Guide d’installation & configuration

www.pfsense.org

Par Laura Giannico

1. Introduction & Contexte :

Dans cette documentation nous allons voir comment installer et configurer pas a pas, une VM afin d'accueillir un outil : PfSense.

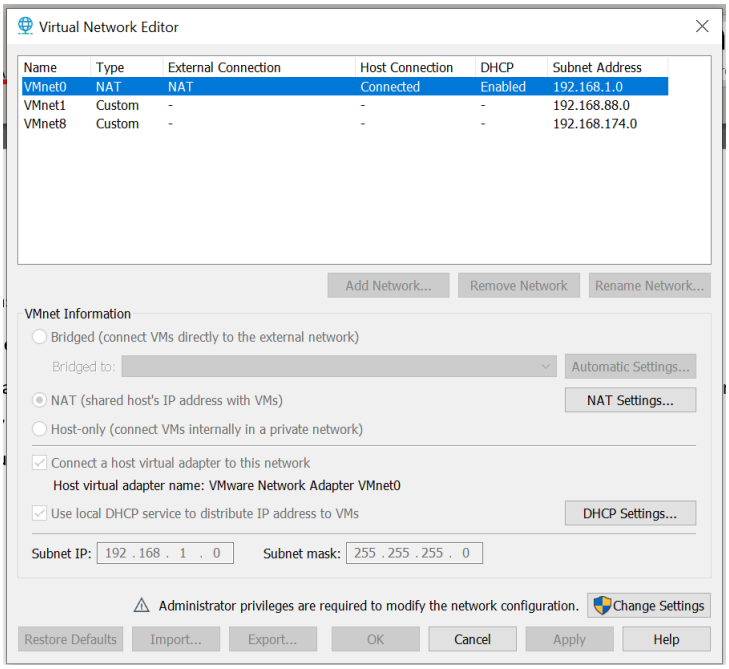
PfSense est un pare-feu base sous FreeBSD, qui a des fonctionnalités de routeur également. Nous verrons comment accéder à la version gratuite (open-source) Community Edition. FreeBSD est un OS sous Linux.

2. Configurer une VM :

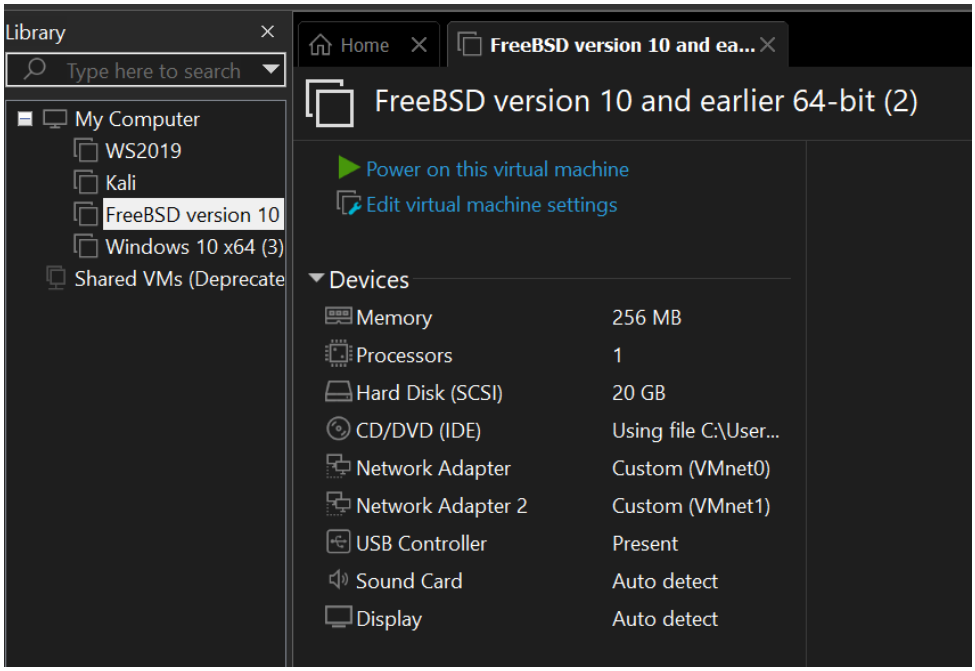
Télécharger l'ISO de **Pfsense** a l'adresse suivante : https://www.pfsense.org/download/

Une fois fait, ouvrez VMware, et créer une nouvelle VM en intégrant l'ISO dessus. Avant de lancer votre VM, il faudra la configurer. Pour commencer, aller sur *Edit > Virtual Network Editor*.

Il vous faudra le VMnet1 en Custom, et pour le VMnet0, il le faut en NAT et configurer de manière suivante :

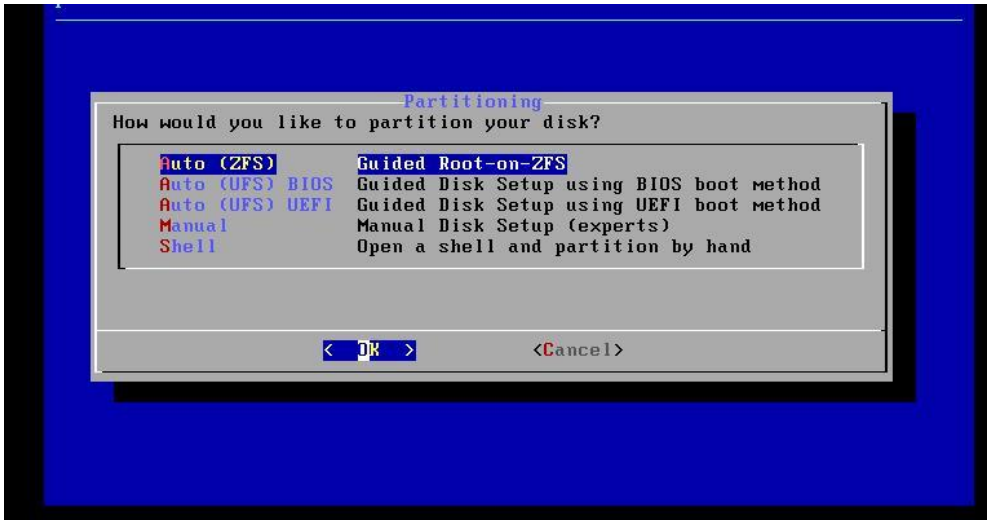


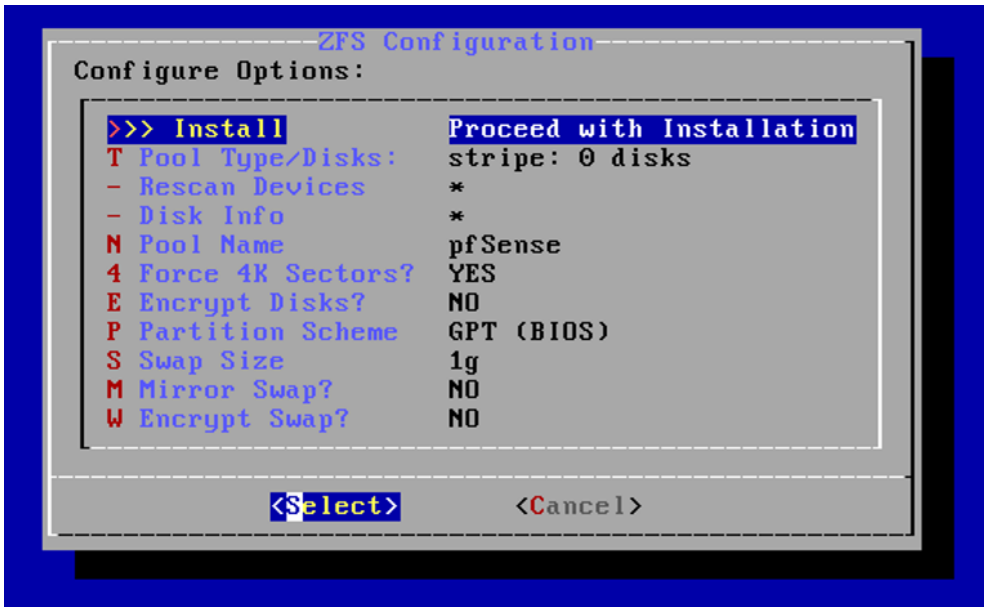
Puis, il faut ensuite modifier les paramètres de la VM en question. Sélectionner, 2 Network Adapter, en Custom, un pour VMnet0 et l'autre pour VMnet1.

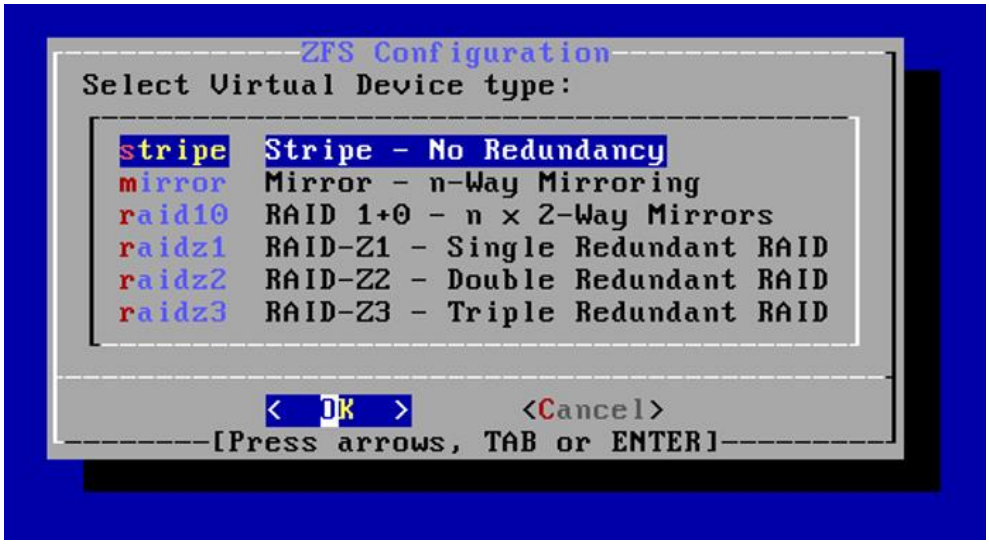


3. Installer Pfsense :

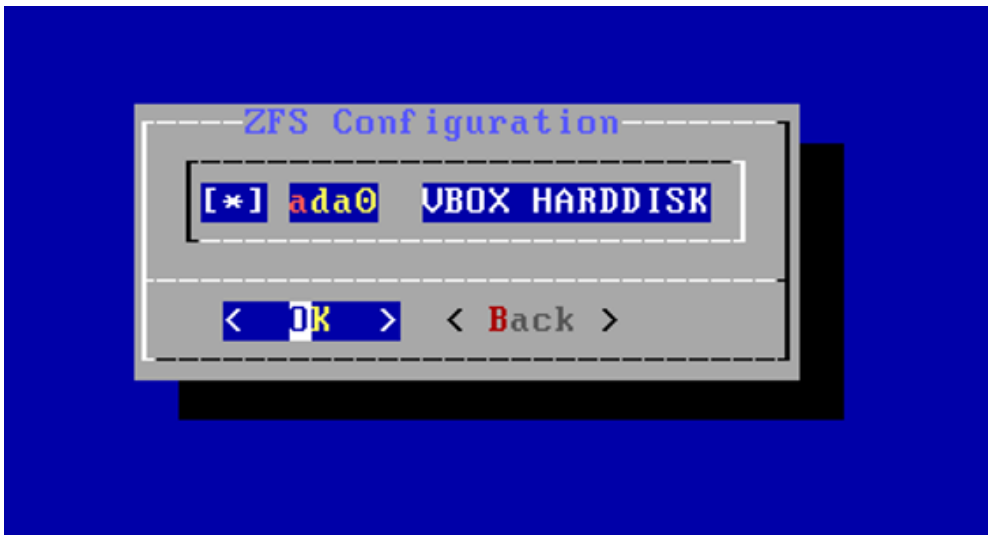
Allumez votre VM, l'installer de **Pfsense** va alors vous guider. Globalement, il y a juste à faire suivant sans modifier quoi que ce soit, mais juste au cas où, voici le guide complet :



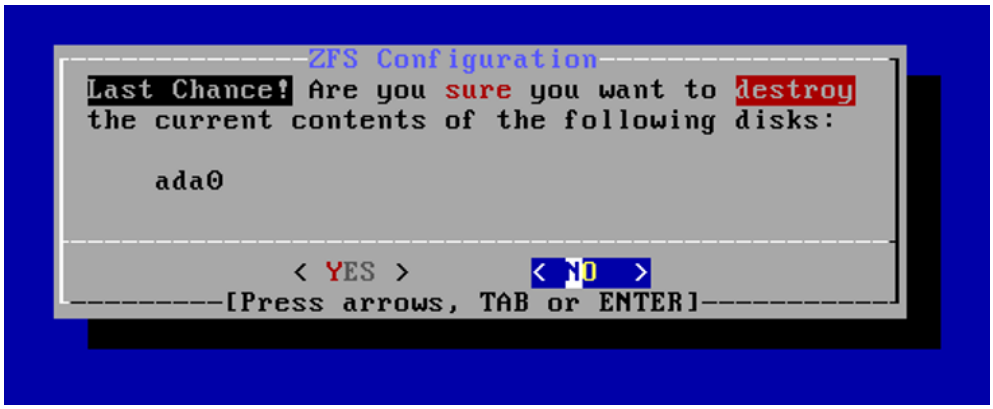


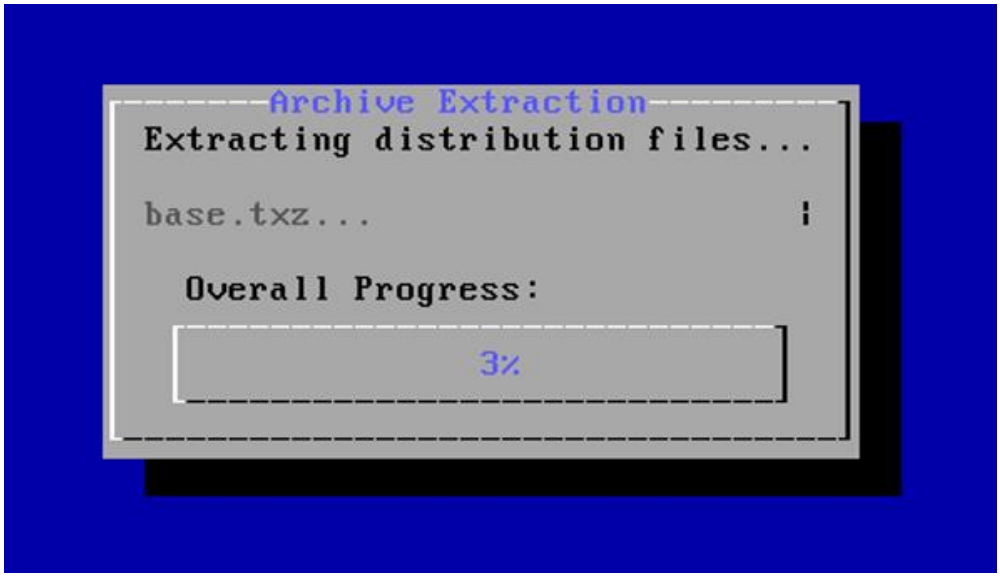


Sur le menu suivant, faite « *espace* » pour cocher :

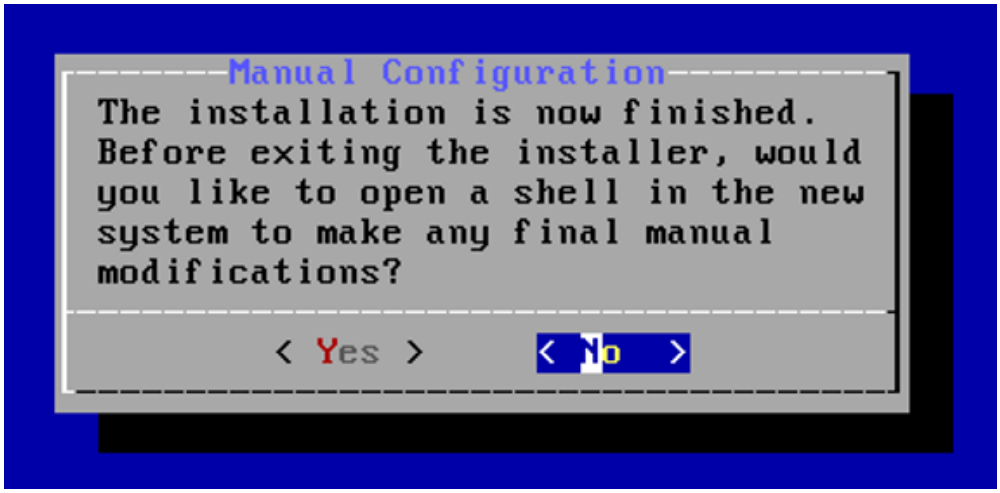


Sur le menu suivant, il faut dire « yes », vous n'avez pas le choix :

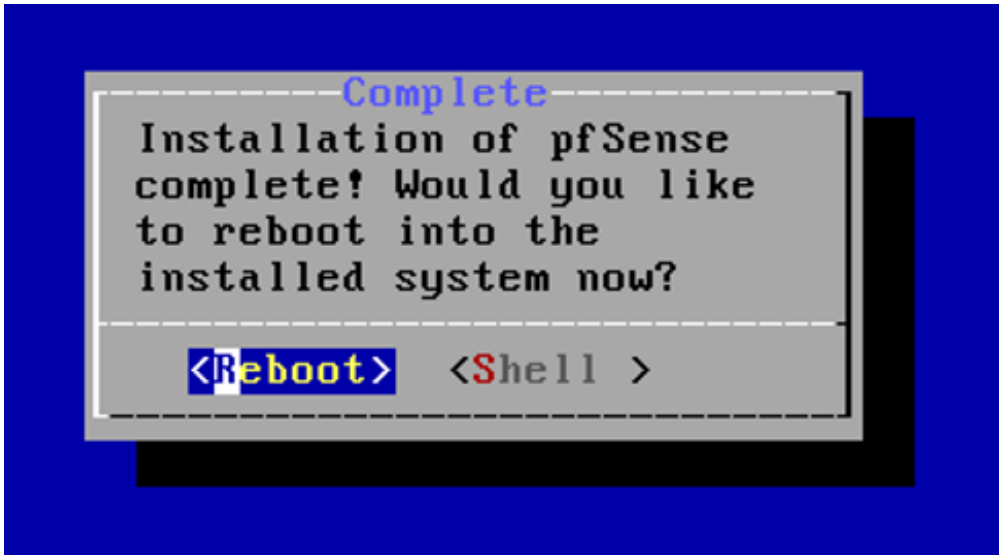




Dans le menu suivant, vous pouvez dire « non » :

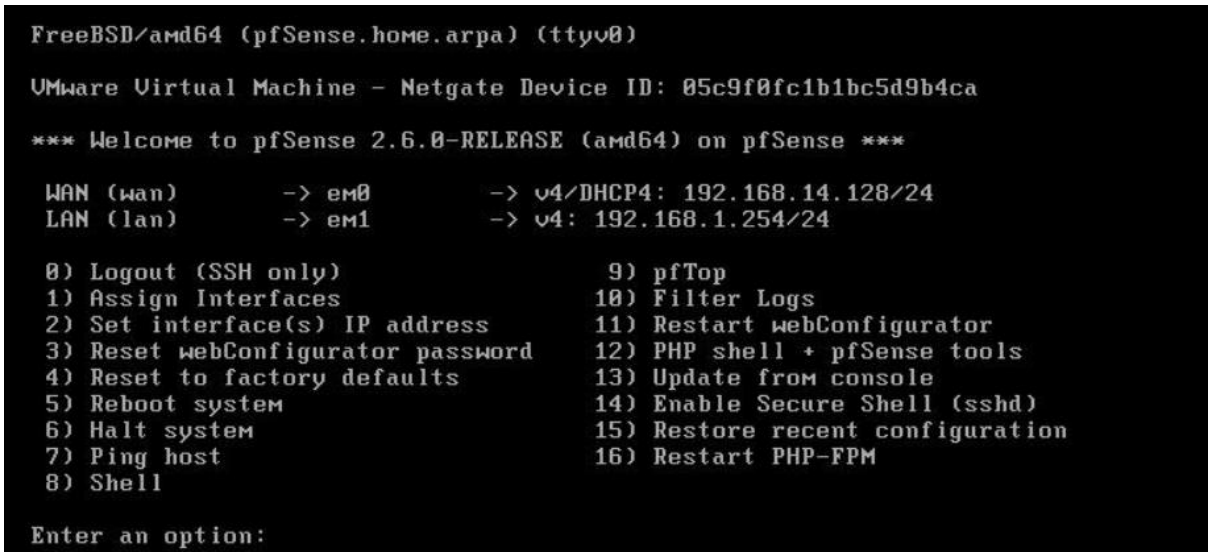


Terminez l'installation en redémarrant votre VM :



4. Configurer Pfsense :

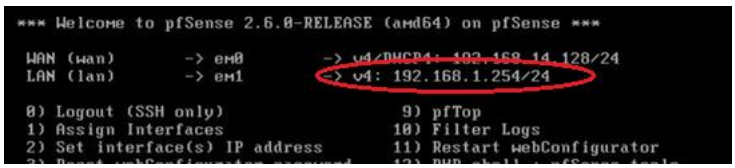
Lorsque votre VM redémarre, il faudra faire quelques modifications finales avant de pouvoir accéder à l'interface de Pfsense. De plus, ici tout se fera sous ligne de commande. Voici le menu que vous devriez voir apparaitre si votre installation s'est bien passée :

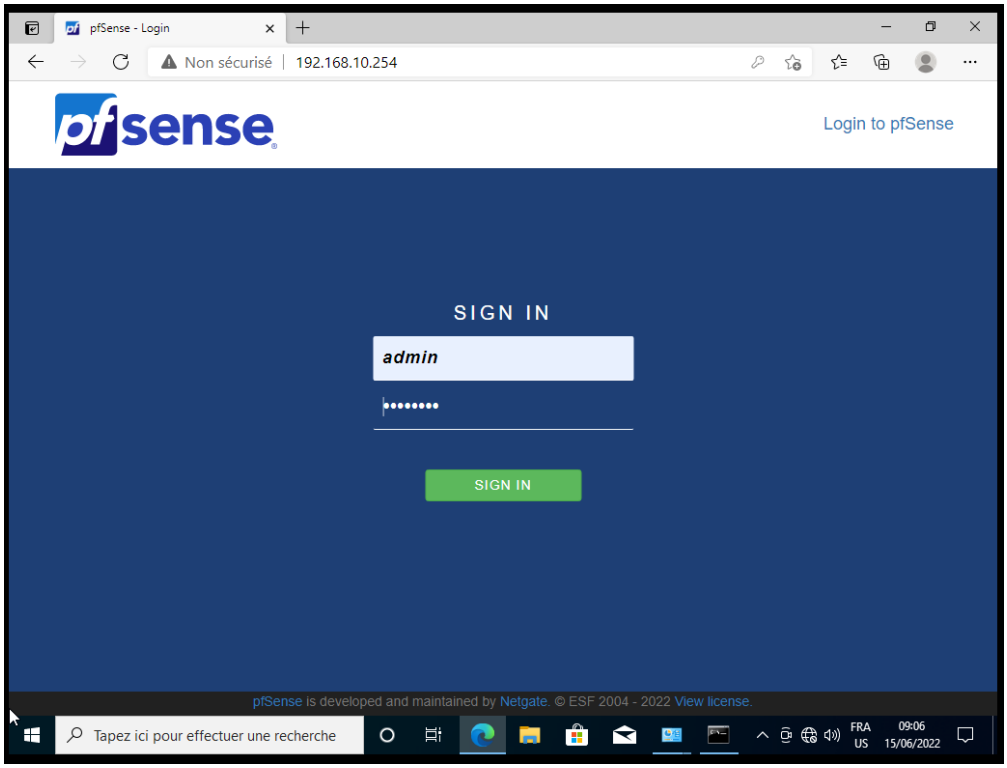


Sélectionner l'option 2, puis encore 2 (pour modifier l'IP du LAN) et entrez une adresse IPv4 statique :

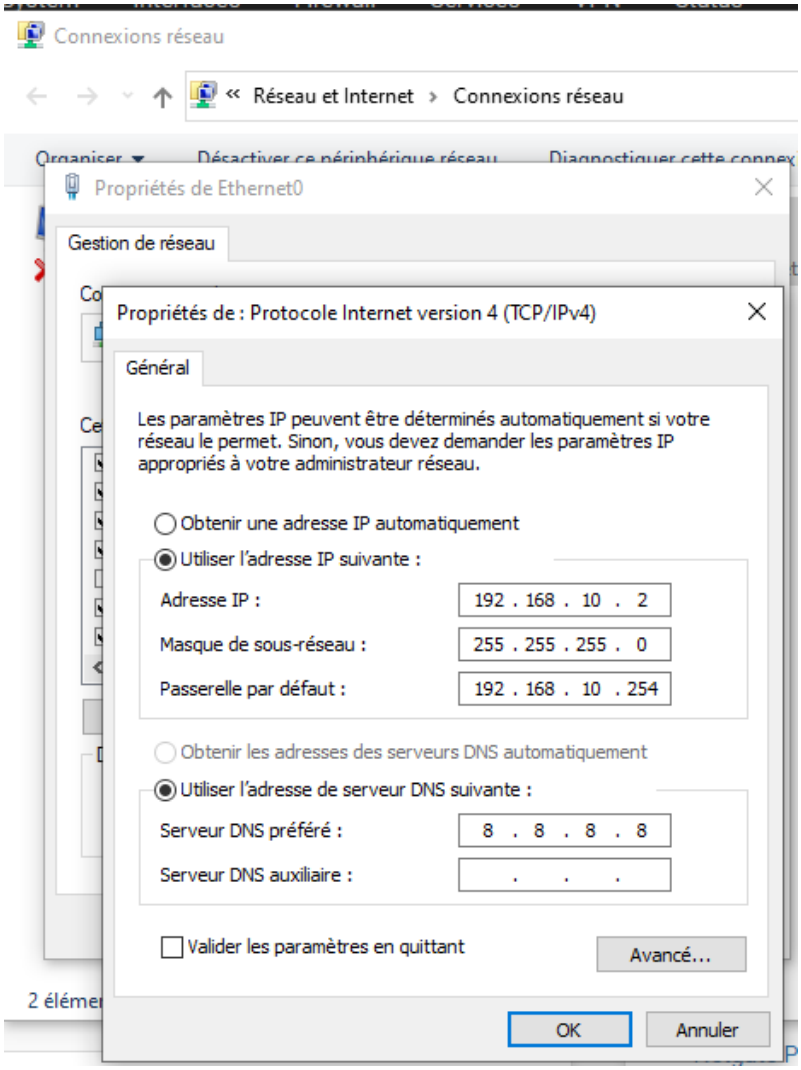
L'interface va vous posez les questions suivantes, il faudra répondre par :

La configuration devrait être terminée. Hors de votre VM, sur votre ordinateur hôte, ouvrez votre navigateur et entrez l'adresse IP du LAN de votre VM :





Dans le cas où cela ne fonctionnerait pas, il faut changer les configurations IPv4 de votre machine. Cependant, ne le faites pas, et préférez l'utilisation d'une VM sous Windows10. Les configurations réseaux pour cette nouvelle VM sont les suivantes :

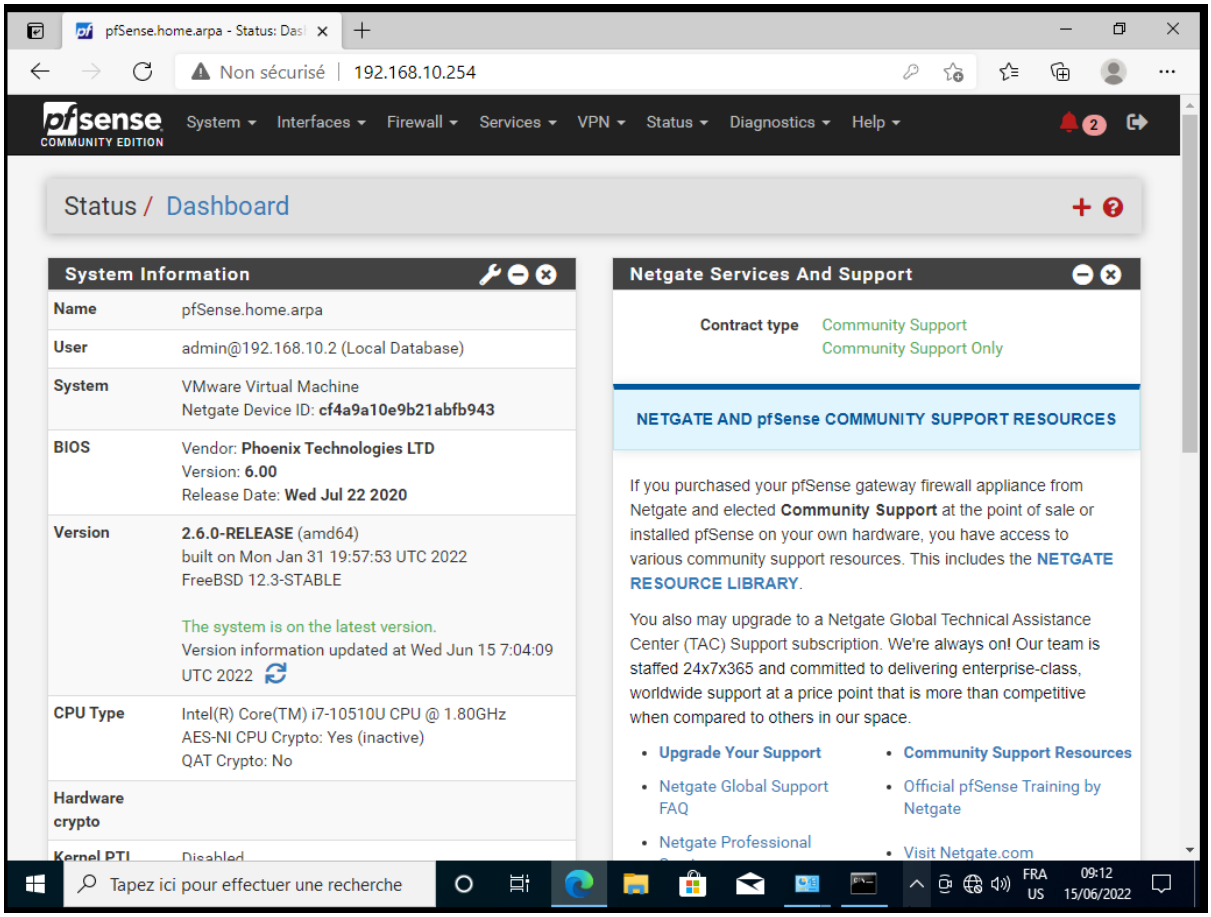


Ouvrez ensuite le navigateur sur la VM de Windows 10 et accédez à l'interface de **PfSense** grâce a l'adresse IP du LAN. Les identifiants par défaut pour se connecter à l'interface sont :

Username : *admin*

Mot de passe : *pfsense*

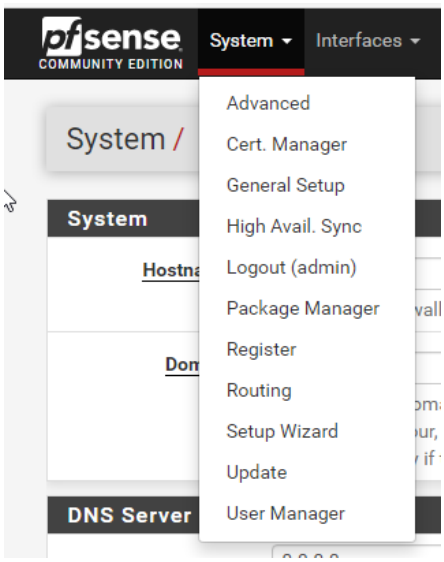
Bienvenue sur le dashboard de **Pfsense**, vous pouvez commencer à travailler !



5. Appréhendez l'interface de Pfsense :

a. Configurations générales :

La première chose à faire est d'aller dans *System > General Setup* :

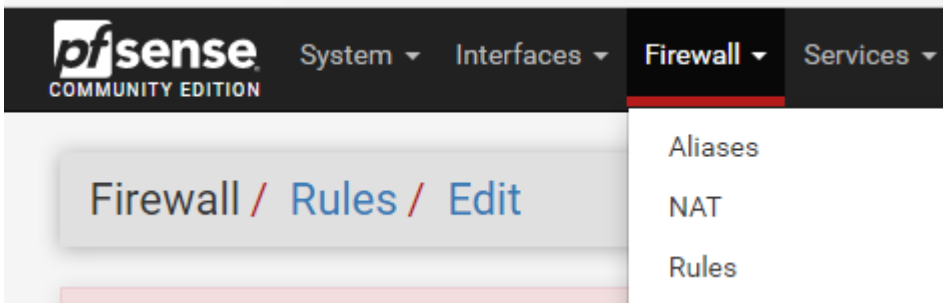


Laissez tout par défaut, sauf l'adresse du DNS Server : j'ai personnellement mis 8.8.8.8

Cliquez sur [Save], on vous demandera d'autres configurations, dont le mot de passe. Changez-le ou remettez celui par défaut.

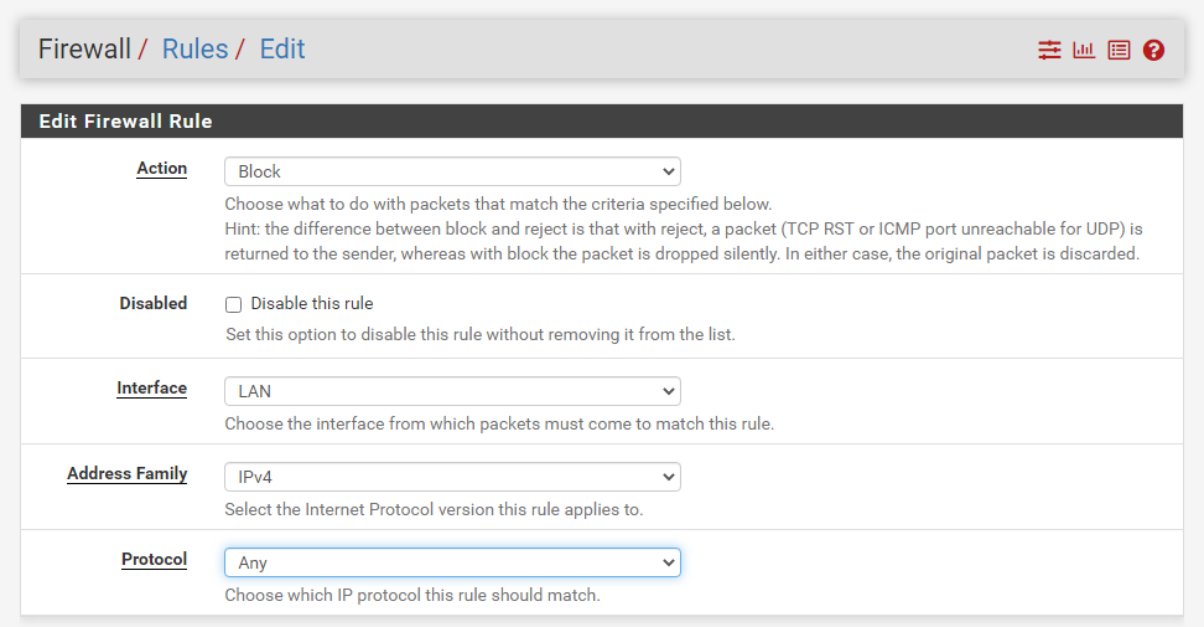
b. Filtrage « deny all » :

Nous allons performer un filtrage qui bloque tout connexion internet. Pour faire un filtrage grâce a **Pfsense**, il faut se rendre ici : *Firewall > Rules*



Ajouter une nouvelle règle en cliquant sur [Add].

Puis configurer votre règle comme ceci :

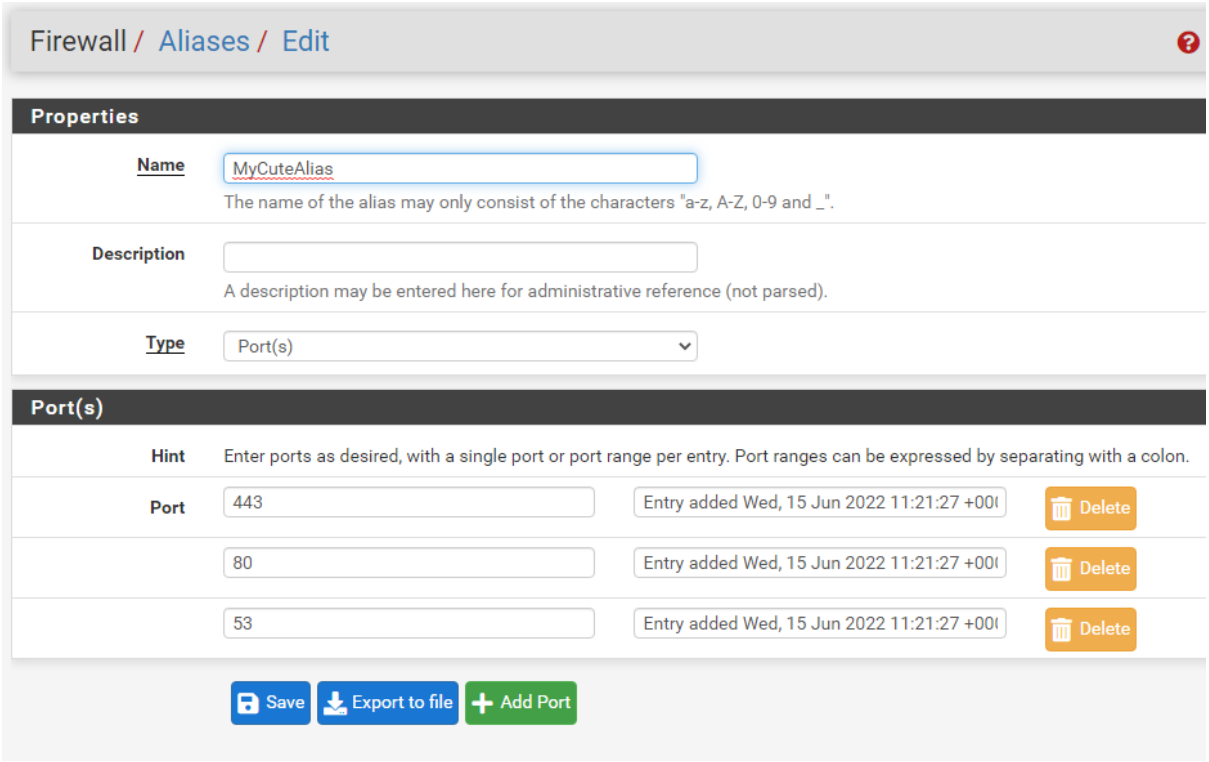


La source et la destination devront être configurées a « *any* » pour se laisser aucune connexion entrante ni sortante. Enregistrez votre règle. Votre pare-feu bloque désormais toute tentative d'entrées et de sorties de n'importe quels protocoles.

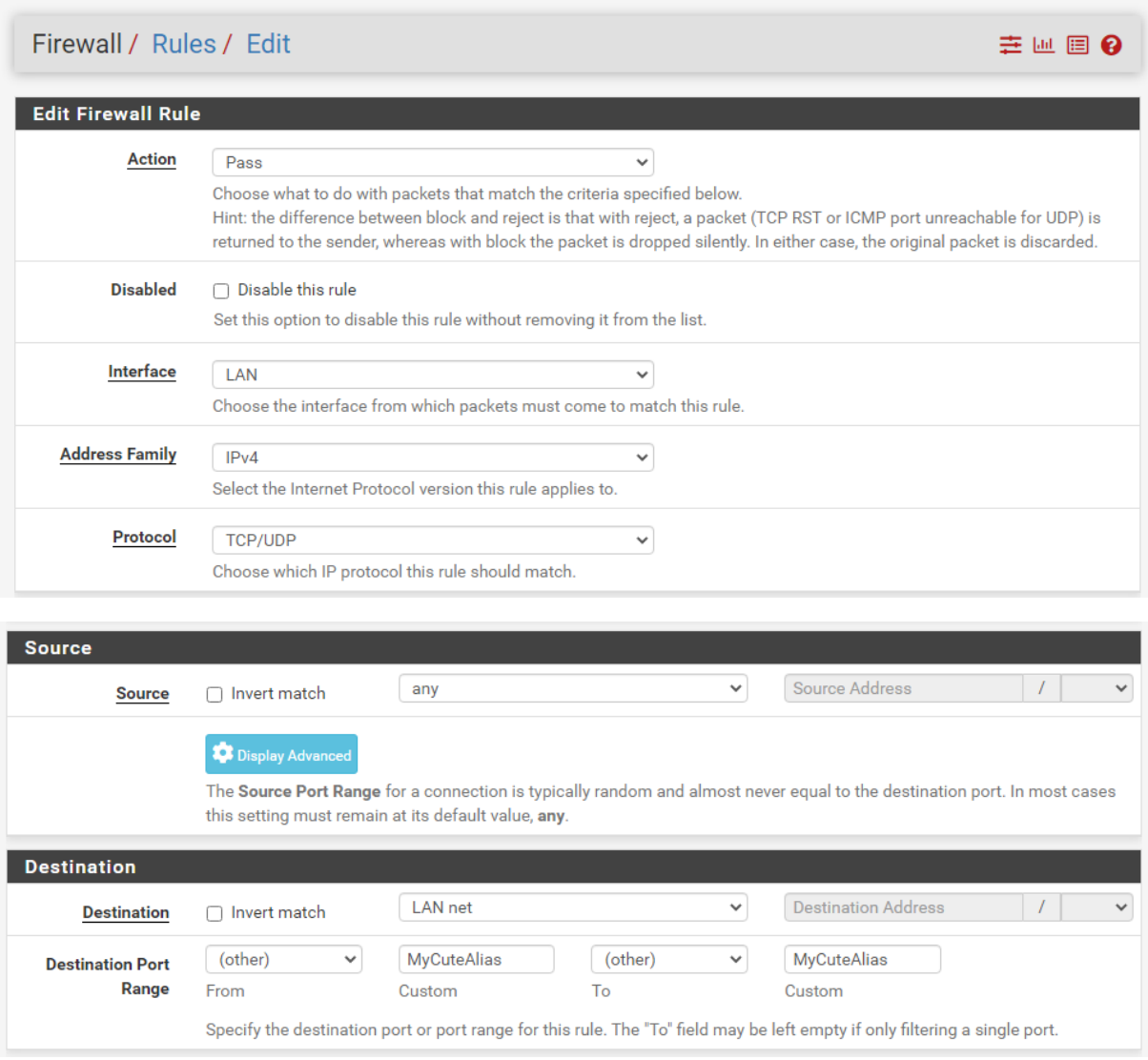
c. Filtrage internet :

L'exercice précédent n'est pas très pratique : plus rien ne peut entrer ou sortir sur votre réseau. Cette fois-ci, nous allons configurer une règle pour faire en sorte qu'uniquement le traffic internet puisse passer.

Retournez sur l'interface, vérifiez que votre règle précédente est toujours active, car nous allons en rajouter une nouvelle par-dessus pour autoriser internet. Allez dans *Firewall > Aliases* pour vous créer un alias qui contiendra les plages de Ports a autorisé. Vous devrez mettre les Ports 80, 53 et 443.



Validez votre alias. Puis retourner dans *Firewall > Rules*, ou il faudra autoriser l'accès à ces Ports (il faudra mettre en Destination votre Alias). Voici les screenshots de la configuration de la règle :

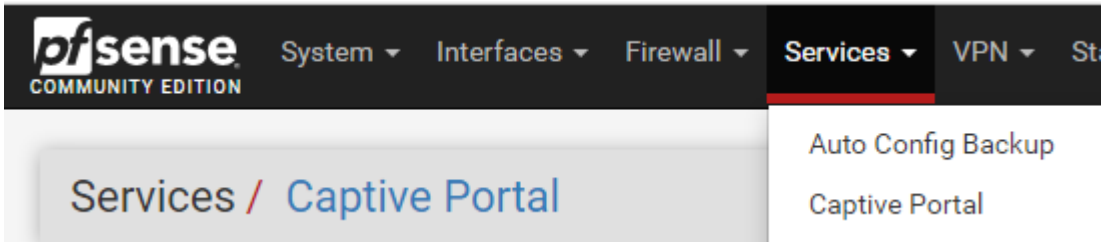


Sauvegardez votre configuration, et normalement, tout le traffic est bloqué, a l'exception d'internet.

d. Portail captif :

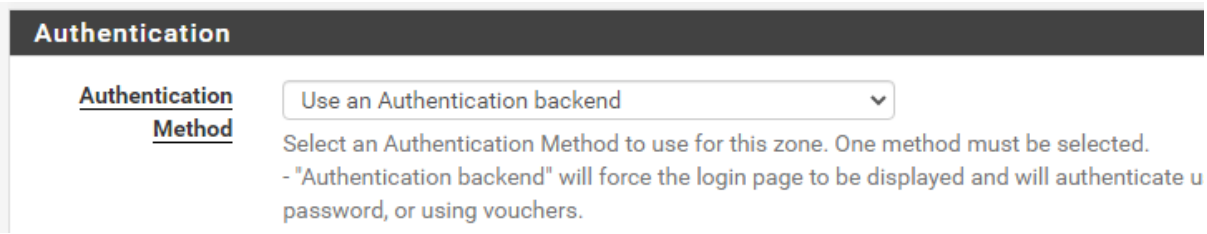
Un portail captif est une interface web qui s'affiche sur le navigateur vous demandant des identifiants afin d'accéder au réseau. Exemple, vous vous connectez sur le réseau Wi-Fi d'un hôtel, et l'interface vous demande des identifiants pour savoir si vous avez bien payé la connexion ou non. Vous ne serez pas autorisé à naviguer sur internet si les codes d'accès ne sont pas renseignés.

Nous allons mettre en place cette solution grâce à **Pfsense**, un portail captif avec authentification interne. C'est-à-dire que vous ne pourrez qu'accéder à Internet si vous avez des identifiants (créer sous **Pfsense**). Il faut aller dans *Services > Captive Portal.*



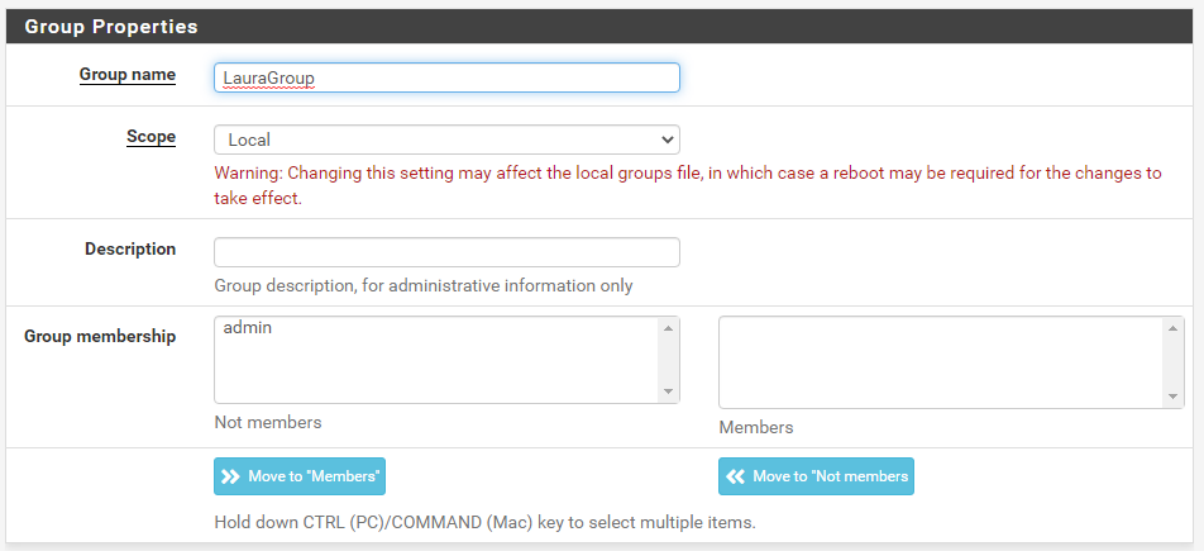
Puis cliquez sur [Add]. Donnez un nom et une description puis cliquez sur [Save]. Cochez la case « *Enable Captive Portal* », et d'autres options vont apparaitre.

Sélectionnez LAN dans le champ « Interfaces » et laissez tout le reste par défaut. Aller ensuite dans la section « Authentification » et sélectionnez :

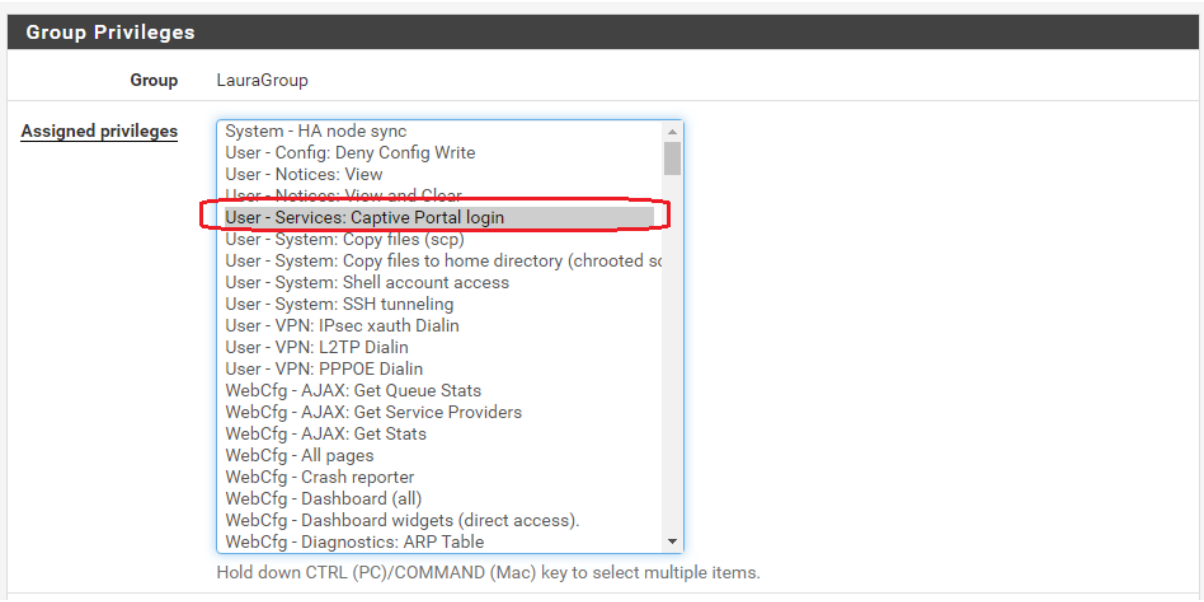


Sauvegardez votre règle.

Puis allez dans *System > User Manager > Groups*. Créer un groupe :



Ensuite, sauvegardez le groupe et rééditez-le. De nouvelles configurations sont disponibles. Sélectionnez les suivantes :



Sauvegardez votre groupe. Et voilà le travail ! Il faudra par la suite créer vos utilisateurs, et les assigner au groupe que vous venez de créer. Ils auront alors l'obligation de passer par votre portail captif pour se connecter, avec les identifiants que vous leur avez créés.