FIREWALL

Pare-Feu (pfSense)

Nous allons mettre en place le Pare-feu pfSense. Nous le paramétrons pour qu'il puisse faire les liens entre les Vlan pour que les Serveurs et les clients puissent fonctionner ensemble et donc, avoir une adresse avec le DHCP, communiquer avec l'AD pour rejoindre le domaine et aller chercher des données dans les serveurs de fichier SAMBA. Ensuite nous allons mettre en place un Proxy pour gérer les trafics. Et pour finir nous mettrons en place le load balancing des deux serveurs web depuis pfSense

Un pare-feu (de l'anglais firewall) est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il surveille et contrôle les applications et les flux de données (paquets).

Sources: Wikipedia

pfSense est un routeur/pare-feu open source basé sur le système d'exploitation FreeBSD. À l'origine un fork de m0n0wall, il utilise le pare-feu à états Packet Filter, des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. pfSense convient pour la sécurisation d'un réseau domestique ou de petite entreprise.

Après une brève installation manuelle pour assigner les interfaces réseaux, il s'administre ensuite à distance depuis l'interface web et gère nativement les VLAN.

Comme sur les distributions Linux, pfSense intègre aussi un gestionnaire de paquets pour installer des fonctionnalités supplémentaires, comme un proxy, serveur VoIP1...

Sources: Wikipedia

Etapes de la procédure :

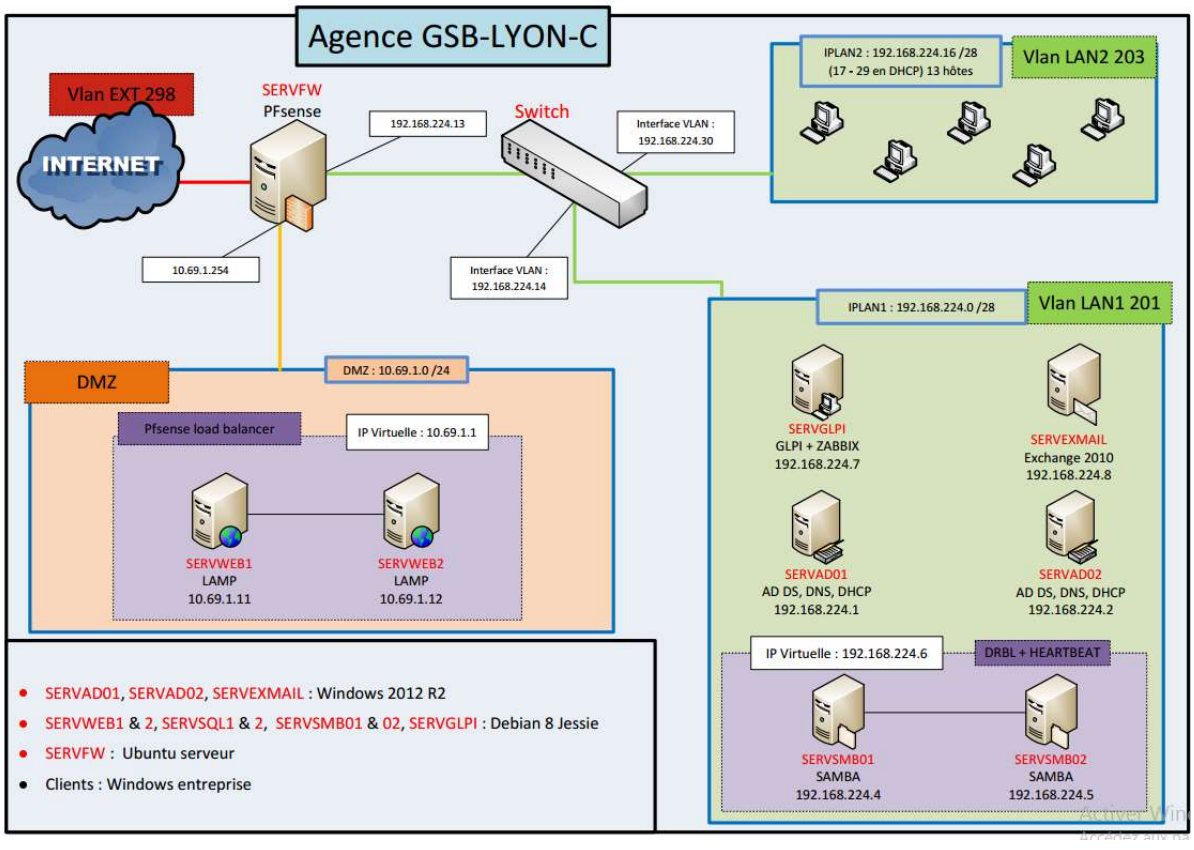
- Installation pfSense
- Administration interface WEB et paramétrage
- Proxy
- "Dhcp relay" et création de la route pour les VLAN
- Haute disponibilité serveur LAMP avec du "load balancing"
- Test du "load balancer"

Prérequis :

Si vous faites ça avec des machines virtuel, créer des machines propres avec l'ISO, et ne pas les cloner pour éviter les problèmes d'ID.

- Une iso " pfSense-CE-2.4.2 "
- Une machine client (dans ce cas-là c'est un Windows 7)
- Deux serveurs web pour le load balancing

Schéma :



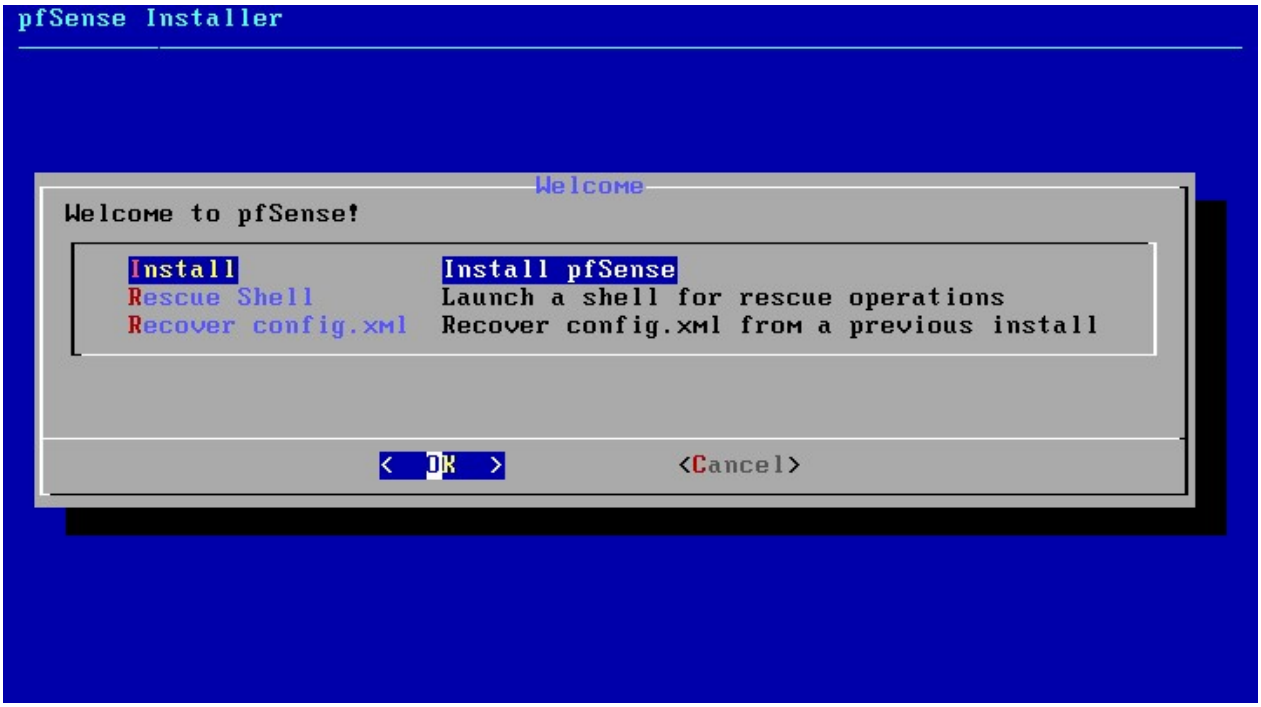
Sur SERVFW

- Paramétrer le nom du serveur " SERVFW "
- Sur SERVFW, il y a cartes 3 réseau :
    - LAN : 192.168.224.13 en VMNET2
    - WAN : DHCP en VMNET0 (bridge)
    - DMZ : 10.69.1.254 en VMNET6

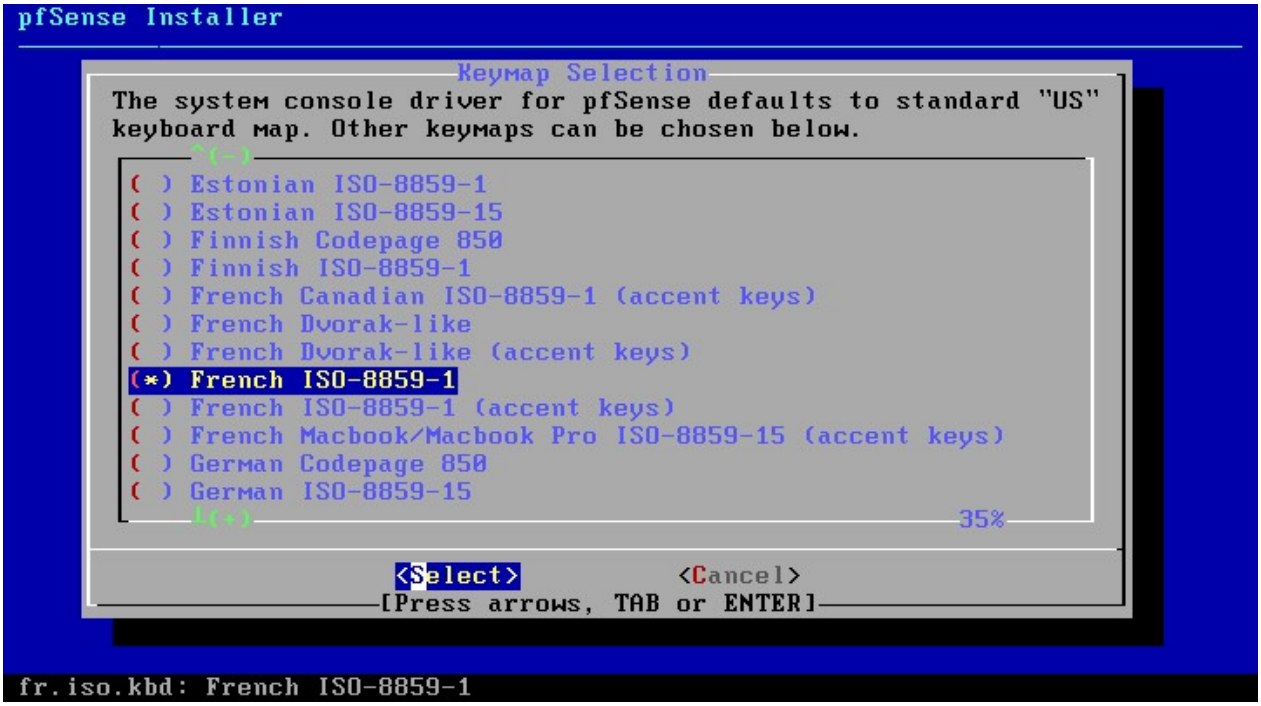
Sur SERVFW

Installation pfSense

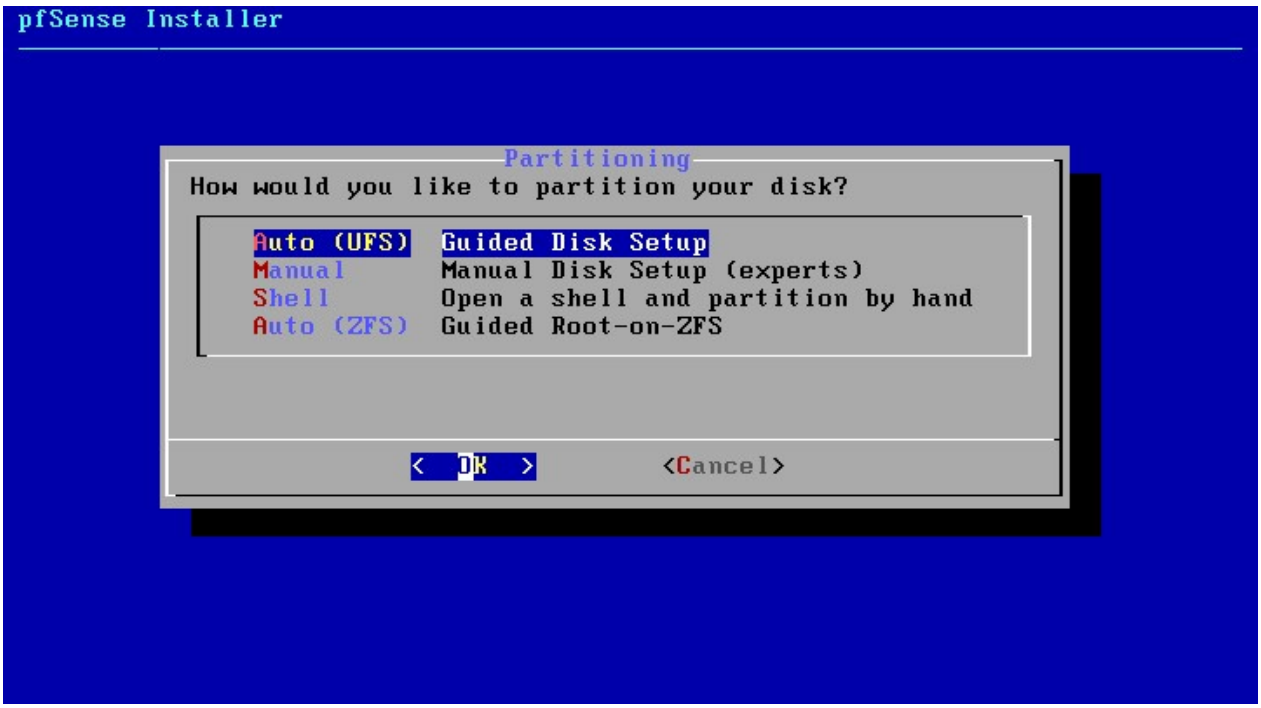
Installer l'ISO " pfSense-CE-2.4.2 "



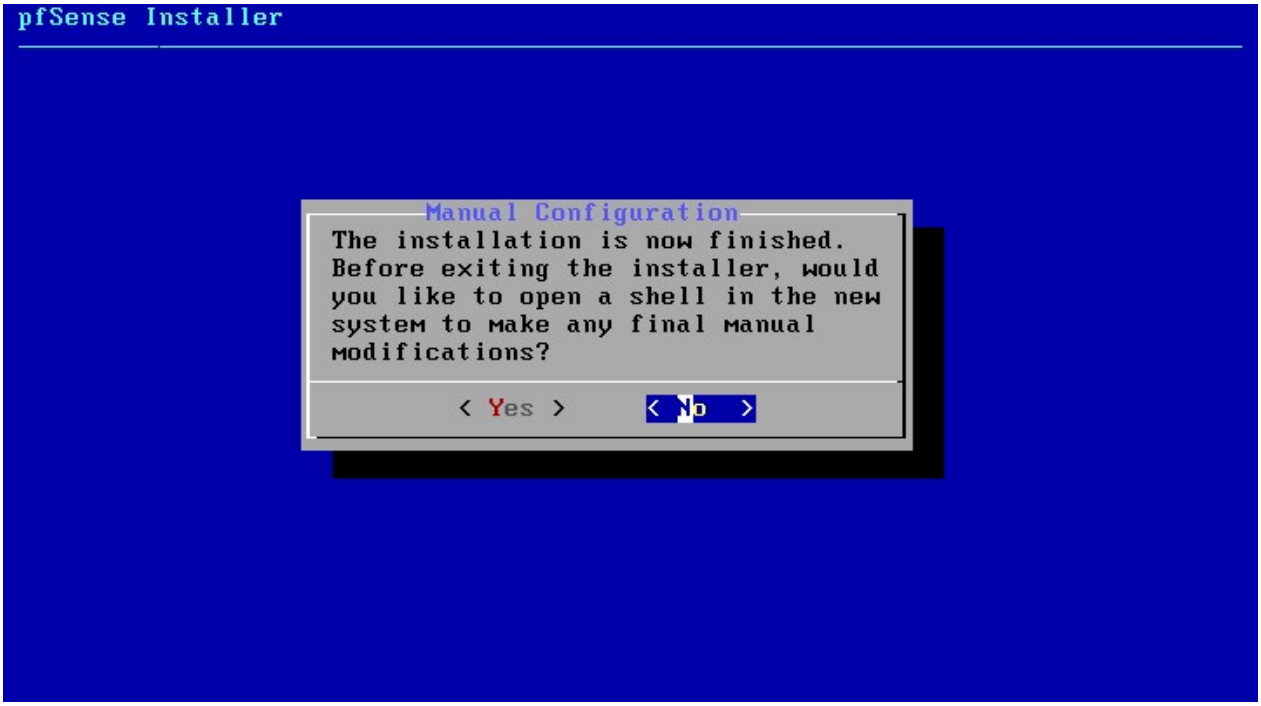
Choisir la langue



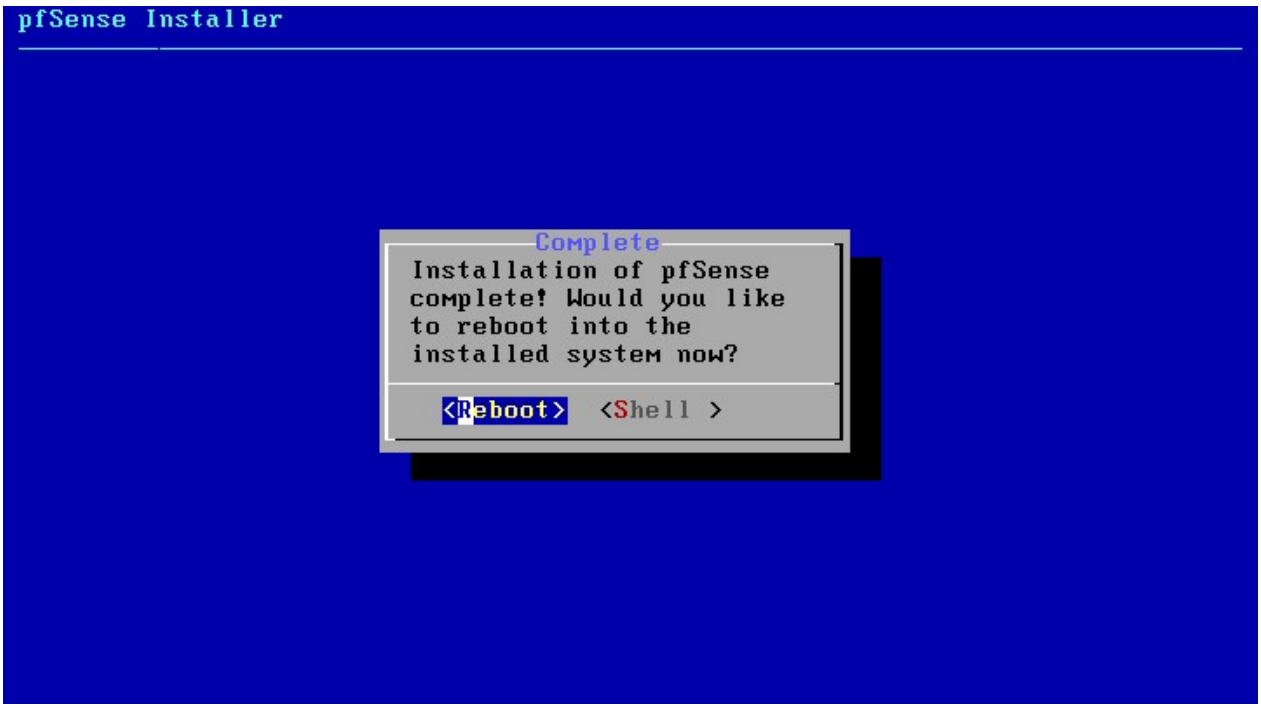
Laisser le partitionnement en Auto



Valider "NO"



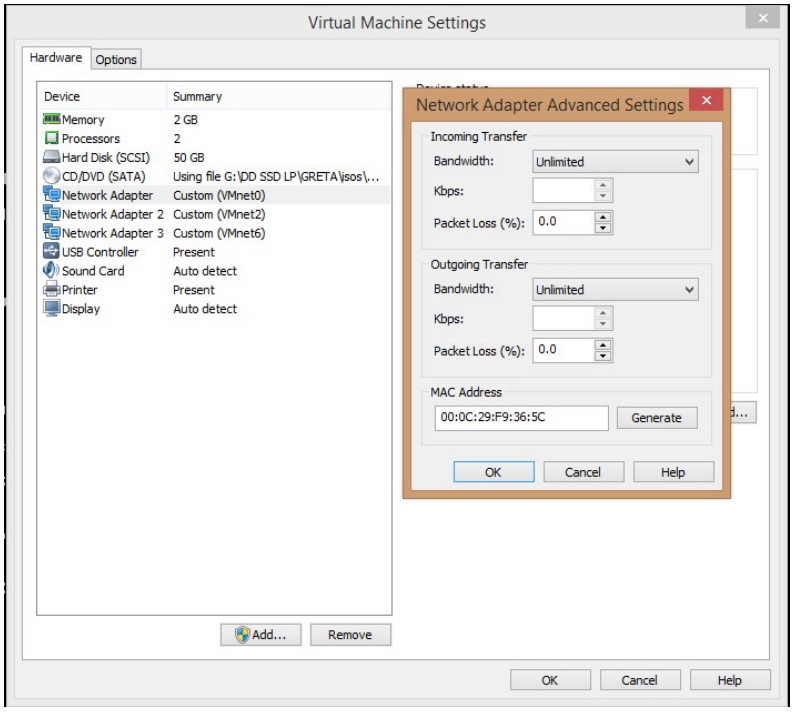
Valider "REBOOT"



Au redémarrage, il vous demandera si vous voulez paramétrer les VLAN maintenant.
Nous le feront plus tard, allez entrer "n"

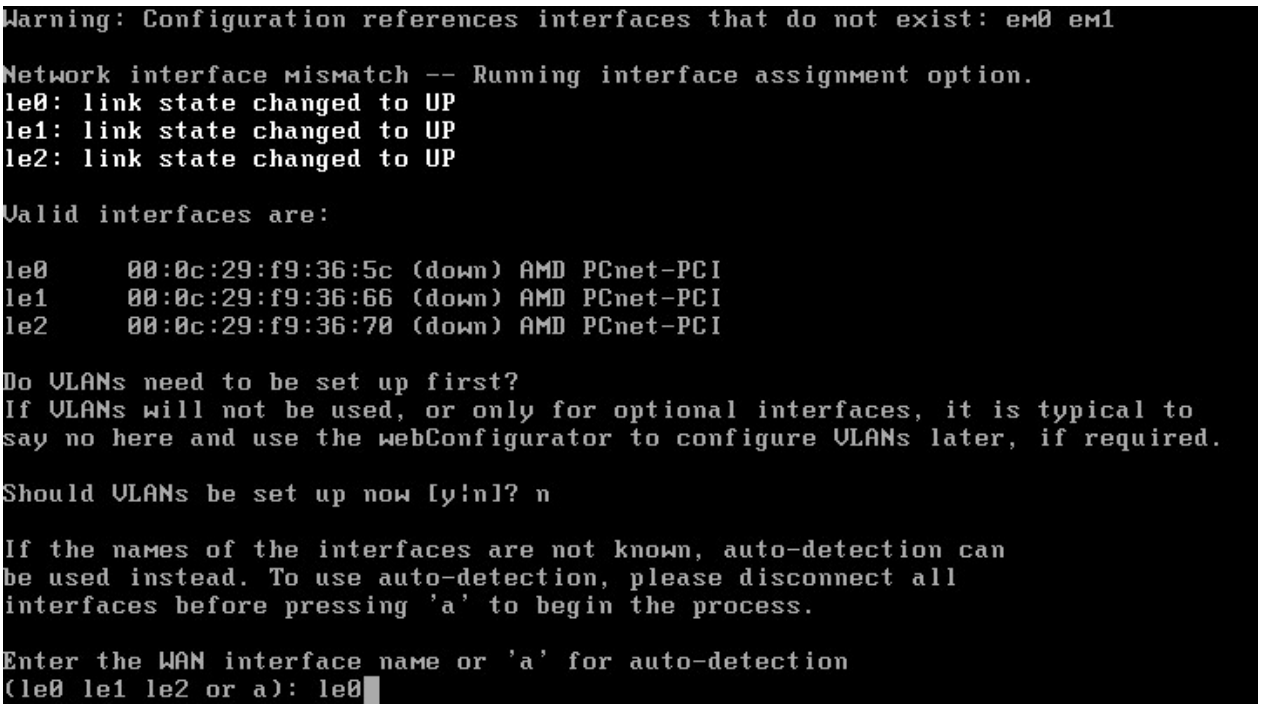
```
Launching the init system..... done.
Initializing..... done.
Starting device manager (devd)...kldload: can't load ums: No such file or direct
ory
done.
Loading configuration......done.
Updating configuration...done.
Warning: Configuration references interfaces that do not exist: em0 em1

Network interface mismatch -- Running interface assignment option.
le0: link state changed to UP
le1: link state changed to UP
le2: link state changed to UP

Valid interfaces are:

le0     00:0c:29:f9:36:5c (down) AMD PCnet-PCI
le1     00:0c:29:f9:36:66 (down) AMD PCnet-PCI
le2     00:0c:29:f9:36:70 (down) AMD PCnet-PCI

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

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

Maintenant, nous allons configurer les cartes réseau, et pour cela il faut les adresses MAC de chacune, pour les connaitre.
Dans VMware, faites clic droit sur votre VM puis settings. Sélectionner votre première carte réseau puis dans la partie droite sélectionner "Advanced" et là vous verrez votre adresse MAC, notez la et faites la même chose pour les 2 autres cartes réseau.



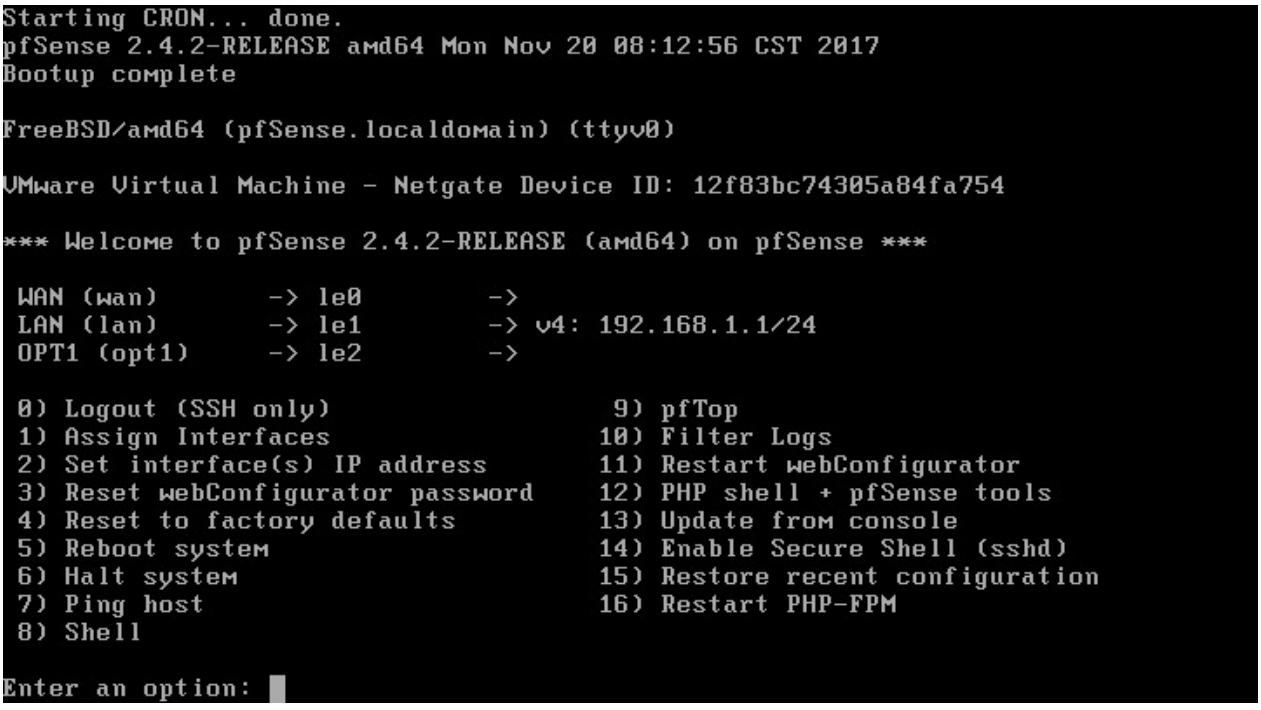
Maintenant il va vous demander de faire le liens entre vos carte réseau
Et vu que vous avez récuperer les adresses MAC, vous pouvez faire le liens pour que :

- LAN : 192.168.224.13 en VMNET2
- WAN : DHCP en VMNET0 (Bridge)
- DMZ : 10.69.1.254 en VMNET6



Faire la meme chose pour chaque carte puis valider.

Vous avez terminé, maintenant vous êtes arrivez sur le menu de pfSense.

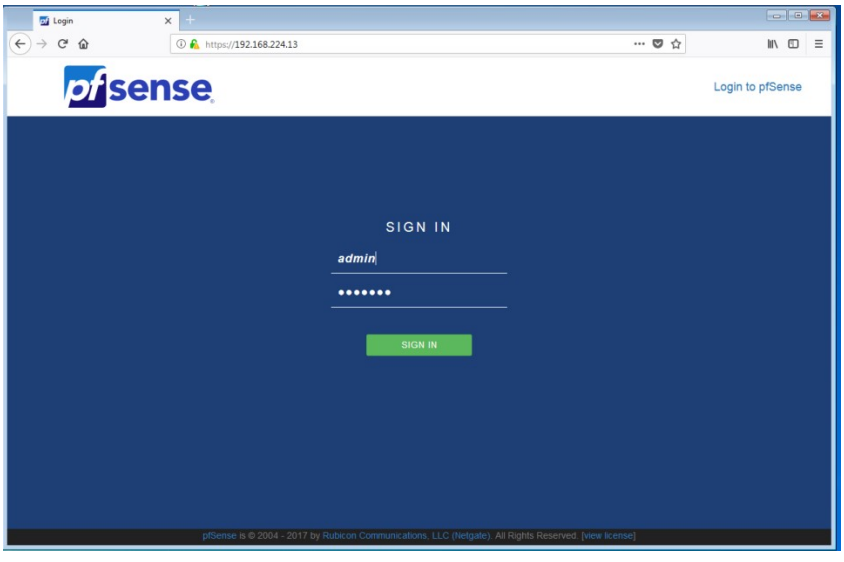


Nous allons configurer l'interface LAN avec l'option "2"

```
Enter an option: 2

Available interfaces:

1 - WAN (le0 - dhcp, dhcp6)
2 - LAN (le1 - static)
3 - OPT1 (le2)

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

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.224.13

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):
> 28

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

- Choisir l'interface : Lan
- Lui donner l'adresse IP : 192.168.224.13
- Le sous-réseau : 28
- Gateway :Entrer (ne rien mettre)
- adresse IPV6 :Entrer (ne rien mettre)
- DHCP : n
- Ce mettre en http : n
- Pour terminer appuyer sur enter

Administration interface WEB et paramétrage

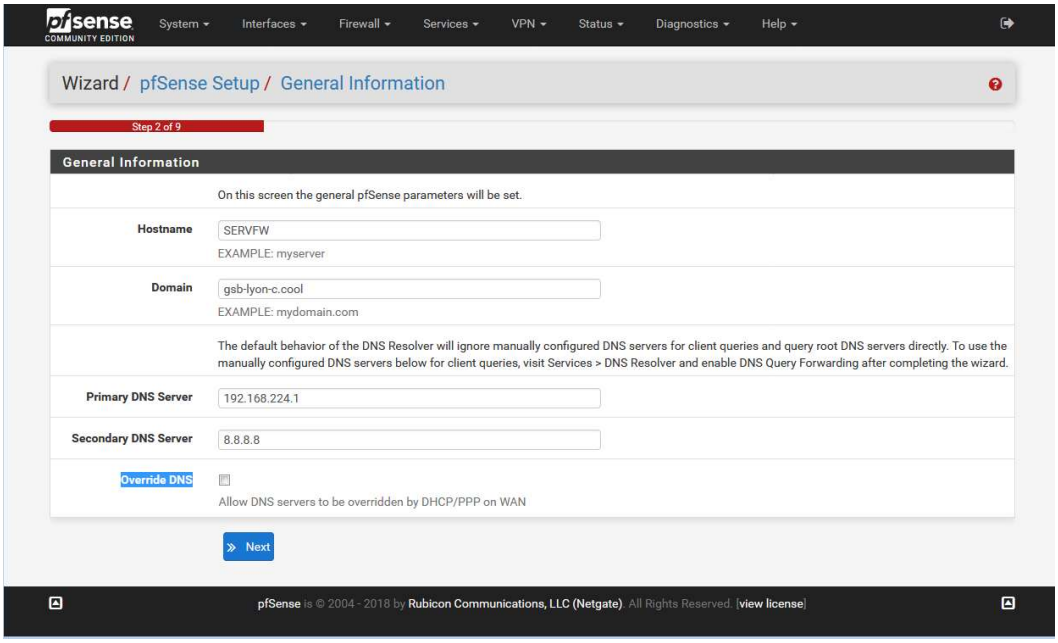


- Prenez la main sur un client dans le réseau LAN configuré en IP fixe Par exemple 192.168.224.5 /28 en vmnet2
- Grace a un navigateur, se connecter à l'interface pfSense à l'adresse 192.168.224.13

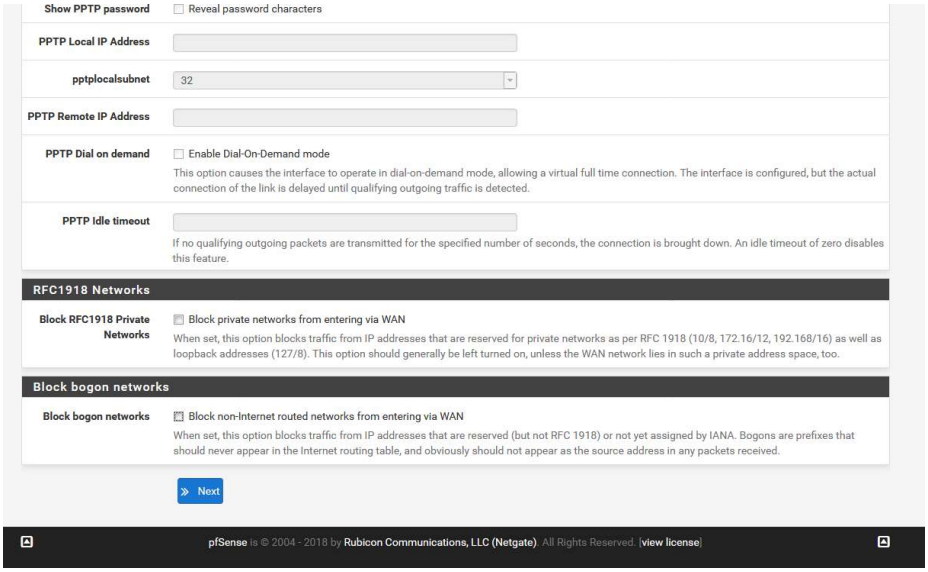
Connectez-vous à pfSense
Login par défaut : admin
Mot de passe par défaut : pfsense

Après l'ouverture de session il vous demandera de faire le complément des paramètres.
Faire suivant jusqu'à la configuration suivante et entrer les même informations

Décocher "Override DNS" sinon le DHCP du LAN va écraser les configurations



Cliquer sur "Next" pour passer à l'étape suivante

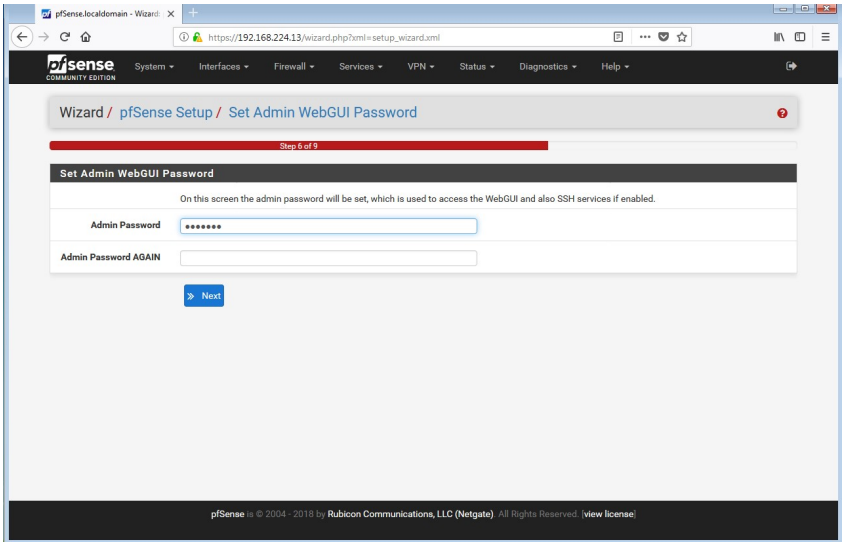


Sur la page suivante il faut juste décocher :

- Block private networks from entering via WAN
- Block non-Internet routed networks from entering via WAN

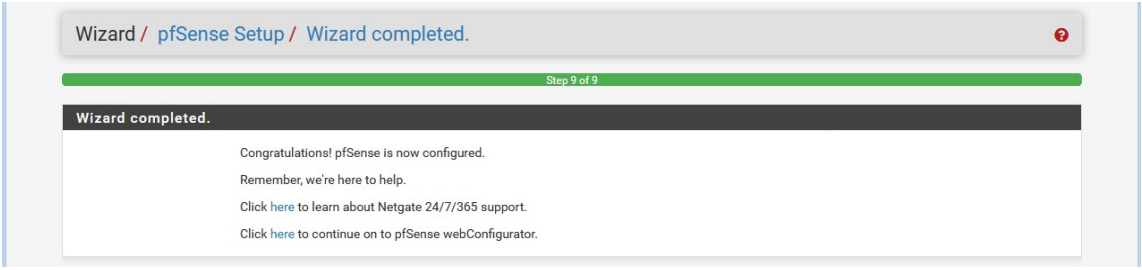
Car si le serveur n'a pas assez de mémoire vive cela peut engendrer un dysfonctionnement du firewall.
Cliquer sur "Next" pour passer à l'étape suivante

Configurer un nouveau mot de passe : " gsblyon "

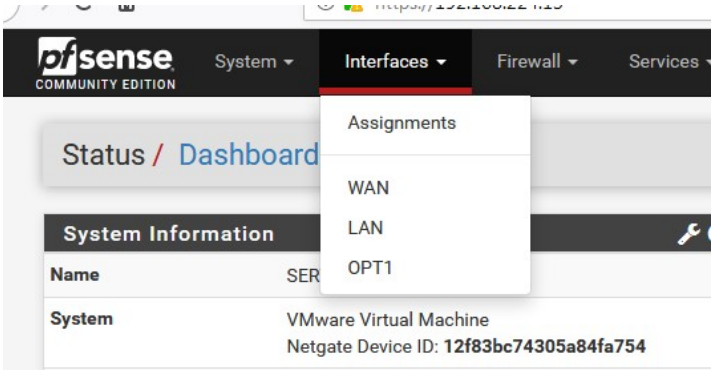


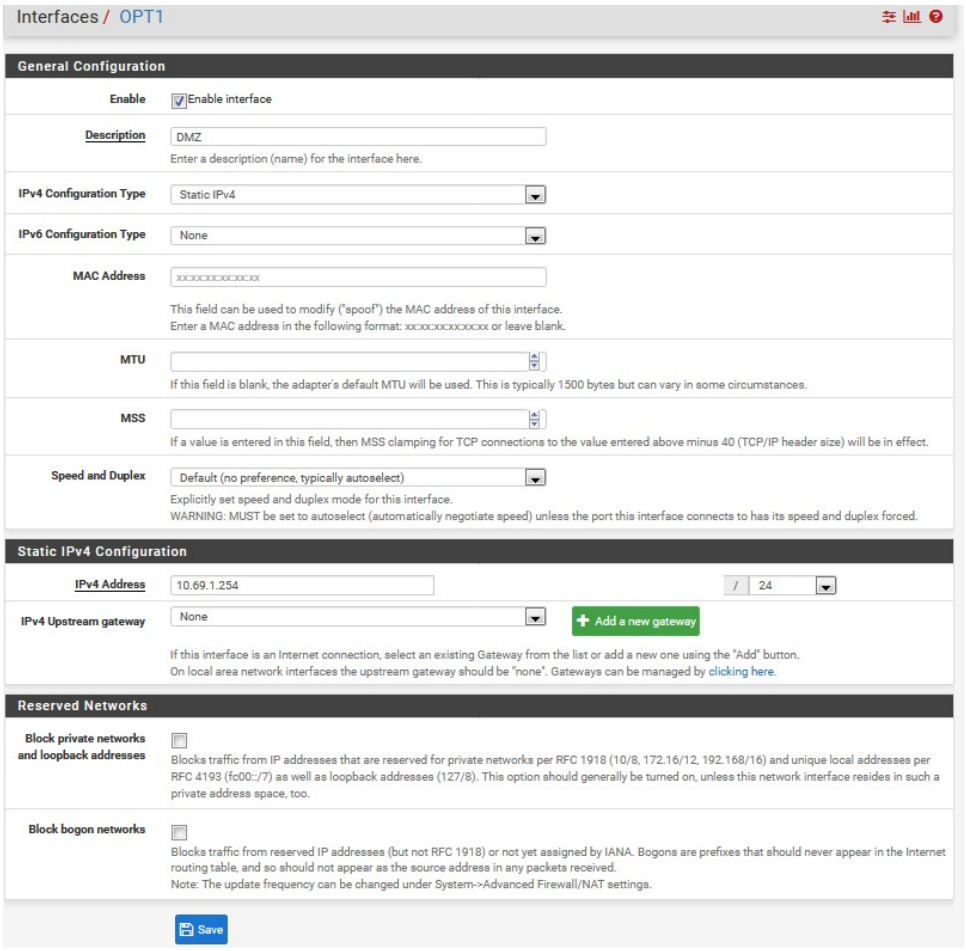
Cliquer sur "Next" pour passer à l'étape suivante
Cliquer sur "reload" (prend à jour les modifications)

Cliquer sur le "here" de :
"Click here to continue on to pfSense webConfigurator."



On va configurer l'adresse IP de notre DMZ.
Aller dans : Interfaces / OPT1

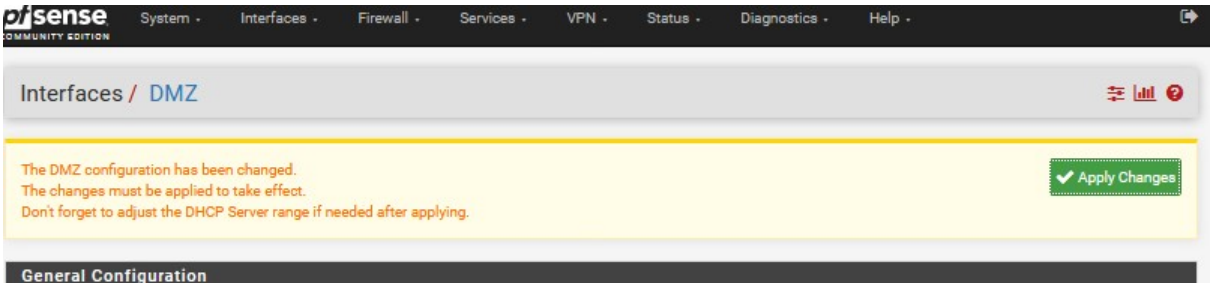




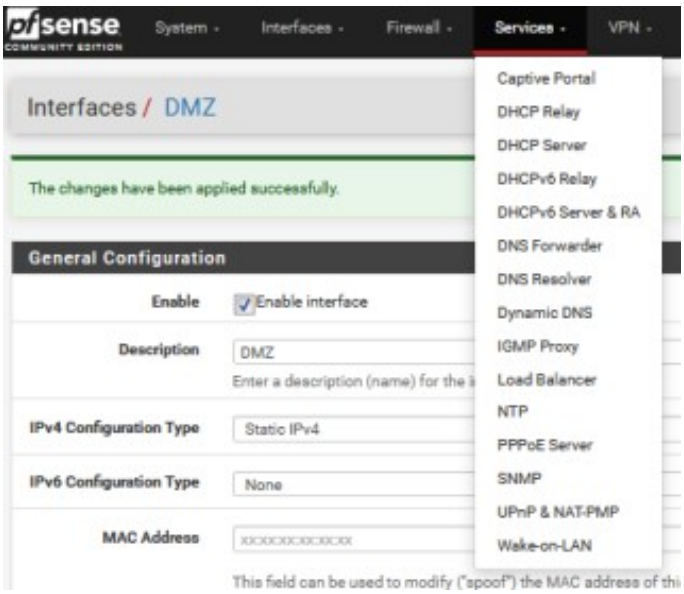
Remplir avec les mêmes informations

Puis cliquer sur "Save"

Puis cliquer sur "Apply changes" pour appliquer les changements



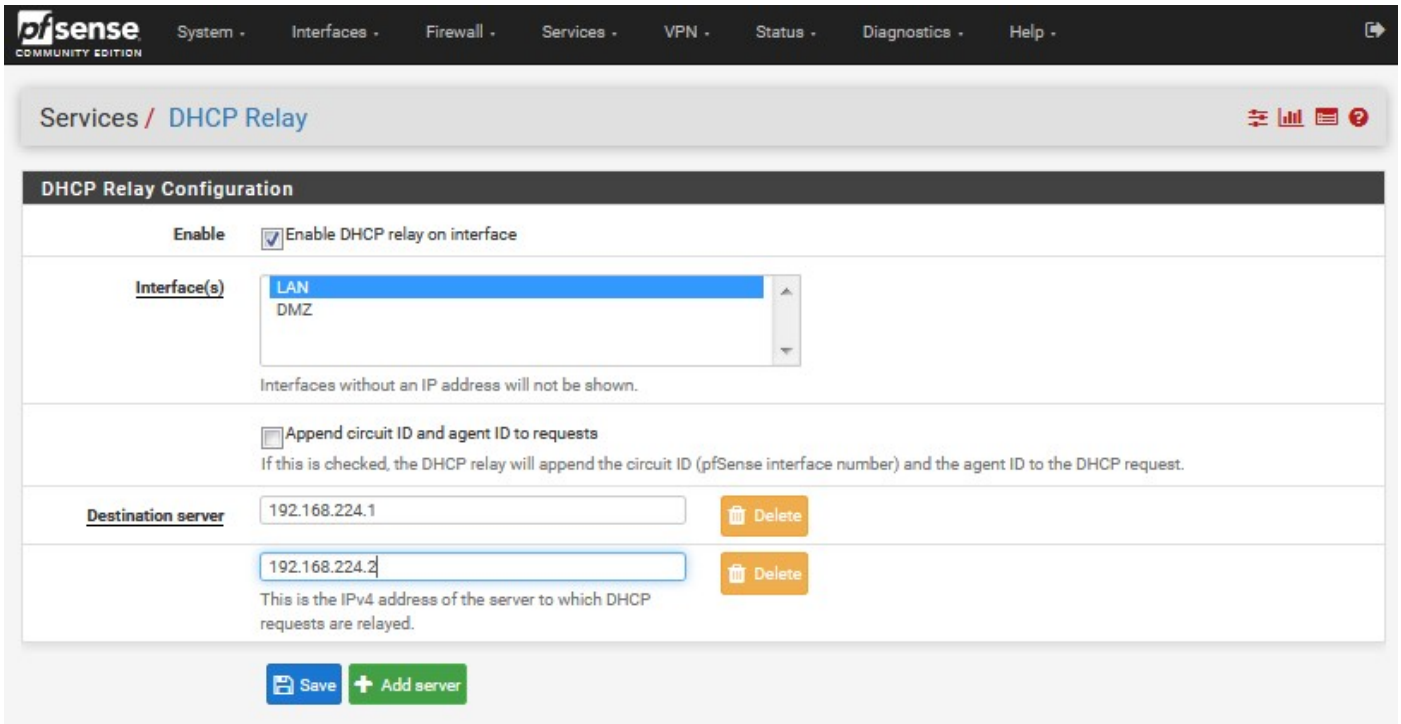
"Dhcp relay" et création de la route pour les VLAN

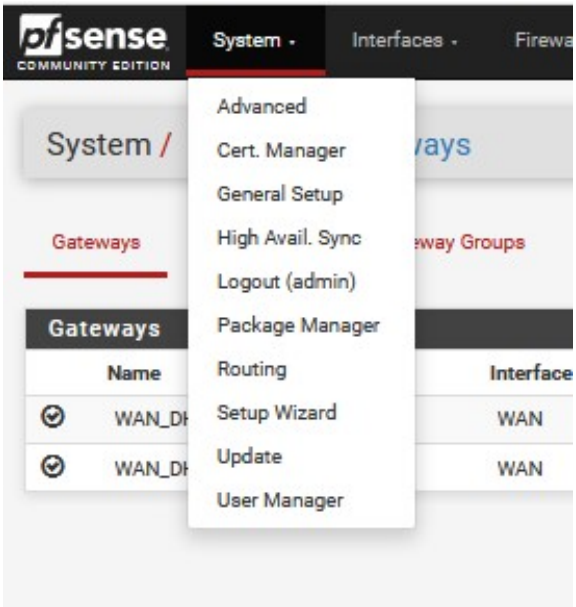


Aller dans Services / dhcp relay

Remplissez le formulaire de la même façon pour que le "DHCP relay" soit actif et que votre serveur DHCP et les clients puissent communiquer ensemble.

Cliquer sur "Add server" pour rentrer le deuxième AD.
Cliquer sur "Save" pour enregistrer votre paramétrage.

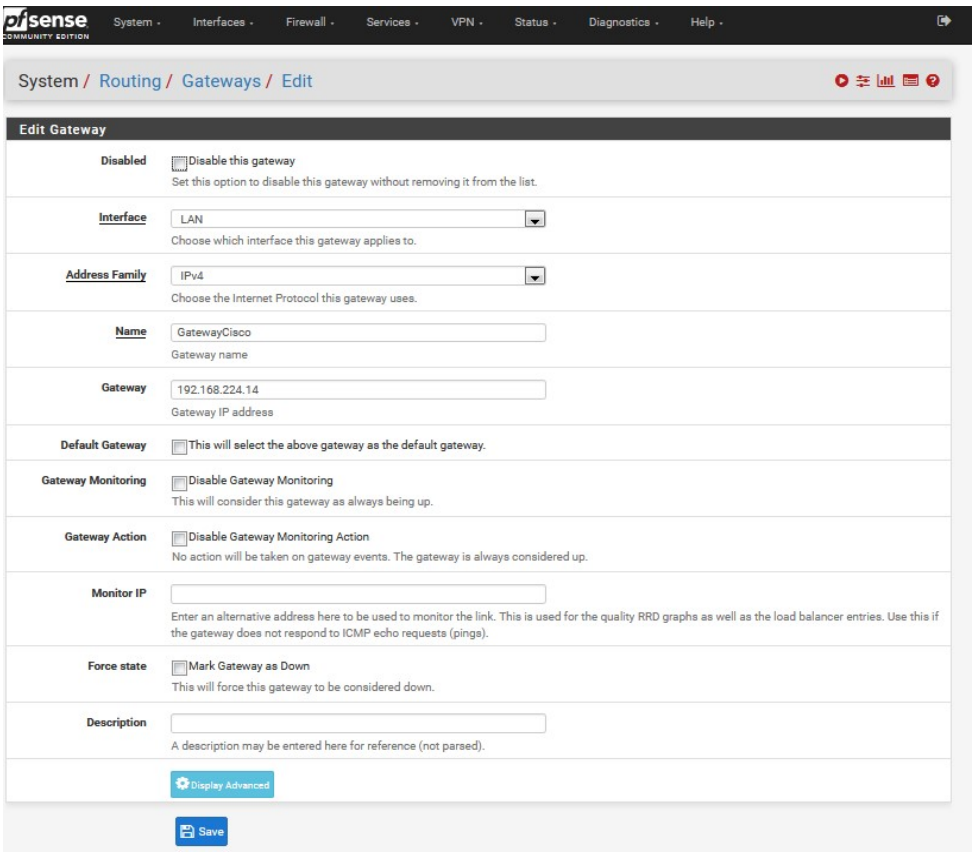




Aller dans system / routing / gateways

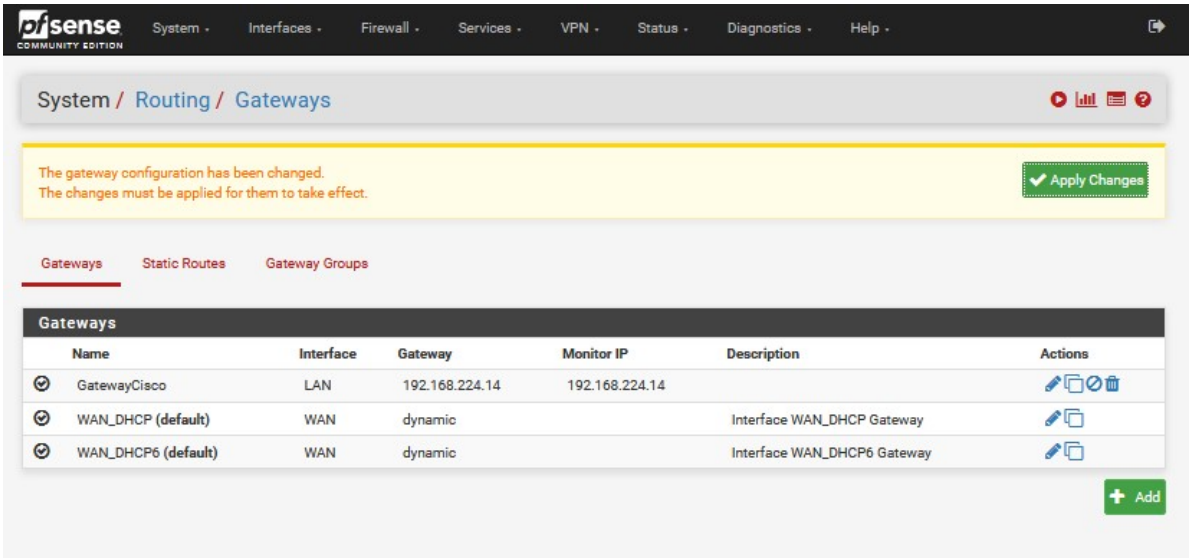
Cliquer sur "+add" pour ajouter

Remplissez le formulaire de la même façon

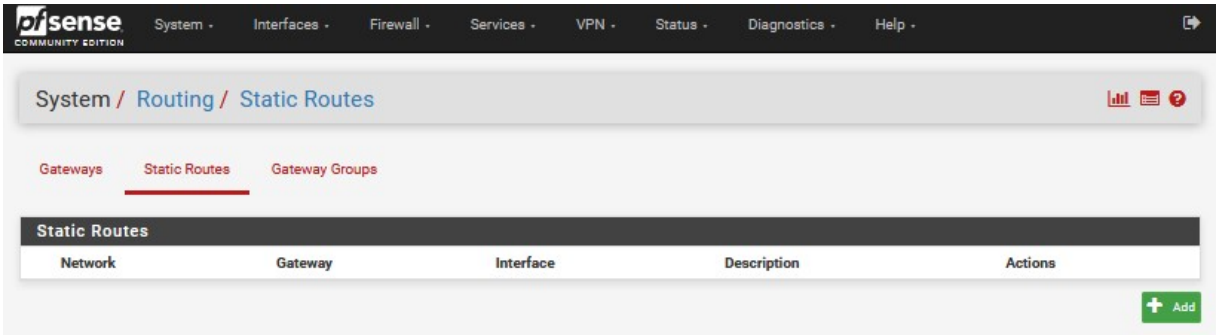


Cliquer sur "Save" pour enregistrer votre paramétrage.

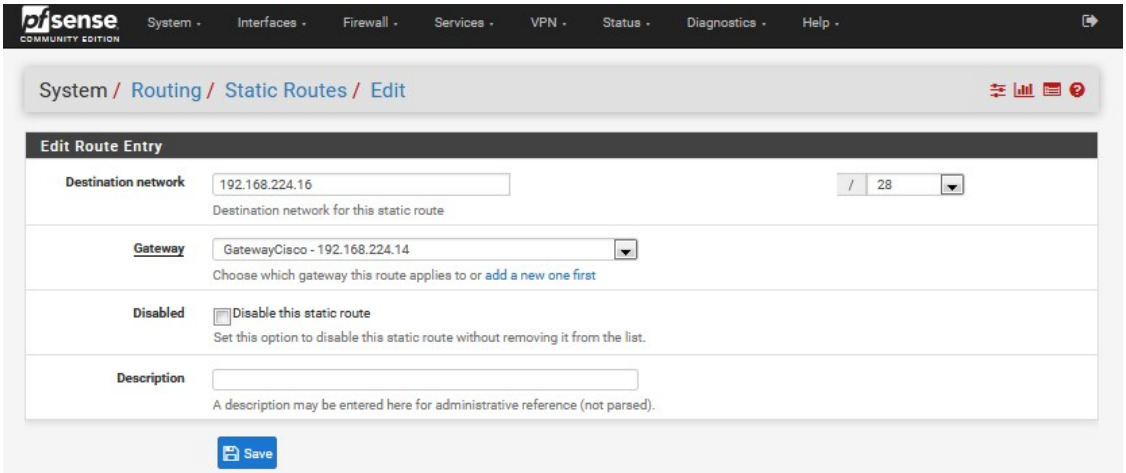
Cliquer sur "Apply changes" pour appliquer les changements



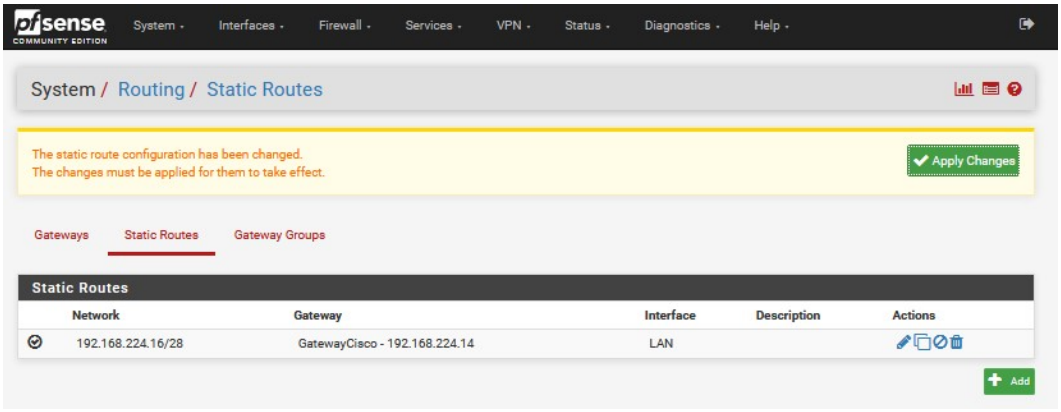
Dans "static routes"
Puis ajouter une route statique en cliquant sur "+add"



Remplissez le formulaire de la même façon
Cliquer sur "Save" pour enregistrer votre paramétrage.



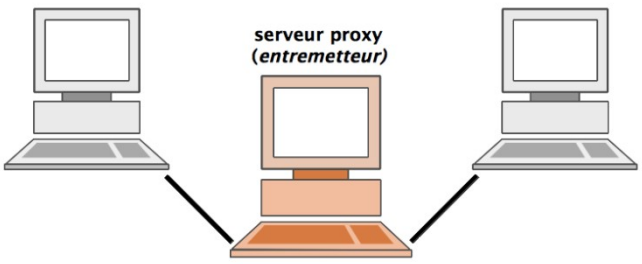
Cliquer sur "Apply changes" pour appliquer les changements



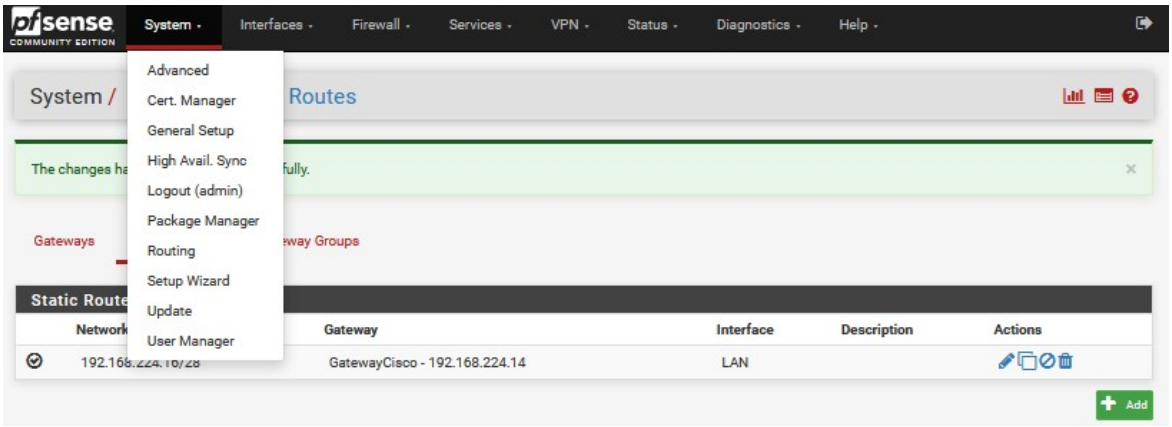
Proxy

Un proxy est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges.

Dans le cadre plus précis des réseaux informatiques, un proxy est alors un programme servant d'intermédiaire pour accéder à un autre réseau, généralement internet. Par extension, on appelle aussi « proxy » un matériel comme un serveur mis en place pour assurer le fonctionnement de tels services.

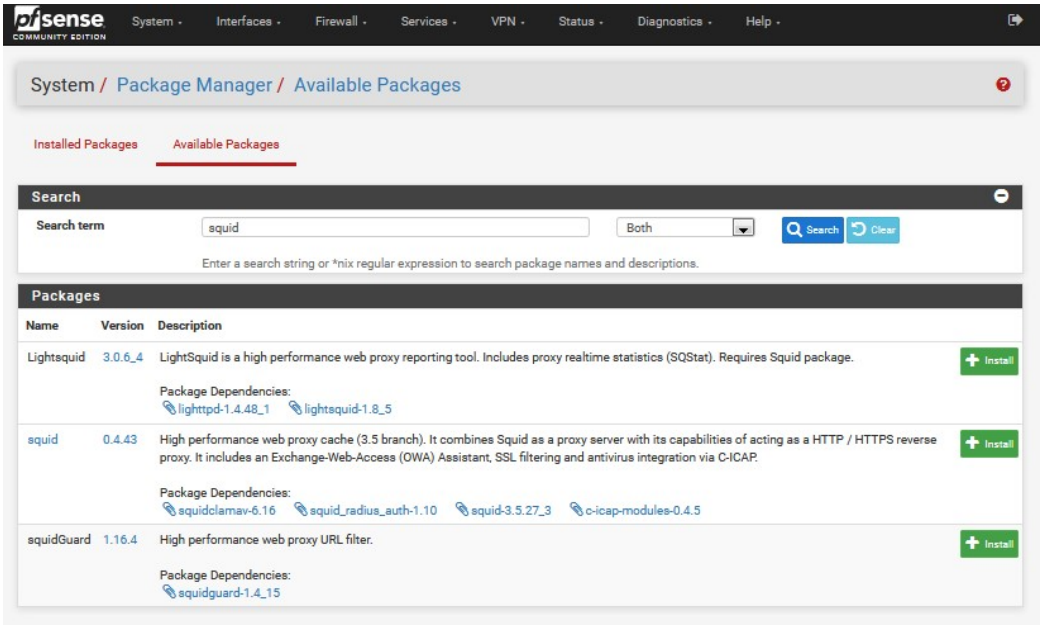


Sources: Wikipedia



System / package manager
Available package

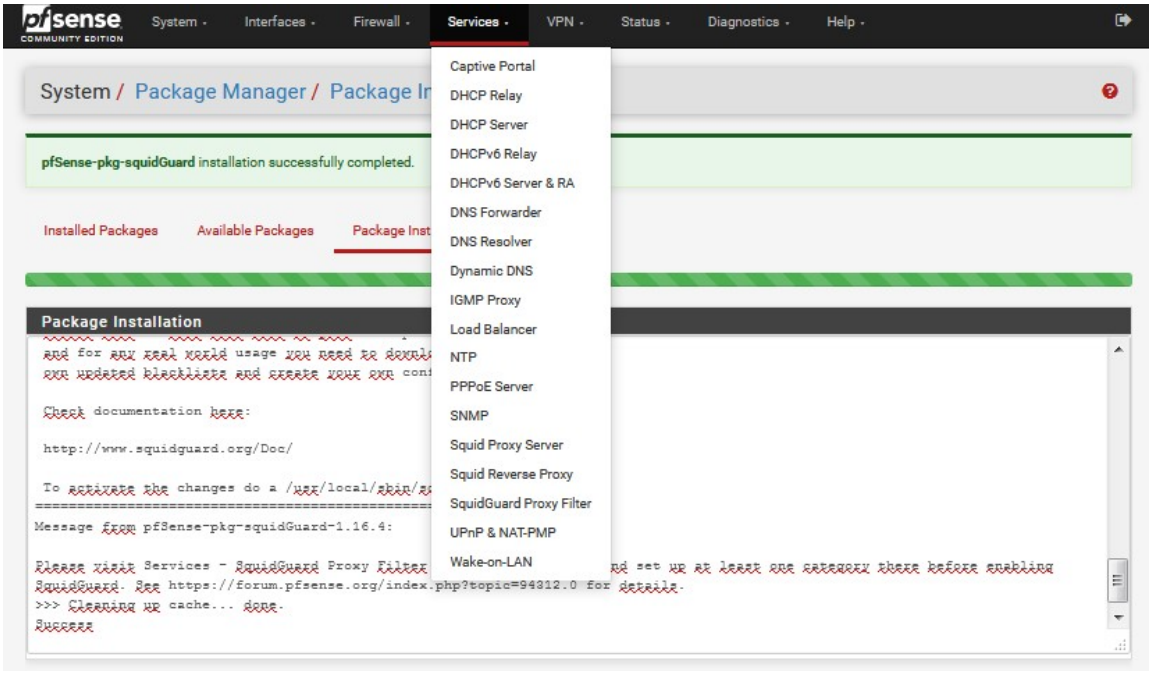
On va installer squidguard



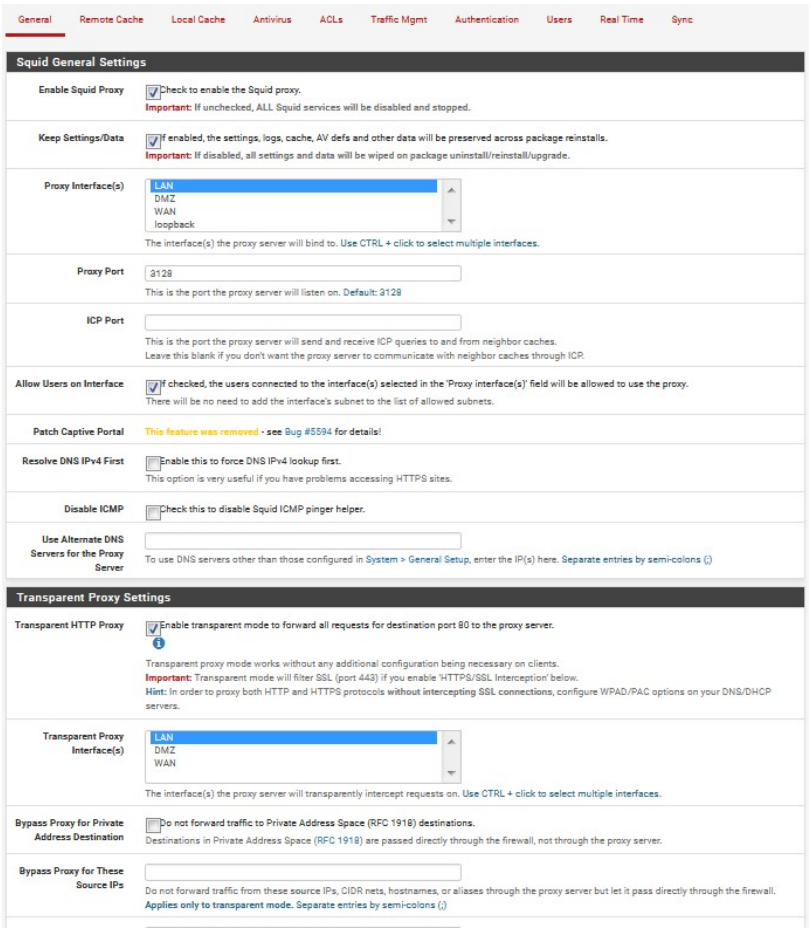
Installer "squid" puis "squidgard"

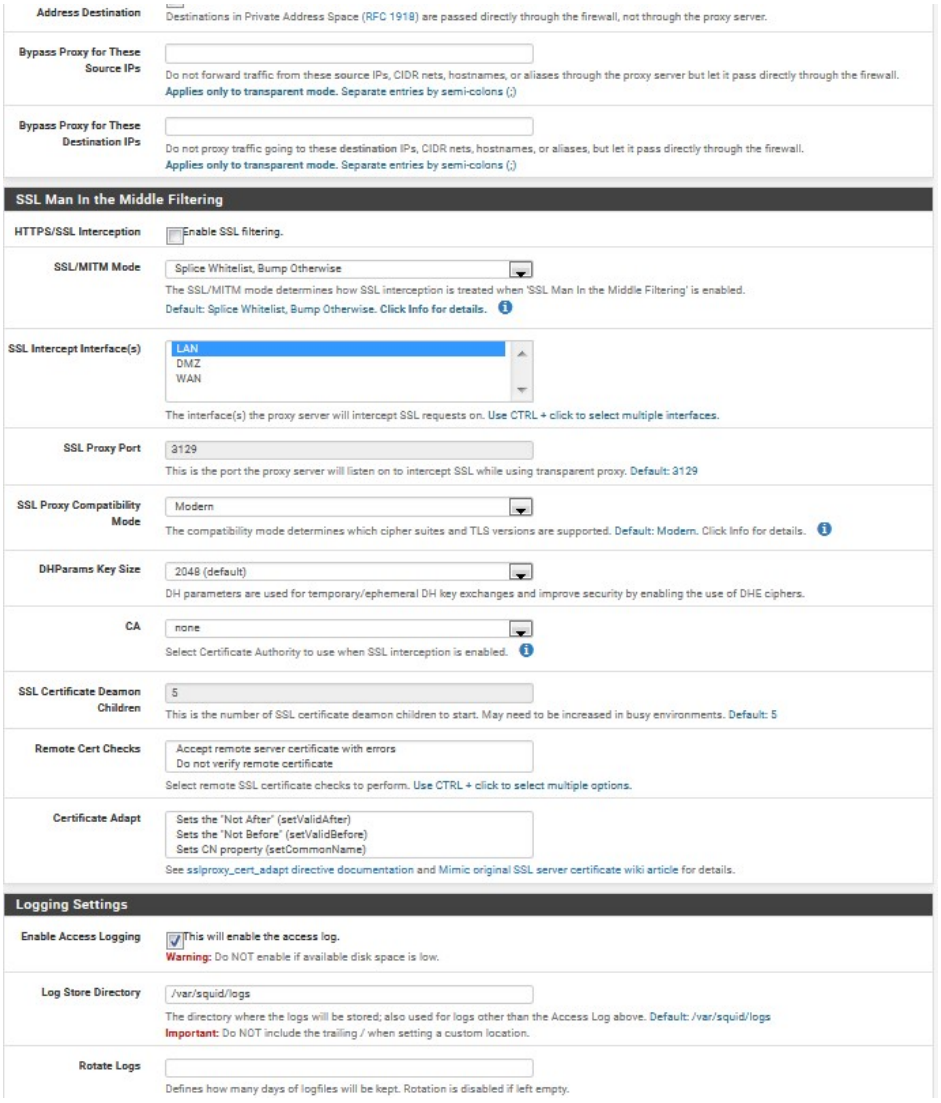
- "Squid" est un serveur proxy
- "Squidguard" fait filtrage web

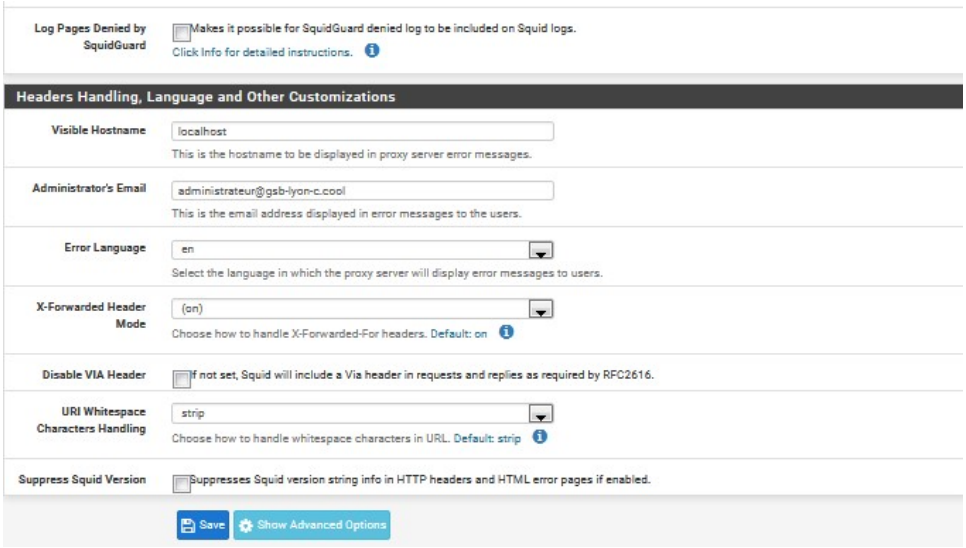
Aller dans : Service / squid proxy server



Remplissez le formulaire de la même façon

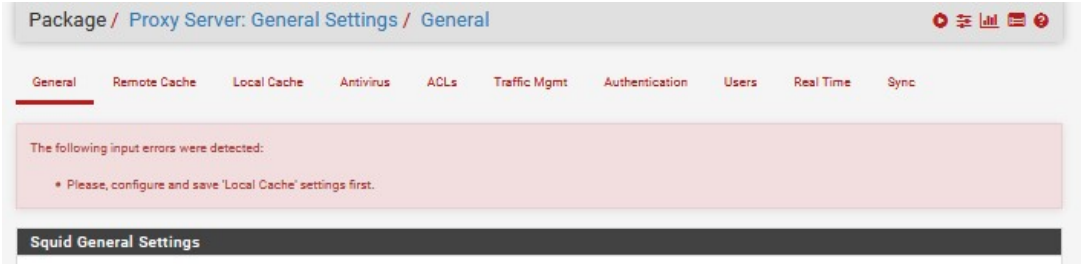






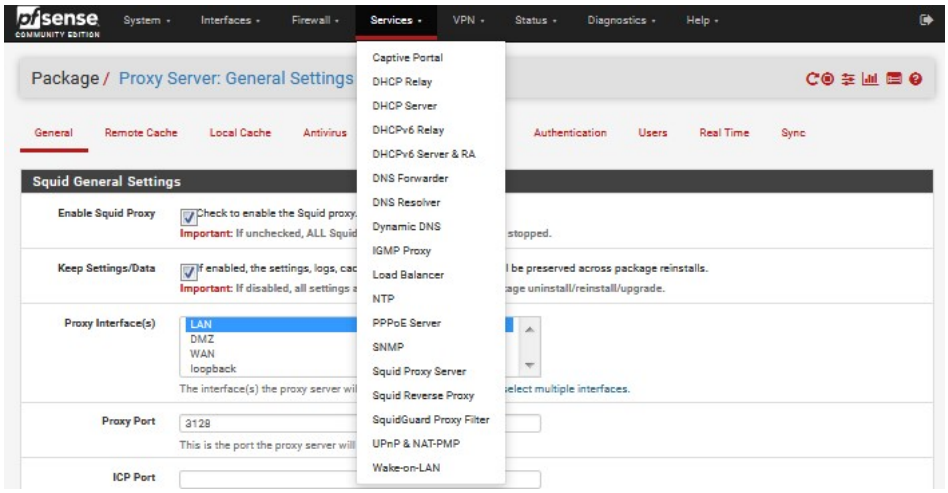
Cliquer sur "Save" pour enregistrer votre paramétrage.

Un message d'erreur va apparaitre, c'est normal.

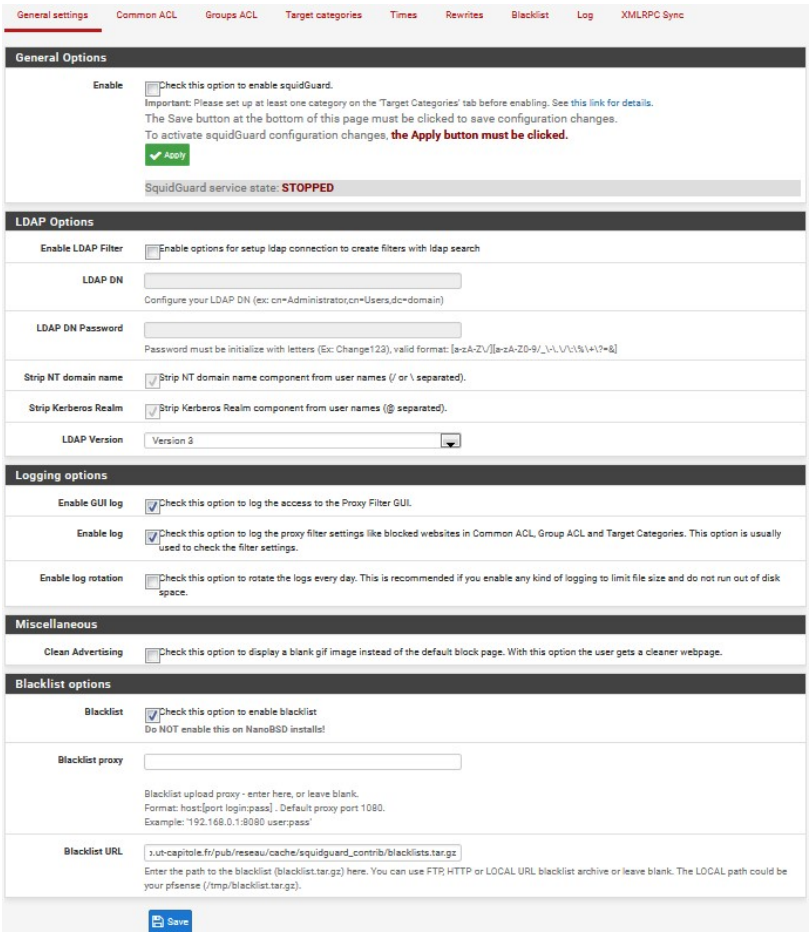


Aller dans "local cache"
Faire "save" tout en bas sans modifier les réglages.
Retourner sur "général" (vérifier bien que tout soit bien paramétrer car parfois la modification change) puis refaite "save"

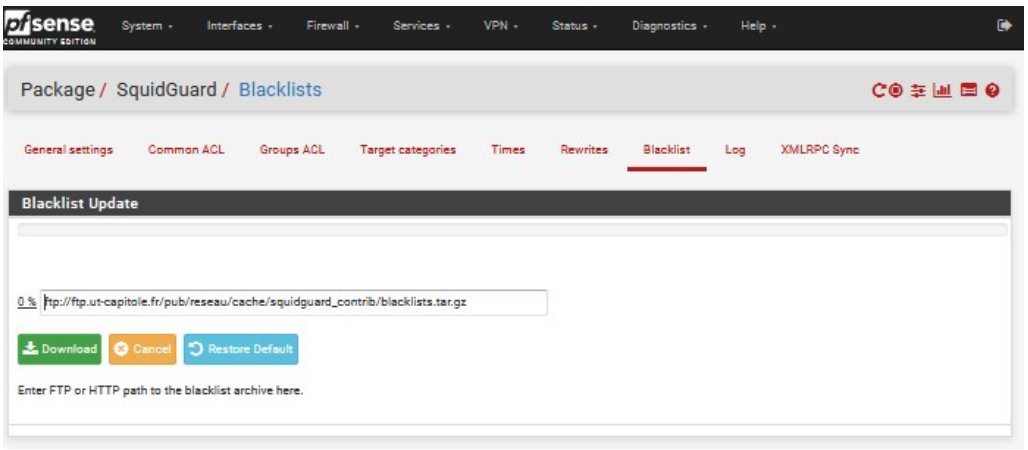
Aller dans service / squidguard proxy filter



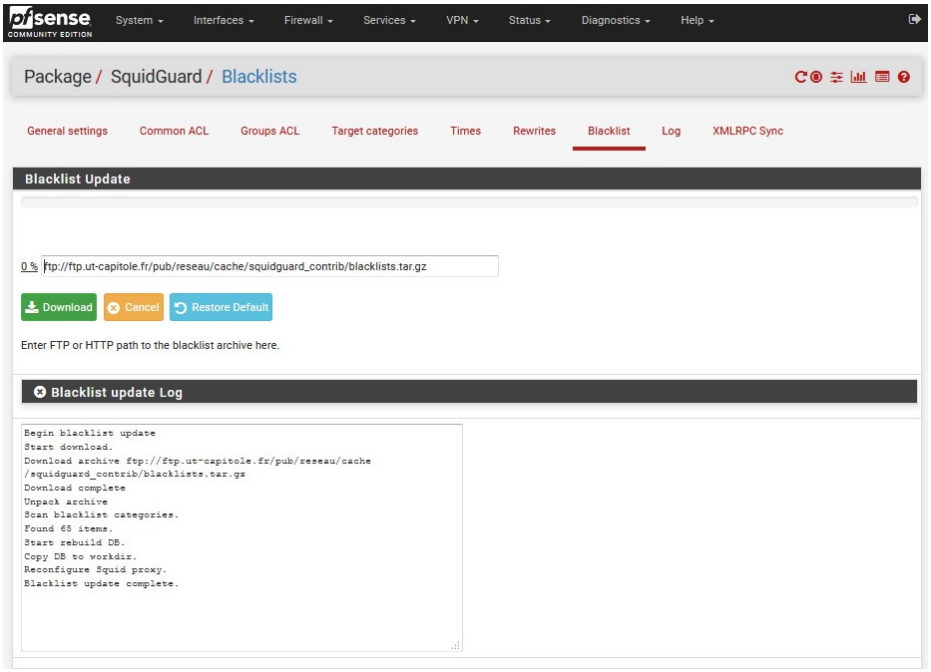
Remplissez le formulaire de la même façon
Récupérer la blacklist de l'IUT de Toulouse et rentrer le lien dans "Blacklist url" :
ftp://ftp.ut-capitole.fr/pub/reseau/cache/squidguard_contrib/blacklists.tar.gz



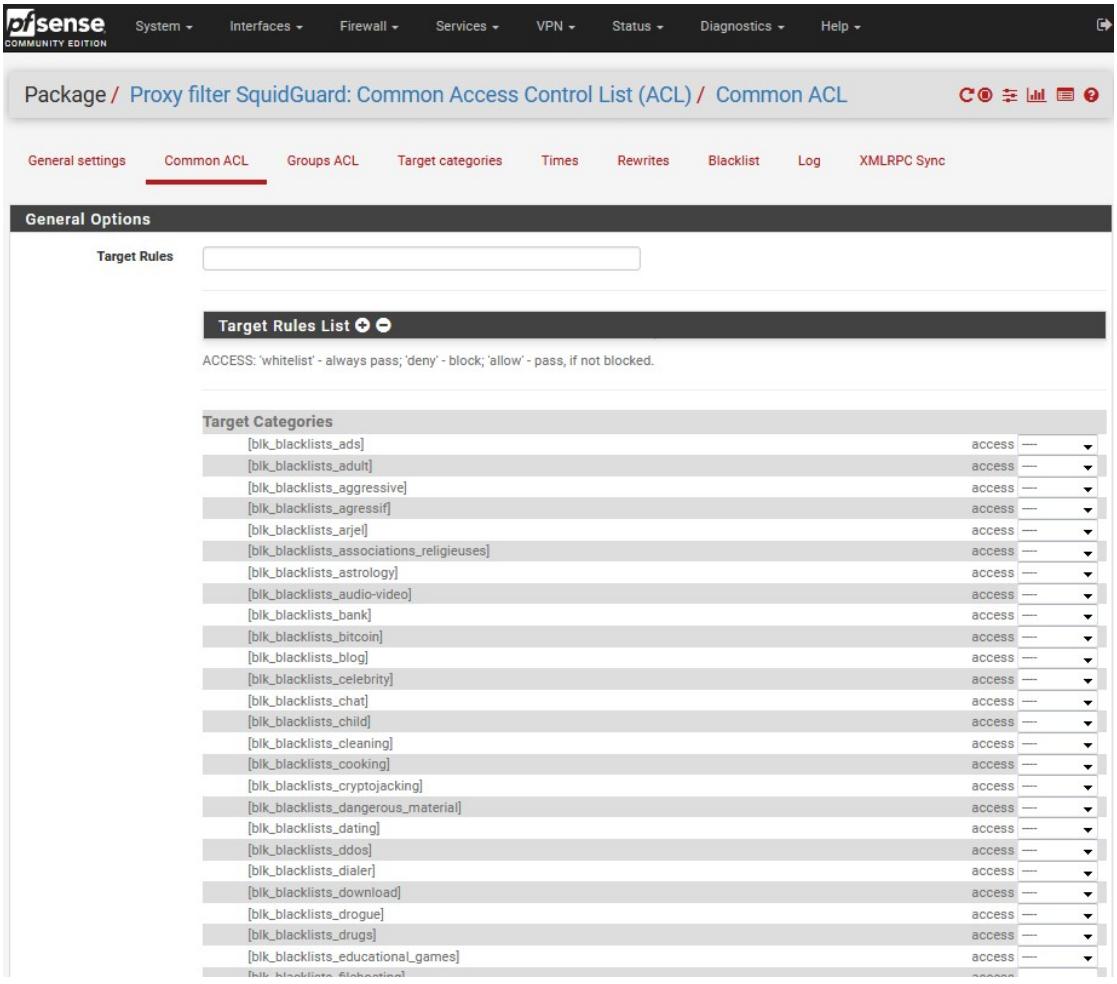
Dans l'onglet "blacklist", cliquer sur "download"
(spamer le bouton download j'usqu'a ce que ca marche)

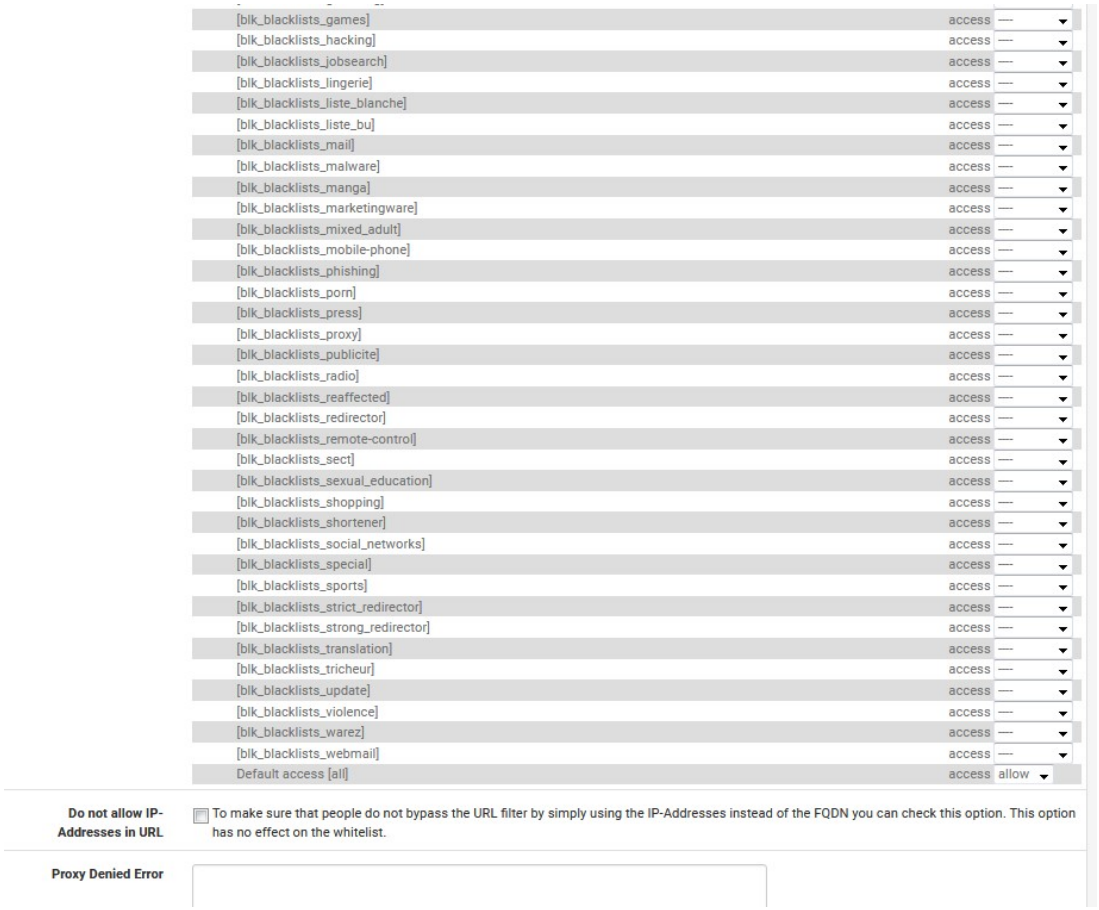


A la fin du téléchargement vous verrez



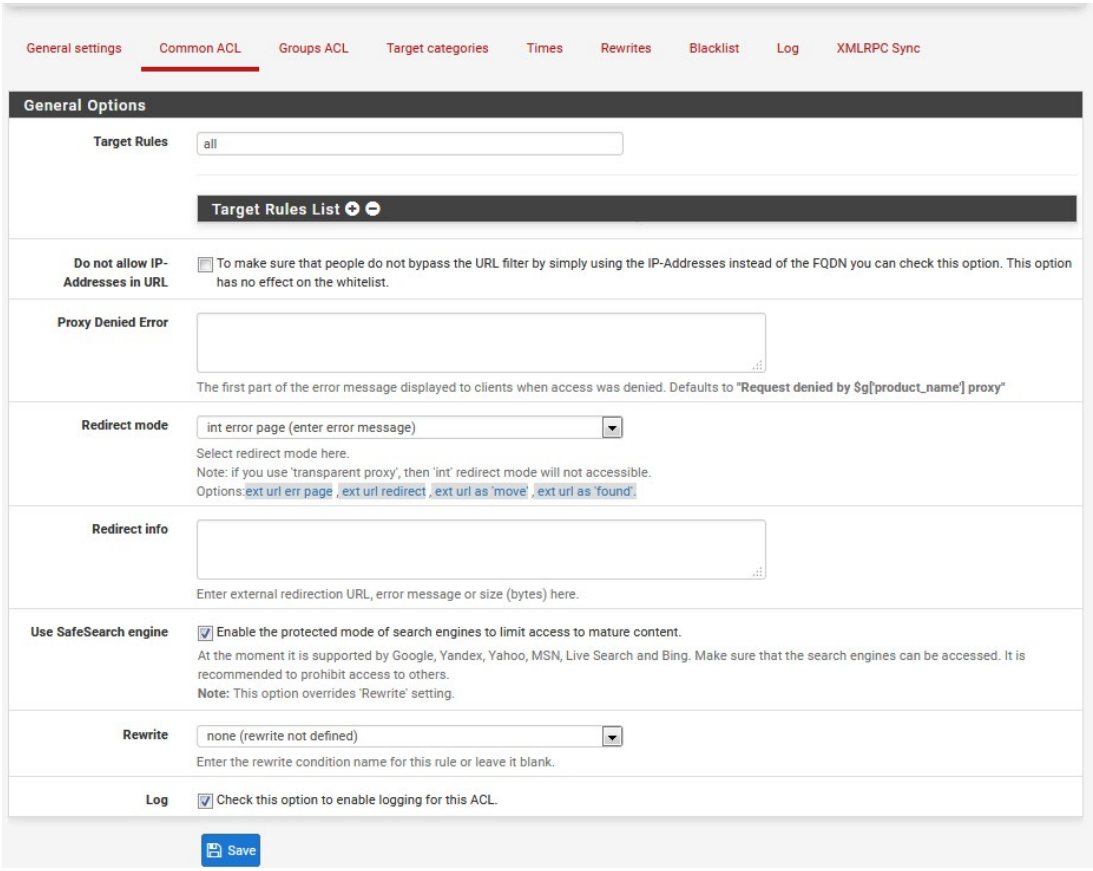
Dans l'onglet "common acl"
Cliquer sur +
Aller tout en bas et mettre "Default access [all]" sur "allow"
Puis choisir les catégorie a interdire en les mettant sur "deny"





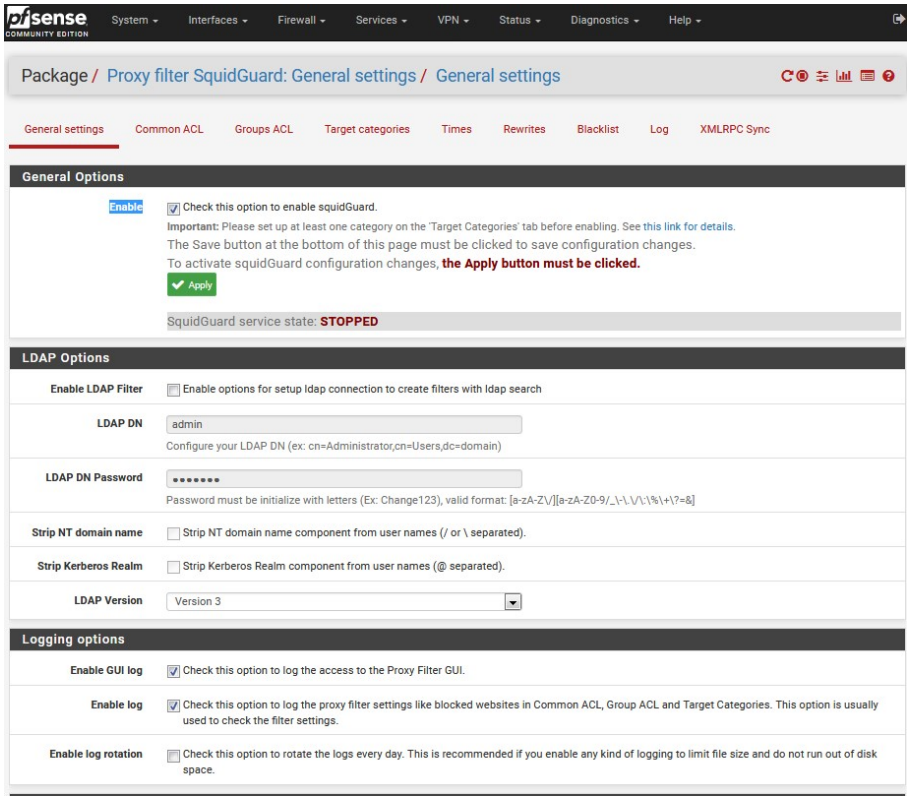
Et cliquer sur "Save"

Remplissez le formulaire de la même façon

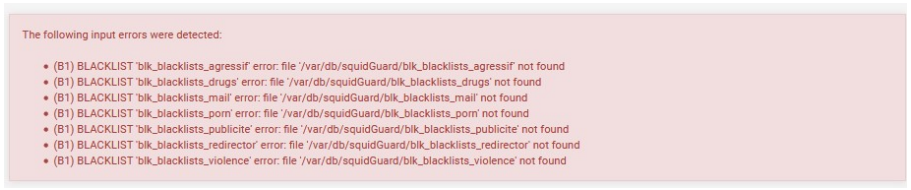


Et cliquer sur "Save"

Ensuite dans "general settings"
Puis "Enable"
Puis "apply"



Il va afficher des erreurs Blacklist, n'en tenez pas compte et faite "Save" tout en bas



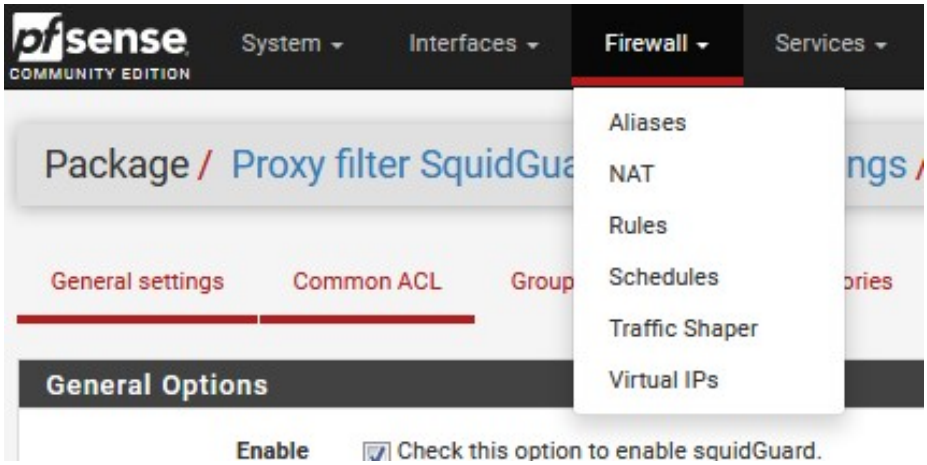
Maintenant le proxy est actif, il ne plus qu'à configurer les navigateurs.

Haute disponibilité serveur LAMP avec load balancing

En informatique, la répartition de charge (en anglais : load balancing) est un ensemble de techniques permettant de distribuer une charge de travail entre différents ordinateurs d'un groupe. Ces techniques permettent à la fois de répondre à une charge trop importante d'un service en la répartissant sur plusieurs serveurs, et de réduire l'indisponibilité potentielle de ce service que pourrait provoquer la panne logicielle ou matérielle d'un unique serveur.

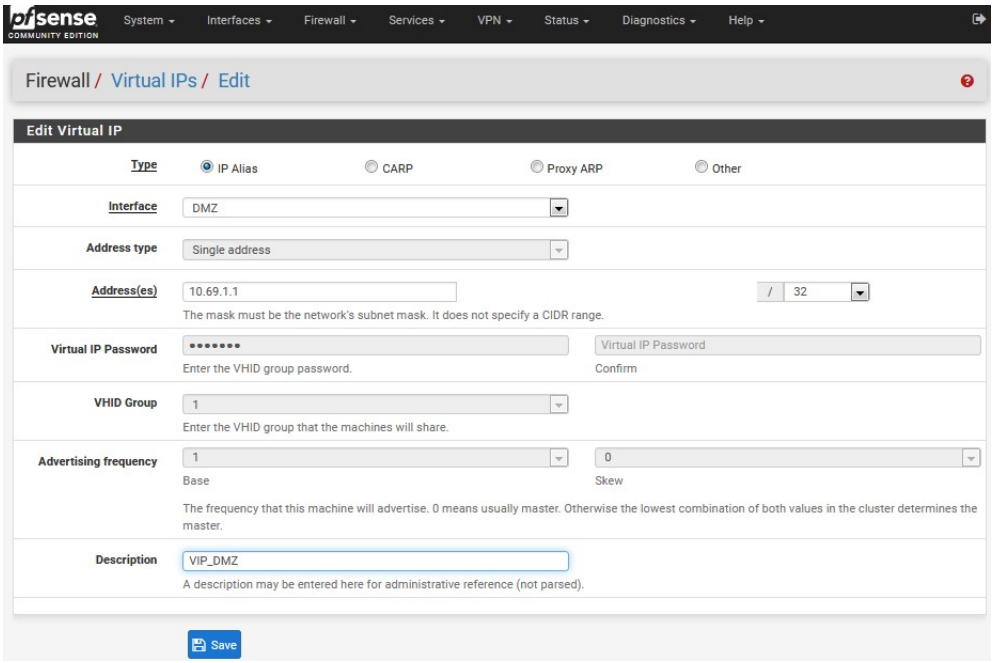
Sources: Wikipedia

On commence par crée l'ip virtuel en 10.69.1.1
On va dans firewall / Virtual IP

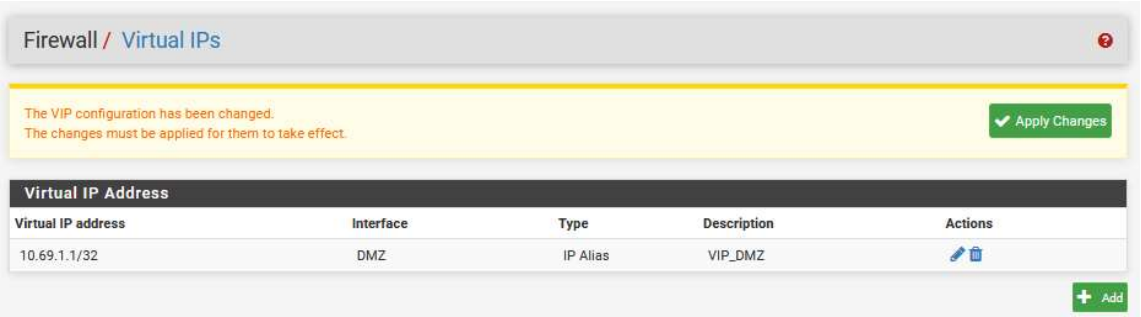


On clique ensuite sur "+add"

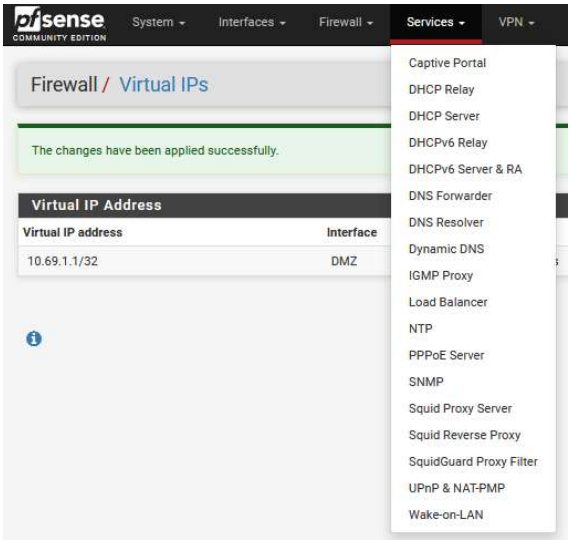
Remplissez le formulaire de la même façon



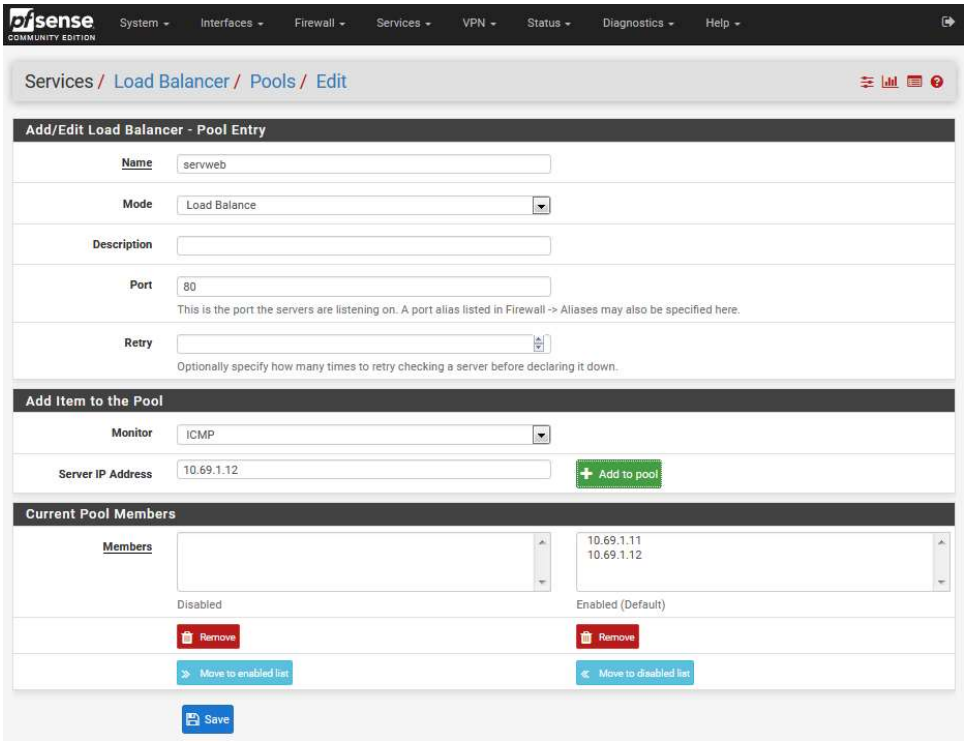
Cliquer sur "Apply changes" pour appliquer les changements



Maintenant allumer vos deux serveurs web

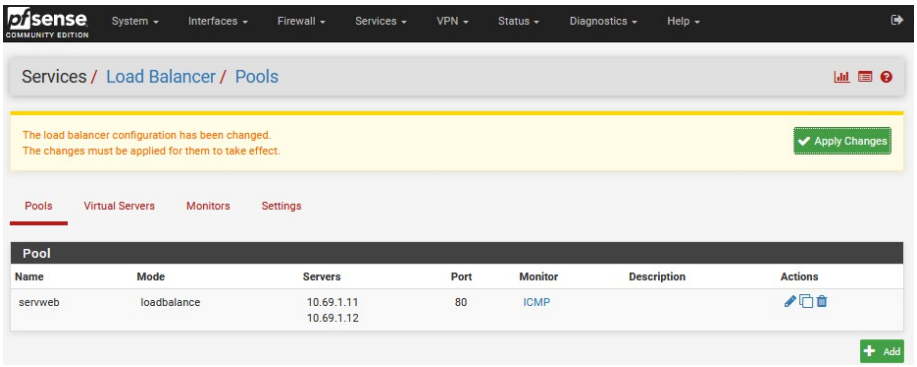


Aller dans : services / load balancer

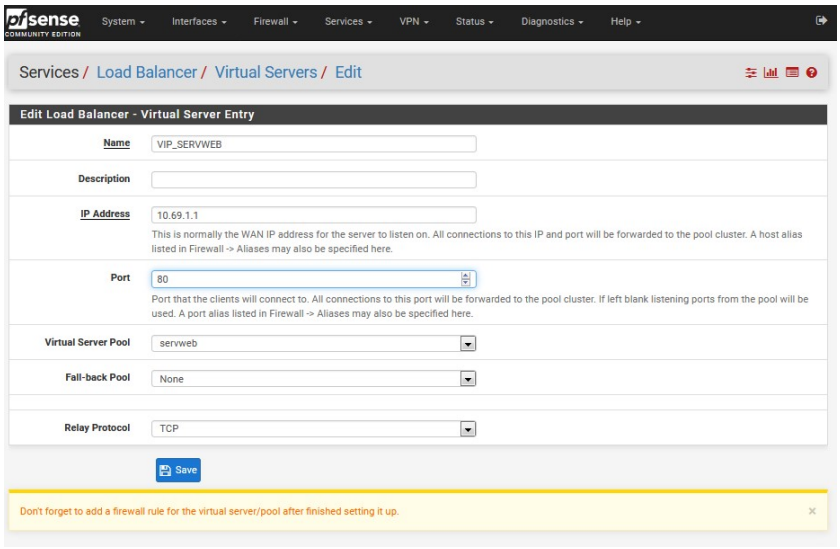


- Aller dans : pools
- Puis faite : "+add"
- Remplissez le formulaire de la même façon
- Et cliquer sur "Save"

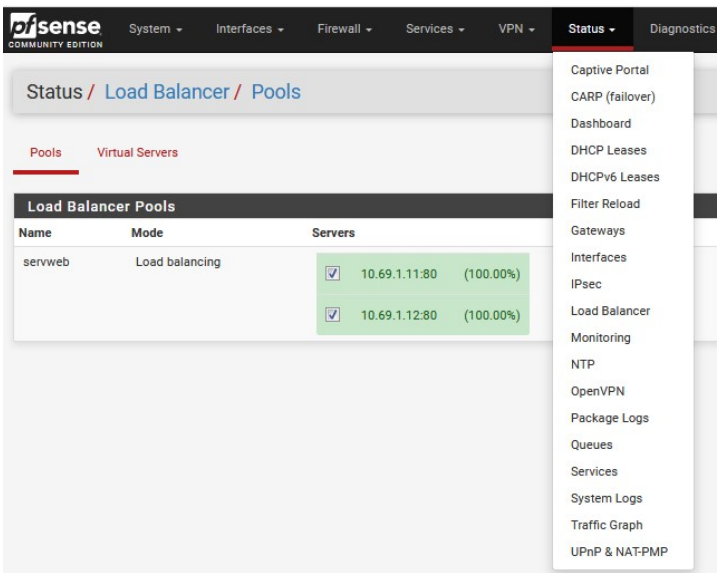
Cliquer sur "Apply changes" pour appliquer les changements



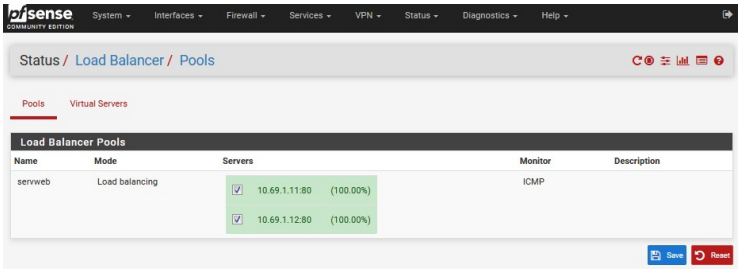
Aller dans l'onglet : "virtual server" puis "+add"

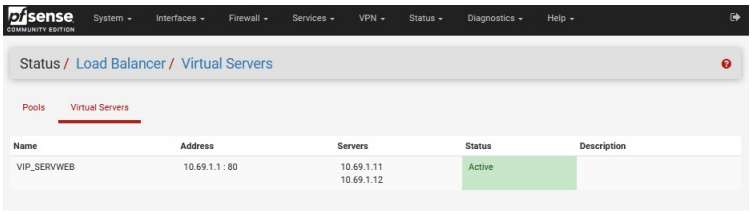


Puis cliquer sur "Apply changes" pour appliquer les changements



Aller dans status / load balancer





Nous pouvons voir que le load-balancing a bien été pris en compte sur les deux serveurs WEB.

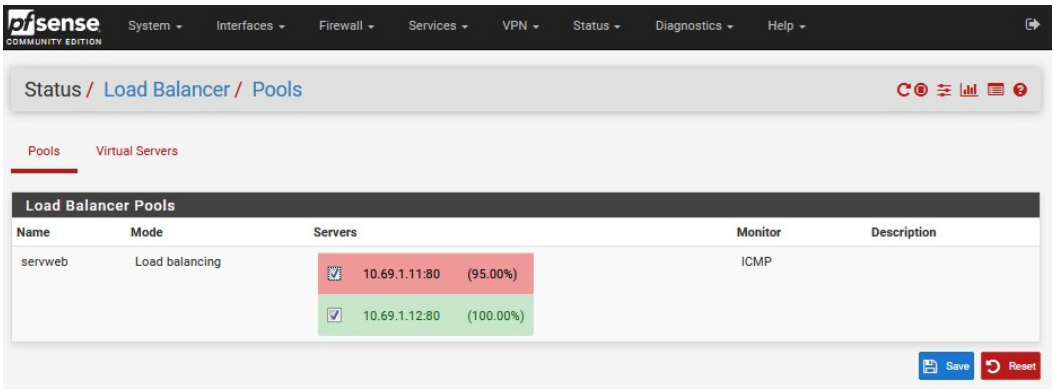
Les deux serveurs sont en vert, ce qui signifie qu'ils sont bien connecté et ont chacun une charge de 100%.

On peut voir qu'il a bien identifier et pris en compe les 2 adresses des serveur et leurs IP Virtuelle.

Test du load balancer

Pour tester le load balancer des serveur web, on va couper l'un des deux serveur web

- Couper l'un des deux serveurs WEB
- Aller dans status / load balancer grace a votre interface WEB de pfSense



On peut voir que le serveur en 10.69.1.11 est tombé et que le load balancer a bien fonctionné.

Donc le serveur WEB en 10.69.1.12 a pris la charge de l'autre serveur automatiquement sans que personne ne s'en rende compte car les utilisateurs pointe vers l'IP virtuelle.