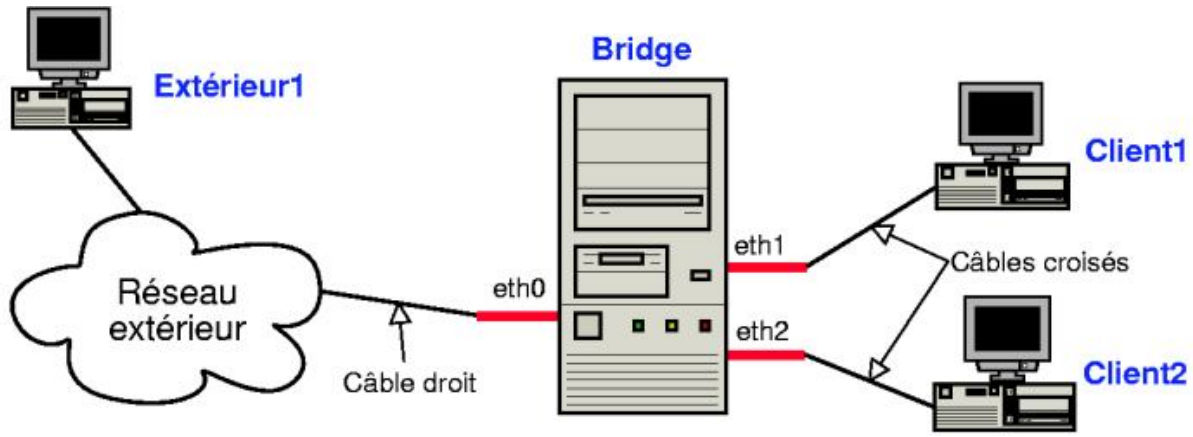
Mise en place d’une solution de pare-feu pfsense

Documentation :

1. Qu’est-ce qu’un Linux bridge ?
   L'idée est d'ajouter à votre ordinateur sous Linux la fonction de switch Ethernet aussi appelée bridge ;
   Pour ajouter à votre ordinateur sous Linux cette fonction de bridge, il lui faut au minimum deux cartes réseau. Chaque carte réseau devient alors l'équivalent d'un port du switch. Le bridge fonctionnera comme un switch Ethernet classique : il apprend tout seul les adresses MAC qui sont derrière ses interfaces réseau et aiguille les paquets Ethernet comme un switch. Par contre, contrairement à un switch classique, il ne croise pas la connexion réseau : il faudra donc relier le bridge aux autres ordinateurs par des câbles croisés, et aux autres switchs par des câbles droits (les câbles "normaux" sont des câbles droits).



2. Qu’elle est sa fonction ici ?

3. Définissez la fonction d’un pare-feu.
   Un pare-feu 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.

4. Sur quel système d’exploitation est basé pfsense ?
   pfSense est une distribution de type « routeur / pare-feu », sous FreeBSD. C'est un système d'exploitation à part entière dont les maîtres mots sont fiabilité, rapidité, robustesse.

5. Relevez les services essentiels fournis par cette solution.

pfSense permet :

Filtrage par IP source et destination, port du protocole, IP source et destination pour le trafic TCP et UDP
Capable de limiter les connexions simultanées sur une base de règle
pfSense utilise p0f, un utilitaire permettant de filtrer le trafic en fonction du système d'exploitation qui initie la connexion.
Possibilité d'enregistrer ou de ne pas enregistrer le trafic correspondant à chaque règle.

Politique très souple de routage possible en sélectionnant une passerelle sur une base par règle (pour l'équilibrage de charge, basculement, connexions WAN multiples, etc).
Utilisation d'alias permettant le regroupement et la désignation des adresses IP, des réseaux et des ports, rendant ainsi votre jeu de règles de pare-feu propre et facile à comprendre, surtout dans des environnements avec plusieurs adresses IP publiques et de nombreux serveurs.
Filtrage transparent au niveau de la Couche 2, le pare-feu est capable d'agir en pont filtrant.
La normalisation des paquets est utilisée, il n'y a donc aucune ambiguïté dans l'interprétation de la destination finale du paquet. La directive « scrub » réassemble aussi des paquets fragmentés, protège les systèmes d'exploitation de certaines formes d'attaque, et laisse les paquets TCP contenant des combinaisons de Flags invalides.
Activé dans pfSense par défaut Vous pouvez le désactiver si nécessaire. Cette option provoque des problèmes pour certaines implémentations NFS, mais elle est sûre et devrait être laissée activée sur la plupart des installations. Désactiver le filtre - vous pouvez désactiver entièrement le filtre de pare-feu si vous souhaitez configurer pfSense comme un routeur pur.

Network address translation (NAT)
Rediriger les ports y compris les rangs et l'utilisation de plusieurs adresses IP publiques NAT pour les adresses IP individuelles ou des sous-réseaux entiers.
Redirection NAT Par défaut, le NAT redirige tout le trafic sortant vers l'adresse IP WAN.
Dans le cas de connexions WAN multiples, le NAT redirige le trafic sortant vers l'adresse IP de l'interface WAN utilisée.
NAT réflexion : dans certaines configurations, NAT réflexion est possible si les services sont accessibles par IP publique à partir de réseaux internes.

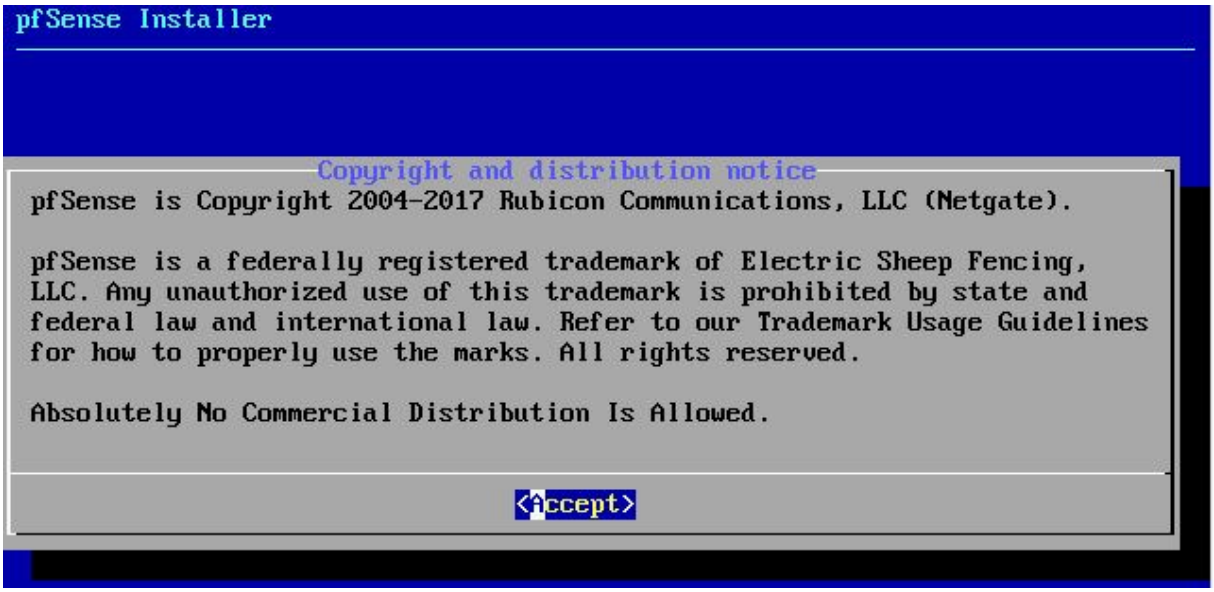
Basculement base sur CARP et pfsync
Common Address Redundancy Protocol ou CARP est un protocole permettant à un groupe d'hôtes sur un même segment réseau de partager une adresse IP.
Le nom CARP est en fait un sigle qui signifie « Common Address Redundancy Protocol » (Protocole Commun De Redondance D'Adresse), à ne pas confondre avec « Cache Array Routing Protocol » utilisé pour faire de la répartition de charge de mandataires caches web. Il a été créé pour contourner des brevets.
Ce protocole peut être utilisé pour faire de la redondance et de la répartition de charge. Il supporte IPv4 et IPv6, et à le numéro de protocole 112. Il est supporté par pfSense.

pfsync assure la table d'état du pare-feu qui est répliquée sur tous les pare-feu configurés de basculement.
Cela signifie que vos connexions existantes seront maintenues dans le cas d'échec, ce qui est important pour prévenir les perturbations du réseau.
Load Balancing/ Répartition de charge :
La répartition de charge du trafic sortant est utilisée avec plusieurs connexions WAN pour assurer la répartition de charge et des capacités de basculement.
Le trafic est dirigé vers la passerelle souhaitée ou le groupe d'équilibrage local.

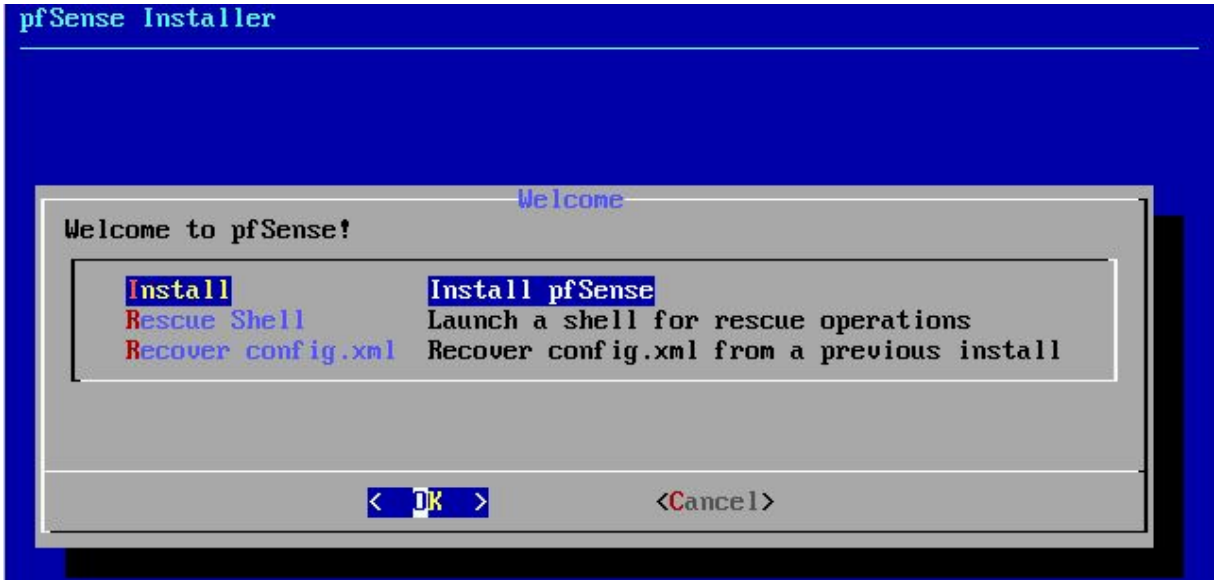
6. Relevez les services nécessaires à la navigation internet
   Http/https port 80/443 et DNS

Installation pfSense

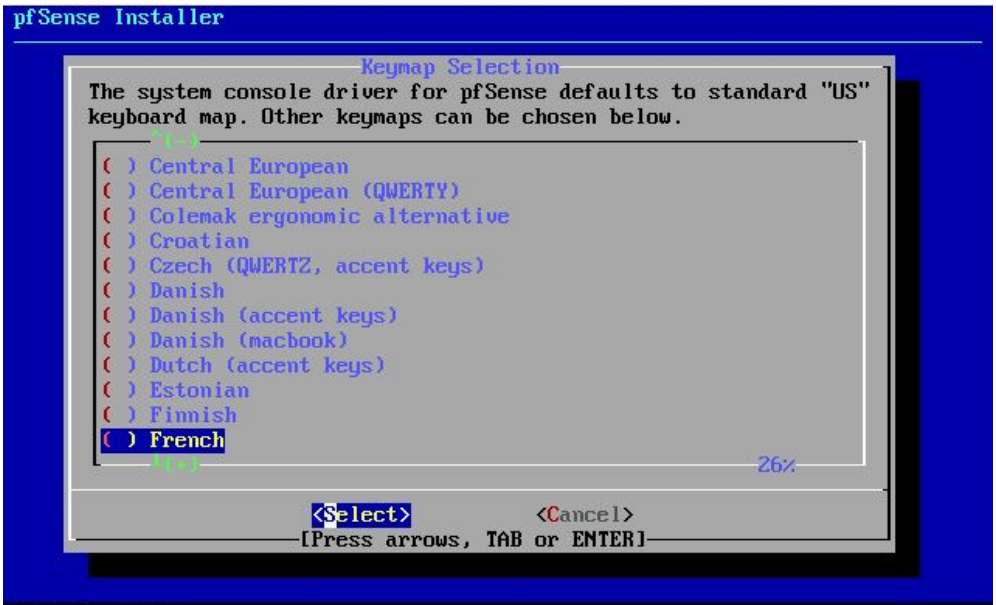
Accepter la licence.



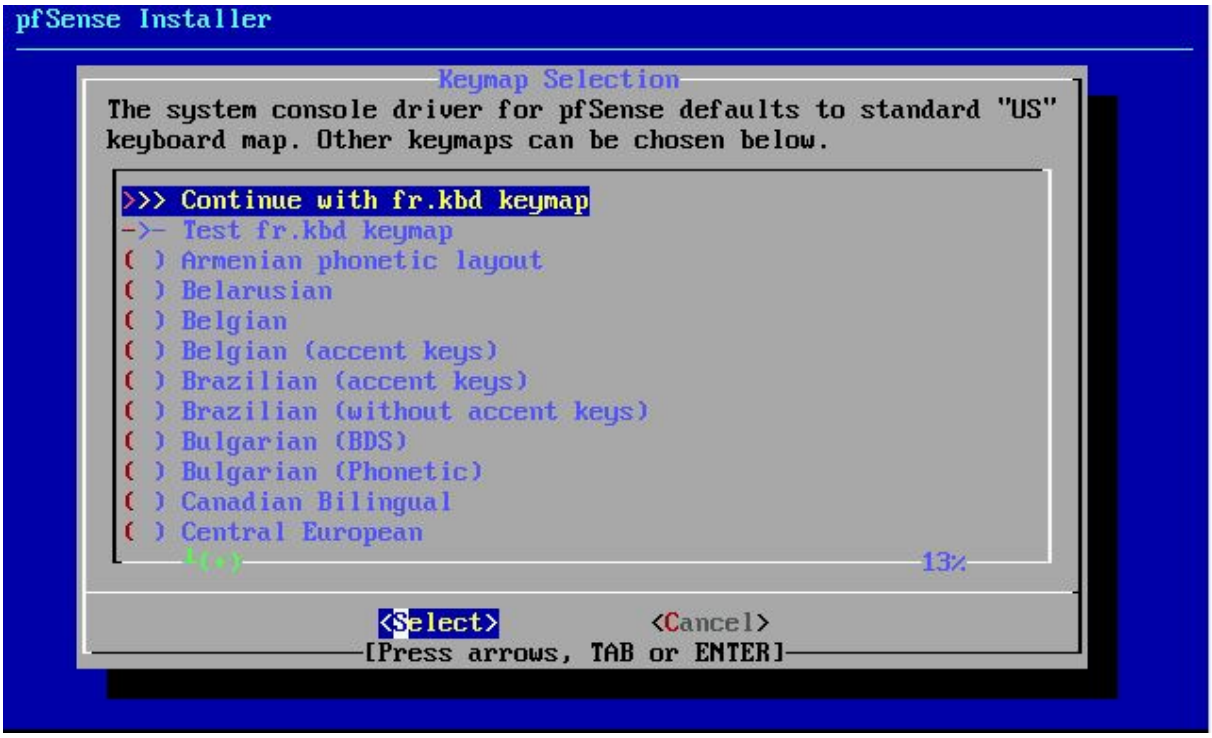
Installez pfSense : OK



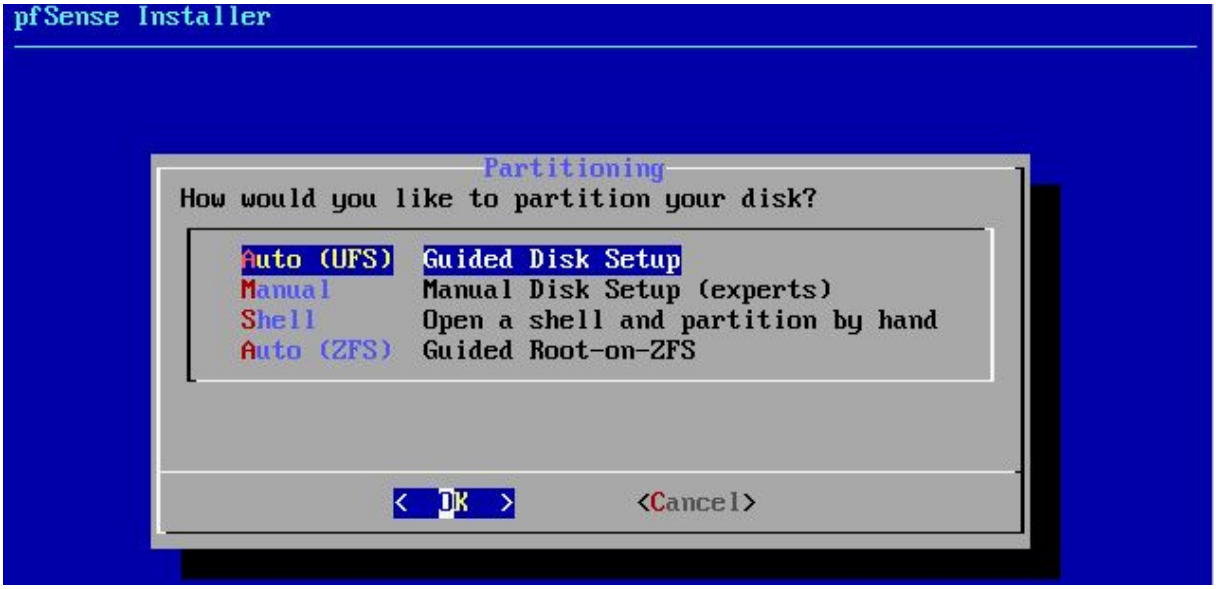
Sélectionnez la langue « French »



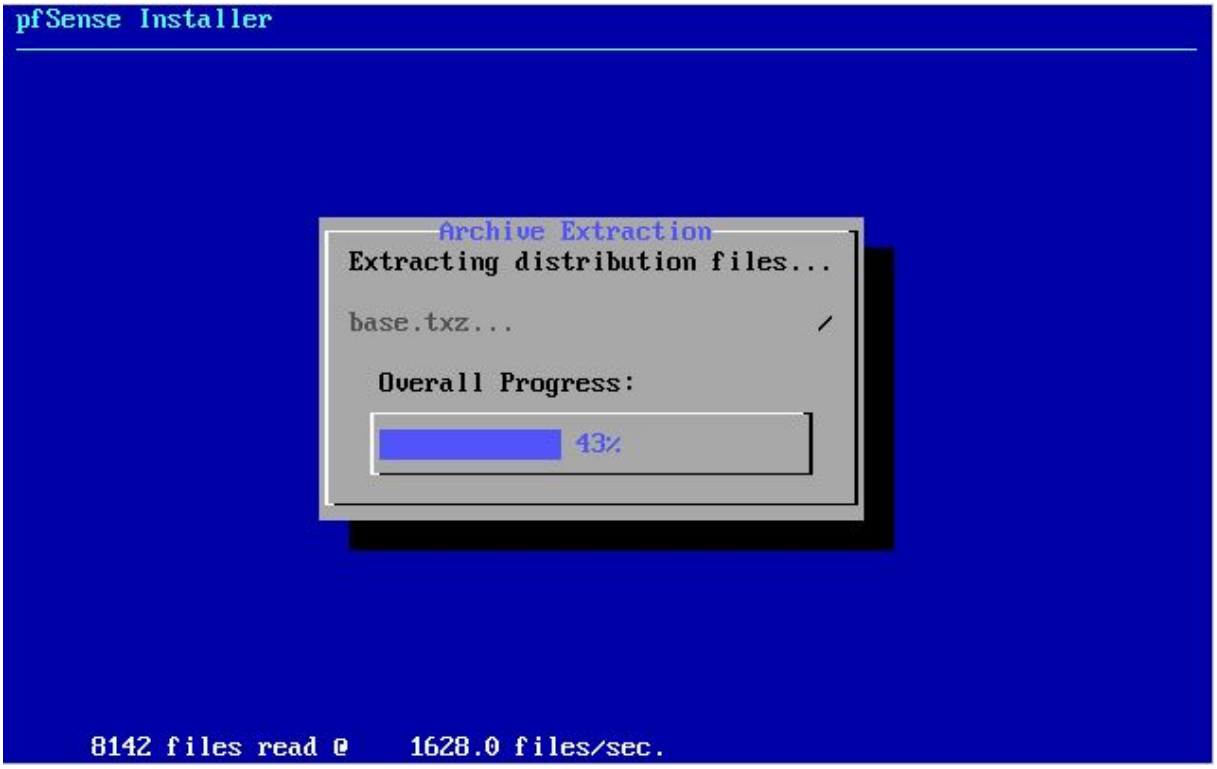
Sélectionnez : Continue With fr.kbd Keymap



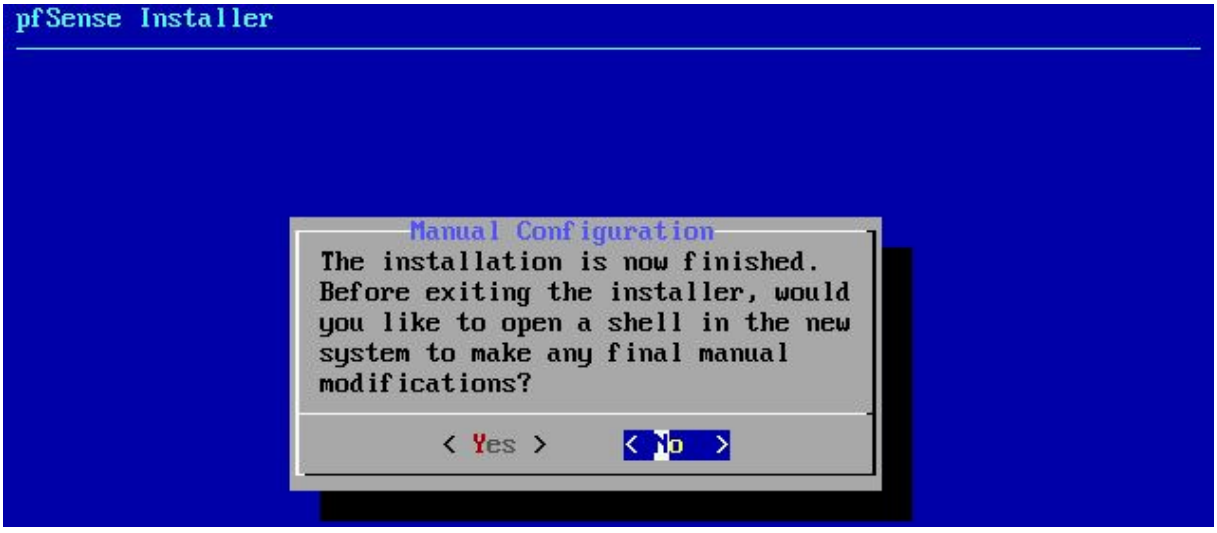
Sélectionnez Auto (UFS) (la configuration de disque guidée) qui veut dire fixer automatiquement les partitions disque et utilise le système de fichiers UFS.
UFS, abréviation de Unix File System, est un système de fichiers utilisé par de nombreux systèmes d'exploitation de type Unix, FreeBSD, NetBSD, OpenBSD.



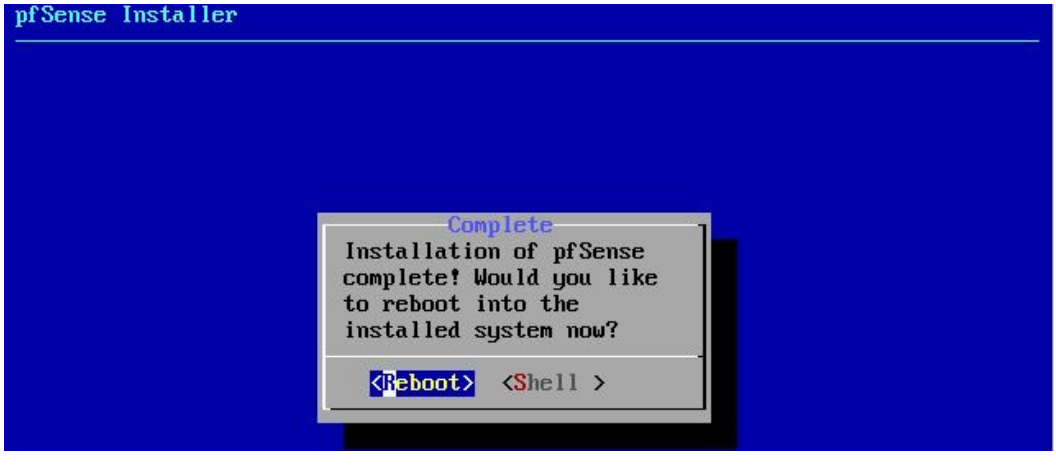
Patientez pendant l'installation.



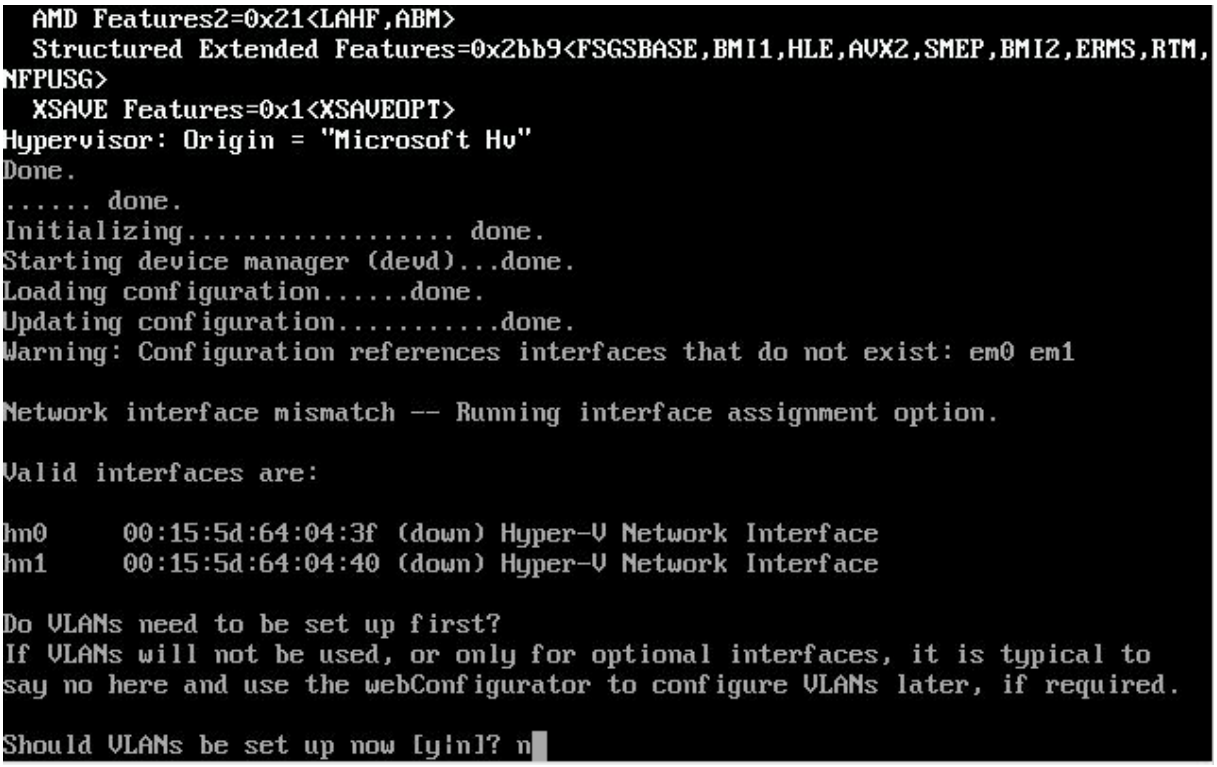
Avant de quitter le programme d'installation, souhaitez-vous ouvrir un shell dans le nouveau système pour effectuer les dernières modifications manuelles ?
Faites oui ou non. Dans notre cas on fait non.



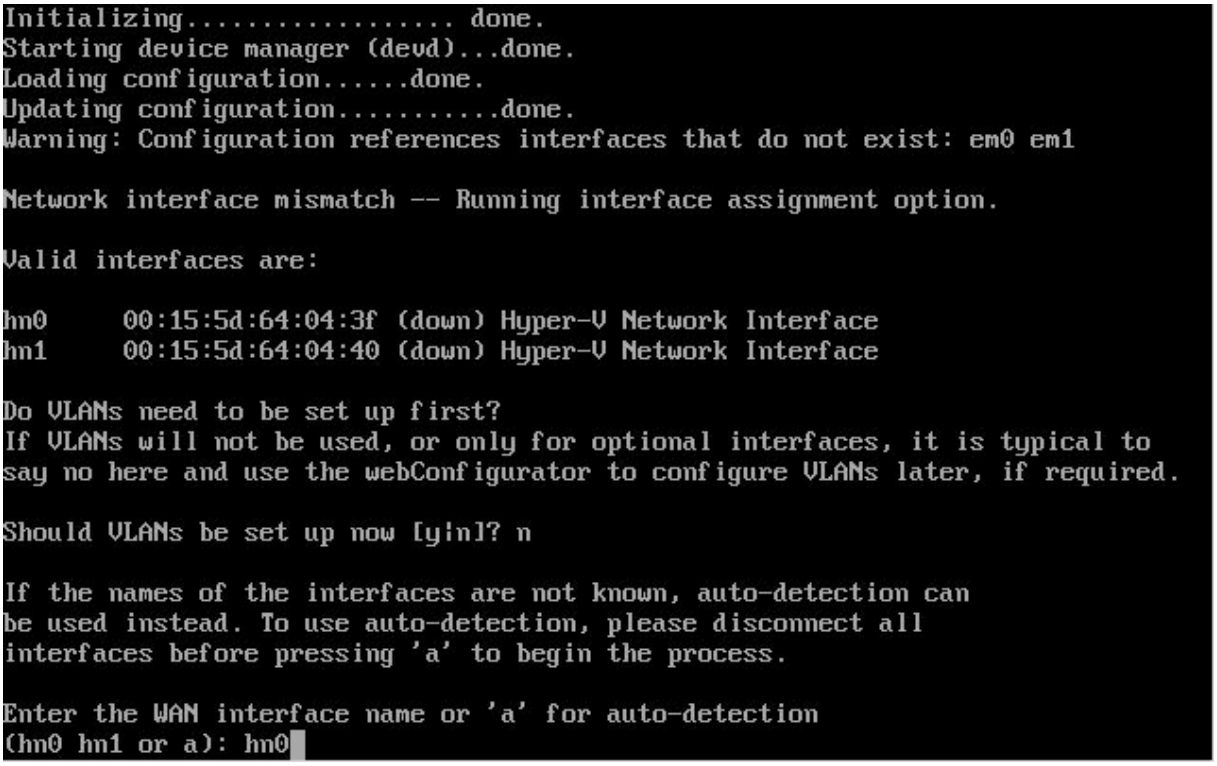
Sélectionnez Reboot (ne pas oublier d'éjecter le cd si vous ne voulez pas que l'installation se relance)



Saisissez “n” si vous voulez faire des VLAN sinon sélectionner “no”.



Sélectionnez la carte réseau internet Wan hno (sélectionnez votre carte réseau).



Sélectionnez la carte réseau local LAN hn1

```
Warning: Configuration references interfaces that do not exist: em0 em1

Network interface mismatch -- Running interface assignment option.

Valid interfaces are:

hn0     00:15:5d:64:04:3f (down) Hyper-V Network Interface
hn1     00:15:5d:64:04:40 (down) Hyper-V Network Interface

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

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(hn0 hn1 or a): hn0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(hn1 a or nothing if finished): hn1
```

Appliquez les changements : “y” pour “yes”.

```
The interfaces will be assigned as follows:

WAN  -> hn0
LAN  -> hn1

Do you want to proceed [y|n]? y
```

Et nous voici au Menu.

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.4.4-RELEASE amd64 Thu Sep 20 09:03:12 EDT 2018
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

Hyper-V Virtual Machine - Netgate Device ID: 391ed73786ee43989c09

*** Welcome to pfSense 2.4.4-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> hn0        -> v4/DHCP4: 192.168.100.150/24
 LAN (lan)       -> hn1        -> 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:
```

Configuration de l'adresse IP de la carte réseau local LAN hn1

Sélectionnez : 2 (Set interface IP address)
Sélectionnez la carte réseau local LAN : 2

```
Available interfaces:

1 - WAN (hn0 - dhcp, dhcp6)
2 - LAN (hn1 - static)

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

Saisissez l'adresse IP souhaitée :
Saisissez le masque sous réseau au format CIDR : 24
Laissez vide pour ne pas définir la passerelle : Tapez ENTREE.

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

Laissez vide pour ne pas définir d'adresse IPV6 : Tapez ENTREE.

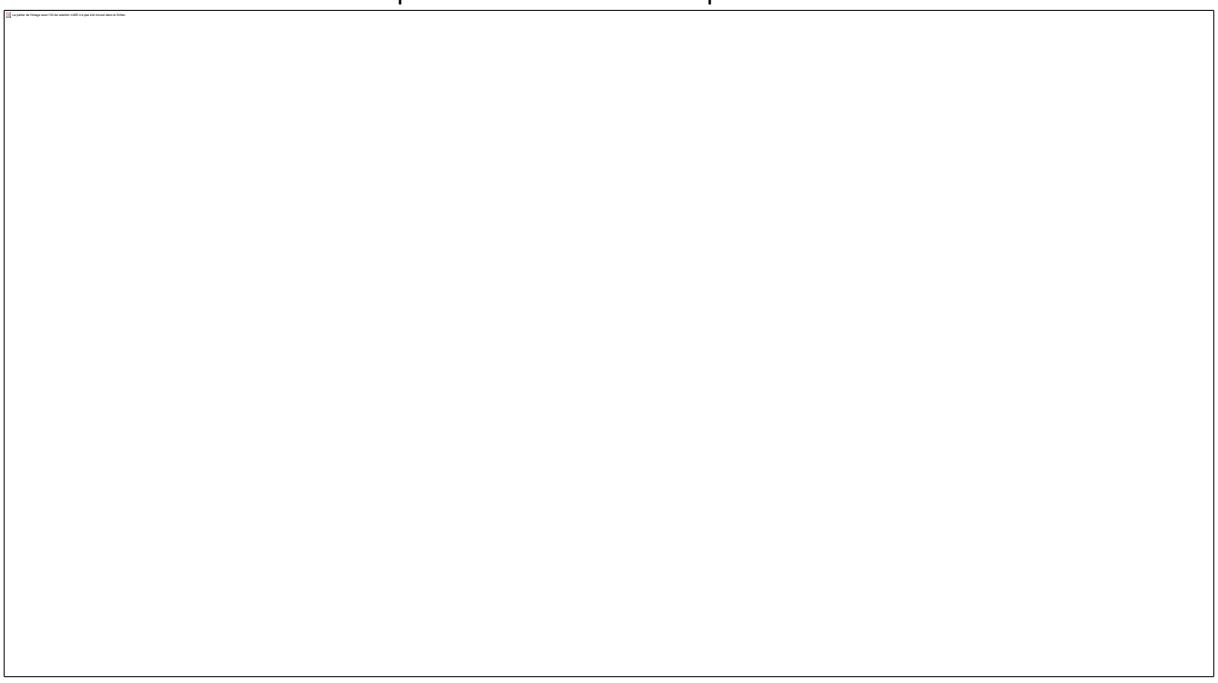
```
Enter the new LAN IPv6 address.  Press <ENTER> for none:
>
```

Activez le Serveur DHCP : "y" pour "yes".

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

Définir la plage d'adressage IP du DHCP (exemple : 192.168.200.10 jusqu'à 192.168.200.30)
Ne pas activer le retour http car il ne sera pas sécurisé, faites non.

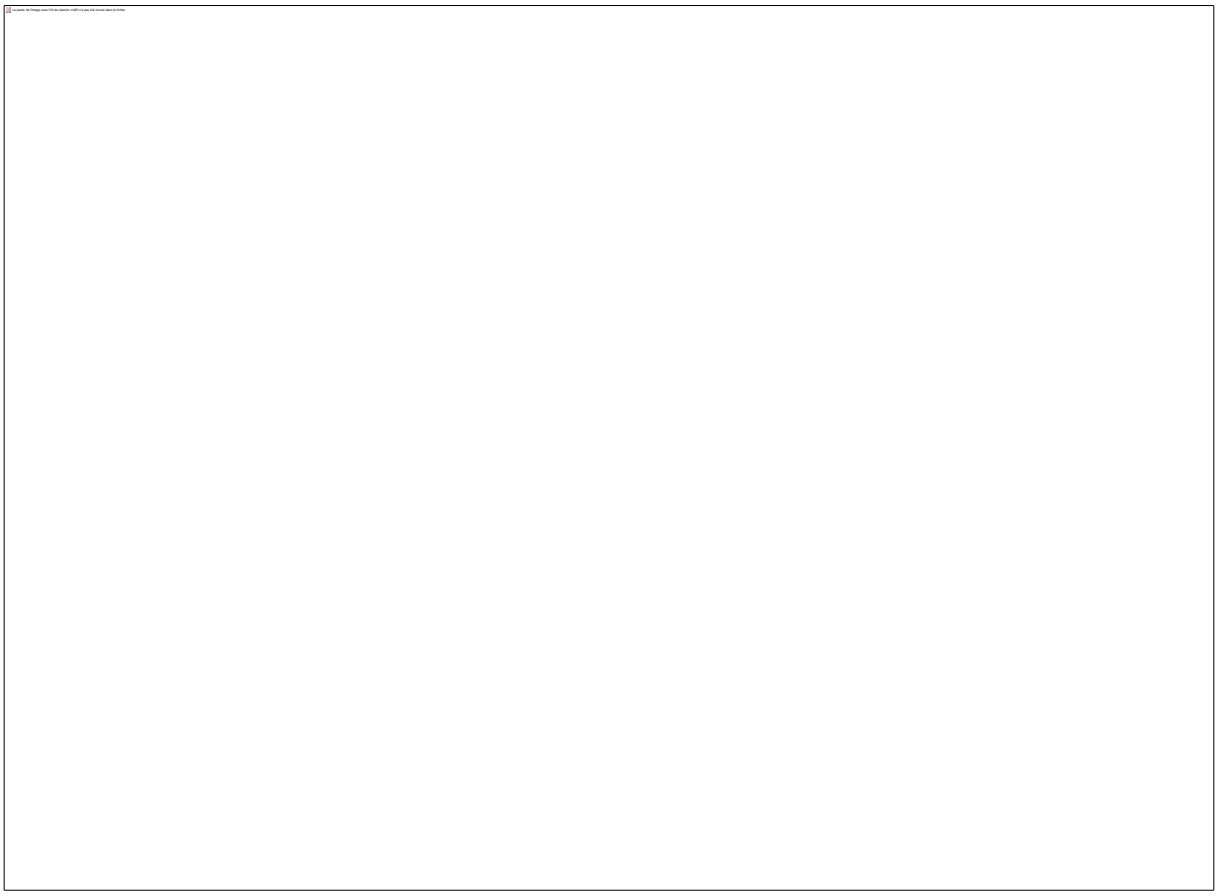
Ce qui nous permet de nous connecter en https.
Configuration terminée.
Retour au Menu. L'adresse IP de pfSense est notée dans la partie LAN : 192.168.200.254



On se connecte au portail pfSense avec l'IP du LAN.

Dans system information vous pouvez trouver toutes les informations de votre machine, le CPU, ID de pfSense, BIOS, Version, combien de temps la machine est allumée, la date, les DNS (si vous en avez plusieurs), combien de RAM est utilisé et la quantité de disk utilisé.

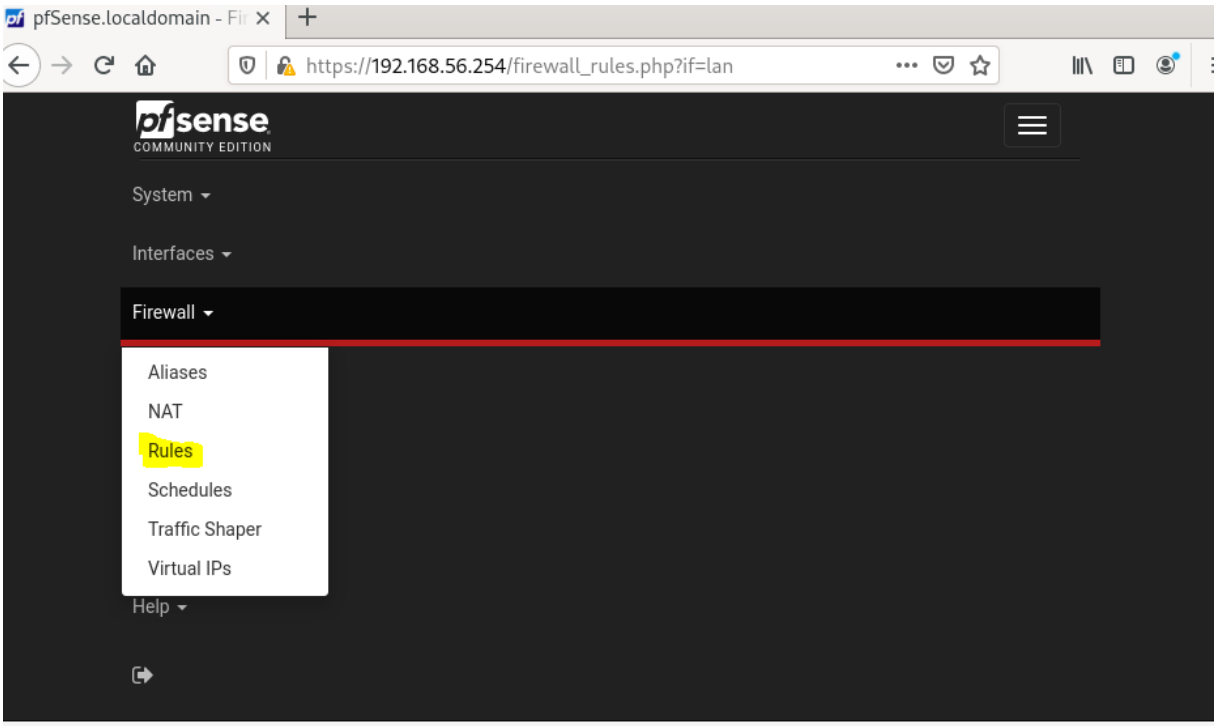
Vous pouvez ajouter une représentation graphique du trafic LAN / WAN.

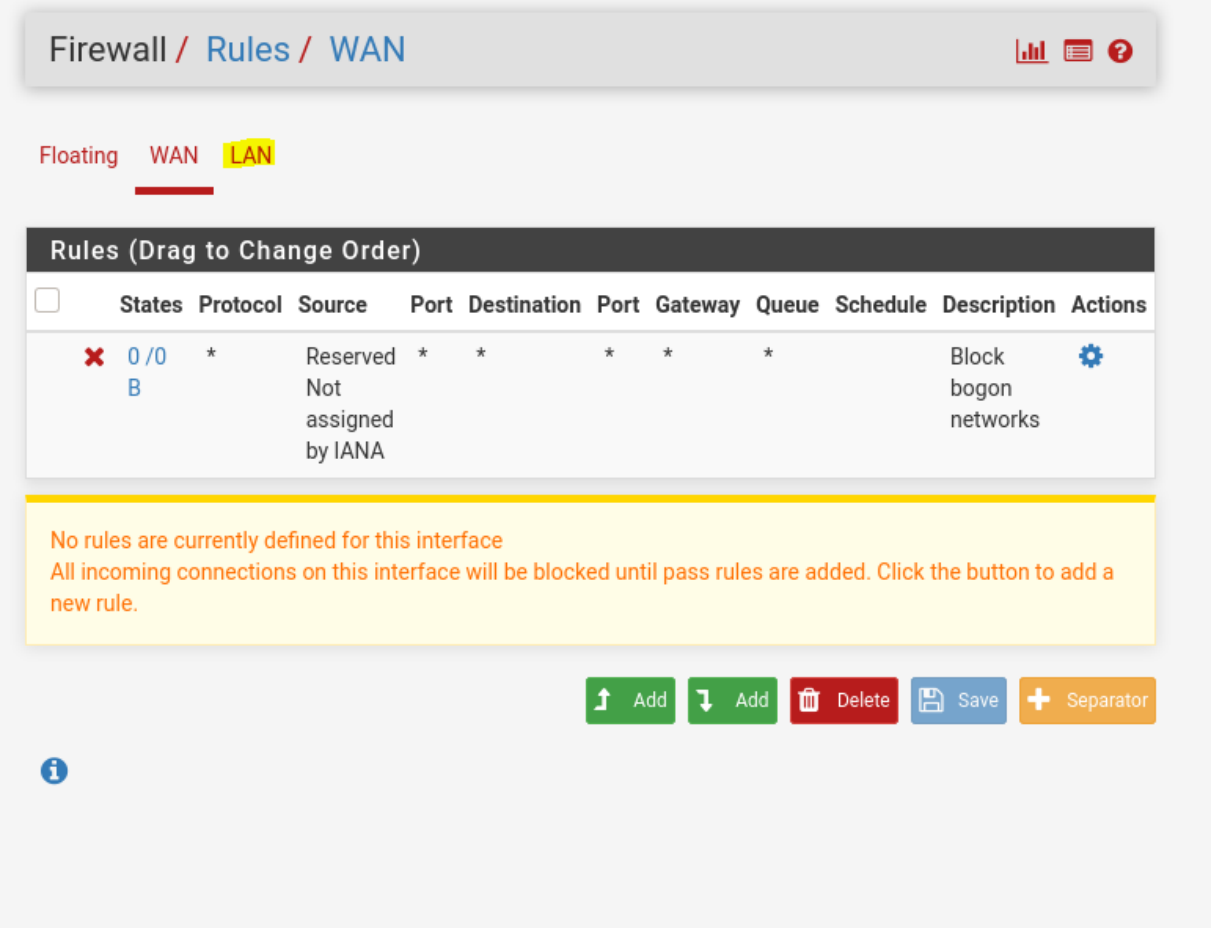


Pour se faire, remontez tout en haut de la page, suivez la ligne Status / Dashboard, au bout de cette ligne vous trouverait un +, cliquez et ajoutez les fonctionnalités qu'il vous convient.

Création de règle de filtrage.

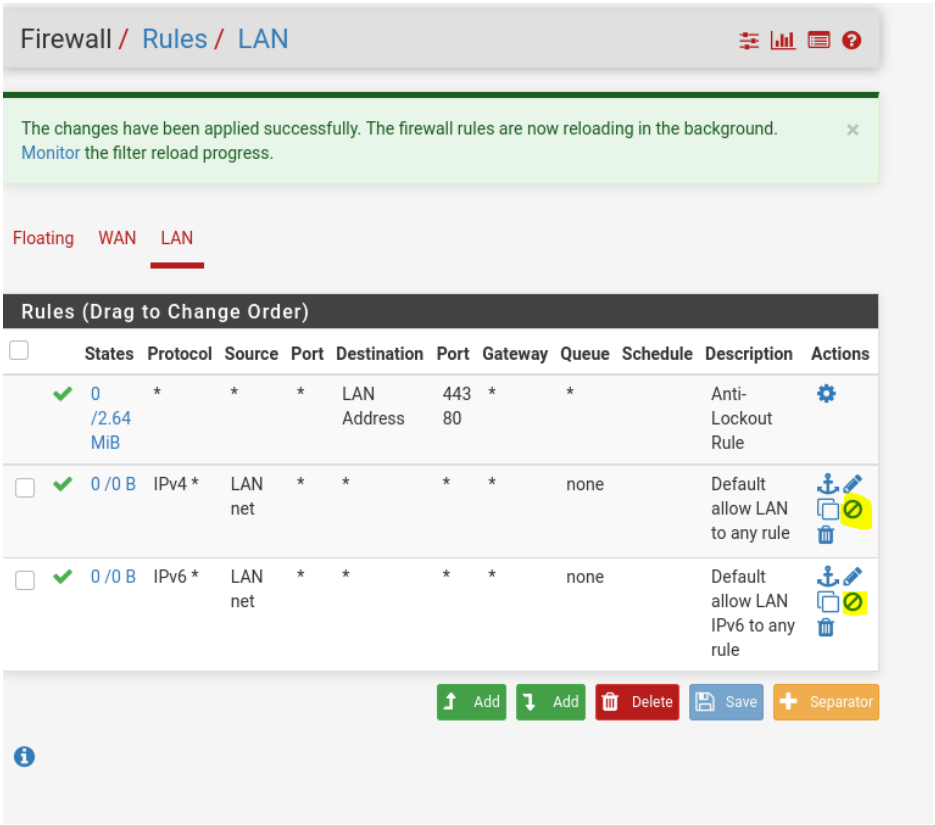
Il faut se rendre dans Firewall, Rules et on choisit l'interface LAN.



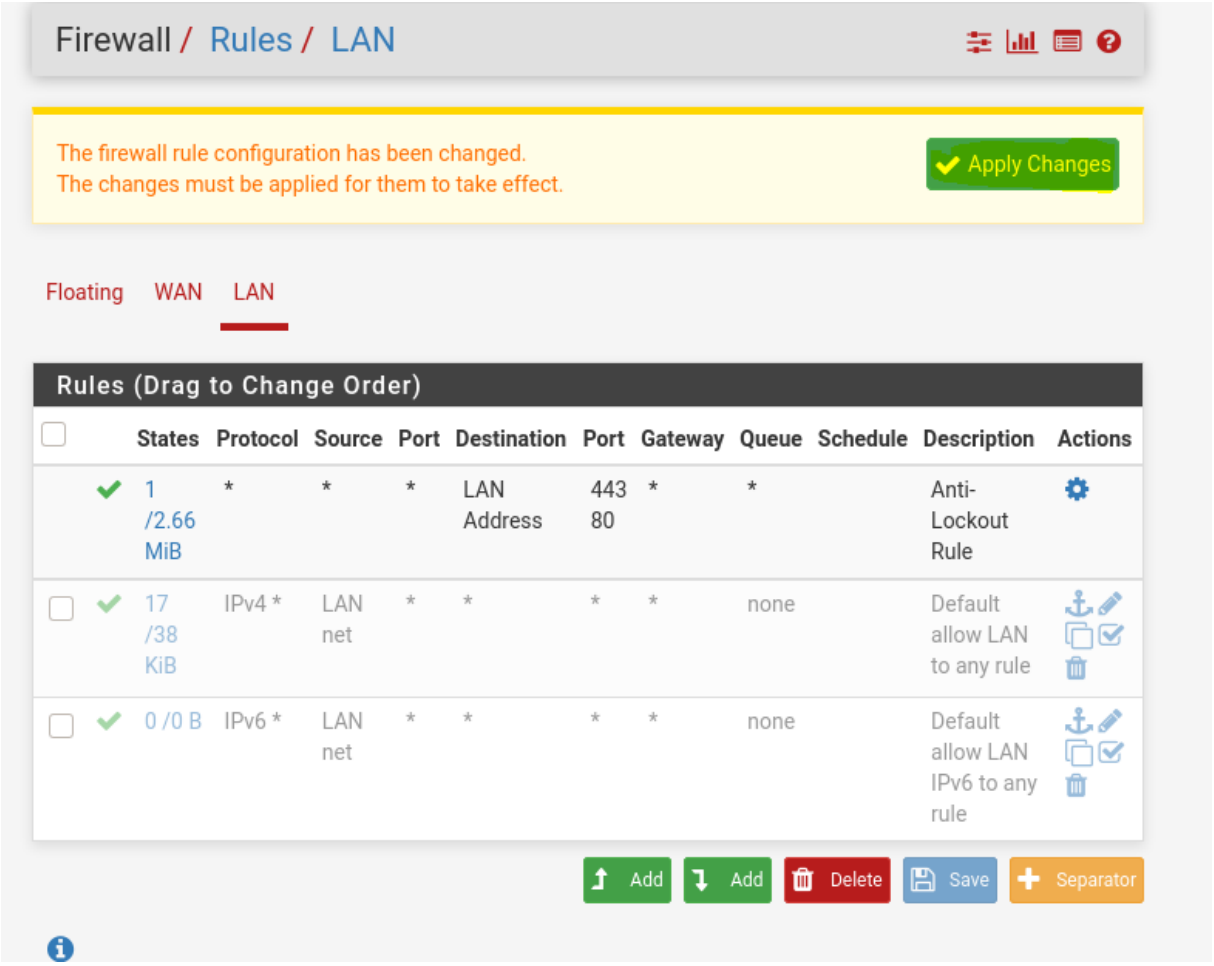


Nous voulons restreindre les protocoles réseaux pour effectuer un premier filtrage.

Sur cette image tout est autoriser donc nous allons les désactiver (ne pas supprimer ça pourrait vous servir à des tests si cela ne fonctionne pas). Pour les désactiver cliquer sur l'icône en jaune.

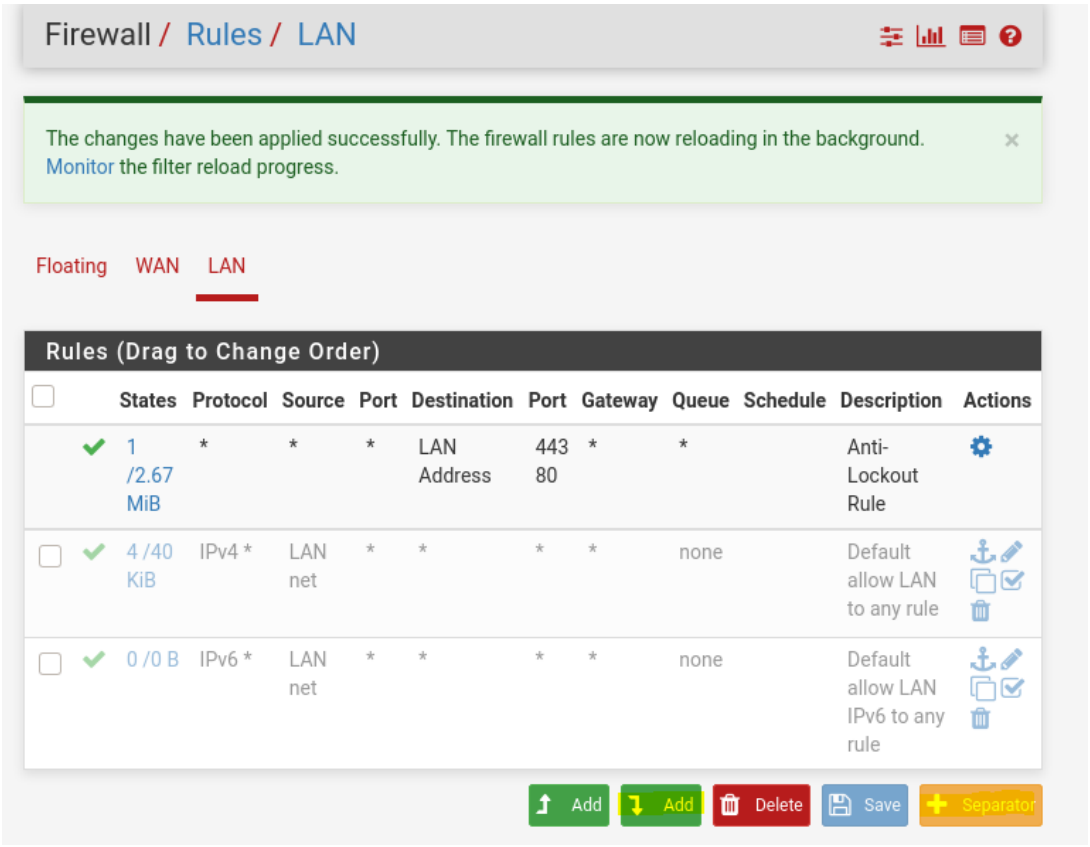


Il ne faut pas oublier d'appliquer les changements après chaque modification.

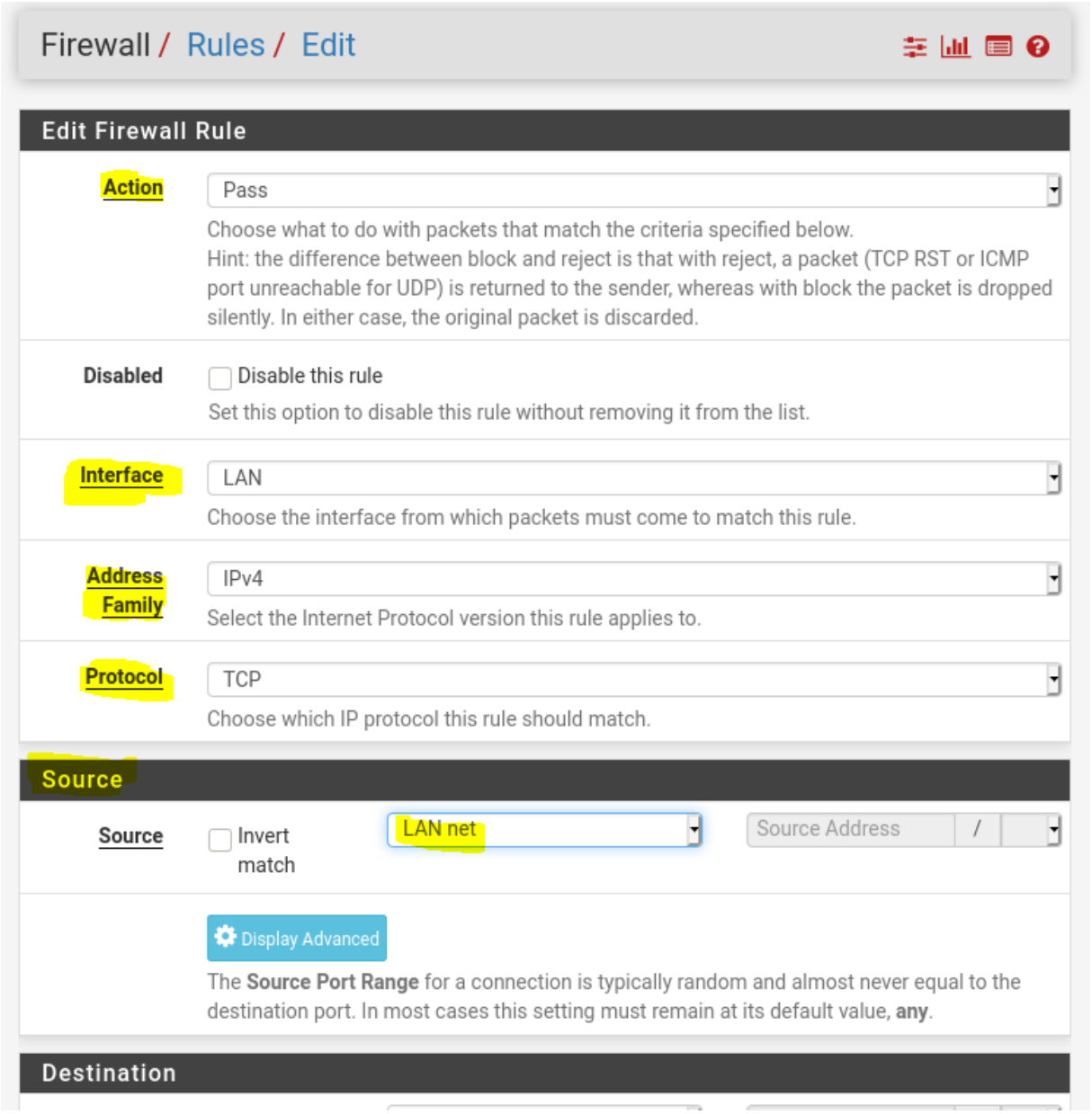


Mise en place des règles.

Créer un séparateur pour ordonner les règles, nommer le Pass http/https



Puis cliquez sur Add pour ajouter une règle juste en dessous de votre séparateur.



Logiquement les champs sont préinscrits :

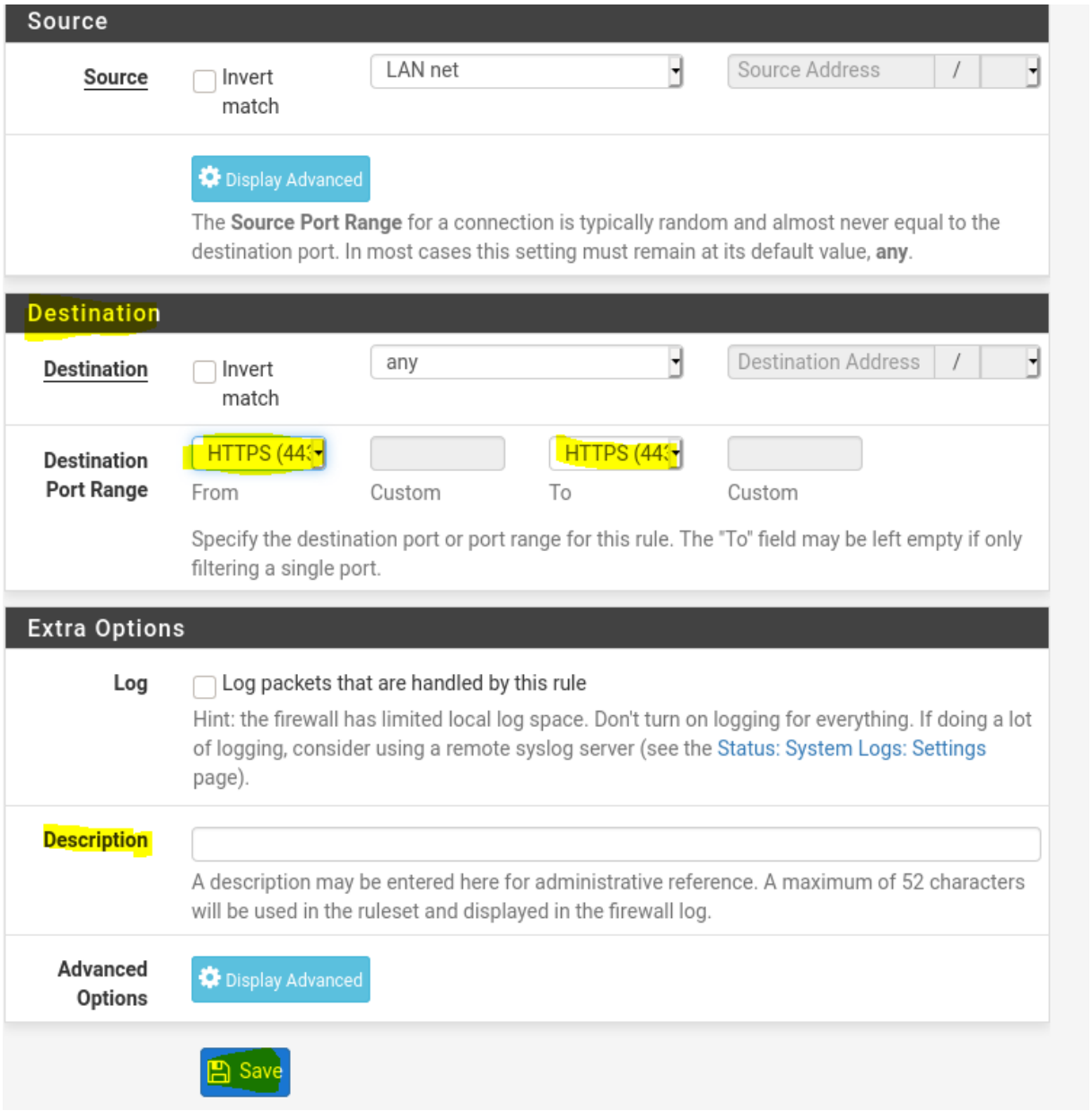
Action Pass c'est pour autoriser / interdire

L'interface ou les paquets vont passer par rapport à la règle.

Sélectionnez le protocole IP que vous avez en fonction de votre réseau.

Le Protocole = le protocole que vous voulez autoriser.

La Source = la destination. C'est-à-dire d'où vient la requête, c'est le client qui demande s'il peut passer.

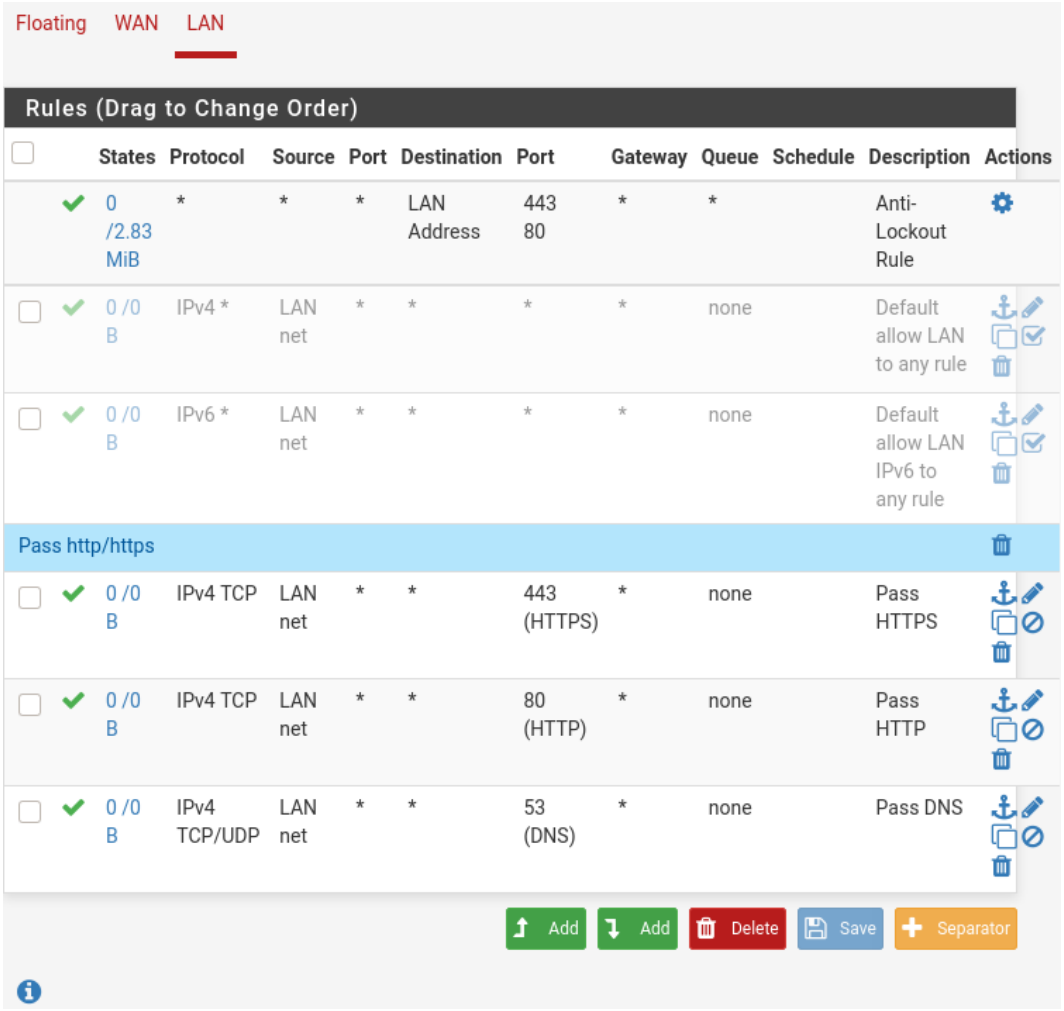


La destination c'est d'où va le paquet et sur qu'elle interface dans mon cas je mets any vers tous les interfaces.

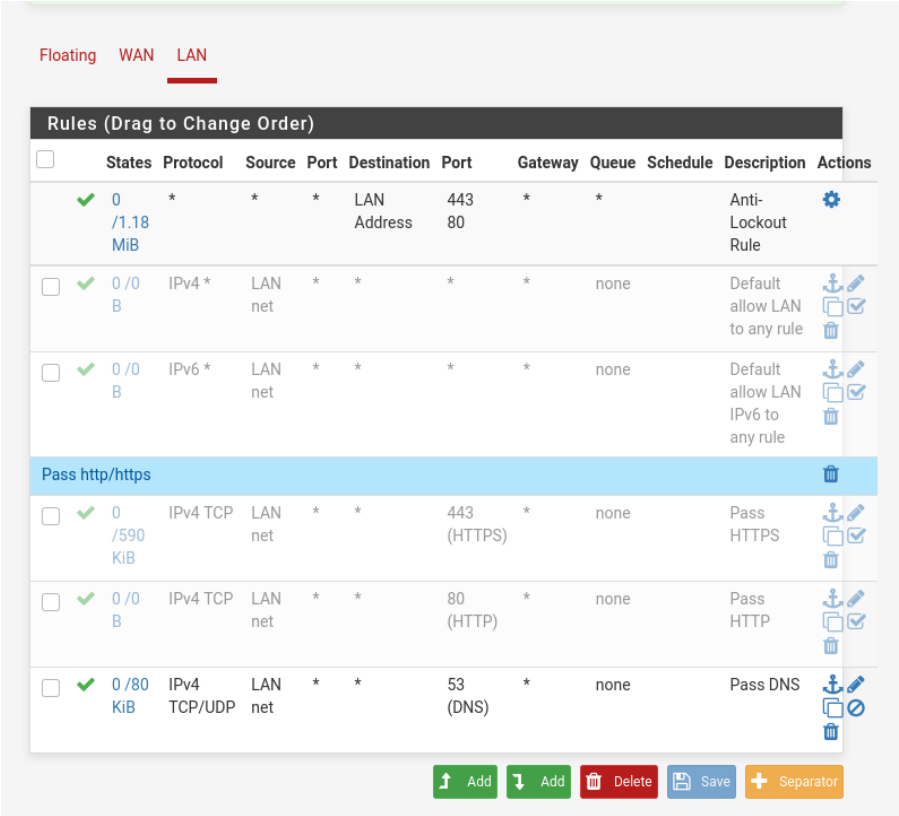
Le port de destination, dont du HTTPS sur le port 443

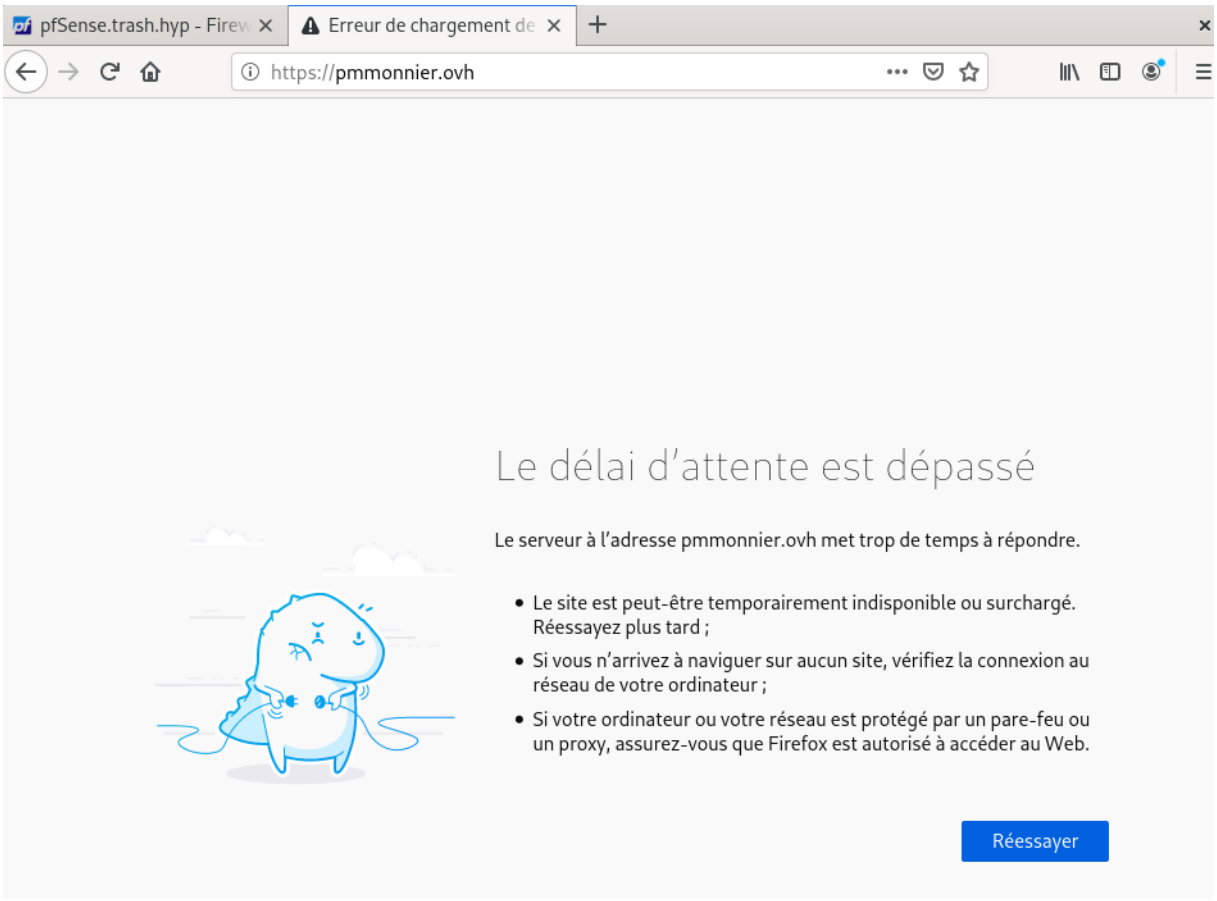
Une description de la règle.

Ce qui devrait ressembler à ceci :



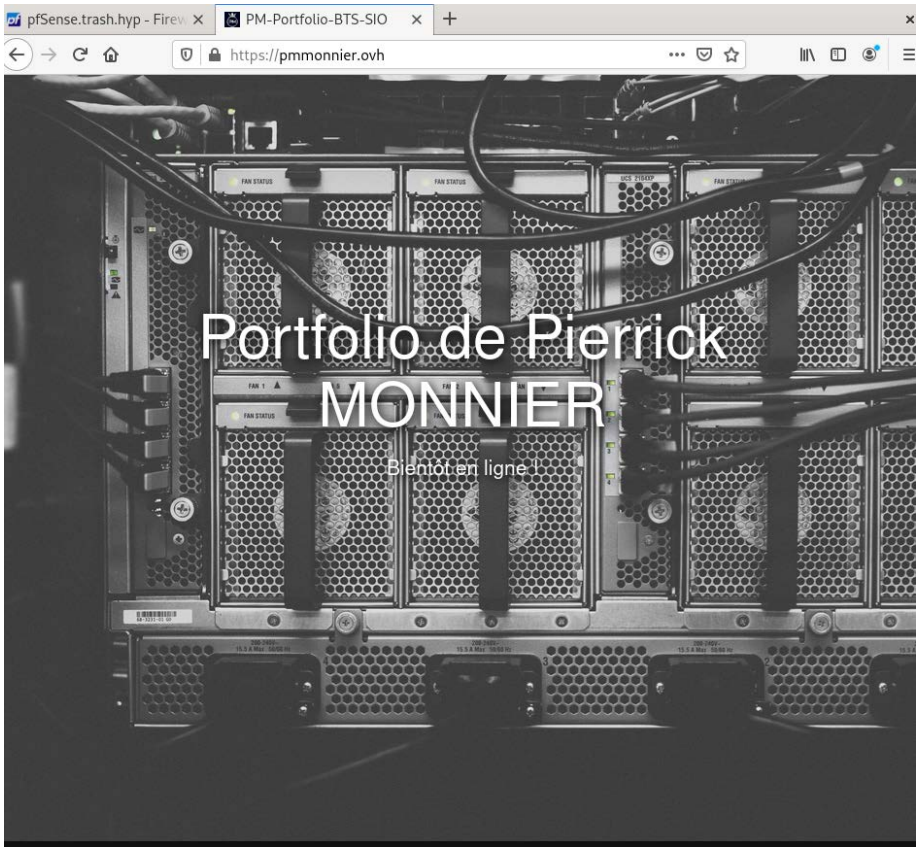
Si nous désactivons le DNS.





Test de recherche, nous pouvons voir que nous arrivons pas à afficher la page.

Sinon réactivons les règles nous pouvons accéder aux sites internet rechercher.



2 Documentation

1. Qu’est-ce qu’un serveur mandataire ?

Un serveur mandataire il filtre les sites internet que nous consultons, le navigateur envoi une requête pour recevoir la ou les pages à afficher.

2. Explicitez le fonctionnement d’un serveur mandataire. Quelques éléments à considérer :

— Modèle.

— Ports utilisés est le port du protocole utiliser exemple https 443

— Cache est utiliser pour enregistrer les pages web les plus visités, quand un client visite une page assez souvent, elle est enregistrée, elle est plus rapide à recevoir car elle est en cache.

— Filtrage c’est une constitution d’activité les logs qui enregistre toutes les requêtes des utilisateurs lorsqu’il se connecte à internet.

— Sécurité c’est le fiewall qui assure la sécurité.

3. Quelles peuvent être ses fonctions dans un réseau ?

Ses fonctions dans un réseau sont de filtrer les connections, bloquer des sites ou des services.

4. Expliquer les avantages et inconvénients d’un fonctionnement en mode "normal".

Les avantages c’est qu’on peut faire ce qu’on veut, voir n’importe quel site web. Les inconvénients c’est qu’on peut rencontrer des sites web malicieux ou réduire la bande passante.

5. Expliquer les avantages et inconvénients d’un fonctionnement en mode "transparent".

Le mode "transparent" permet de bloquer des sites ou des services. L’utilisateur en revanche ne le voit pas d’où le nom transparent. L’inconvénient c’est que si l’utilisateur veut visiter un site web bloqué il sera averti qu’il n’a pas le droit de voir cette page web.

Installation du proxy :

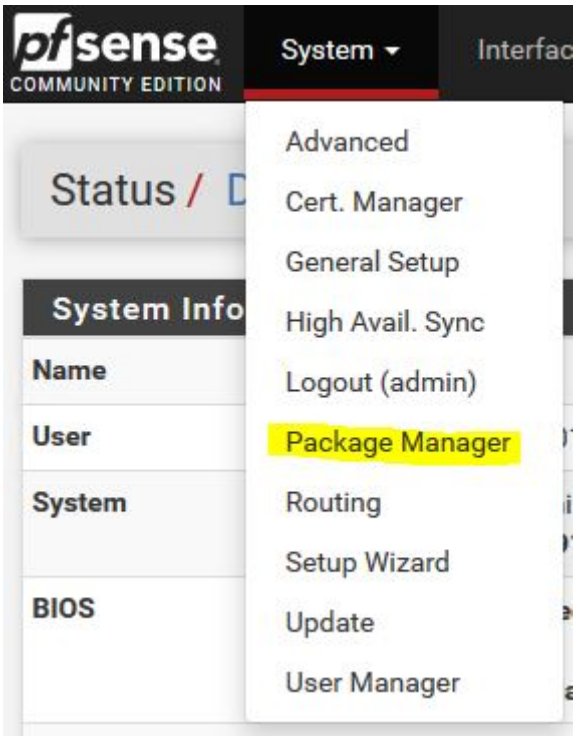
Proxy Transparent Filtrage Web URL Squid SquidGuard

Mise en place d'un proxy transparent Squid avec filtrage d'URL SquidGuard permettant de filtrer les accès à Internet de l'ensemble des utilisateurs connectés au réseau interne, de bloquer l'accès aux sites à caractères indésirables ou offensant.

Rapport de connexion LightSquid. Il s'agit d'un analyseur de logs qui affiche sous forme de pages Web, l'utilisation du Proxy.

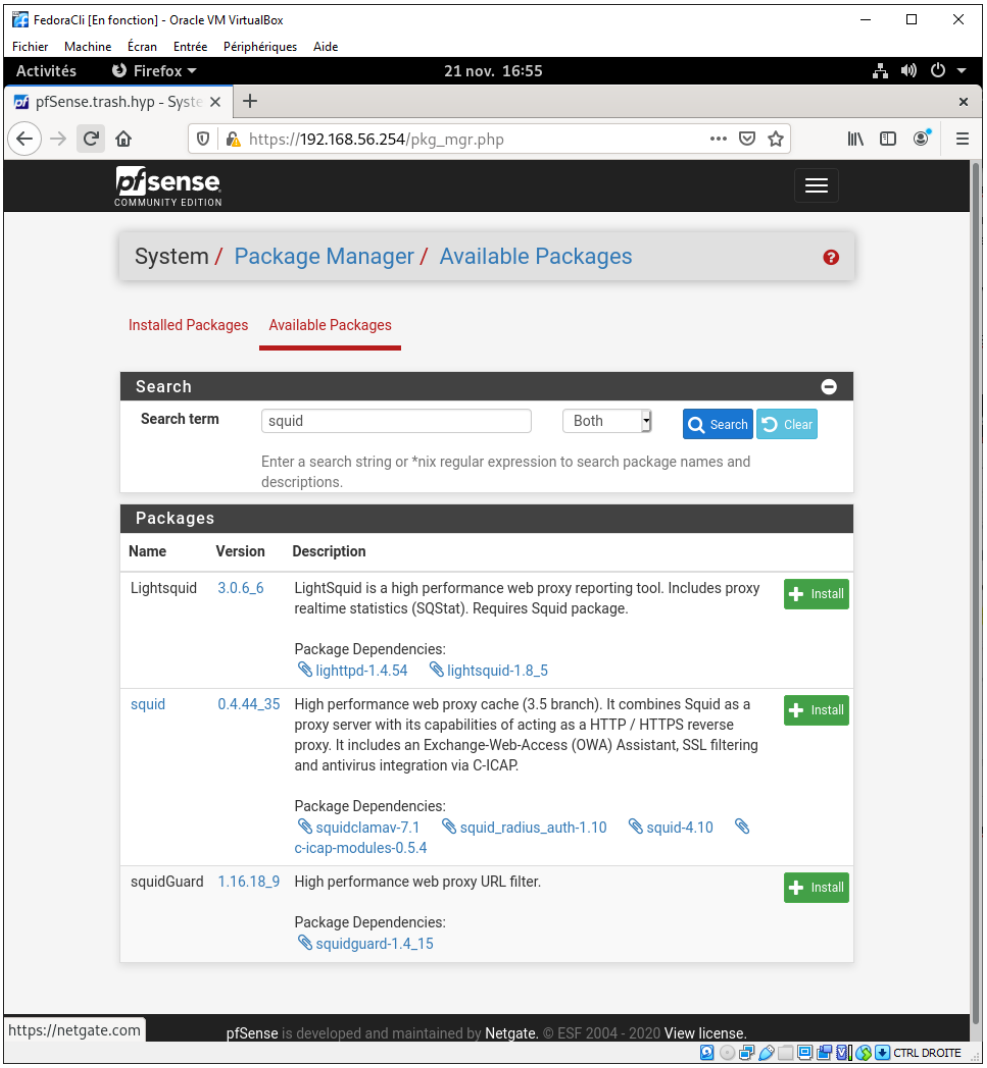
Installation des packages Squid SquidGuard et LightSquid

System, Package Manager

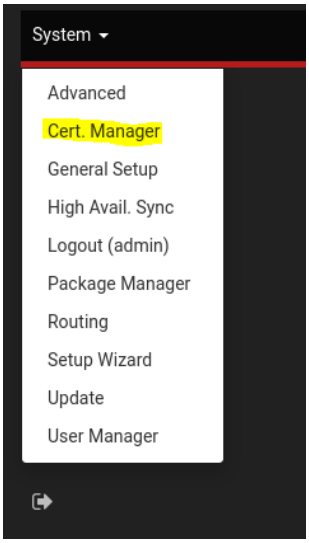


Allez dans “Available Packages”, dans la recherche taper “squid” puis cliquez sur “Search”.

Installez les 3 packages un par un : Squid, SquidGuard, LightSquid.

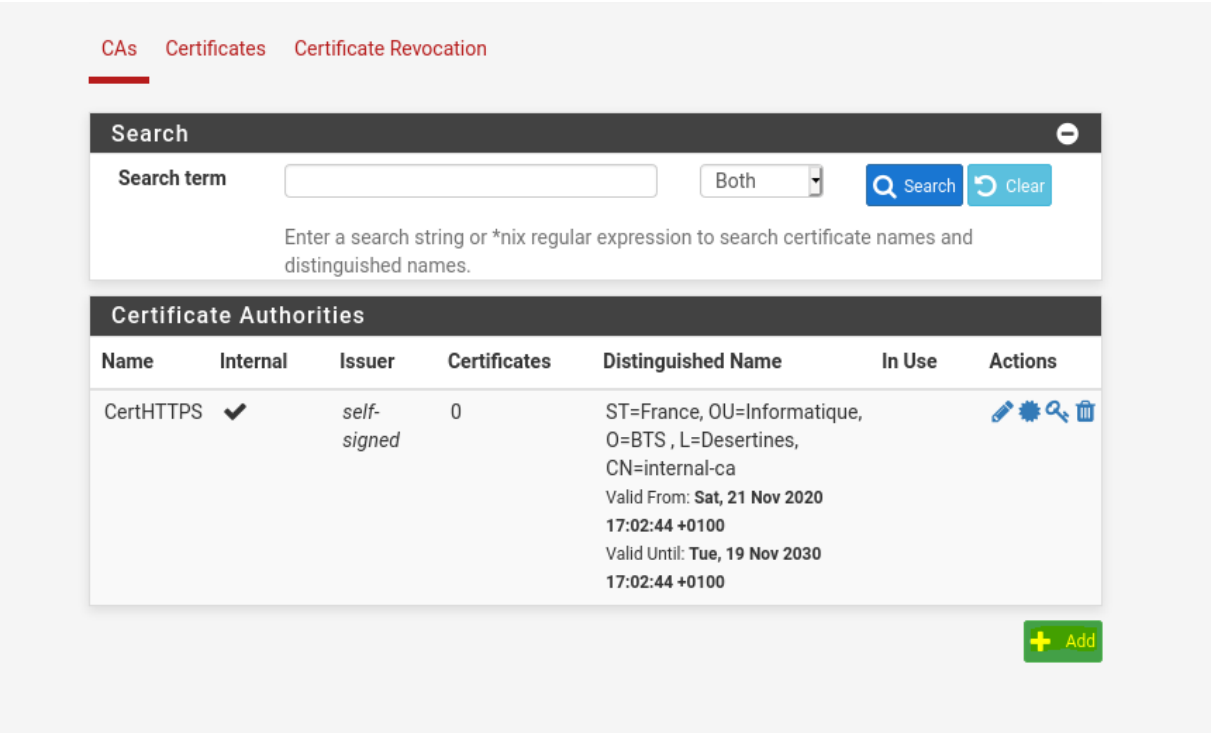


Création du Certificat pour le filtrage en HTTPS :
Sélectionnez : System, Cert. Manager



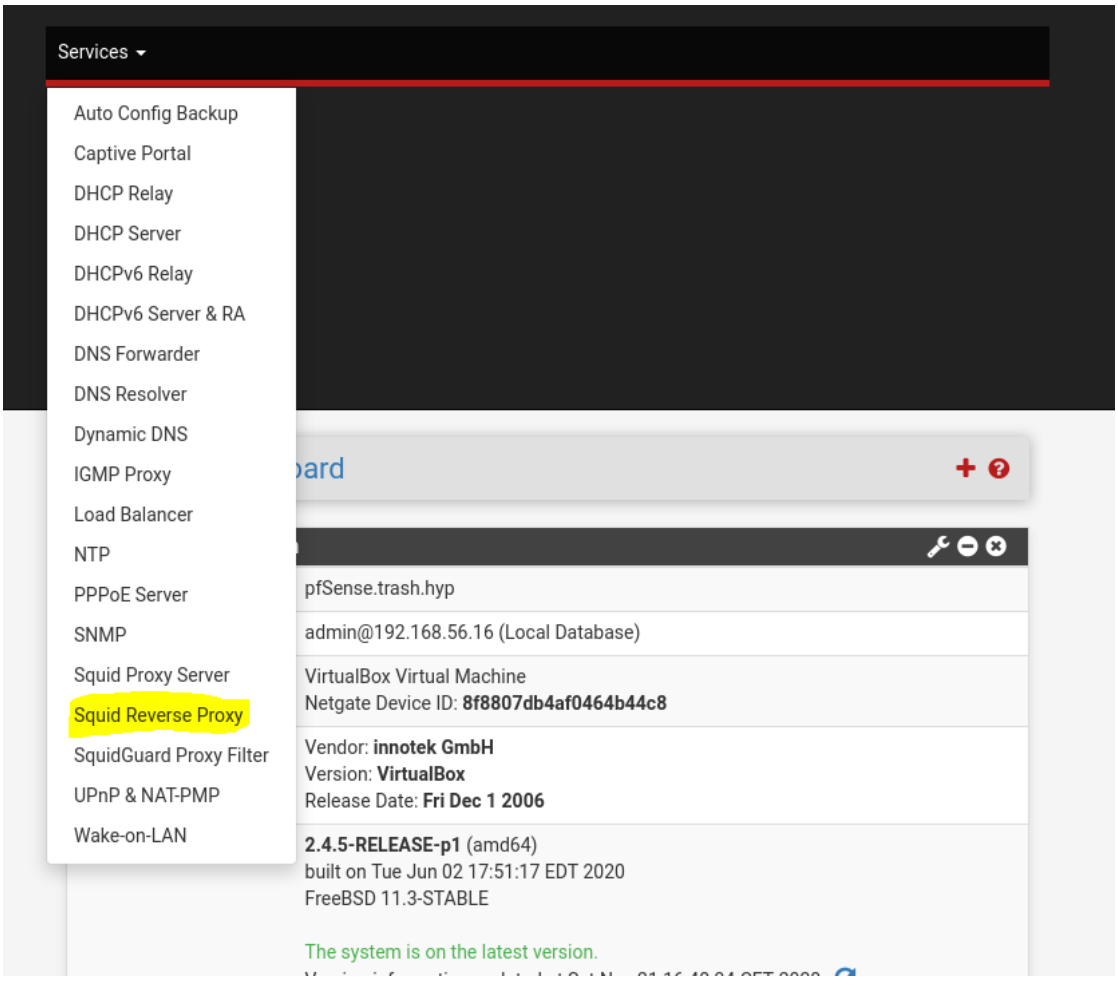
Cliquez sur Add :

Donnez un “Nom“, sans espace. Exemple : “CertHTTPS ”, remplissez les informations du certificat et cliquez sur “Save”.

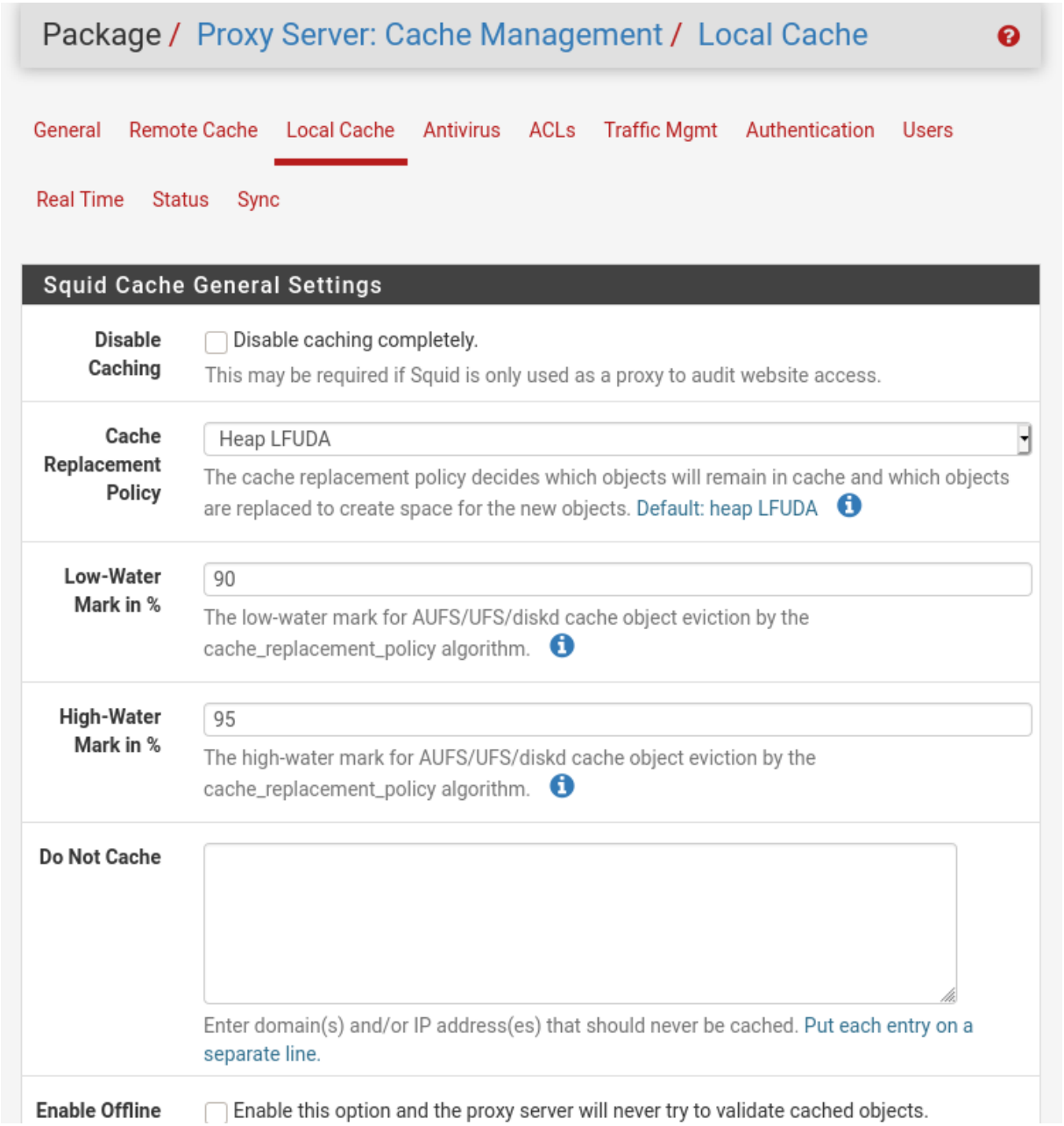


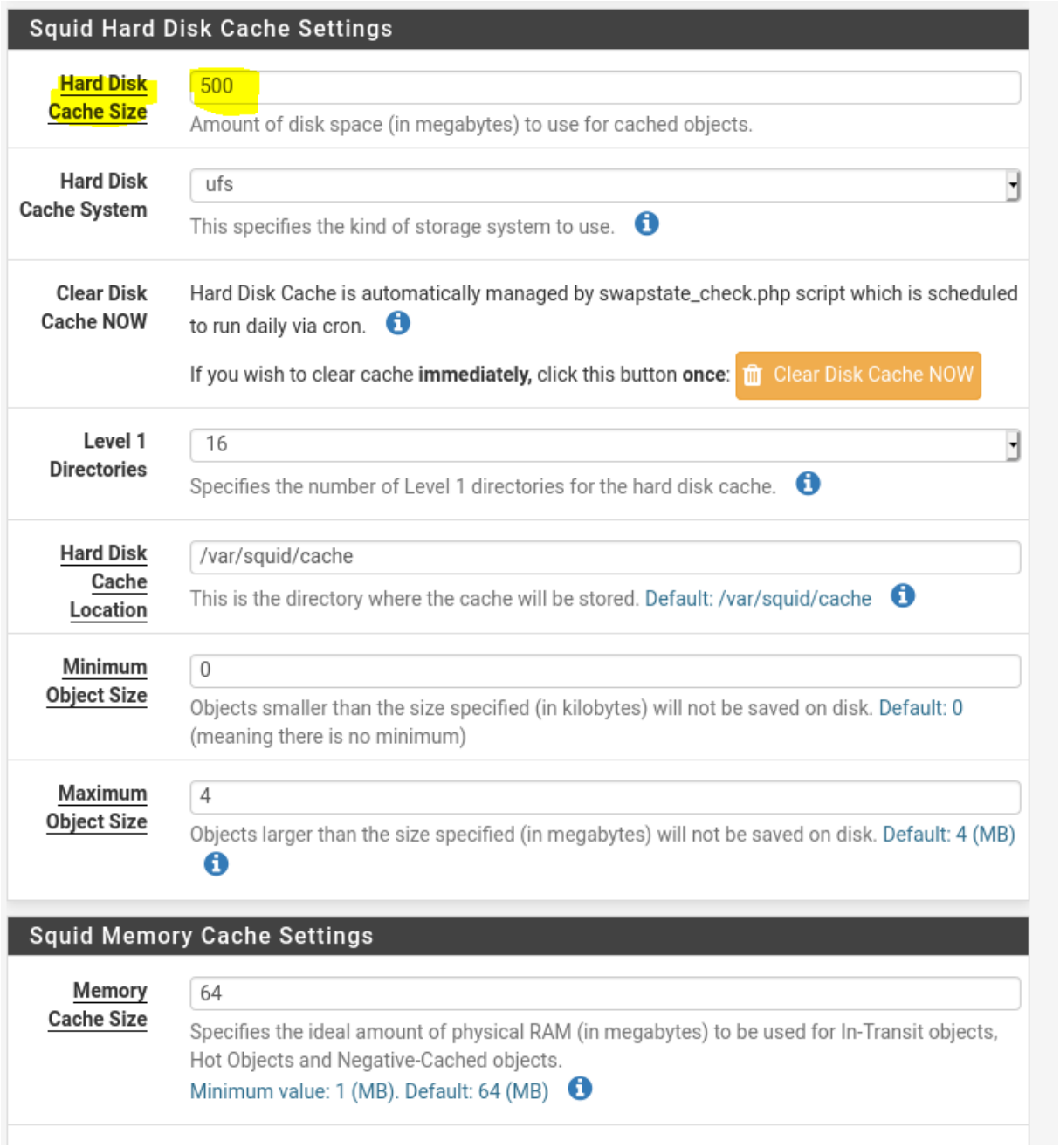
Configuration de Squid :

Sélectionnez “Services” et “Squid Proxy Server”

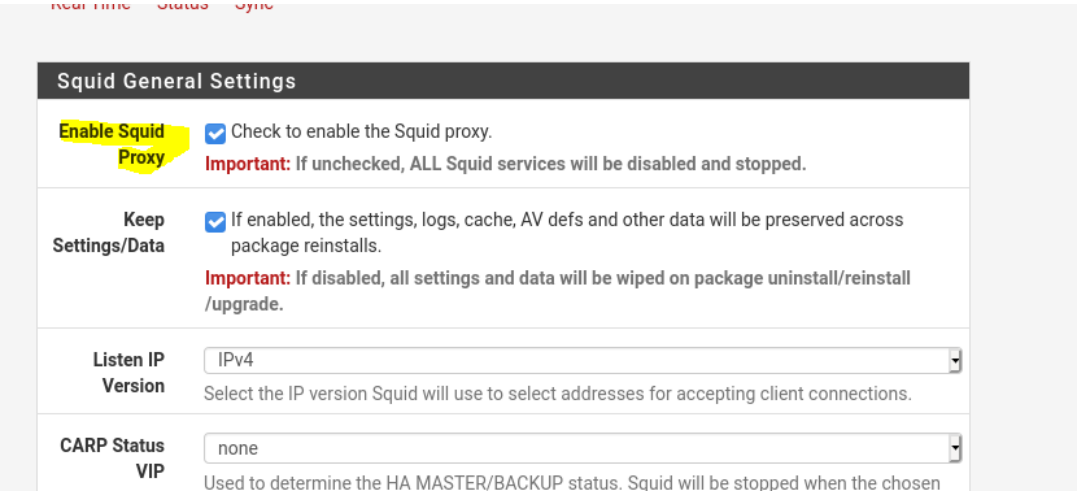


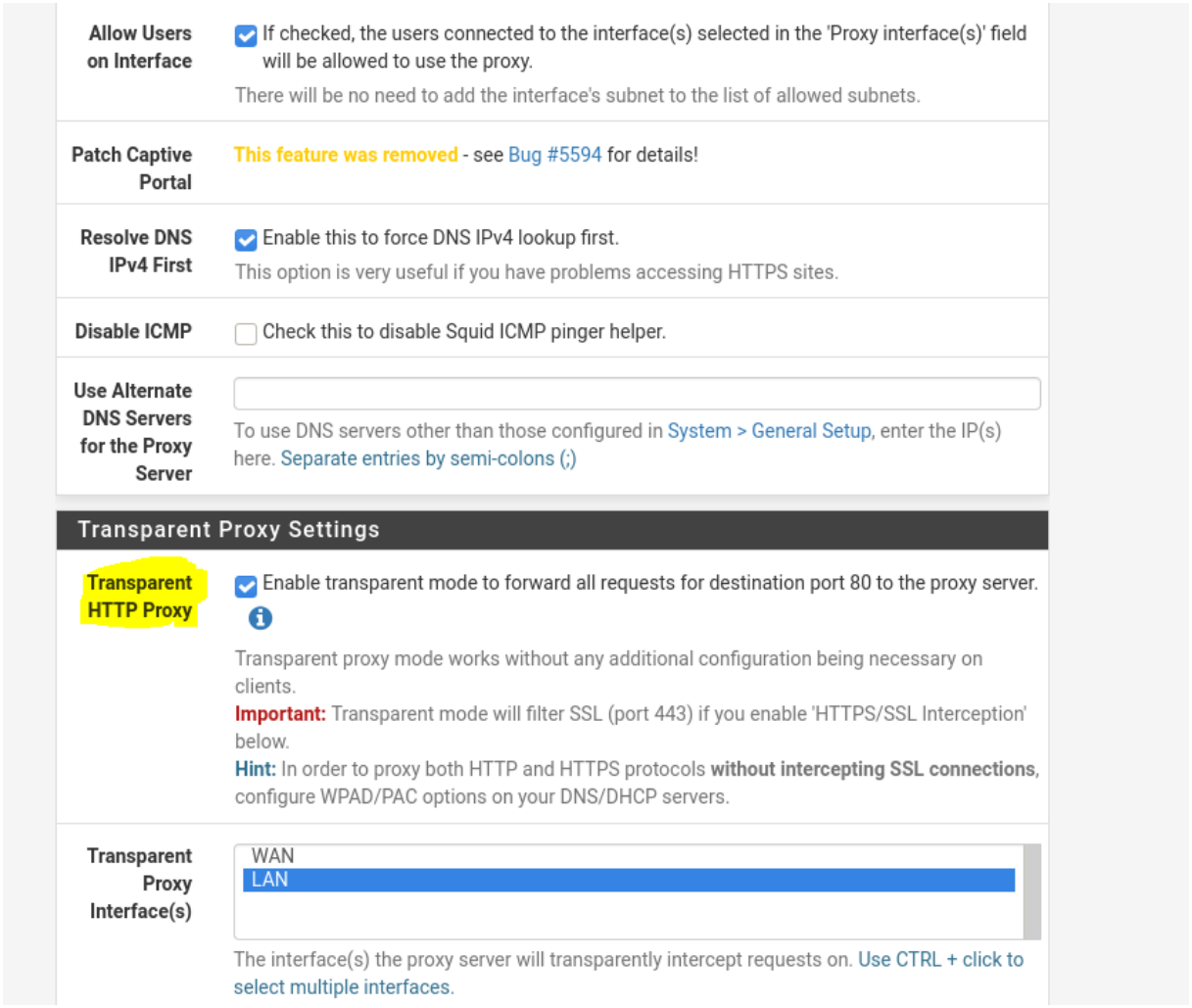
Sélectionnez : “Local Cache” et paramétrez le “Hard Disk Cache Size” à 500 Mo puis cliquer sur “Save”
Pour avoir plus d’objets (les pages web qui sont souvent rechercher par l’utilisateur) mis en cache.



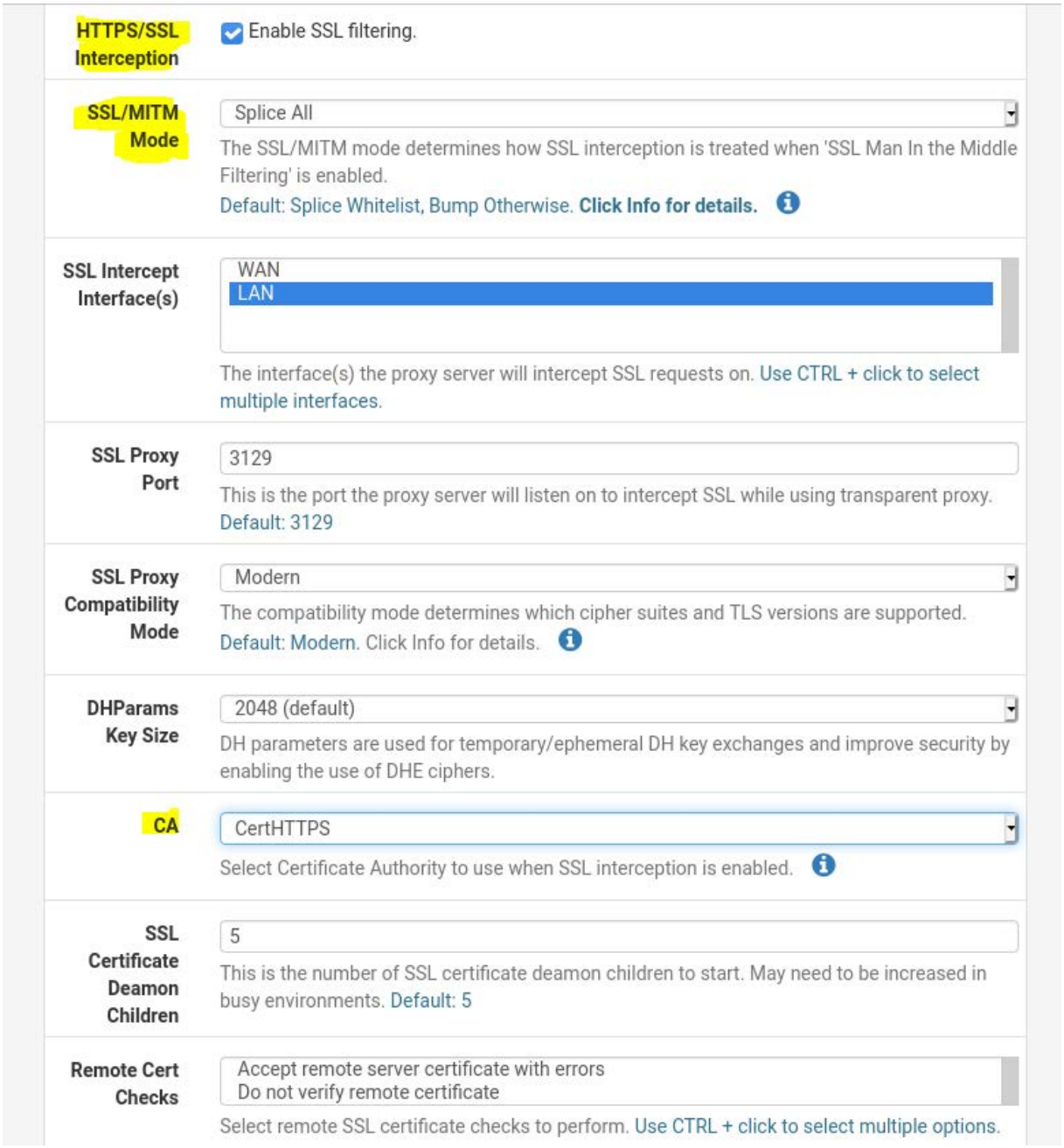


Onglet “General” : Activez “Enable Squid Proxy“, sélectionnez l’interface réseau “LAN“et “Resolve DNS IPv4 First”





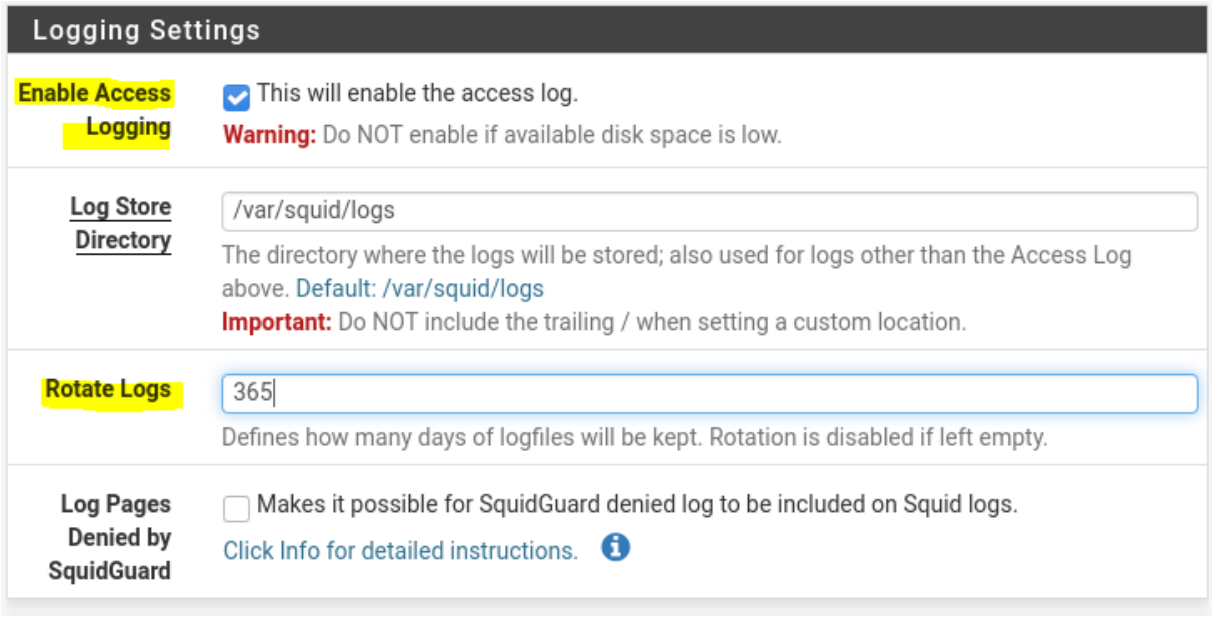
Activez “Transparent HTTP Proxy” et sélectionnez l’interface réseau “LAN”.

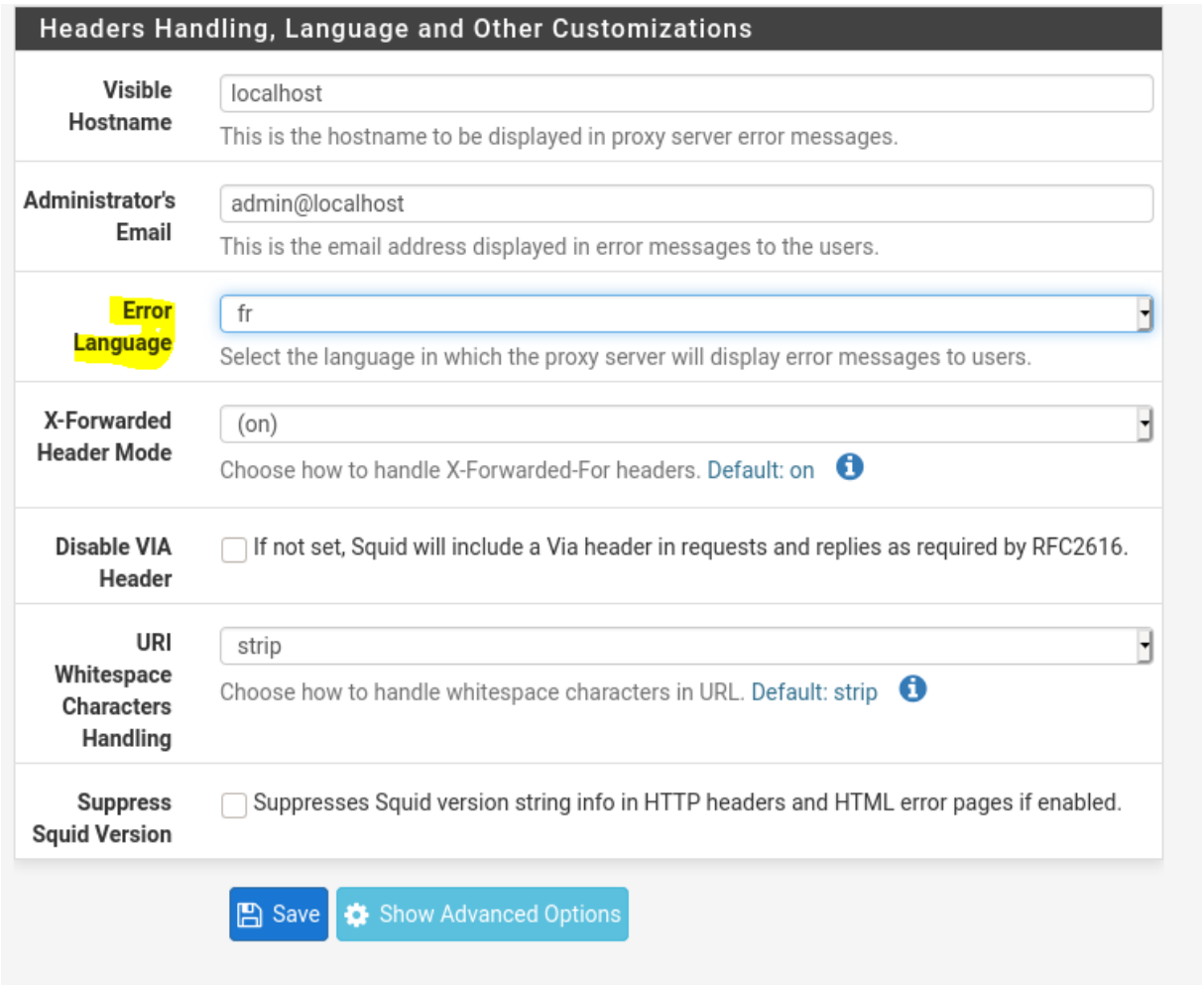


Activez “HTTPS/SSL Interception SSL filtering”, sélectionner “Splice All“, l’interface “LAN” et le Certificat précédemment créé “CertHTTPS”

Le mode « Splice ALL » permet à pfSense de capturer à la volée et d'effectuer le contrôle sur le flux sans devoir faire une quelconque manipulation sur les machines clientes ; De plus, il permet de bloquer les sites web interdits via la rubrique « ACL » de Squid.

Activez “Enable Access Logging” et définir combien de jours les logs seront conservés : 365 (un an)





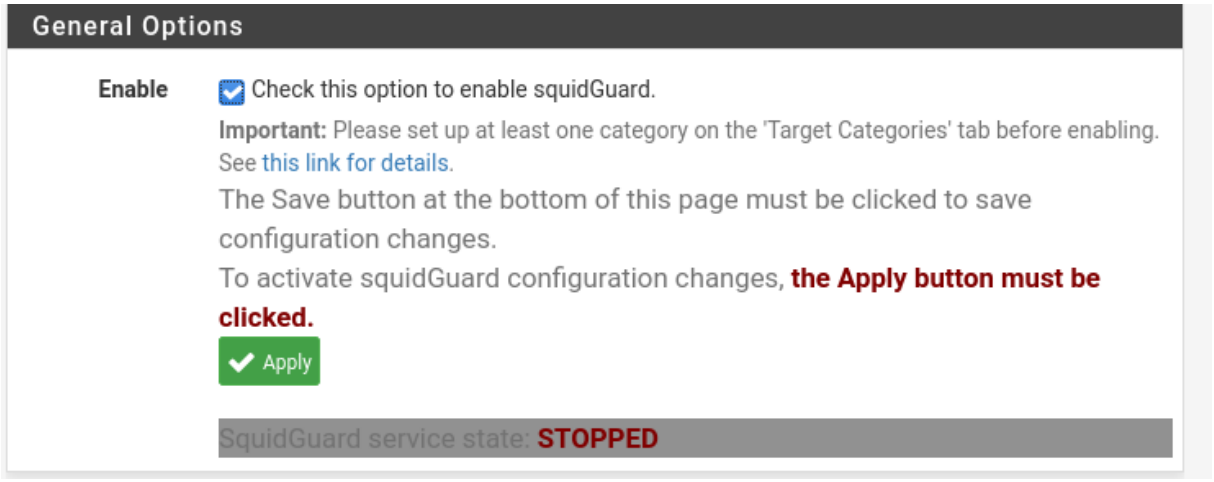
Sélectionnez “fr” pour “Error language” et Activez “Suppress Squid Version”

Puis Cliquez sur “Save” pour enregistrer toutes les modifications effectuées dans Squid.

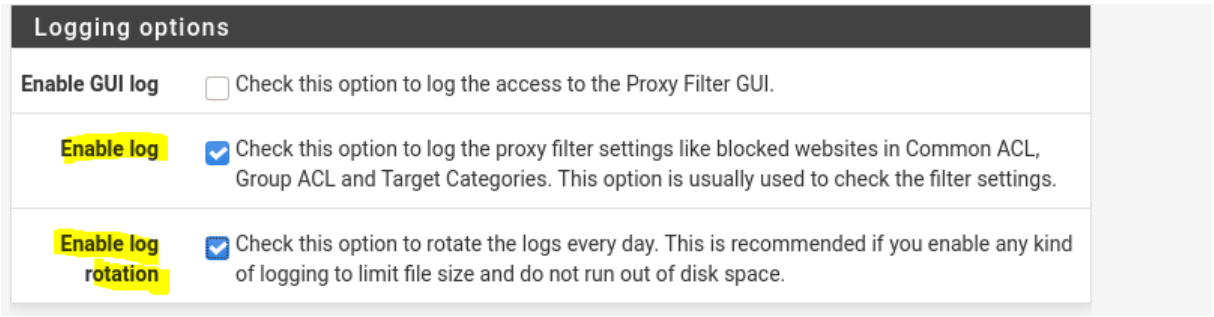
Configuration de SquidGuard :

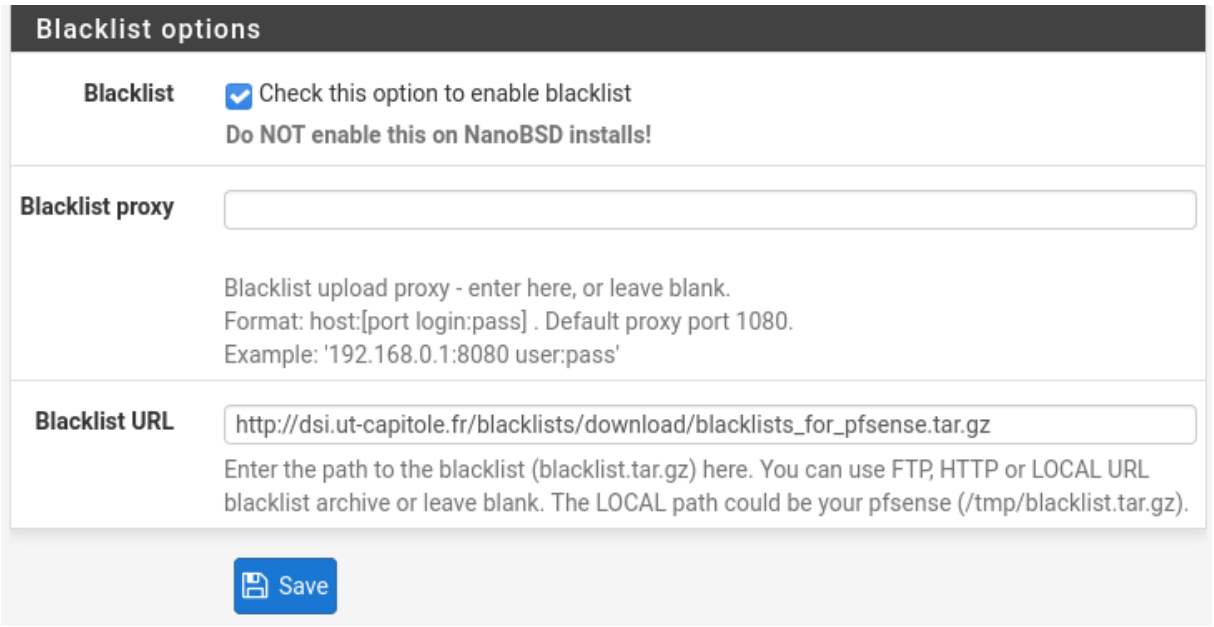
Sélectionnez “Services” et “SquidGuard Proxy Filter”.

Activez SquidGuard “Enable”.



Activez “Enable Log” et “Enable log rotation”.



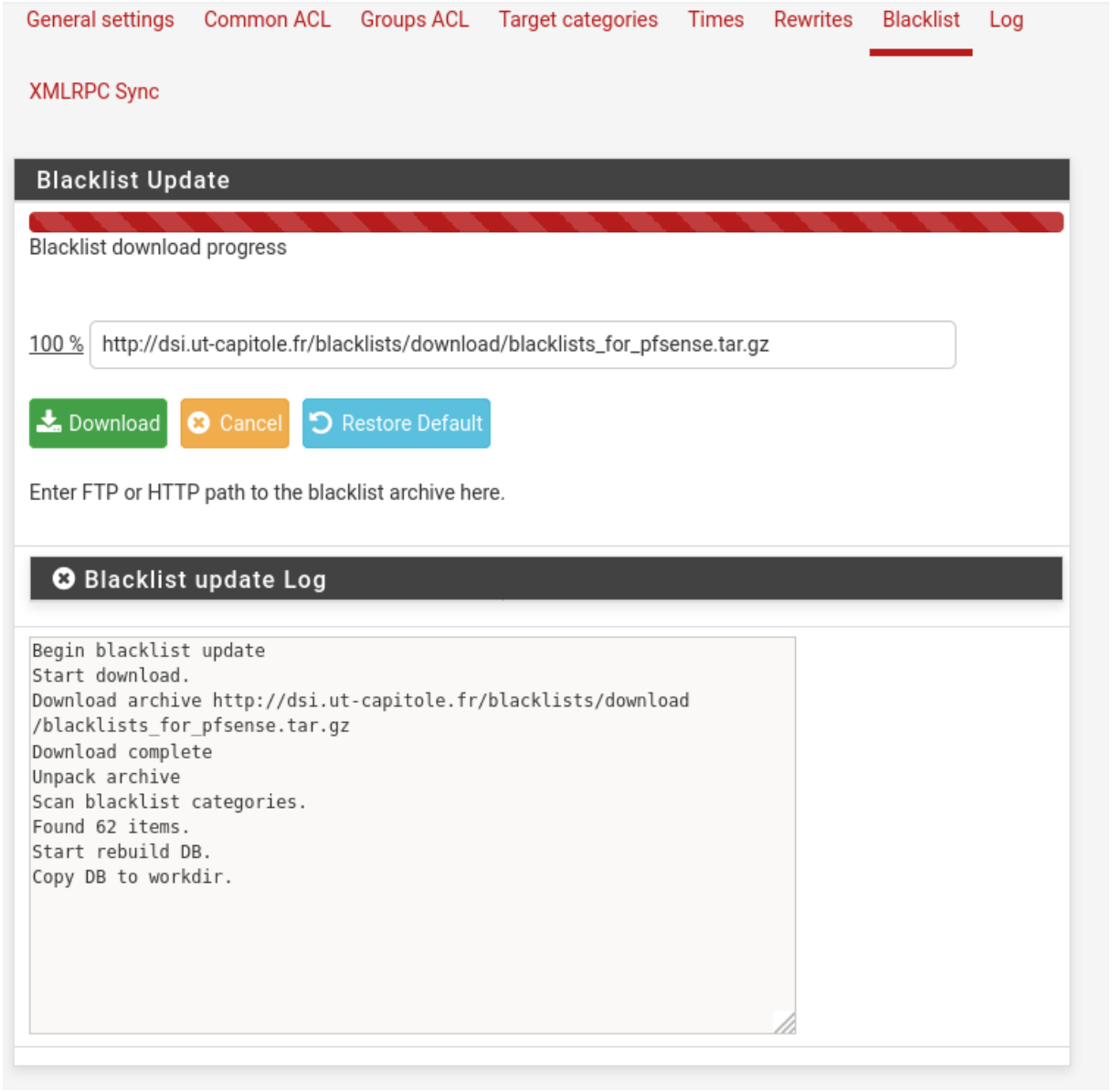


Activez “Enable Blacklist” et insérez dans Blacklist URL :

http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz

Puis cliquez sur “Save”.

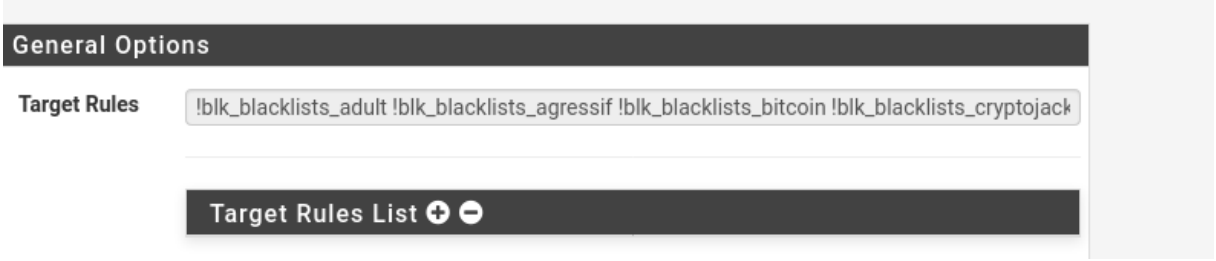
Onglet “Blacklist” : Cliquer sur “Download” pour télécharger les listes de filtrages.



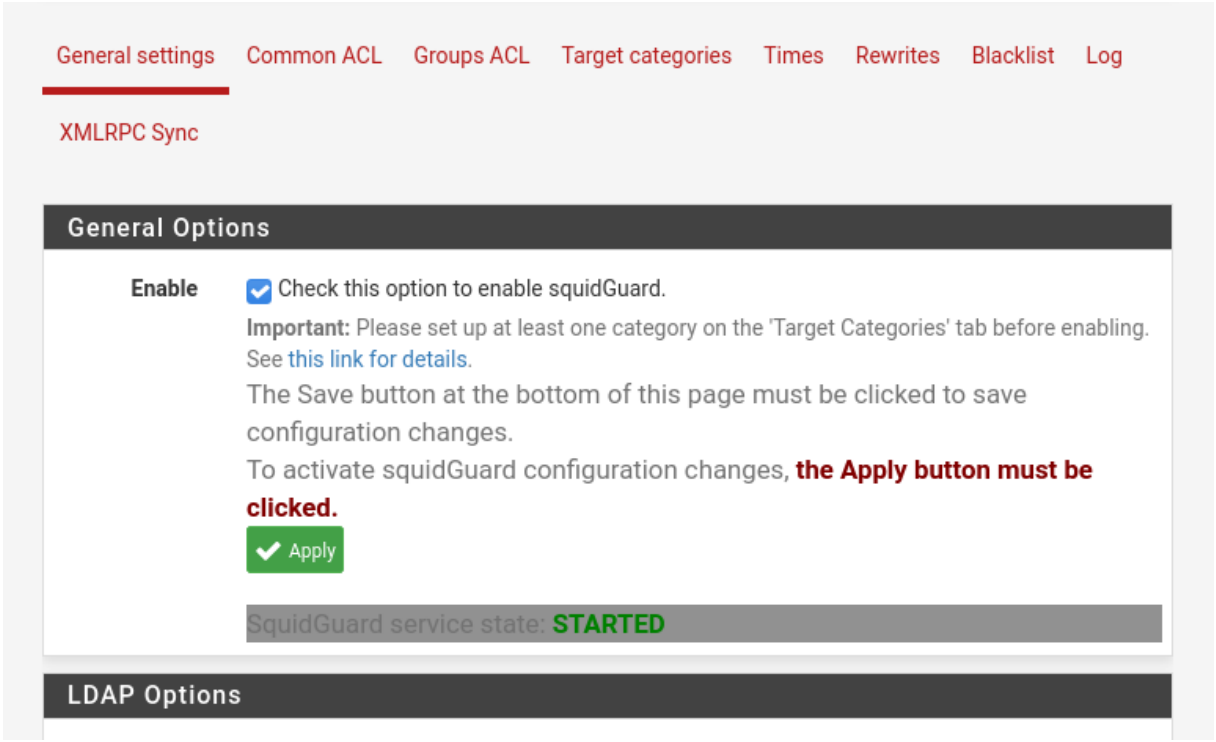
Onglet “Common ACL”, Cliquez, dans “Target Rules List” sur le ” + ”.

Cochez “Do not allow IP addresses in URL” et “Use SafeSearch engine”
Ceci est pour éviter le contournement d’URL en utilisant simplement les adresses IP au lieu du FQND. Activez le mode protégé des moteurs de recherche pour limiter l'accès au contenu mature. Pour le moment, il est pris en charge par Google, Yandex, Yahoo, MSN, Live Search et Bing. Assurez-vous que les moteurs de recherche sont accessibles. Il est recommandé d'interdire l'accès à d'autres.

Les catégories de filtrages sont bien enregistrées dans “Target Rules”.



TRES IMPORTANT : Pour valider les paramétrages, retournez sur l’onglet “General settings” et cliquez sur “Apply”



Il est indispensable de cliquer sur “Apply” après chaque modification de la configuration sinon les paramètres ne seront pas pris en compte (et vous chercherez longtemps pour trouver d’où vient le problème.)

Test de connection sur un site :

Nous pouvons remarquer que le site est bien bloqué.

Documentation

1. Quelle est la fonction d'un portail captif dans un réseau ?

Le portail captif est de forcer l'utilisateur à se connecter au réseau.

2. Comment fonctionne le portail captif ?

Le fonctionnement du portail captif est simple, l'utilisateur voudra se connecter au réseau, une page web lui envoie un formulaire de connections avec identifiant et mot de passe. Si ce dernier n'est pas renseigné alors il ne pourra pas s'authentifier pour accéder a du contenu WEB et réseau.

pfSense : Portail Captif avec Authentification Utilisateur

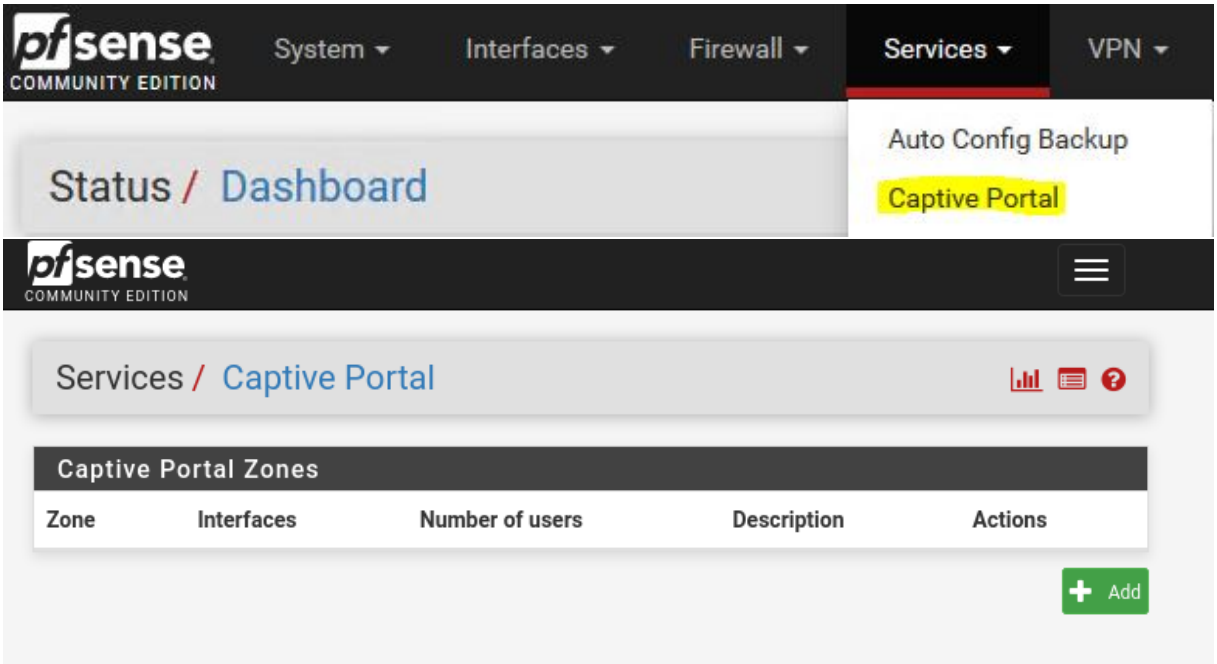
pfSense dispose d'un portail captif. Le portail captif force les clients d'un réseau à afficher une page Web d'authentification avant de pouvoir se connecter à Internet.

Dans notre contexte nous avons un Serveur de DNS sur Debian en utilisant Bind9 en Interne, ce qui veut dire qu'il faut le configurer avec l'IP passerelle dans son fichier de Forwarder et dans le named.conf. Si nous ne faisons pas cette manipulation la page du portail captif ne s'affichera pas.

Ajoutez dans le DNS le nom de votre pfSense, dans mon cas ça sera pfSence.trash.hyp

Configuration du Portail Captif

Sélectionnez : Services – Captive Portal



Renseignez le Nom du Portail Captif et sa description. Pour l'exemple : "PortailCaptife "

Activez "Enable Captive Portal" et sélectionnez l'interface "LAN"

Maximum concurrent connections : 1 (Limite le nombre de connexions simultanées d'un même utilisateur).

Idle timeout (Minutes) : Choisir entre 1 à 5 (Les clients seront déconnectés après cette période d’inactivité).

Activez “Enable logout popup window” (une fenêtre popup permet aux clients de se déconnecter).

Définir “Pre-authentication Redirect URL” (URL de redirection par défaut. Les visiteurs ne seront redirigés vers cette URL après authentification que si le portail captif ne sait pas où les rediriger).

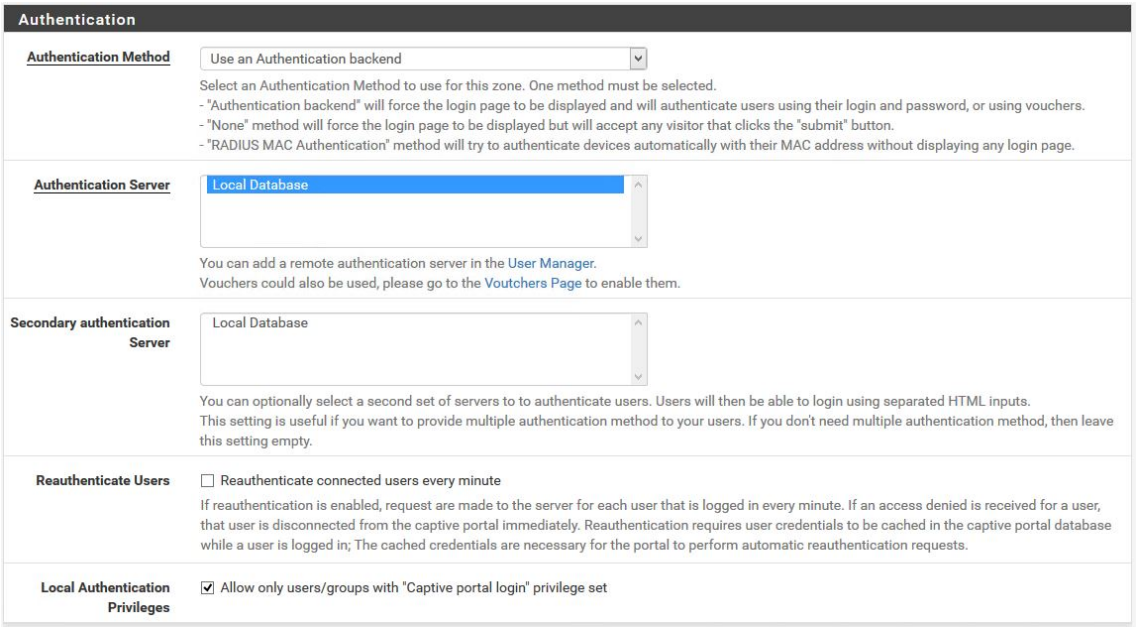
Note : Avec “http://…..” devant le domaine : Exemple : http://www.google.fr

Définir “After authentication Redirection URL” (URL de redirection forcée. Les clients seront redirigés vers cette URL au lieu de celle à laquelle ils ont initialement tenté d’accéder après s’être authentifiés).

Note : Avec “http://…..” devant le domaine : Exemple : http://www.google.fr

Activez “Disable Concurrent user logins” (seule la connexion la plus récente par nom d’utilisateur sera active)

Activez “Disable MAC filtering” (nécessaire lorsque l’adresse MAC du client ne peut pas être déterminée)



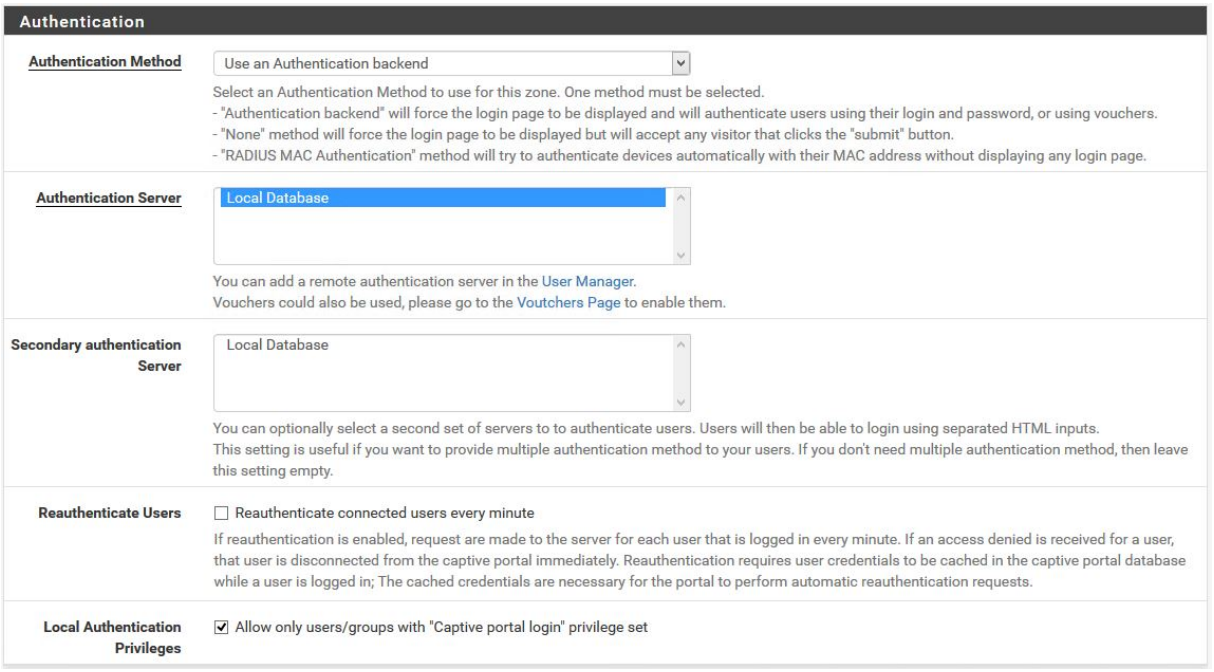
Sélectionnez “Use an Authentication backend”.

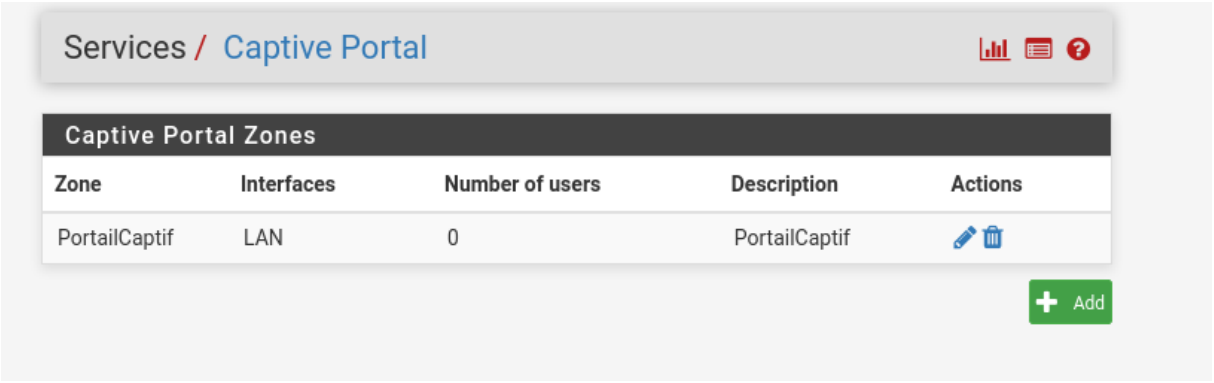
Sélectionnez “Local Database” pour “Authentication Server” vérifier qu’il soit bien sélectionné.

Attention : Ne pas sélectionner “Local Database” pour “Secondary Authentication Server”.

Activez “Local Authentication Privileges” (Autoriser uniquement les utilisateurs avec les droits de “Connexion au portail captif”).

Puis cliquez “Save”.



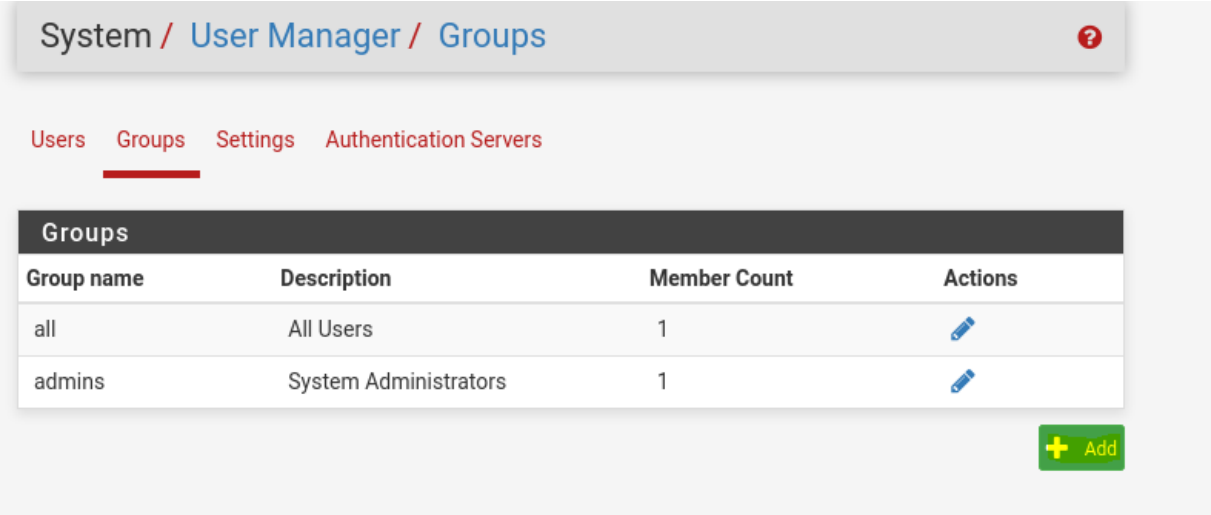


Configuration du Groupe et Utilisateur pour délégation du Portail Captif.

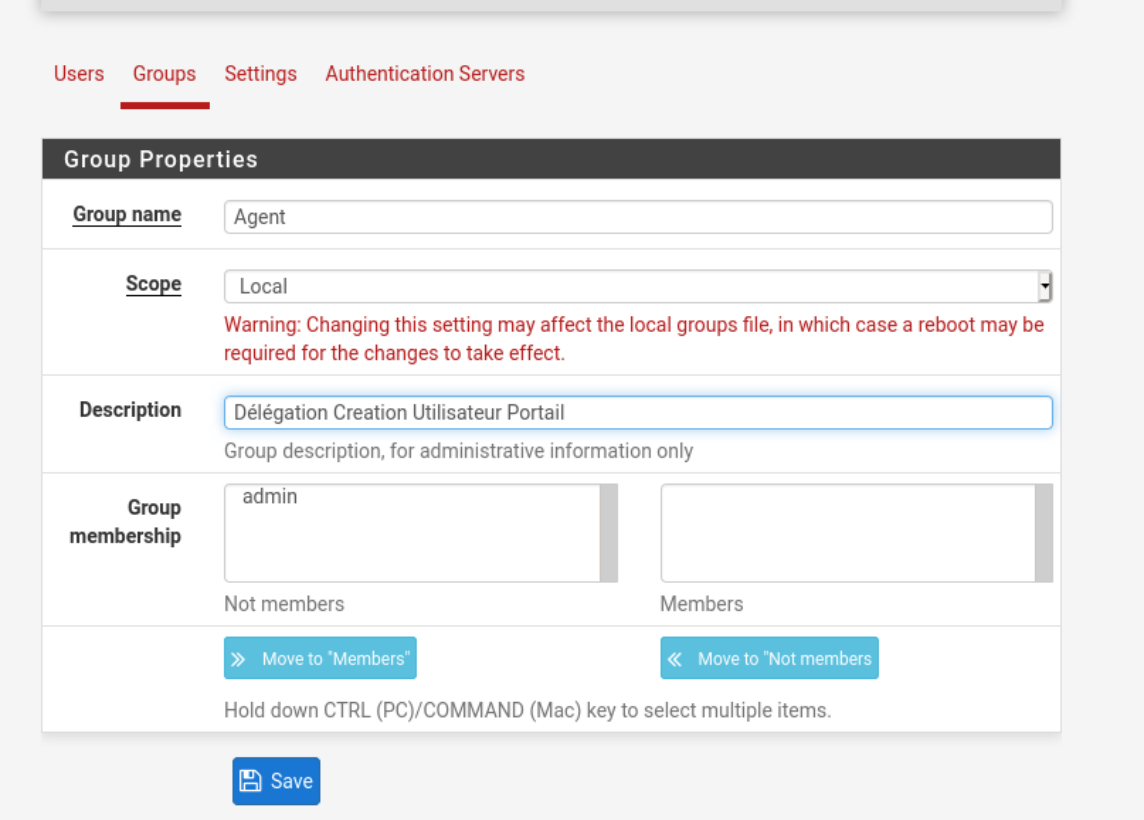
Création d'un groupe et d'un utilisateur qui aura pour fonction de créer des Utilisateurs autorisés à se connecter au Portail Captif. Ce groupe d'utilisateurs associés auront seulement le droit de créer des Utilisateurs du Portail Captif.

Sélectionnez : System – User Manager

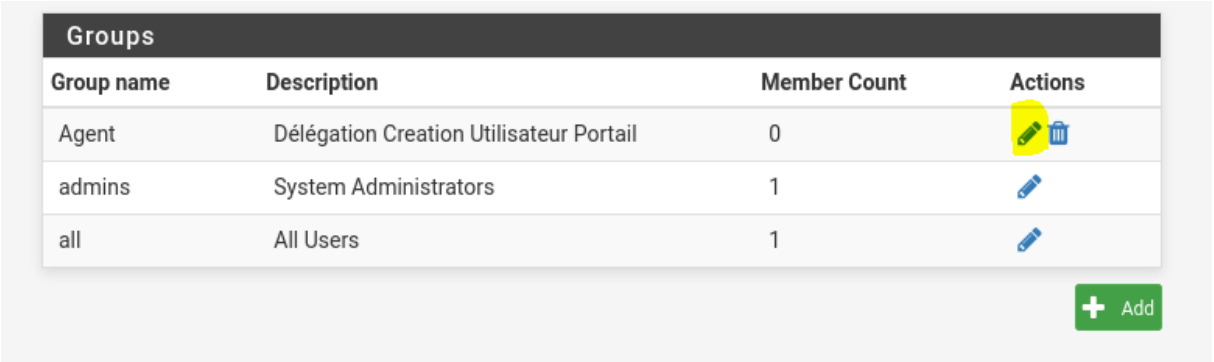
Onglet "Groups", cliquez sur "+ Add".



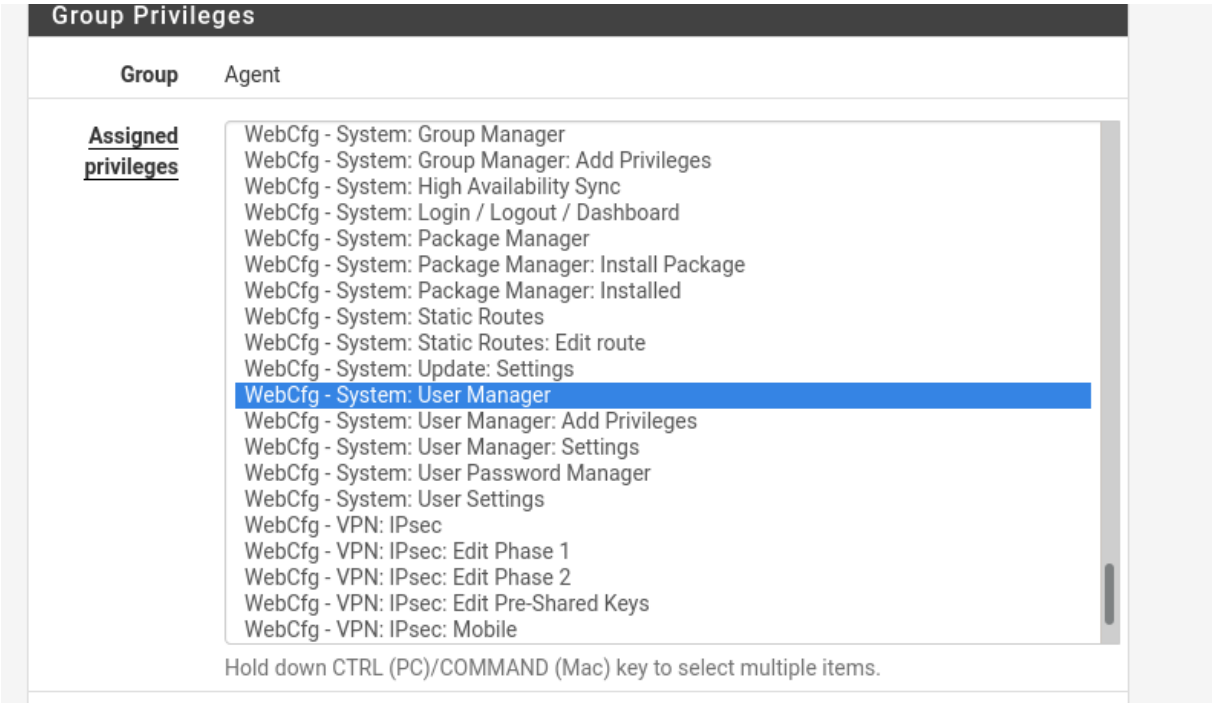
Cliquez sur Add, Renseigner le Nom du Groupe “Agent” et sa description “Delegation Creation Utilisateurs Portail”. Cliquez “Save”.



Dans le menu “Actions”, modifiez le groupe créé en cliquant sur le stylo.



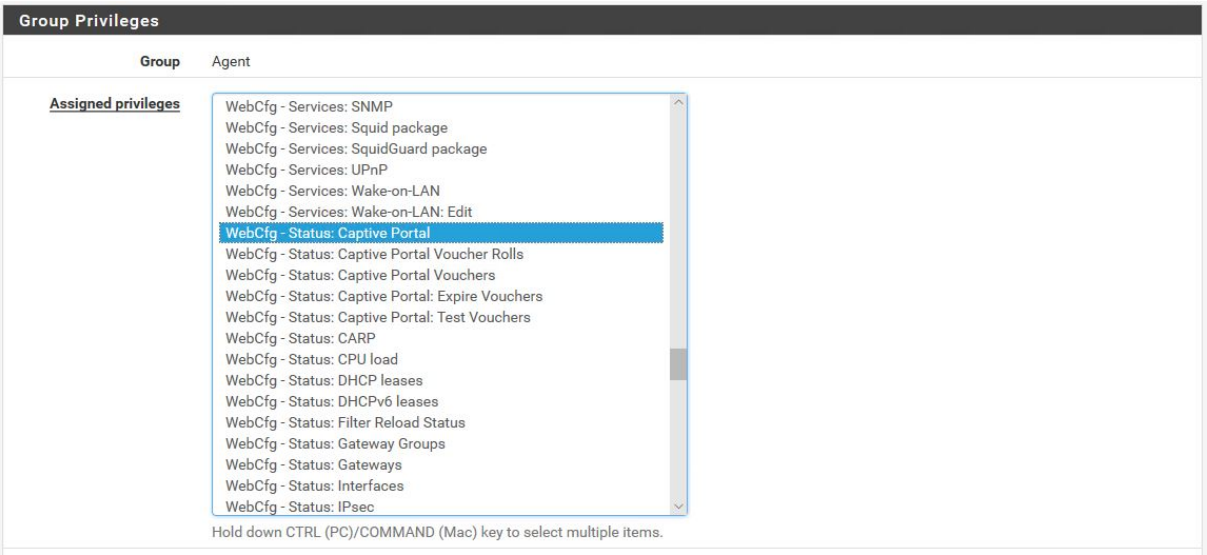
Cliquez sur “+ Add” rubrique “Assigned Privileges“.
Sélectionnez dans la liste “WebCfg – System : User Manager” (Accès à la page de gestion des utilisateurs “User Manager”).



Puis cliquez sur “Save”.

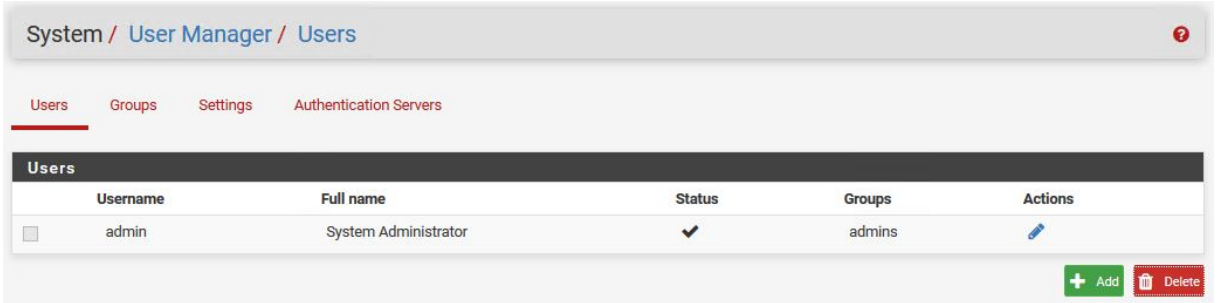
Revenir à la rubrique “Assigned Privileges” en cliquant sur “+ Add”.

Sélectionnez dans la liste “WebCfg – Status: Captive Portal” (Voir le Statut des utilisateurs connectés”).



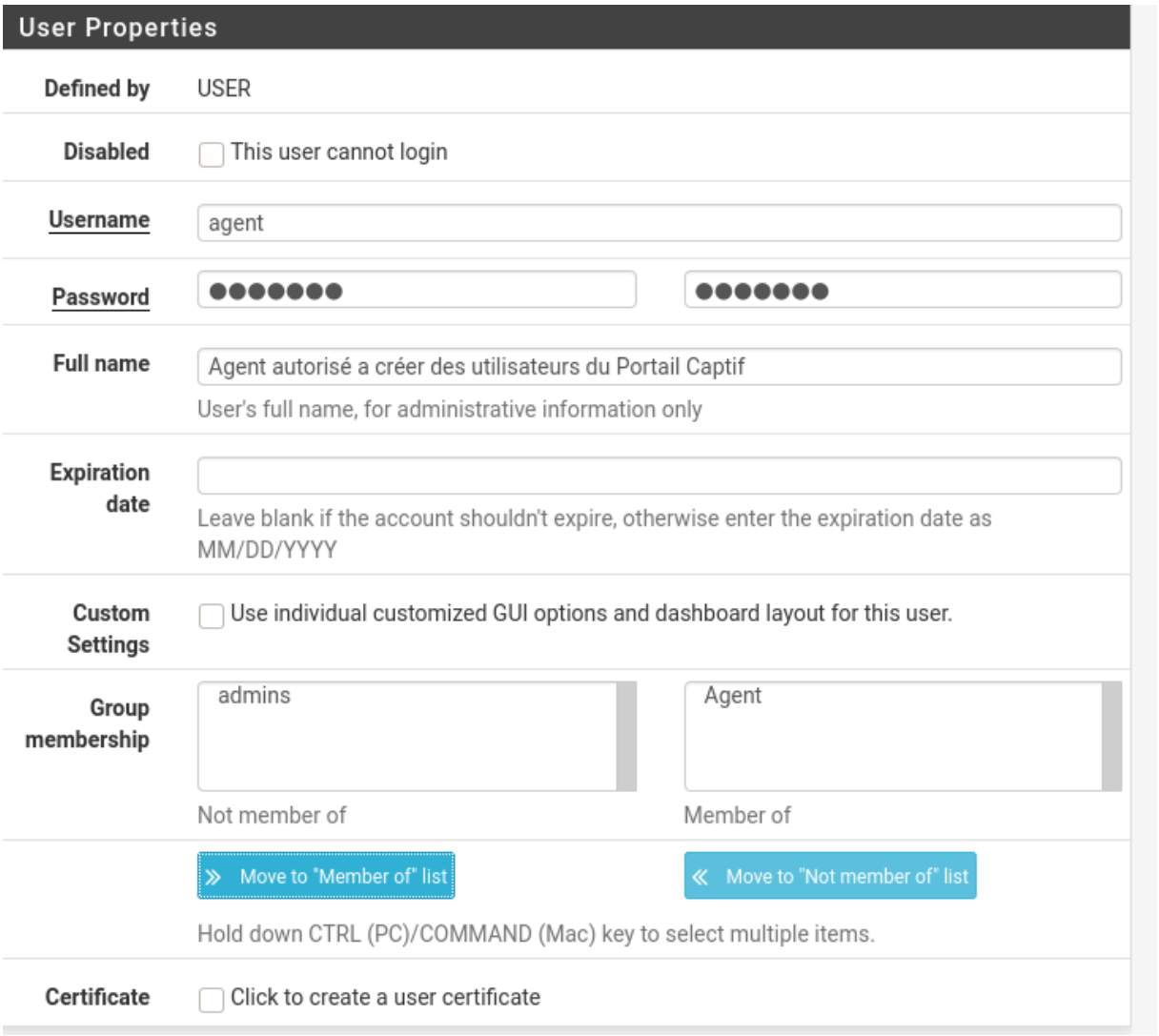
Vérifiez les droits, puis cliquez sur “Save”.

Onglet “Users“, cliquez sur “+ Add”.

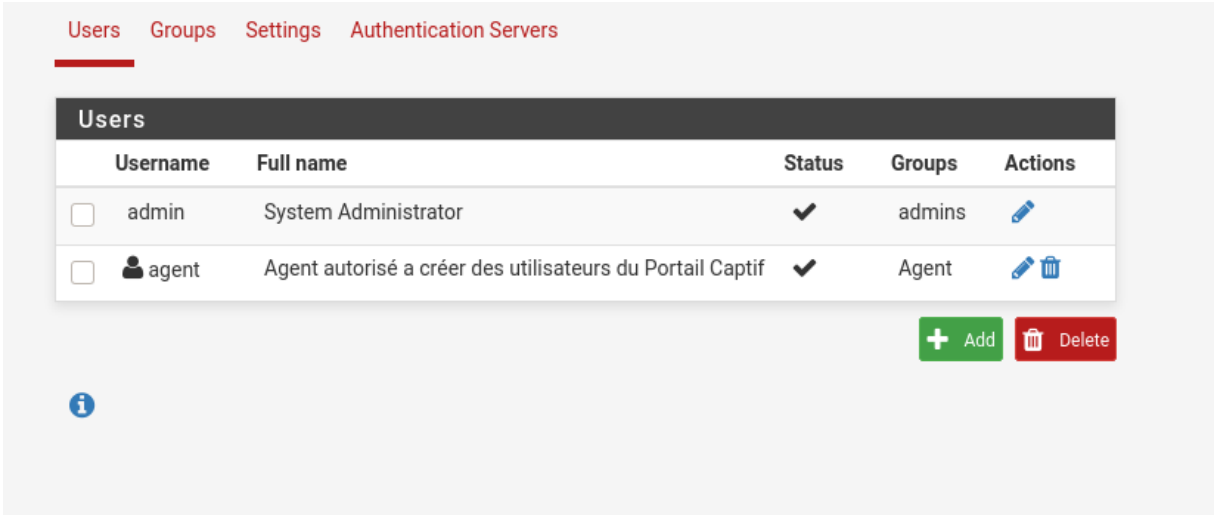


Entrez un Nom d’Utilisateur “agent”, son mot de passe et sa description (Agent autorisé à créer des utilisateurs du Portail Captif).

Sélectionnez dans “Group membership” le groupe “Agent” précédemment créé. Cliquez sur “Move to Member of list” puis “Save”.



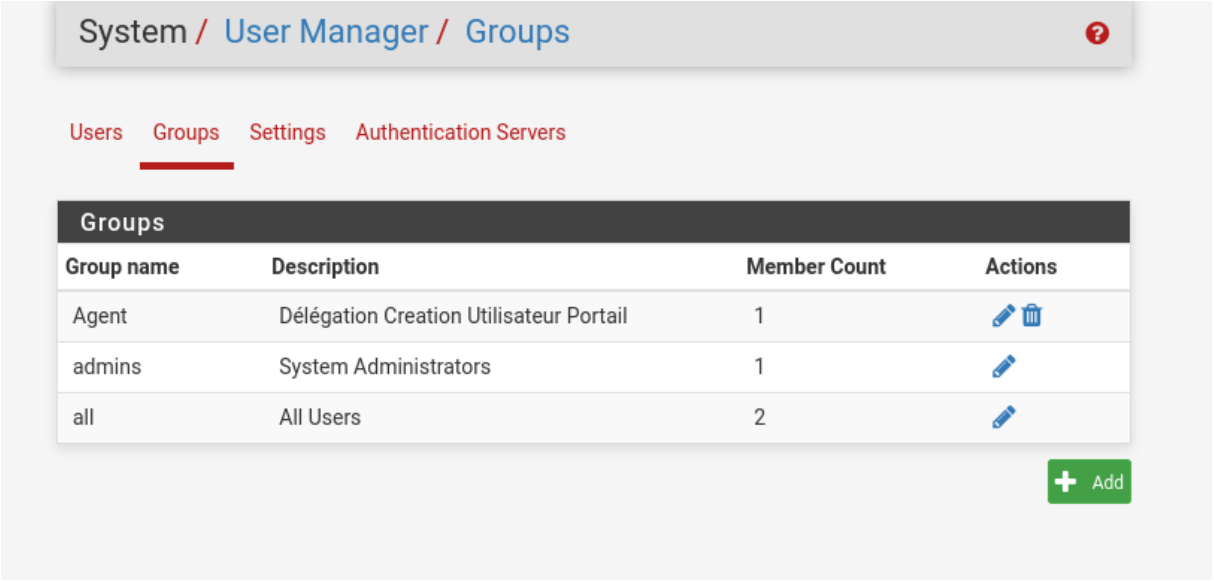
La délégation pour l'utilisateur "Agent" est autorisé à créer des utilisateurs pour connexion au Portail Captif.



Configuration du Groupe et Utilisateurs autorisés à se connecter au Portail Captif.

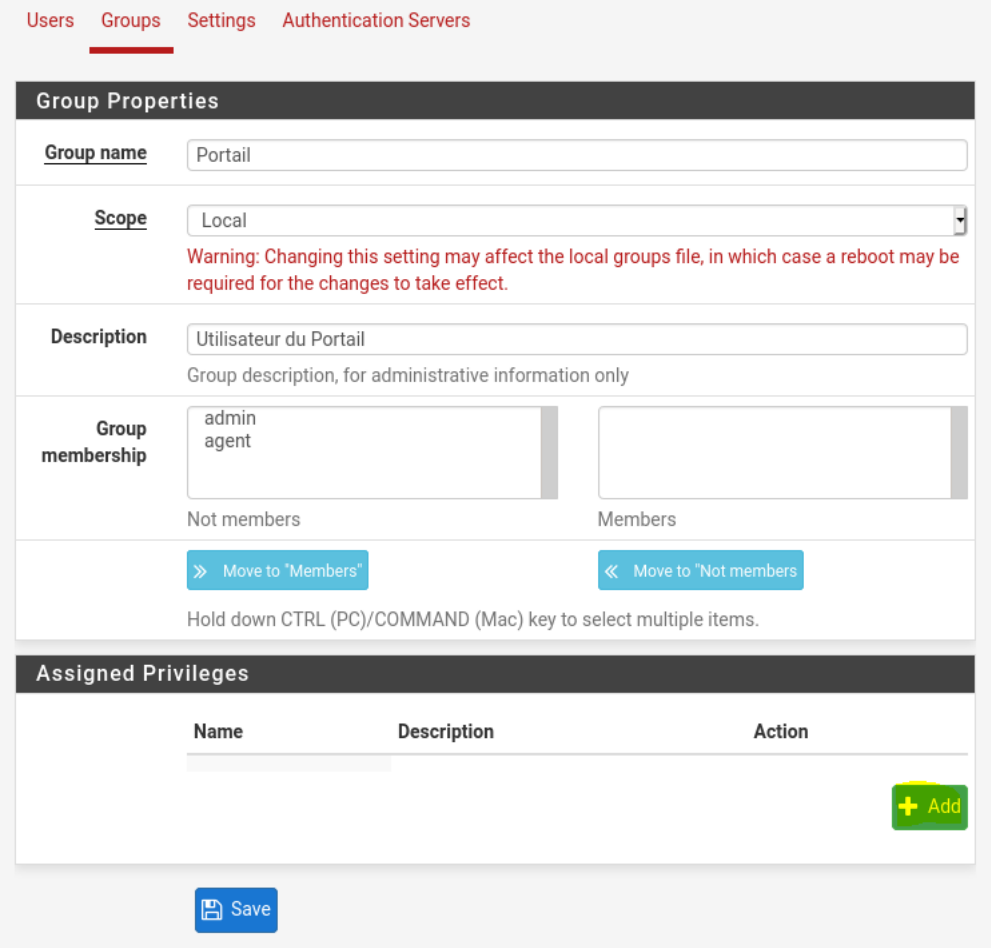
Ce groupe est utilisateurs associés auront seulement le droit d'utiliser le Portail Captif.

Onglet "Groups", cliquez sur "+ Add"

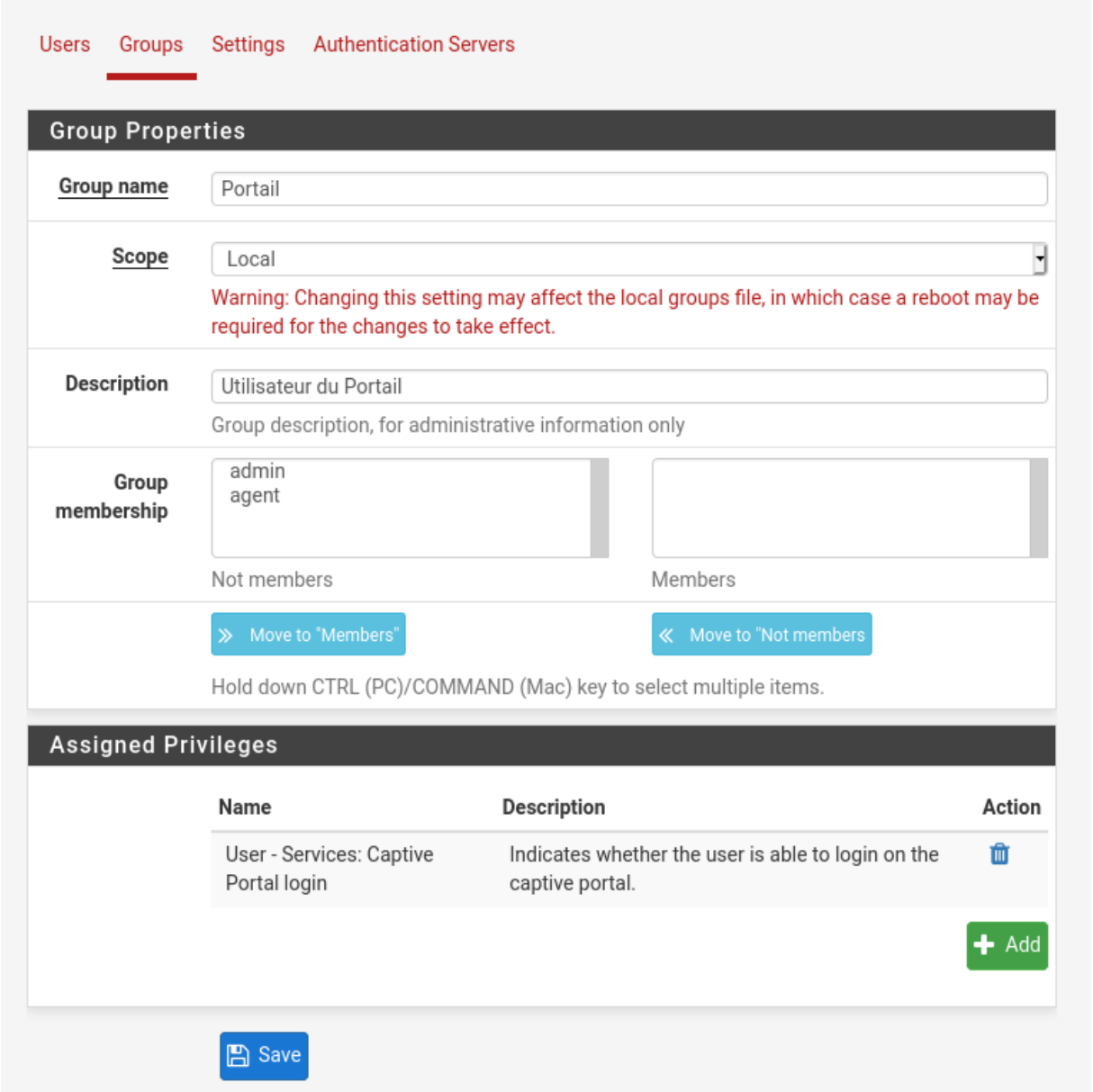


Renseignez le Nom du Groupe "Portail" et sa description "Utilisateurs du Portail". Cliquez "Save"

Dans le menu "Actions", modifier le groupe créé en cliquant sur le stylo.



Sélectionnez dans la liste “User – Services : Captive Portal login” (Autorisé seulement à se connecter au Portail Captif).



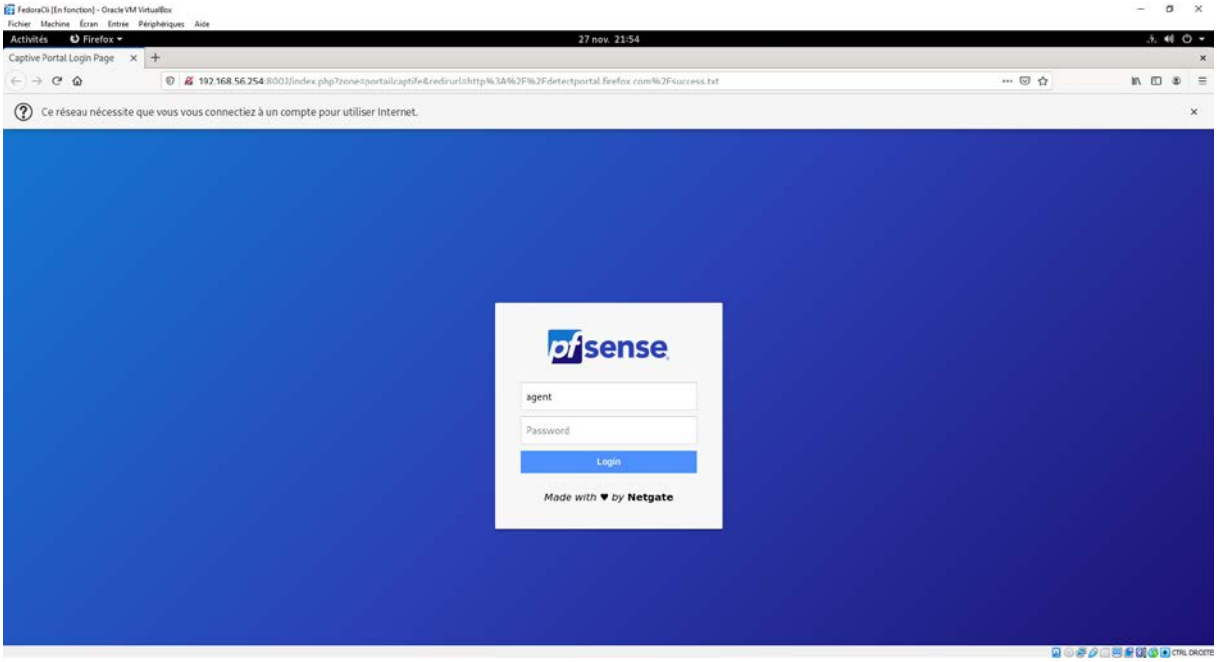
Onglet “Users“, cliquez sur “+ Add”.

Entrer un Nom d’Utilisateur “test”, son mot de passe et sa description “Un Utilisateur du Portail”.

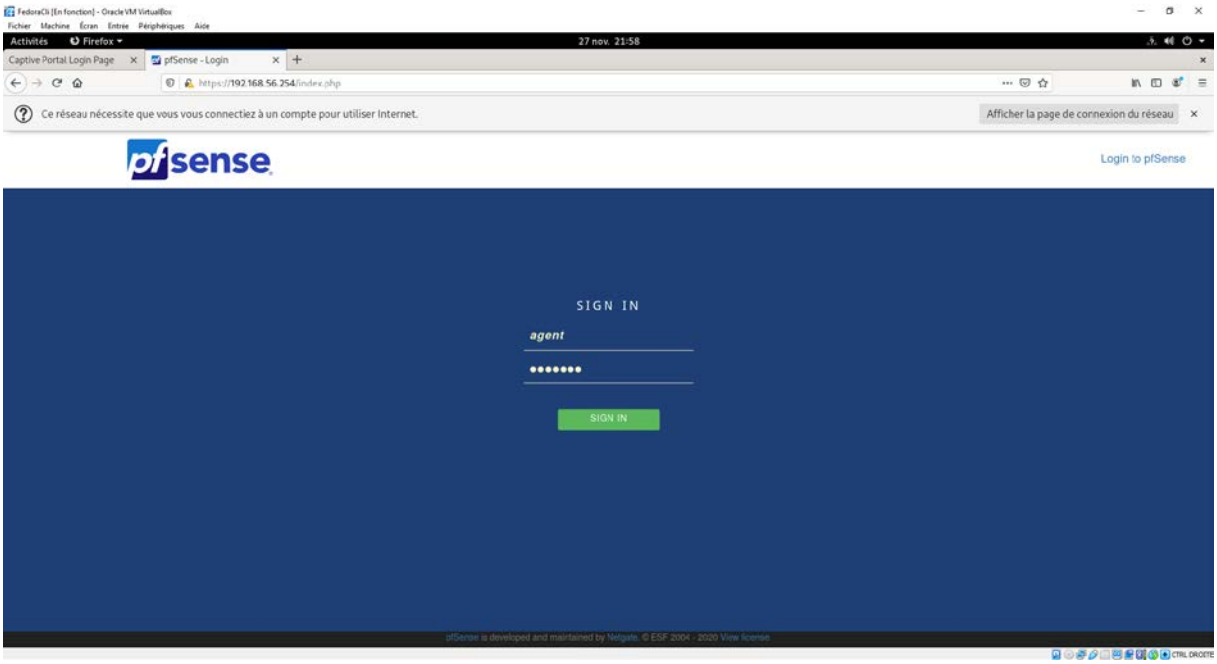
Sélectionner dans “Group membership” le groupe “Portail” précédemment créé. Cliquez sur “Move to Member of list” puis “Save”.

L’utilisateur “test” est autorisé à se connecter au Portail Captif.

Connexion avec le Compte “agent”.

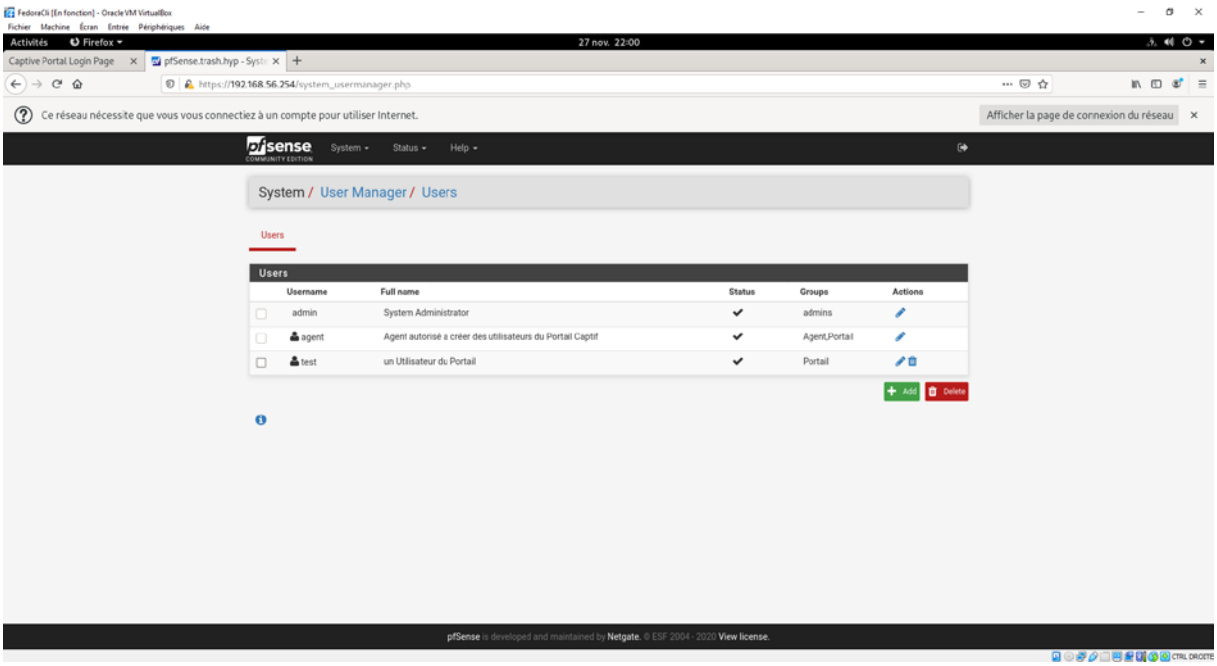


Comme nous pouvons le voir, il nous indique que ce réseau nécessite que nous nous connections pour utiliser Internet. Testons avec le compte Agent.

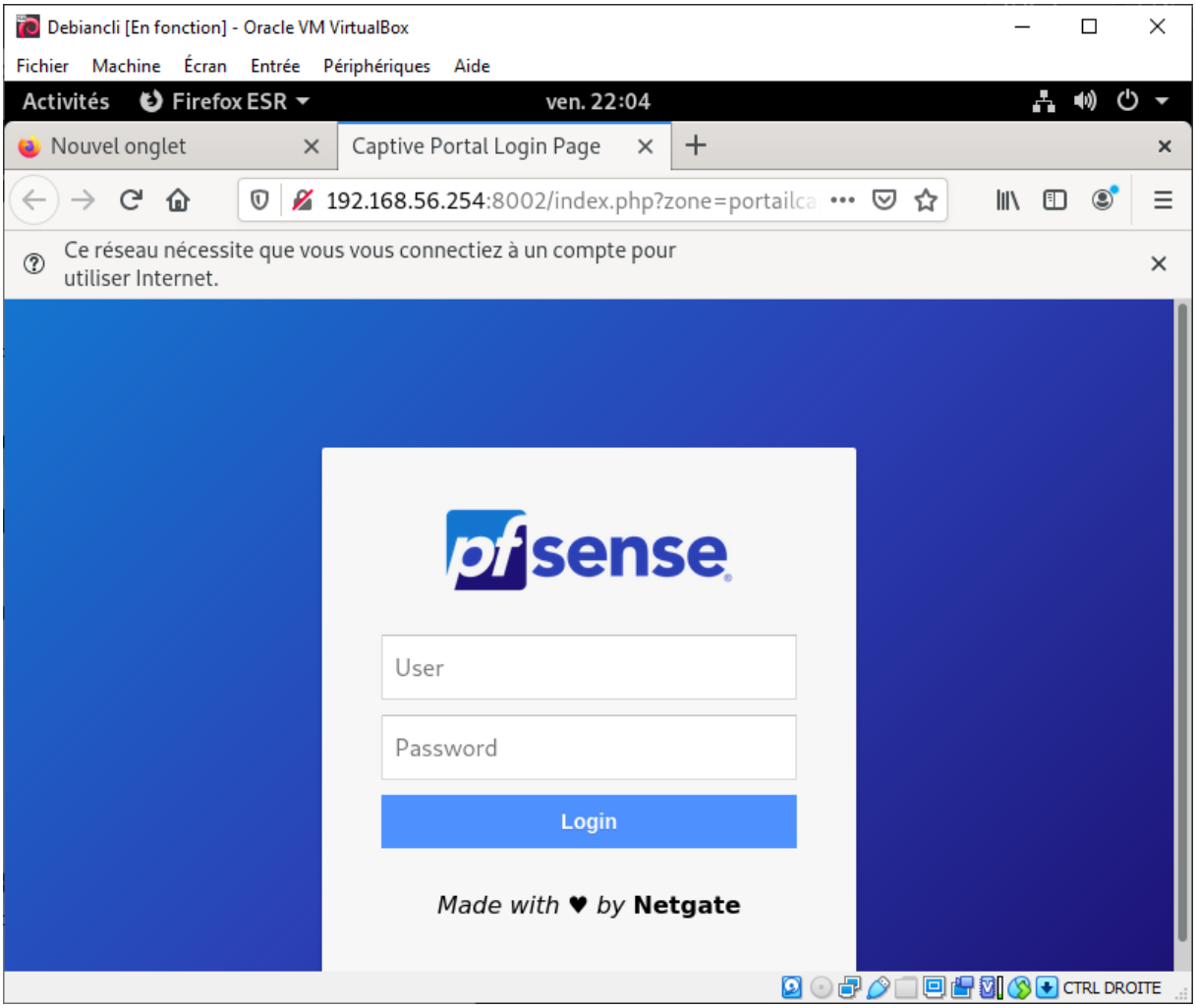


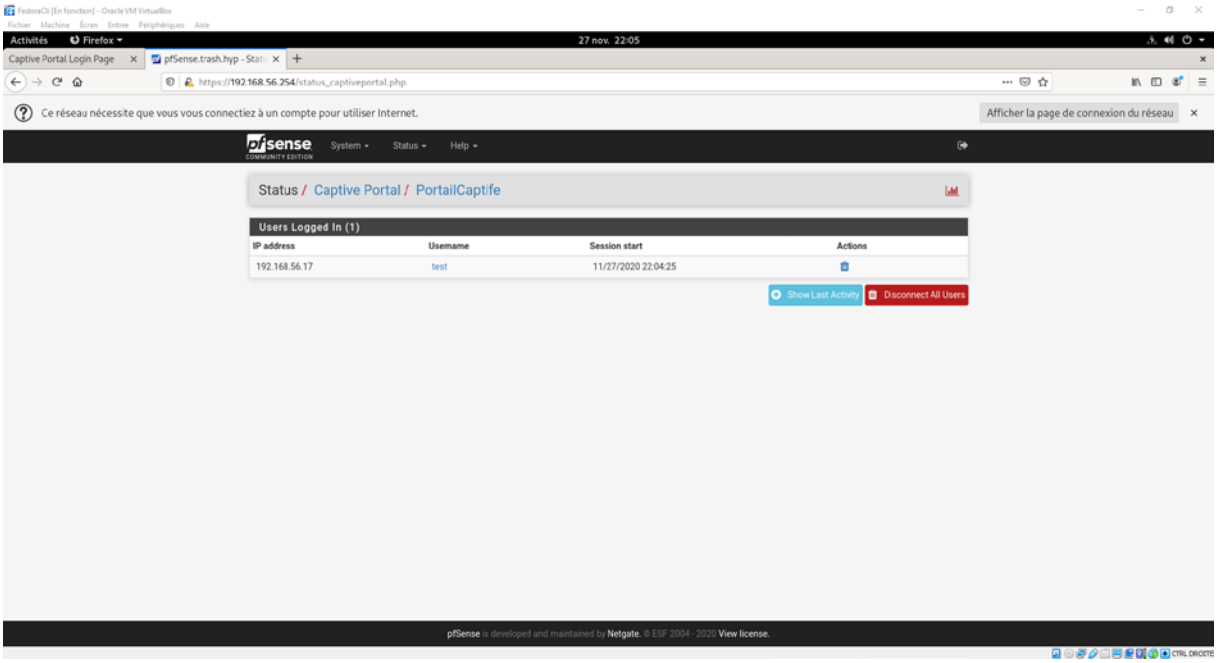
Utilisez la page de connections pfSense d’administration.

Cet utilisateur a seulement le droit de créer des Utilisateurs du Portail Captif par délégation et de voir le Statut des utilisateurs connectés.



Dans l'onglet Status nous pouvons voir les utilisateurs qui sont connecter au portail captif.
testons cela avec un client avec l'identifiant test.





Comme nous pouvons le voir le client s'est connecter et peut faire des recherches internet.