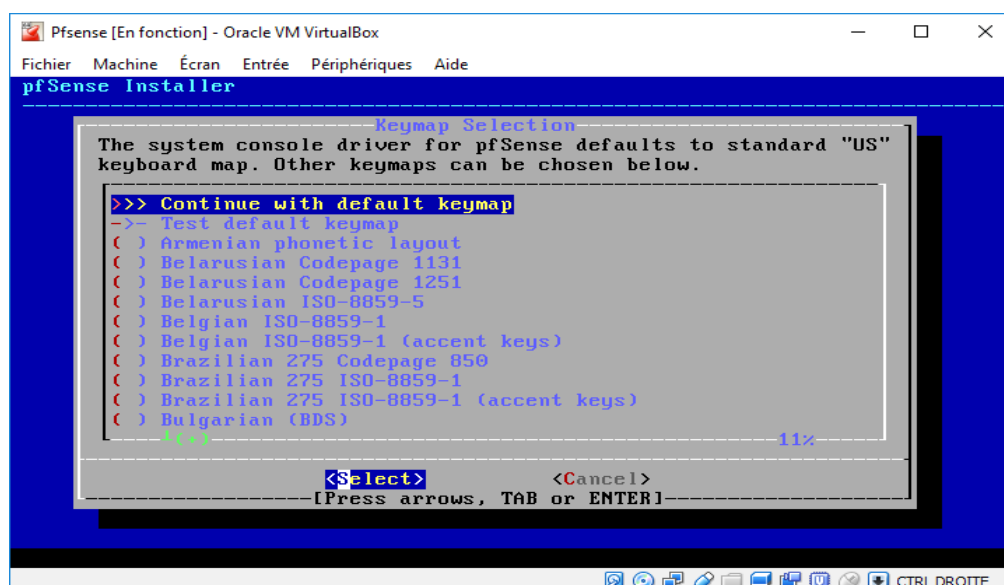


Image 17: Sélection de Keymap

L'étape suivante consiste à sélectionner le système de fichiers. Par défaut, **UFS** est sélectionné. Le support ZFS est actuellement expérimental. Sélectionnez **OK** pour continuer. Cette option configure automatiquement le disque dur.

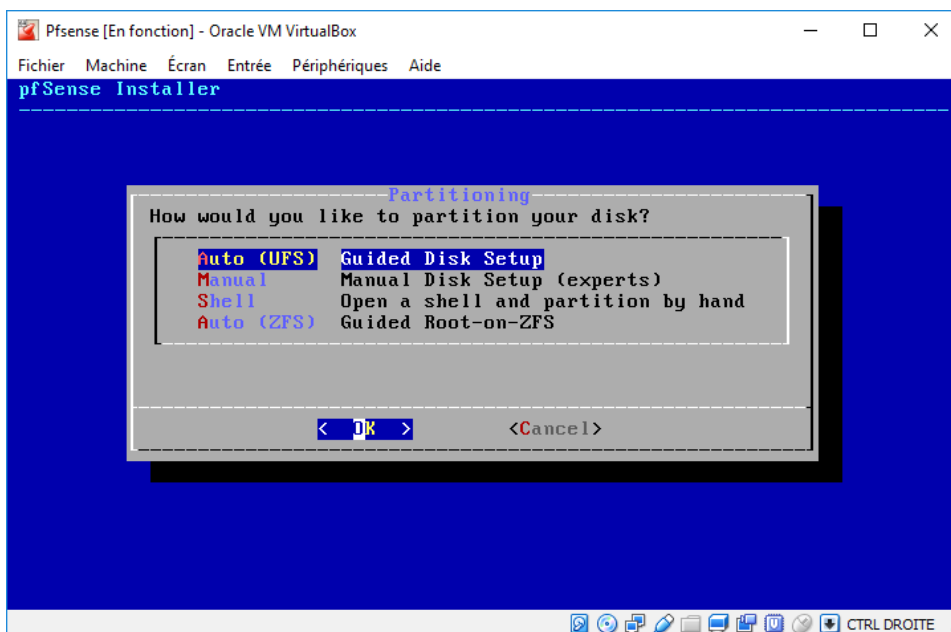


Image 18: UFS pfsense

UFS, abréviation de **Unix File System**, est un système de fichier utilisé par de nombreux systèmes d'exploitation de type Unix.

L'installation va continuer, essayant le disque cible et installant pfSense. La copie des fichiers peut prendre un certain temps pour terminer.

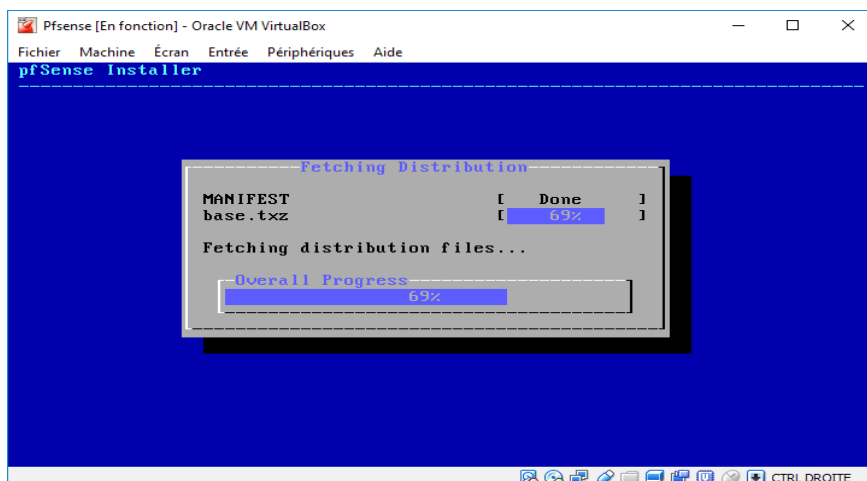


Image 19: Copie des fichiers pfsense

Une fois les options de configuration manuelle de l'installation terminées, sélectionnez **Non** pour continuer.

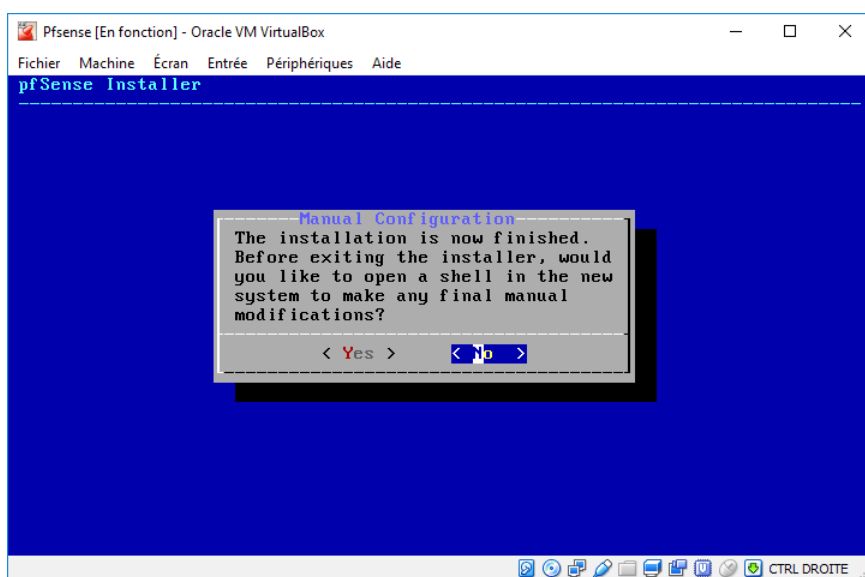


Image 20: Manual configuration

Maintenant, le système doit redémarrer pour que pfSense puisse démarrer à partir du disque cible. Sélectionnez **Reboot**, puis appuyez sur **Entrée**. Assurez-vous de retirer le disque ou la clé USB afin que le système n'essaie pas de démarrer à partir de là, la prochaine fois.

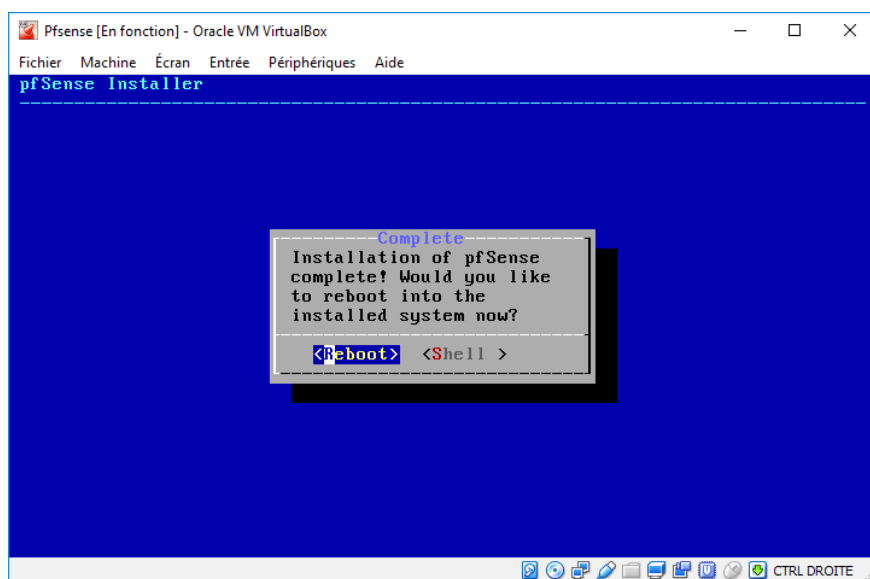


Image 21: Installation complète

Après le redémarrage du système, pfSense sera exécuté à partir du disque cible.

c) Configuration des IP

PfSense comme tous les routeurs est généralement utilisé pour connecter deux ou plusieurs réseaux, tels que:

- un sans fil à un réseau câblé (un routeur sans fil)
- un réseau interne (local) vers un réseau externe (par exemple internet)

PfSense® a également besoin d'une adresse IP pour fonctionner dans votre LAN, et par défaut, il utilise **192.168.1.1**, qui est l'adresse IP la plus couramment utilisée

Pour de nombreuses applications, cette adresse par défaut fonctionne très bien, ce qui explique probablement pourquoi c'est l'adresse par défaut.

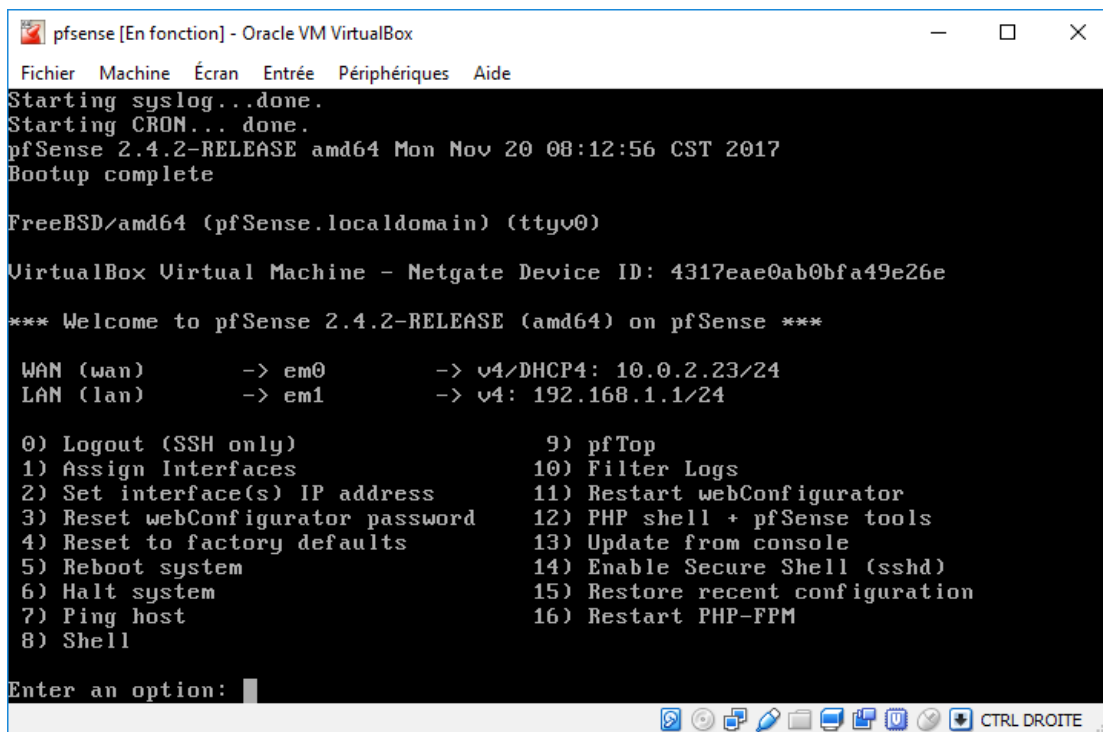
Cependant, il n'est pas du tout rare que d'autres équipements (par exemple un point d'accès sans fil ou un modem ADSL) utilisent exactement la même adresse.

Pour que votre réseau local fonctionne correctement, chaque périphérique doit avoir une adresse unique dans le réseau.

Cela signifie que si deux appareils utilisent la même adresse (192.168.1.1), aucun d'eux ne fonctionnera.

La solution simple est de changer l'un ou les deux pour utiliser une adresse différente.

À la fin du processus, la machine redémarre puis propose un menu textuel comme on peut le voir sur la figure suivante



```
pfsense [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Starting syslog...done.
Starting CRON... done.
pfSense 2.4.2-RELEASE amd64 Mon Nov 20 08:12:56 CST 2017
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 4317eae0ab0bfa49e26e

*** Welcome to pfSense 2.4.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.23/24
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: 
```

Image 22: Menu textuel pfsense

plan réseaux :

WAN : 10.0.2.23/24

LAN : 192.160.1.1/24

d) Configuration de l'interface web

Accéder à l'interface web en entrant l'ip *lan* dans un navigateur pour moi 192.160.1.1 vous arrivez sur la page de connexion de PfSense dont les identifiants sont :

Username :admin

mot de passe : pfsense

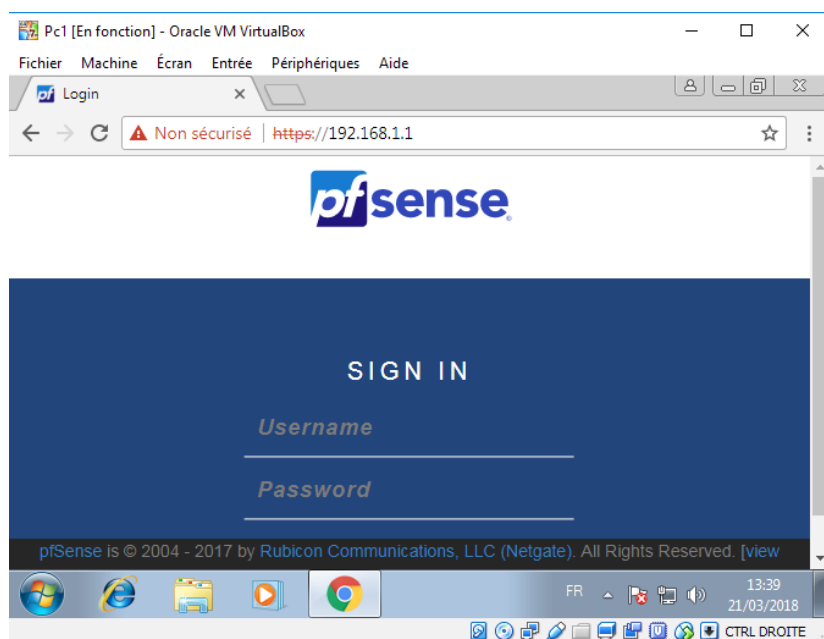


Image 23: Page de connexion pfsense



Image 24: Identifiant pfsense

Lors de la connexion nous remarquons quel est pas sécurisée. Nous nous en occuperons plus tard.

Nous accédons au tableau de bord de Pfsense

le nom

la version de pfsense ect.....

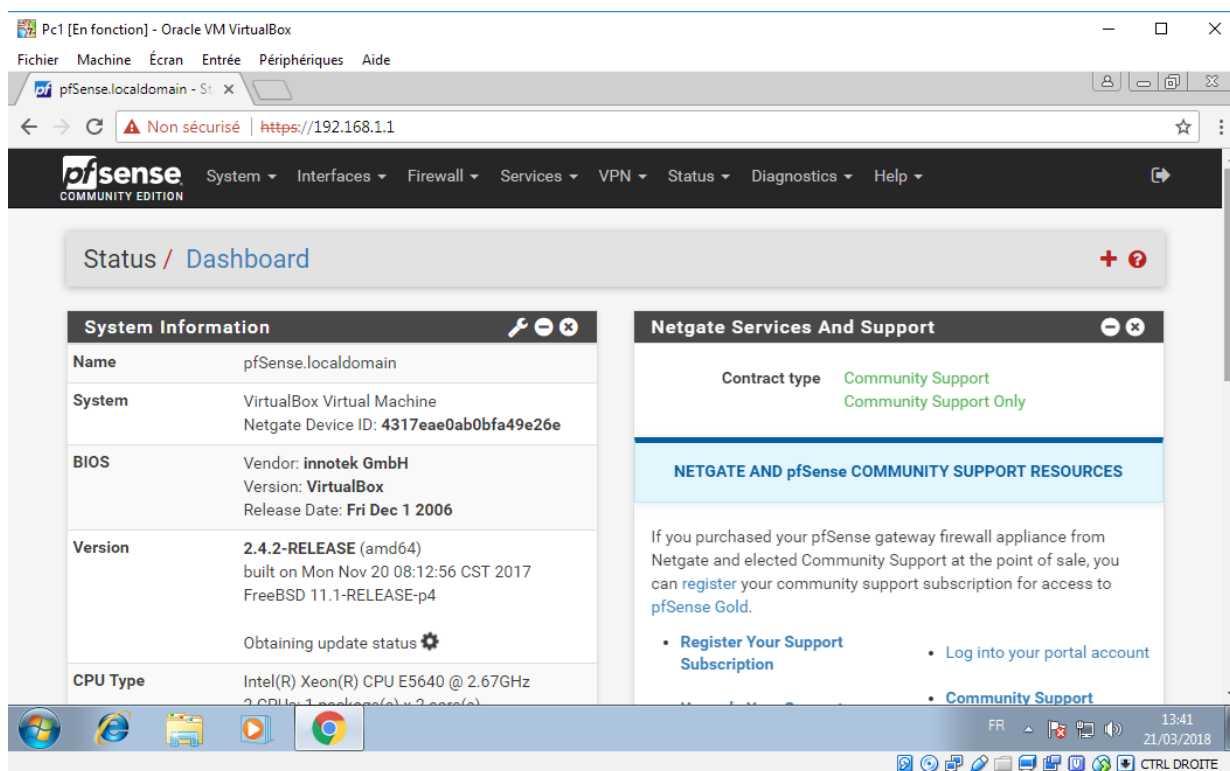


Image 25: Page d'accueil pfsense

III- INSTALLATION ET CONFIGURATION - FILTRE HTTP(S) AVEC SQUIDGARD

Pfsense est un pare-feu open source. Avec l'aide de Squid (un serveur proxy) et de SquidGuard (le filtre web actuel), nous voulons filtrer les connexions HTTP et HTTPS. Pour ce tutoriel, nous avons besoin d'une installation active de pfSense.

Comment ça marche ?

De nos jours, de plus en plus de sites (même ceux que vous souhaitez bloquer) utilisent HTTPS, c'est-à-dire une connexion cryptée entre le navigateur de l'utilisateur et le serveur web. Pour cela nous allons créer aussi un certificat, car cela augmente la sécurité et rend de nombreuses attaques impossibles ou plus difficiles. Cependant, cela rend également le filtrage des contenus indésirables plus difficile.

Avant de commencer configurer l'interface WAN

Cliquez sur **Interfaces** puis sur **WAN**

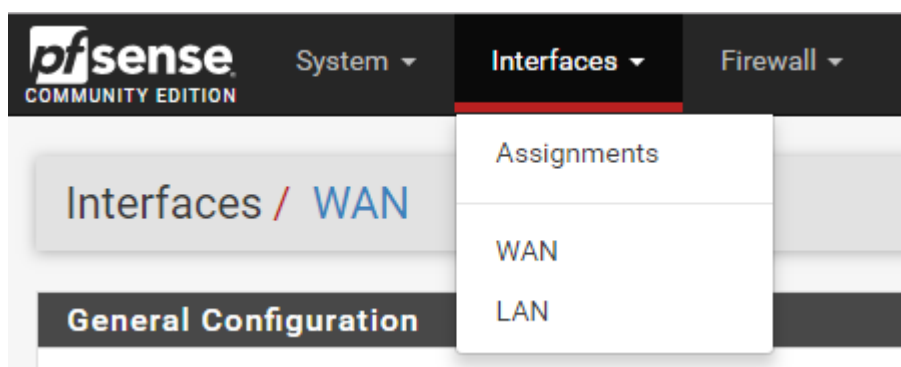
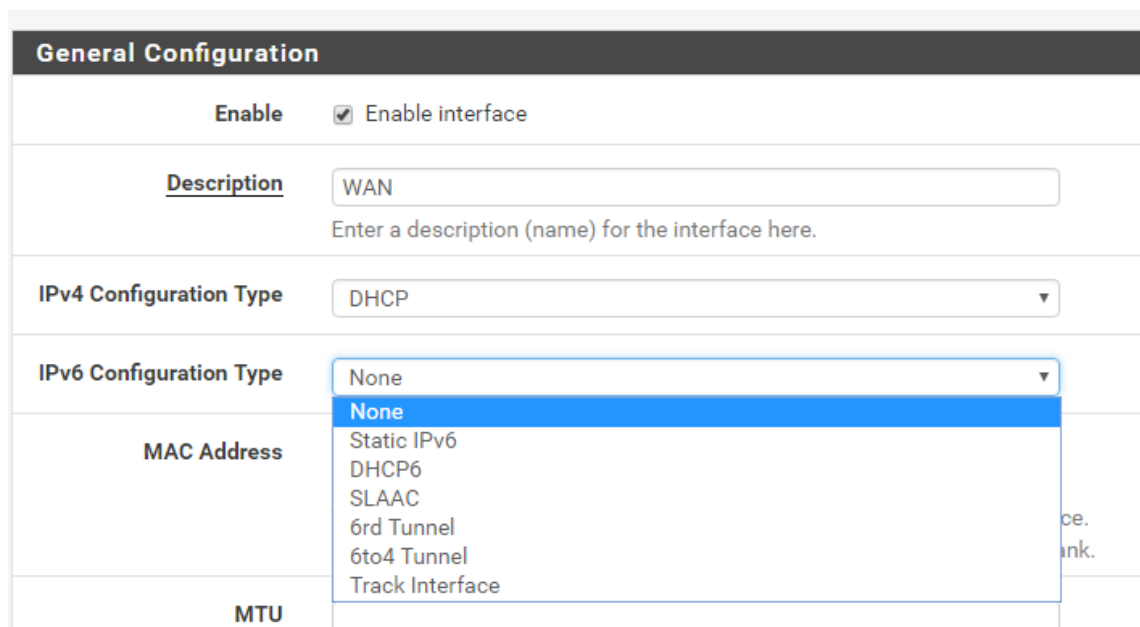


Image 26: Configuration interface WAN

Sur IPV6 Configuration Type cliquer sur **None**
Pour ma part je n'utilise pas d'adresse IPV6



General Configuration

Enable ☒ Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address

MTU

Image 27: IPV6 Configuration type

a) Création du certificat

Créer un certificat SSL dans pfSense (ou en importer un) Récupérer ce certificat et l'installer dans les machines qui devront accéder au proxy transparent (sans quoi toutes les pages visitées en HTTPS seront en échec).

Avant de pouvoir commencer l'interception SSL et le blocage des sites, il faut créer une autorité de certification dans votre pfSense. En effet, nous considérons que celui-ci est votre routeur principal sur le réseau tous les utilisateurs vont / devront passer par pfSense pour pouvoir accéder au net. C'est donc pfSense qui va se charger d'être (en plus le routeur) le « déchiffreur » et le bloqueur.

La création d'un « **Certificat Authorities** » dans pfSense se fait via le menu « **System** » puis sur « **Cert. manager** ». Utilisez le bouton vert « + Add » pour créer un nouveau certificat. Remplissez bien toutes les lignes de façon correct, pour avoir un certificat et une autorité fiable et réelle.

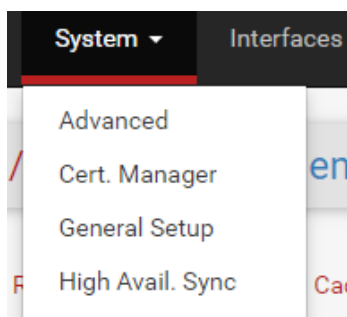


Image 28: Cert.Manager

Cliquer sur **Add** pour créer un nouveau certificat

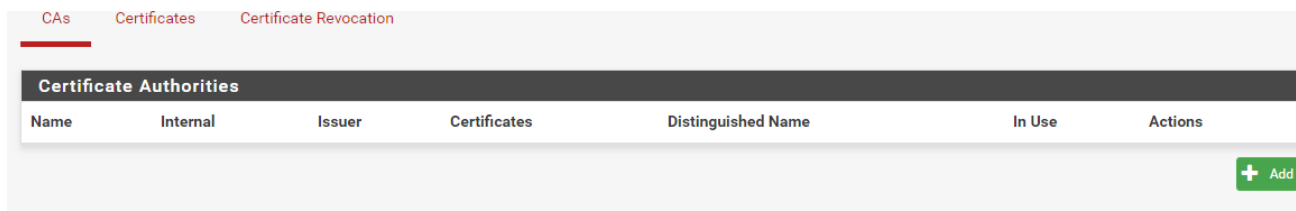


Image 29: Ajouter un nouveau certificat

Cliquer sur **Method** et Sélectionner **Create an Internal Certificate Authority**

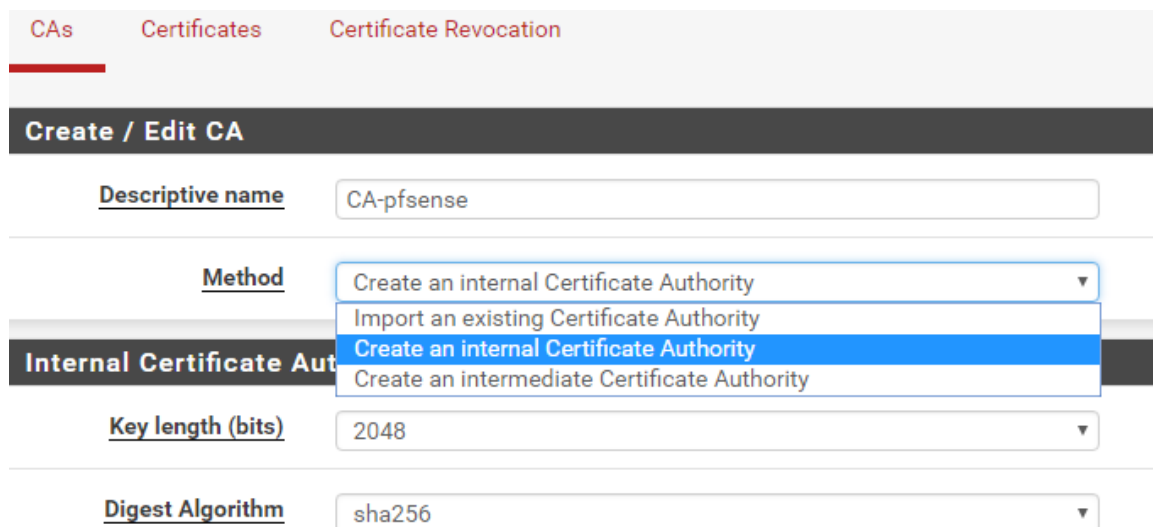


Image 30: Create an internal Certificate Authority

Un certificat permet d'associer une clé publique à une entité (une personne, une machine, ...) afin d'en assurer la validité. Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé *autorité de certification* (souvent notée **CA** pour *Certification Authority*)

Compléter le fichier

nommer le certificat : pour ma part je l'ai nommé **CA-pfsense**

CA
Certificates
Certificate Revocation

Create / Edit CA

Descriptive name
CA-pfsense

Method
Create an internal Certificate Authority

Internal Certificate Authority

Key length (bits)
2048

Digest Algorithm
sha256

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

Lifetime (days)
3650

Country Code
FR

State or Province
France

City
Albi

Organization
AC2A

Organizational Unit
AC2A

Email Address
AC2A@pfsense.com

Common Name
pfsense-internal-ca

Save

Image 31: Information certificat

Les champs à renseigner sont les suivants :

- **Method** : 3 méthodes sont possibles :
 1. Import an existing Certificate : permet d'importer la clé publique et la clé privée d'un certificat existant
 2. Create an internal Certificate : permet de créer un nouveau certificat
 3. Create a certificate Signing Request : permet de créer un fichier de requête qui pourra être envoyé à un CA tiers pour être signé. Cela peut être utile pour obtenir un certificat d'un CA root de confiance.

Dans notre cas, nous créons un nouveau certificat (***Create an internal Certificate***).

- **Descriptive name** : le nom que l'on souhaite donner à notre certificat serveur.
- **Method** : l'autorité de certification qui signera le certificat que nous sommes en train de créer. Dans notre cas, nous choisissons le CA que nous venons de créer.
- **Key length** : la longueur de la clé de chiffrement du certificat. Plus elle est longue, plus elle sera sécurisée (mais plus la charge CPU sera grande également...). Nous gardons la valeur par défaut : 2048
- **Digest Algorithm** : la fonction de hachage qui sera utilisée. Nous gardons la valeur par défaut : SHA256.
- **Lifetime** : la durée de vie du certificat. Si nous n'avons pas de raison de réduire sa durée de vie, nous laissons la valeur par défaut (10 ans).
- **Distinguished name** : l'ensemble de ces champs sont principalement cosmétiques et doivent permettre d'identifier l'organisation émettrice du certificat. Par défaut, l'ensemble des champs sont pré-complétés avec les informations issues du CA. Le seul élément important est le "Common name" dans lequel il ne doit pas y avoir d'espace (il est possible d'en mettre, mais cela peut poser des problèmes...) et qui doit, rester unique.

Après avoir créé le certificat d'autorité, il faut l'exporté en cliquant sur l'étoile

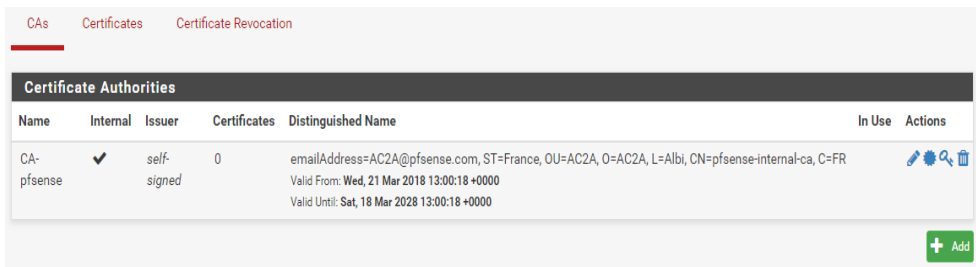


Image 32: Importation certificat

Afin d'empêcher les navigateurs Web sur les ordinateurs clients d'afficher des erreurs de certificat, le certificat CA de l'autorité de certification pfSense doit être installé sur tous les ordinateurs clients qui utiliseront le serveur proxy.

Pour installer un certificat, ouvrir le certificat

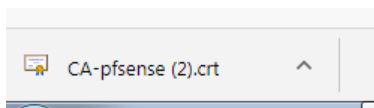


Image 33: Ouvrir certificat

et choisir **Installer le certificat**

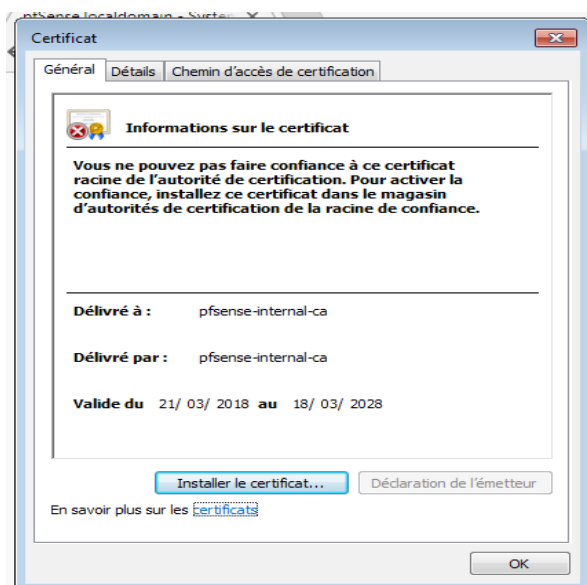


Image 34: Installation certificat

cliquer sur **suivant**

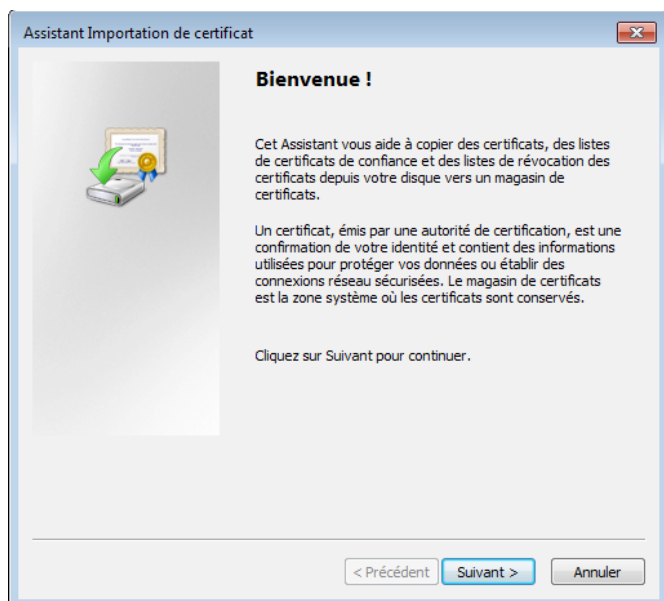


Image 35: "Bienvenue" certificat

Sélectionner selon l'image suivante

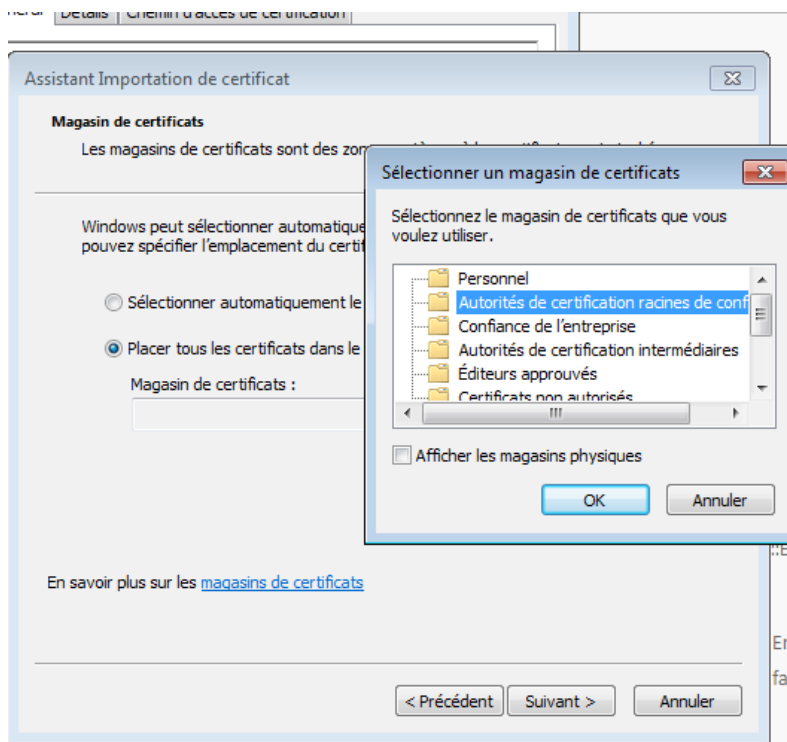


Image 36: Magasin certificat

Cliquer sur **Terminer** pour la fin de l'installation

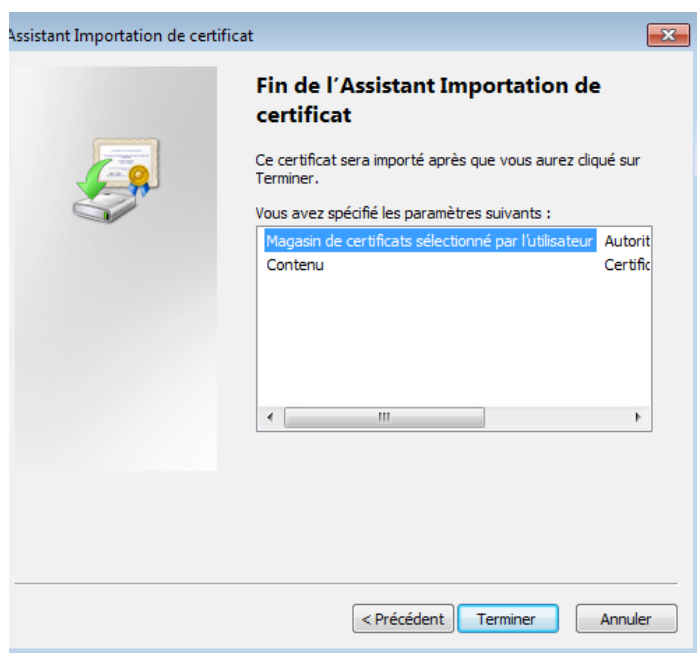


Image 37: Fin de l'installation Importation de certificat

confirmation de l'installation

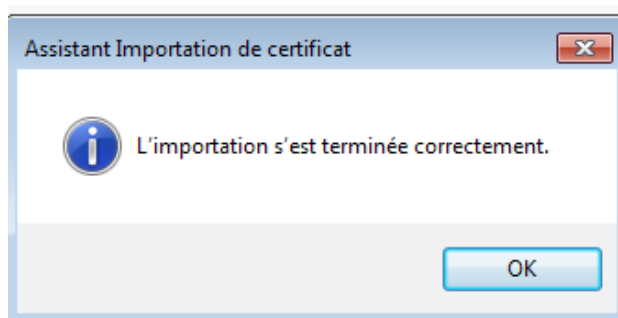


Image 38: Importation terminée

Nous pouvons vérifier que le certificat que nous avons créé est bien présent.
Dans l'invite de commande ouvrir **.certmgr**

.certmgr : L'outil Certificate Manager (Certmgr) gère les certificats, les listes de certificats de confiance (CTL) et les listes de révocation de certificats (CRL).

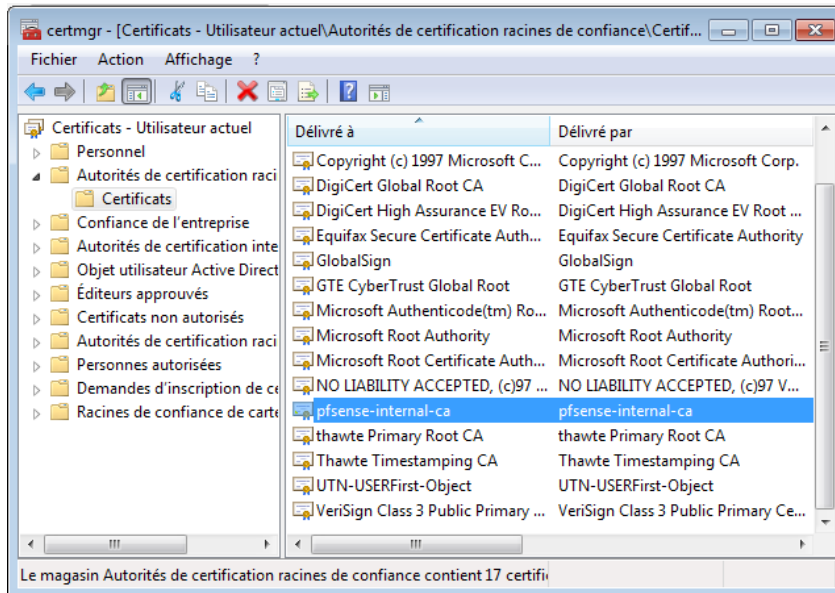


Image 39: Invite de commande .certmgr

Utiliser le certificat créé

Aller dans **System/Advanced/ Admin Acces**

Au niveau de SSL Certificate placer le certificat puis valider

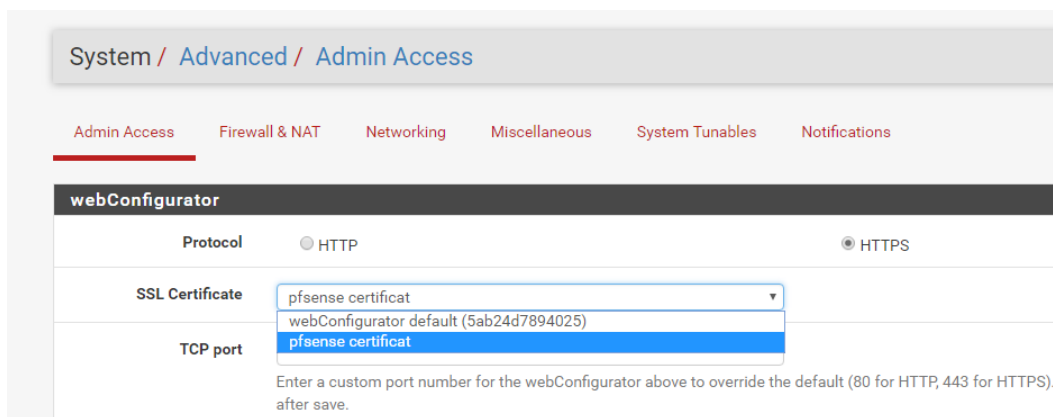


Image 40: Utilisation du certificat créé

Pfsense redémarre sur une page Web « plus sécurisé »

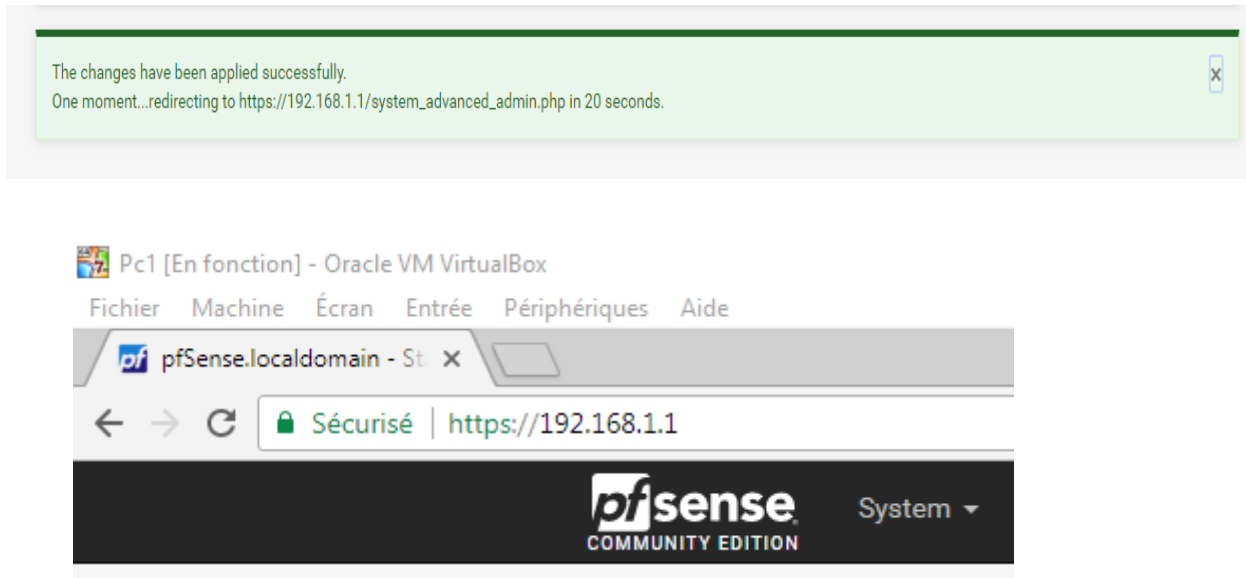


Image 41: Pfsense sécurisé

b) Téléchargement du package Squid et squidguard

Squid :Squid est un proxy de cache pour le Web prenant en charge HTTP, HTTPS, FTP .Squid optimise le flux de données entre le client et le serveur pour améliorer les performances.

Squidguard :SquidGuard est un logiciel de redirection d'URL , qui peut être utilisé pour le contrôle du contenu des sites Web auxquels les utilisateurs peuvent accéder. Il est écrit en tant que plug-in pour Squid et utilise des listes noires pour définir les sites pour lesquels l'accès est redirigé.

Allez dans **System** puis cliquer sur **Package Manager**

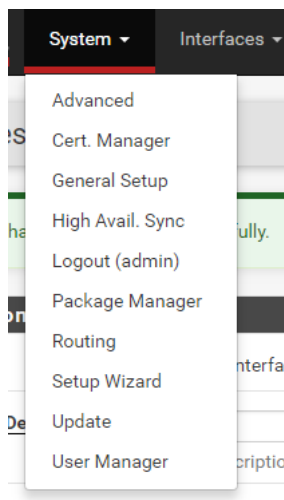


Image 42: Package manager

Pour permettre à pfSense de filtrer les URL, nous avons besoin d'un serveur proxy à travers lequel toutes les requêtes de notre réseau sont routées. Pour cela, nous utilisons Squid. Comme son nom l'indique, SquidGuard est le filtre réel. **Available Packages**, télécharger Squid et SquidGuard.

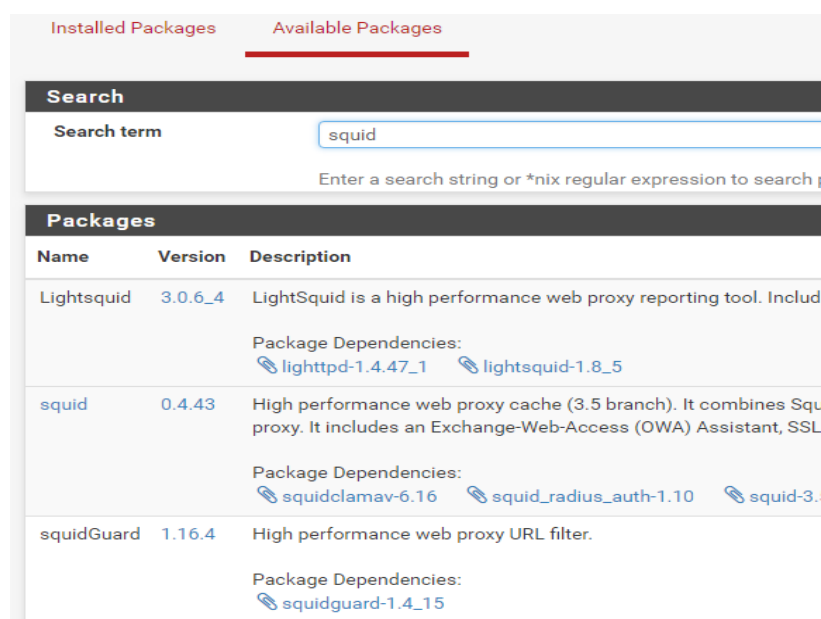


Image 43: Available packages

Cliquer sur install

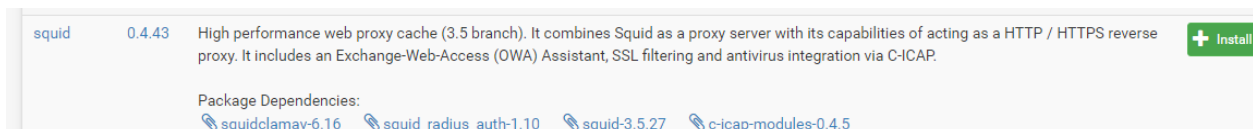


Image 44: Installation de squid

l'installation se fait

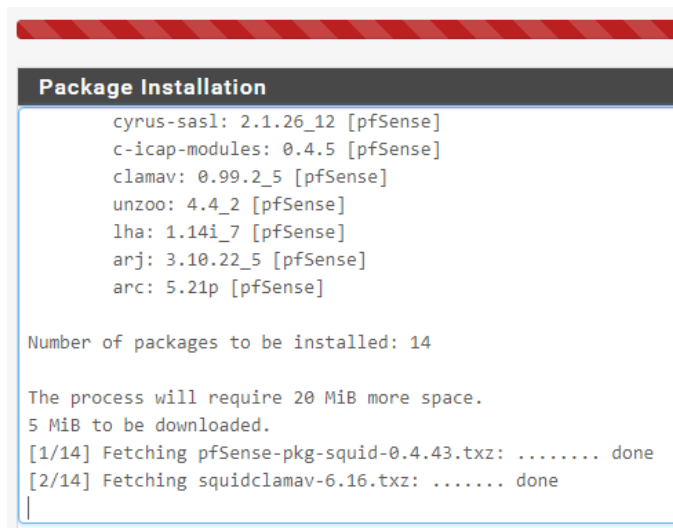


Image 45: Pregression installation squid

Squid a été installé avec succès. Reproduire la même étape avec **Squidguard**.

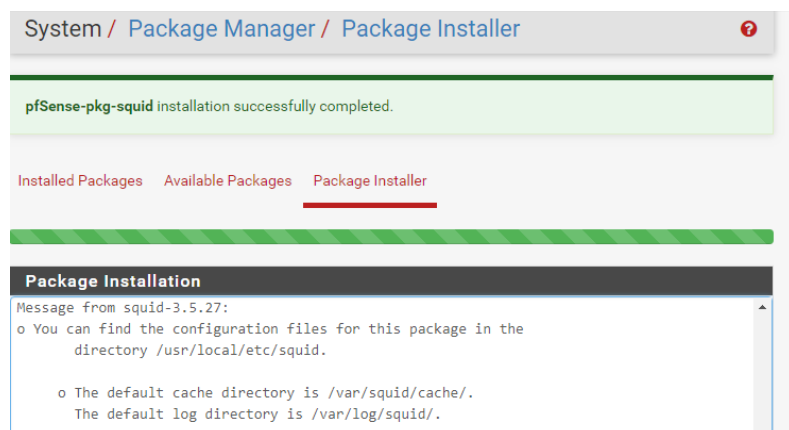


Image 46: Installation terminée

c) Configuration du proxy transparent pour HTTP

Sous **Services** → **Squid Proxy Server**, nous configurons maintenant le proxy transparent pour HTTP. Un proxy transparent présente l'avantage de ne configurer aucun paramètre sur les ordinateurs individuels de notre réseau.

Dans l'onglet **Général**, activer les éléments suivants:

- Activer le proxy Squid

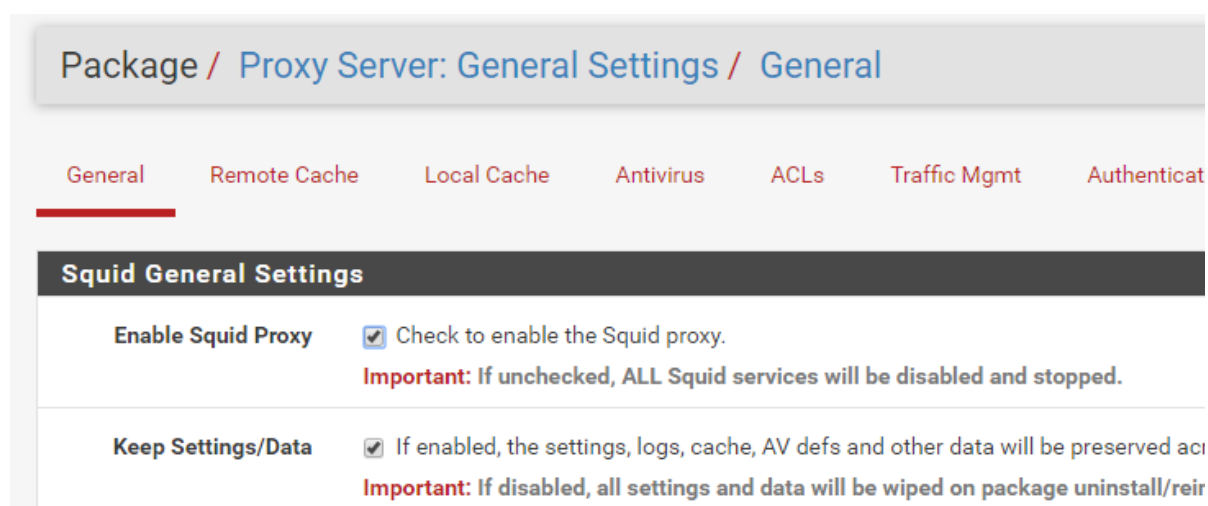
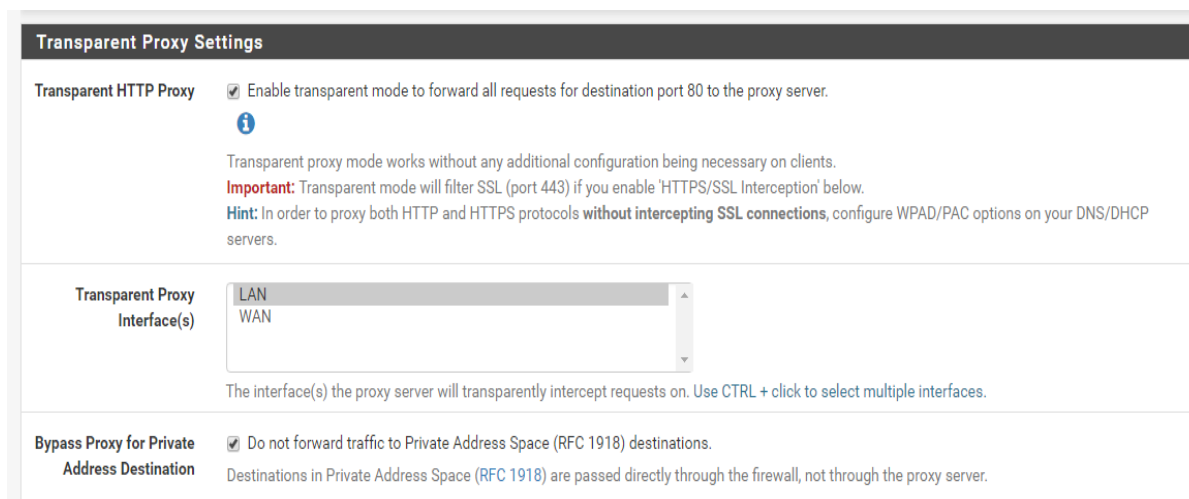


Image 47: Activation du proxy squid

- Cocher la case Transparent HTTP Proxy
- Interface proxy LAN



Transparent Proxy Settings

Transparent HTTP Proxy ☒ Enable transparent mode to forward all requests for destination port 80 to the proxy server.

Transparent Proxy Interface(s) LAN

Bypass Proxy for Private Address Destination ☒ Do not forward traffic to Private Address Space (RFC 1918) destinations.

Image 48: Interface proxy LAN

Cocher **HTTPS/SSL interception** pour activer le filtre SSL



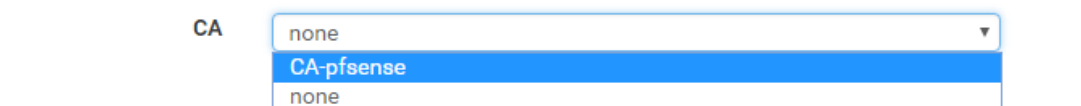
SSL Man In the Middle Filtering

HTTPS/SSL Interception ☒ Enable SSL filtering.

SSL/MITM Mode Splice Whitelist, Bump Otherwise

Image 49: Activation filtre SSL

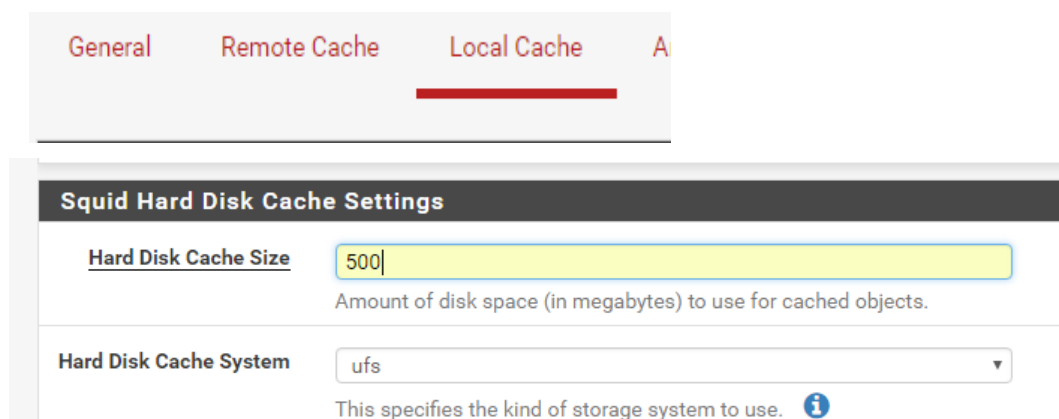
Dans **CA** intégrer le certificat créé au début : pour moi CA-pfsense



CA none

Image 50: CA-Pfsense

Après avoir enregistré avec **Save**, nous déterminons dans l'onglet **Local Cache** combien d'espace disque doit être utilisé pour le cache (ici 500 Mo):



The screenshot shows the 'Squid Hard Disk Cache Settings' window. At the top, there are four tabs: 'General', 'Remote Cache', 'Local Cache', and 'Advanced'. The 'Local Cache' tab is selected and highlighted with a red underline. Below the tabs, the 'Hard Disk Cache Size' is set to '500' in a text input field, with a description 'Amount of disk space (in megabytes) to use for cached objects.' below it. The 'Hard Disk Cache System' is set to 'ufs' in a dropdown menu, with a description 'This specifies the kind of storage system to use.' and an information icon below it.

Image 51: Local Cache

Les paramètres doivent être sauvegardés à nouveau avec **Save**. Le proxy transparent pour les connexions HTTP est maintenant configuré.

d) Activation de SquidGuard

SquidGuard est le composant responsable du filtrage du contenu. Chaque demande est examinée par SquidGuard et décide ensuite de bloquer ou non la demande ou le site Web. Pour cela, nous utilisons une liste noire, que nous configurons plus tard. Avant cela, nous allons définir quelques paramètres généraux sous **Services** → **Filtre proxy SquidGuard**.

Activer en cliquant sur **Apply**

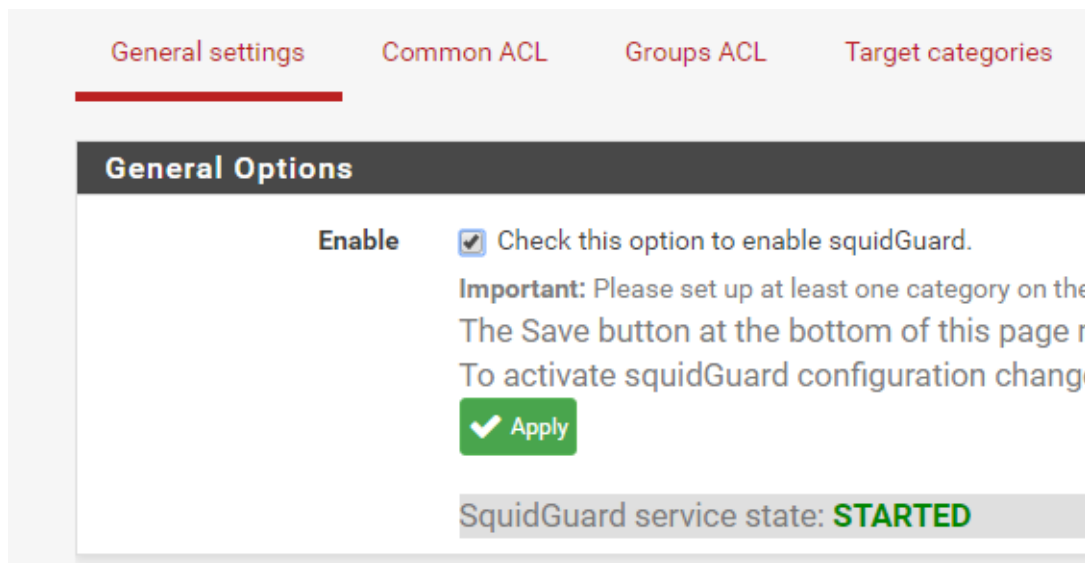


Image 52: Activation Squidguard

Enregistrer à nouveau avec **Save**

e) Configuration de la liste noire

www.shallalist.de/Downloads/shallalist.tar.gz

Munis de ce lien allez dans **Services>SquidGuard Proxy** puis scroller vers le bas jusqu'à atteindre la partie « Blacklist Options »,
Cocher la case à côté de « Blacklist » et entrer l'URL de votre Blacklist au niveau du champ « Blacklist URL » et cliquer sur « save »

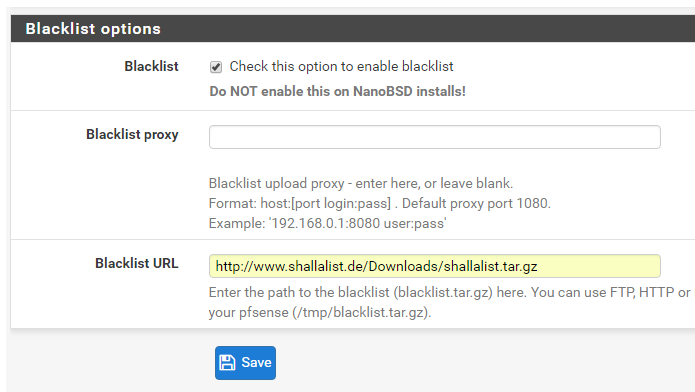


Image 53: URL Blacklist

Téléchargement de la Blacklist

Blacklist Update

Blacklist DB rebuild progress

55 %

Download

Cancel

Restore Default

Enter FTP or HTTP path to the blacklist archive here.

Blacklist update Log

```

Begin blacklist update
Start download.
Download archive http://www.shallalist.de/Downloads/shallalist.tar.gz
Download complete
Unpack archive
Scan blacklist categories.
Found 74 items.
Start rebuild DB.
Completed 55 %

```

La dernière étape pour l'instant est d'établir quelques règles. Nous faisons cela dans l'onglet **Common ACL**. Puis cliquer sur le signe "+" dans "**Target Rules List**" pour ouvrir une liste des différents jeux de règles

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

General settings

Common ACL

Groups ACL

Target categories

Times

Rewrites

Blacklist

Log

XMLRPC Sync

General Options

Target Rules

Target Rules List

+

-

Les autres catégories peuvent être définies selon les besoins. Voici quelques exemples: Bloquer la :

- publicité: [blk_BL_adv] accès refusé
- Blocage de la pornographie: [blk_BL_porn] accès refusé
- etc.

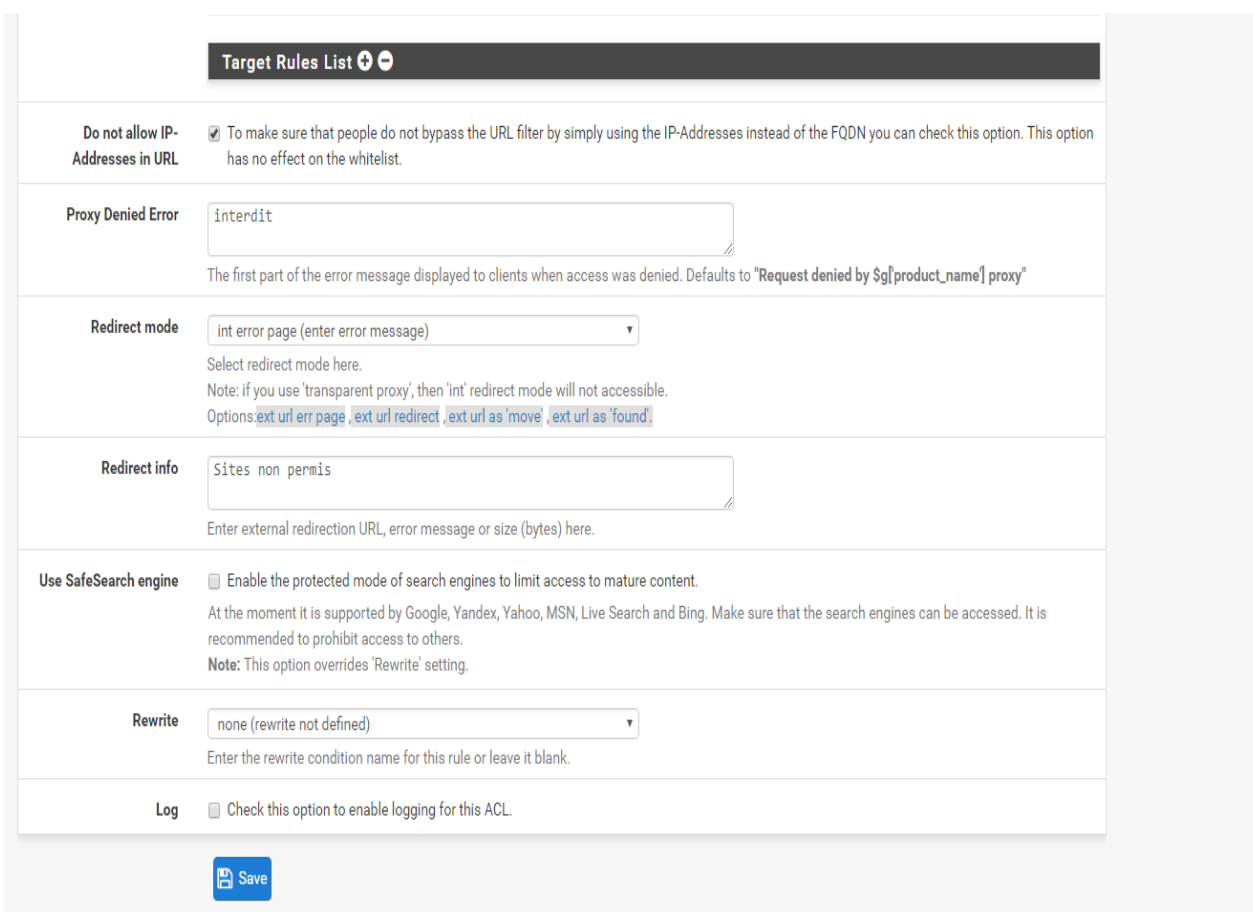
Pour ma part : les réseaux sociaux

Target Categories		
Whitelist [whitelist]	access	whitelist
[blk_BL_adv]	access	deny
[blk_BL_aggressive]	access	deny
[blk_BL_alcohol]	access	deny
[blk_BL_anonvpn]	access	deny
[blk_BL_automobile.bikes]	access	deny
[blk_BL_automobile.boats]	access	deny
[blk_BL_automobile.cars]	access	deny
[blk_BL_automobile.planes]	access	deny
[blk_BL_chat]	access	deny
[blk_BL_coattraps]	access	deny
[blk_BL_dating]	access	deny
[blk_BL_downloads]	access	deny
[blk_BL_sex.lingerie]	access	deny
[blk_BL_shopping]	access	deny
[blk_BL_socialnet]	access	deny
[blk_BL_spyware]	access	deny
[blk_BL_tracker]	access	deny

Image 54: Catégories blacklist

Compléter les cases suivantes : ceci est un exemple

Pour empêcher un utilisateur d'ignorer notre filtre d'URL en entrant l'adresse IP d'une page, nous activons toujours l'option: **Do not allow IP Address in URL**
Compléter le reste comme l'image ci dessous
Ensuite, enregistrer avec **Save**.



Target Rules List + -

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

Proxy Denied Error
The first part of the error message displayed to clients when access was denied. Defaults to "Request denied by \$g[product_name] proxy"

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

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

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

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

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

Save

Image 55: Information blacklist

Lors de la page d'erreur nous devrions voir les termes choisis dans la liste des règles : **interdit et sites non permis**

IV- TEST DU BON FONCTIONNEMENT DU PROJET

Tout est configuré pour les connexions HTTP et nous pouvons tester l'installation. Rien d'autre ne doit être configuré sur un ordinateur dans le réseau local. Le filtre devrait déjà fonctionner.

Le test se fera sur une machine windows 7 que je nommerai PC1

je montrerais une page internet (reseau social) dont le contenu et la visite est interdites.



Image 56: Page web

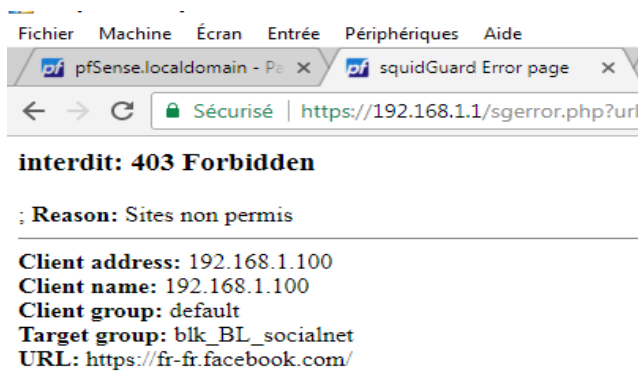


Image 57: Page web non autorisée

En cliquant sur le lien on remarque que la page est bloqué et nous recevons bien les messages d'erreurs.

V- CONCLUSION

Pfsense est une distribution libre et gratuite fondée sur freebsd. Installée sur un équipement doté de plusieurs cartes réseau, elle permet d'optimiser et de sécuriser votre réseau local

Un système a été mis en place pour filtrer tout le trafic réseau dans notre réseau local (ou WLAN). Cela bloque les pages qui ont été définies à l'aide des listes noires.