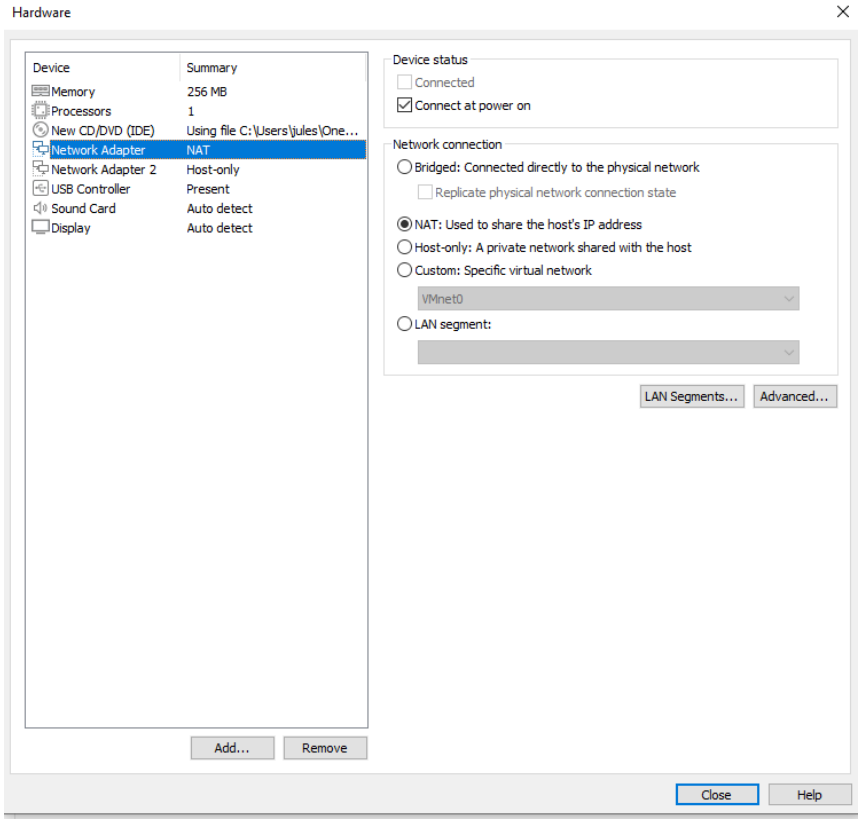
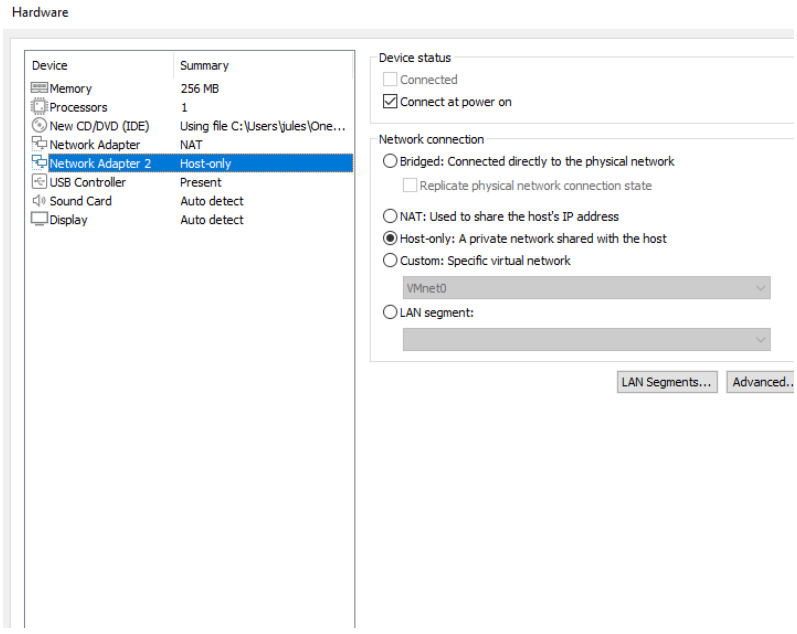
Documentation PFSense

Table des matières

I. Installation pfSence :

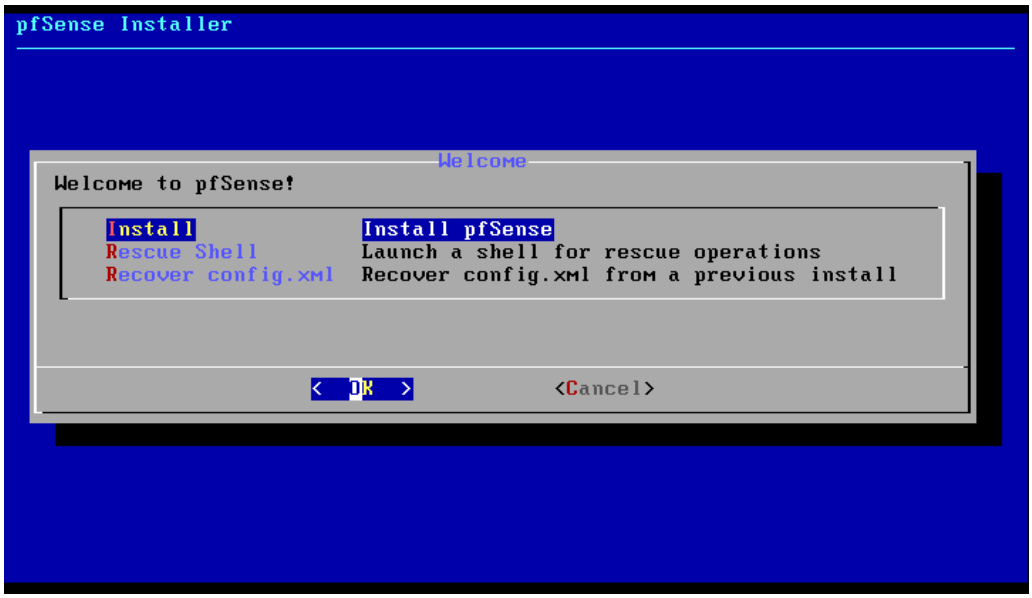
Configuration des cartes réseau de la VM PFsense :



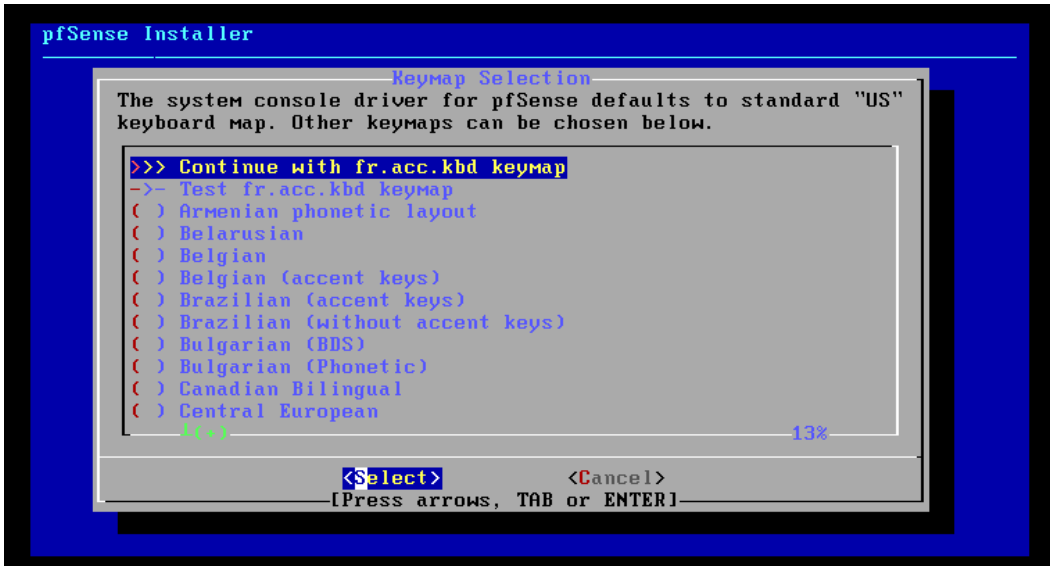


Liste des étapes durant l'installation de pfsense :

sélectionner install pfSense pour procédé à l'installation

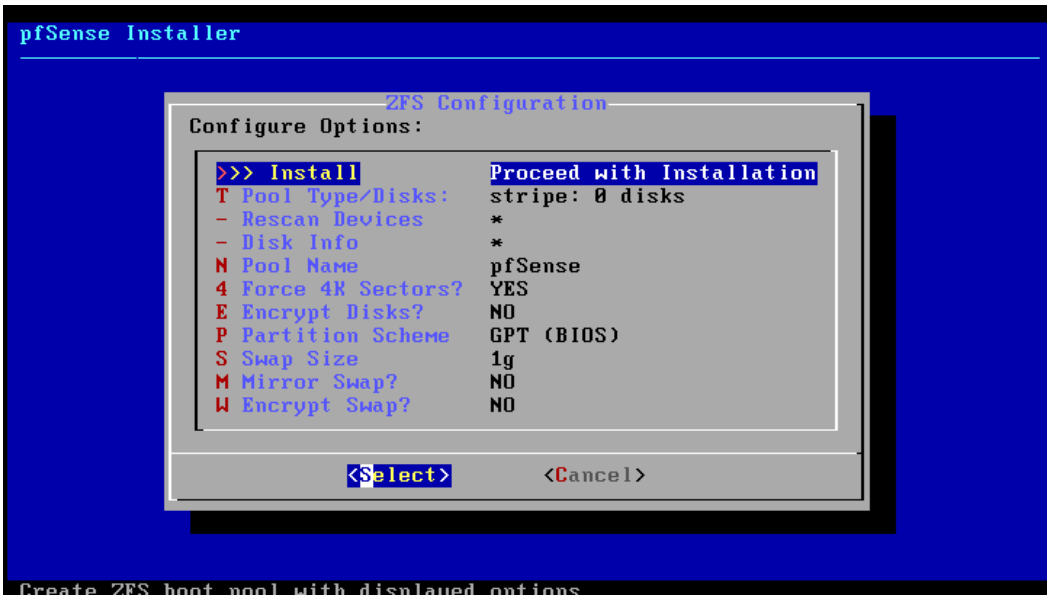


sélectionner votre langue pour le clavier : ici français



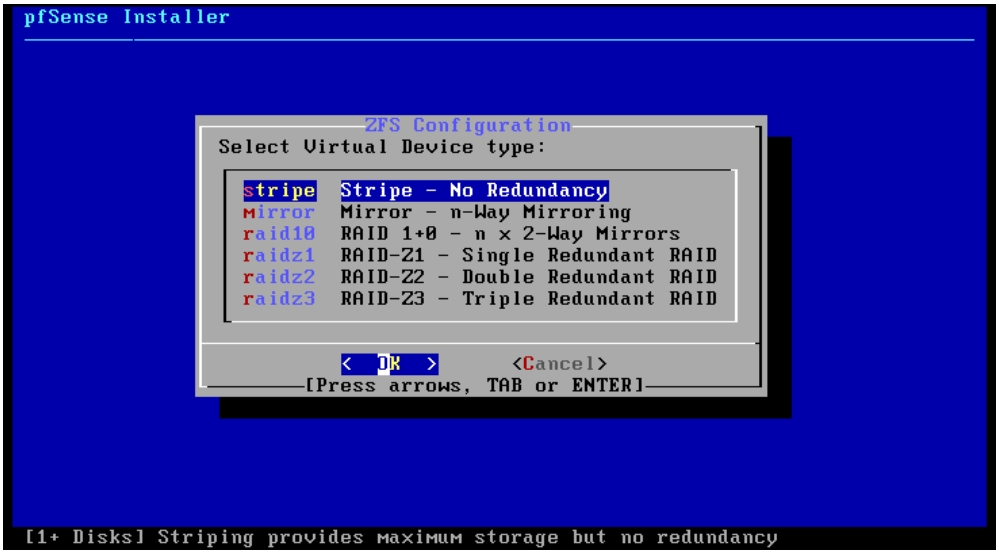
sélectionné auto (ZFS) pour l'installation standard

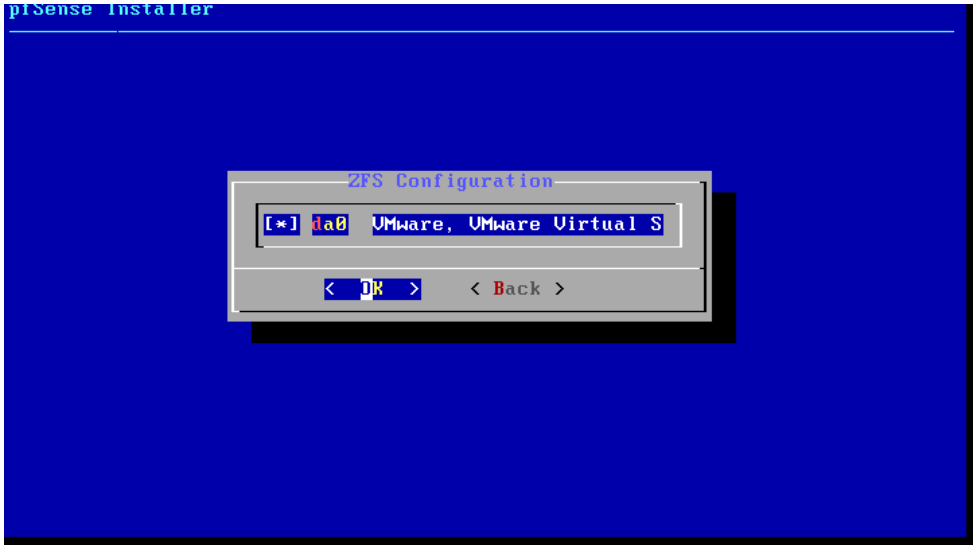
Pour continuer valider install : proceed with installation car notre configuration est bonne

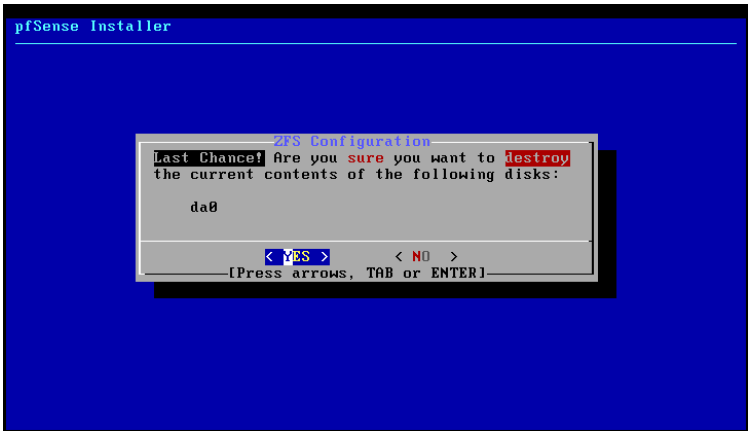


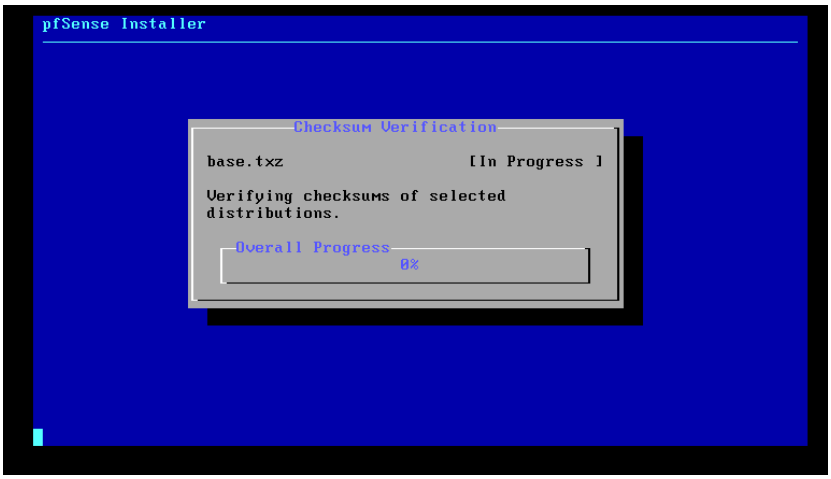
Ensuite choisir le type de stockage pour l'installation que vous souhaiter

Puis valider et attendez que l'installation ce termine.









Une fois installé il faut faire un reboot de la machine. Une fois celui-ci effectue vous arriverez sur l’affichage ci-dessous.

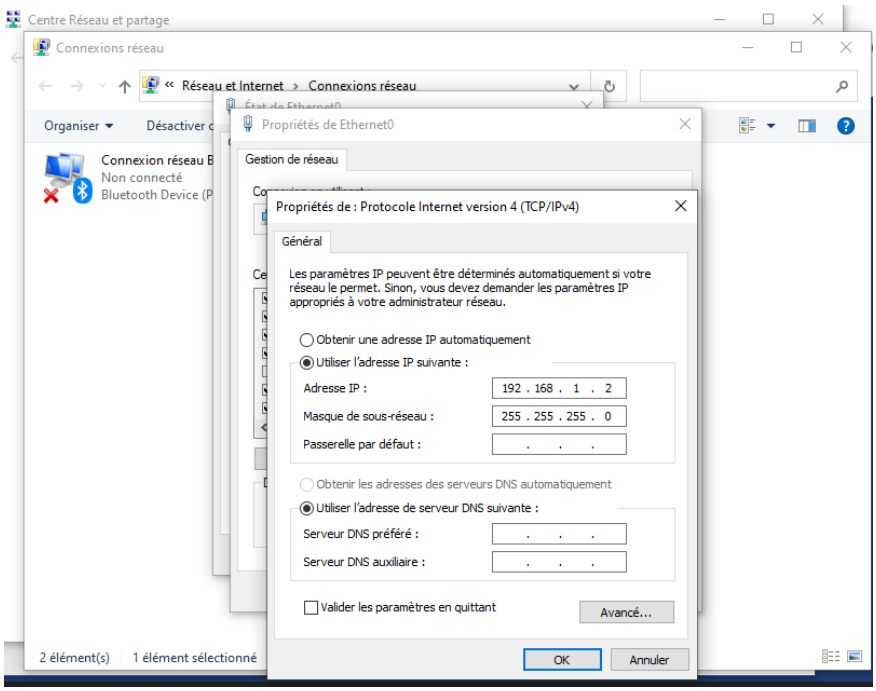
```
VMware Virtual Machine - Netgate Device ID: 74b69c927fac3ed023fb

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.245.143/24
 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
```

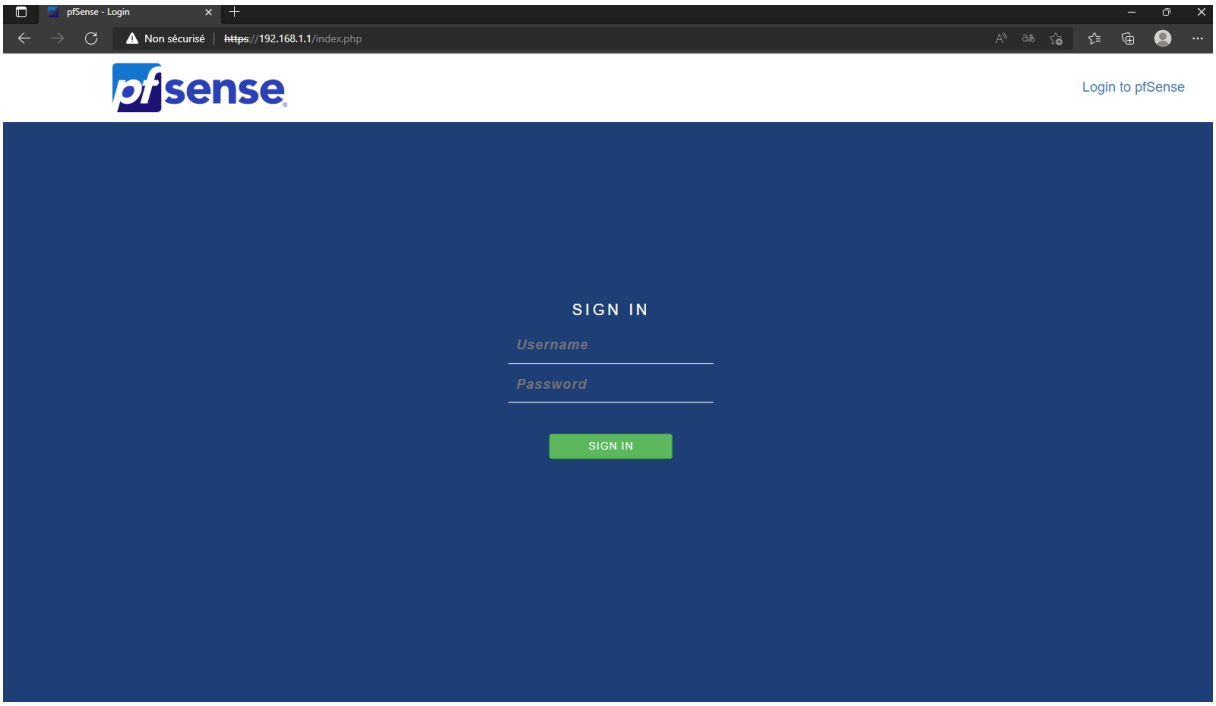
Entrer 2 pour accéder au adresse IP :

Nous ponvons bien voir que notre première carte réseau est configuré en DHCP et que la deuxième est en ip static, donc la première en 192.168.245.143 et la suivante qui est en IP fixe est : 192.168.1.1.

```
VMware Virtual Machine - Netgate Device ID: 74b69c927fac3ed023fb

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.245.143/24
 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: 2

Available interfaces:

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

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

Ensuite pour accéder au firewall, nous prenons une vm sous windows 10 que l'on va configuré sur le même réseau que notre vm pfSense :





Une fois les vm configuré sur le même réseau, taper l'IP du firewall dans le navigateur, ici 192.168.1.1
username : admin

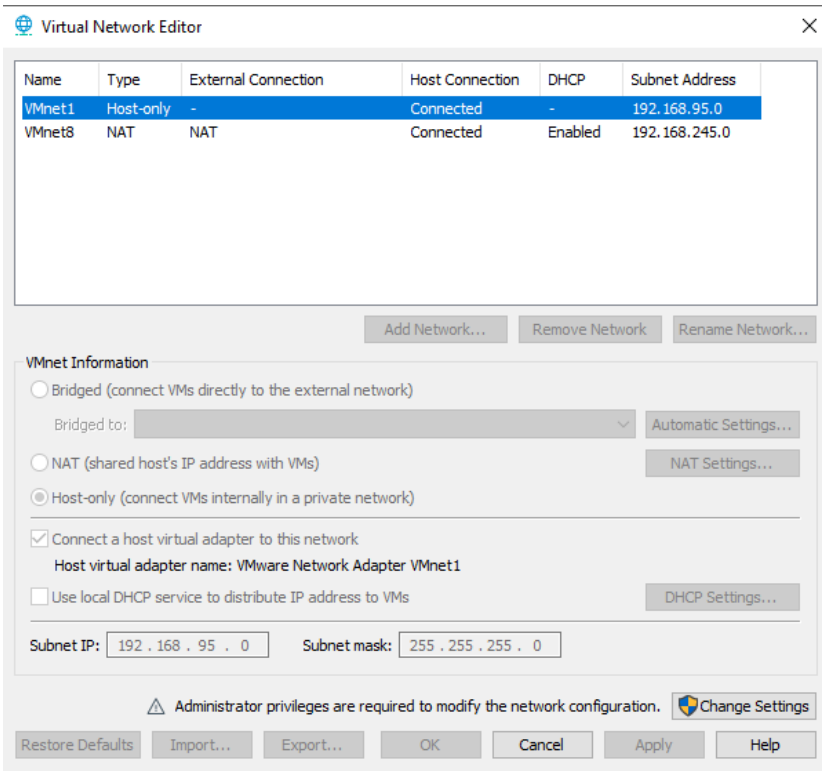
password par défaut : pfsense

il faudra simplement changer au moins le mot de passe pour pouvoir commencer à configurer.

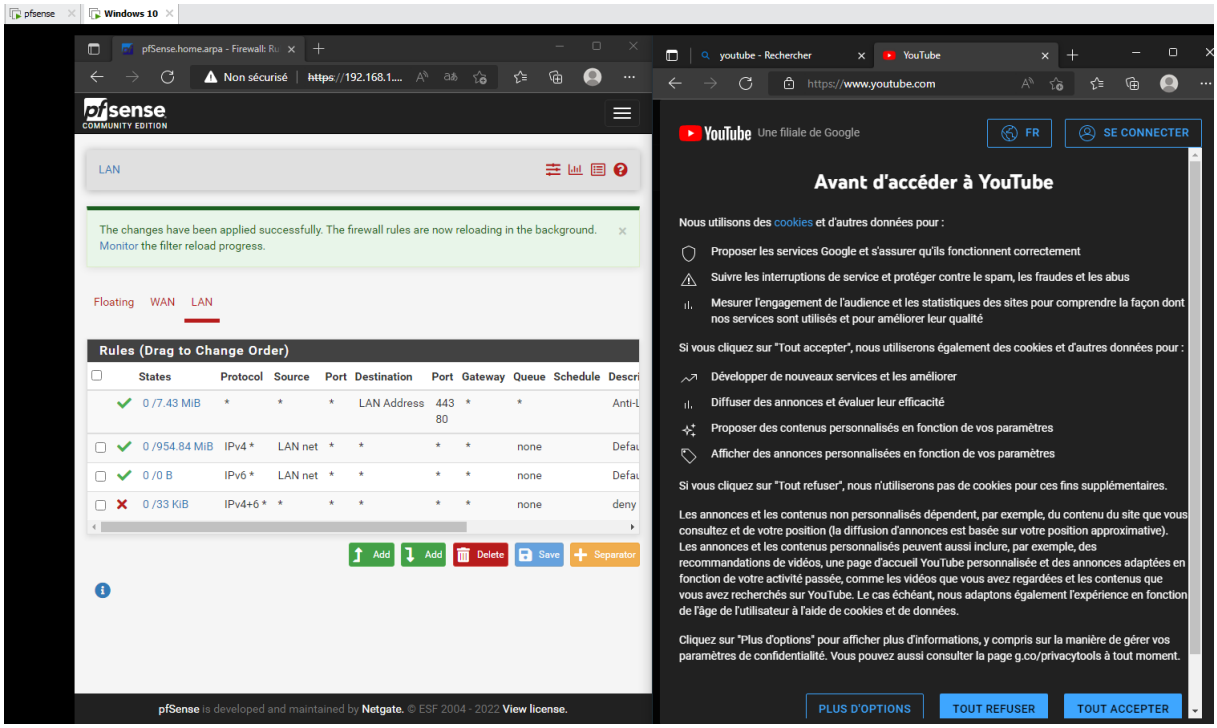
Nous pouvons ici activé ou désactivé le DHCP, configuré notre range d'IP, nos masques, nos DNS etc..

D'ailleurs ici nous allons configuré les DNS de la manière suivante :

Une fois notre serveur DHCP configuré avec l'adresse de la passerelle entré donc ici notre vm pfSense (192.168.1.1) nous pouvons repassé la vm windows 10 en DHCP, et celle-ci devais avoir accès a Mais il ne faut pas oublier de décocher ce paramètre de vmware :

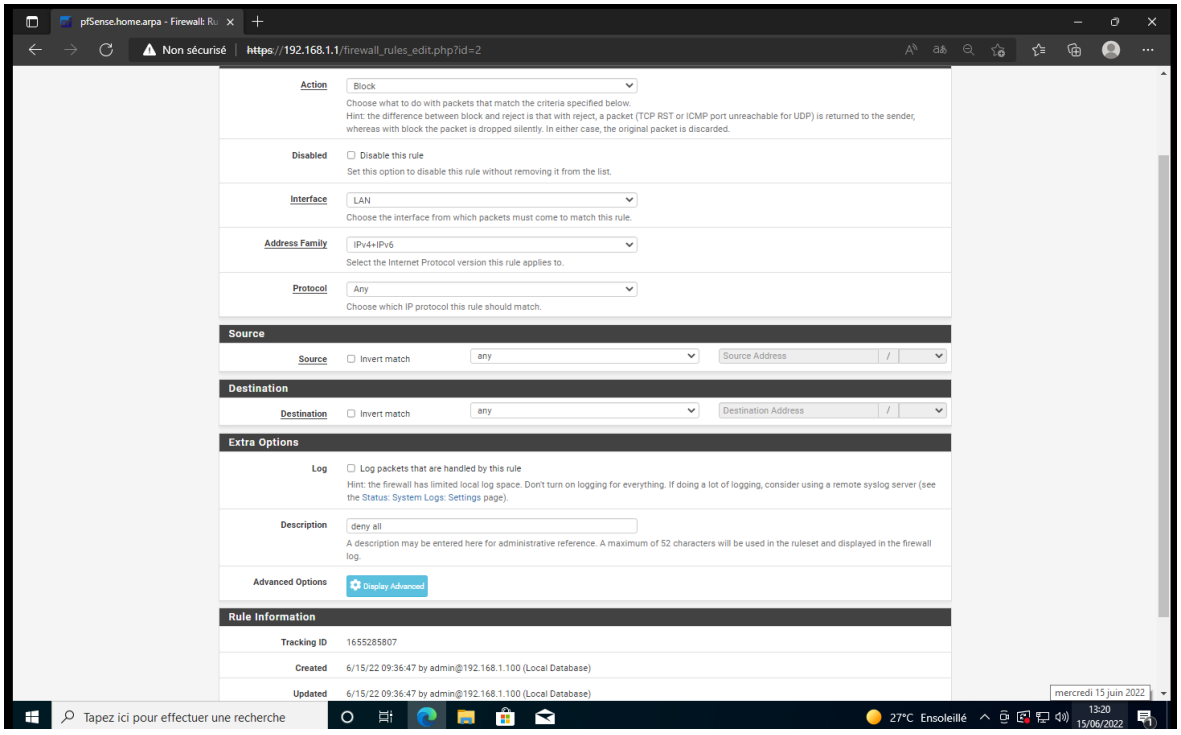


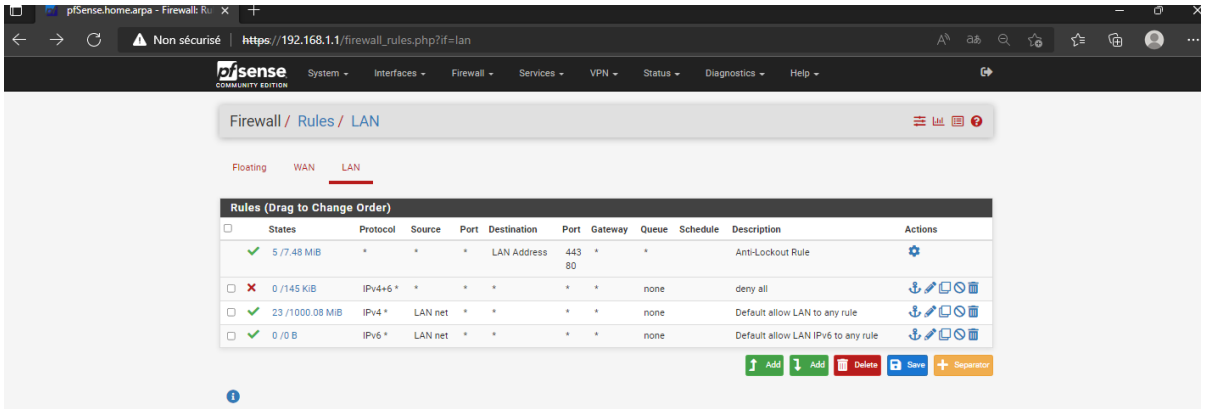
Nous avons maintenant accès à internet et à notre firewall comme le montre l'image ci-dessous :



II. Deny all:

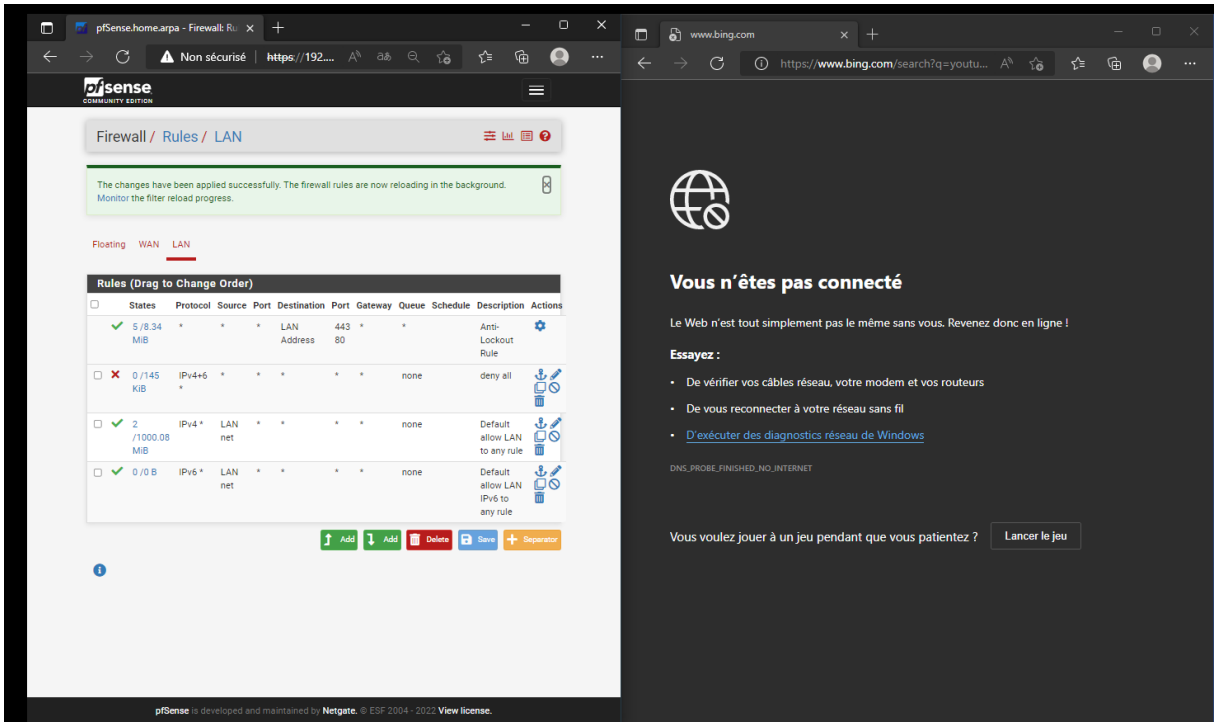
Pour cette règle-là, nous allons configuré les paramètre de manière a ce que rien ne passe, aucune connexion. Ce qui devrais par la même occasion coupé l'accès a internet de la vm windows vu précédemment :





Nous pouvons donc voir maintenant si nous mettons notre nouvelle règles de blocage en vigueur et en avant par rapport au autres que cela bloque correctement.

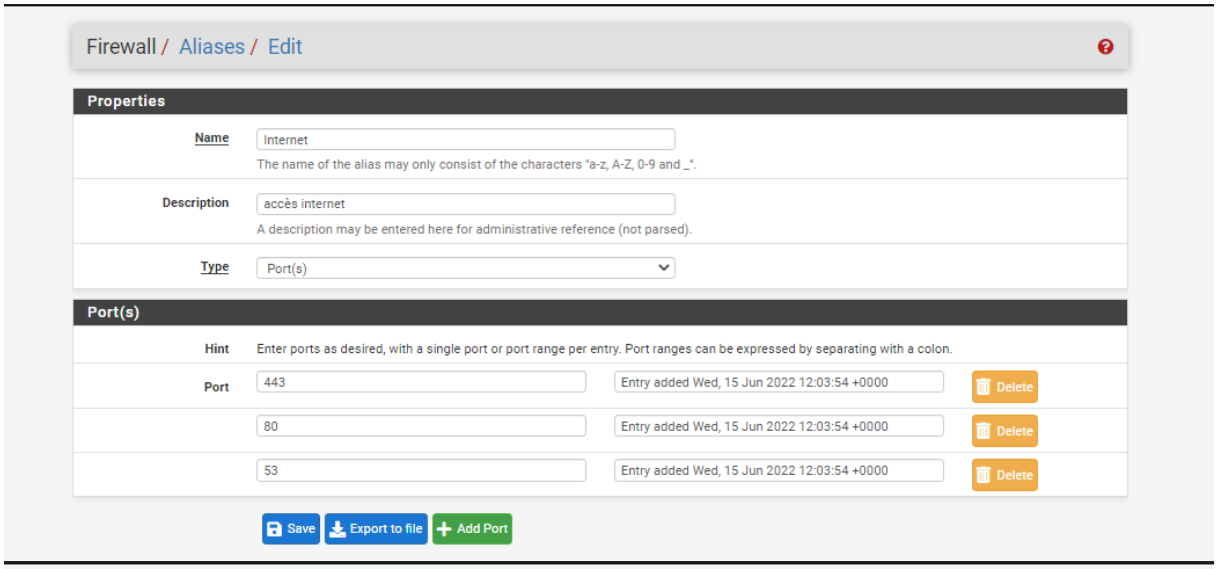
Comme montrer ci-dessous, après application des modifications des règles nous n'avons en effet plus accès à internet.

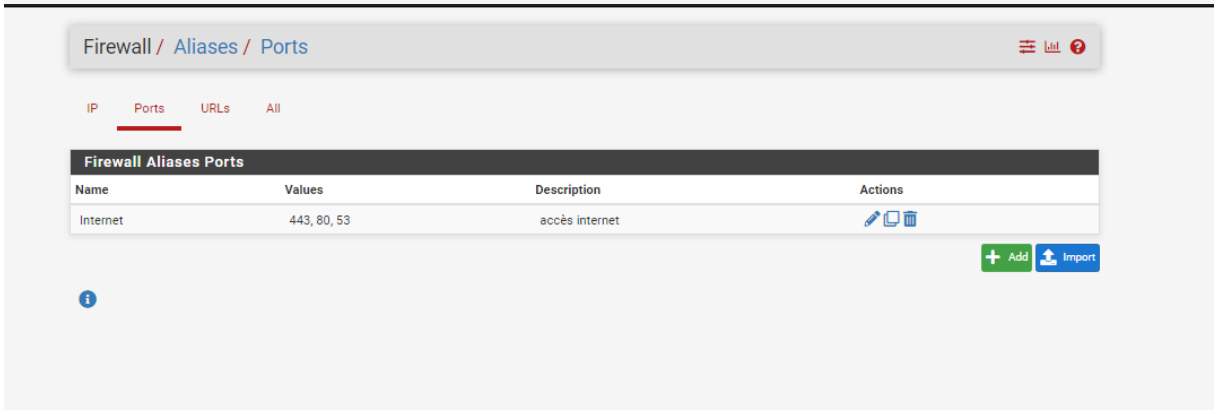


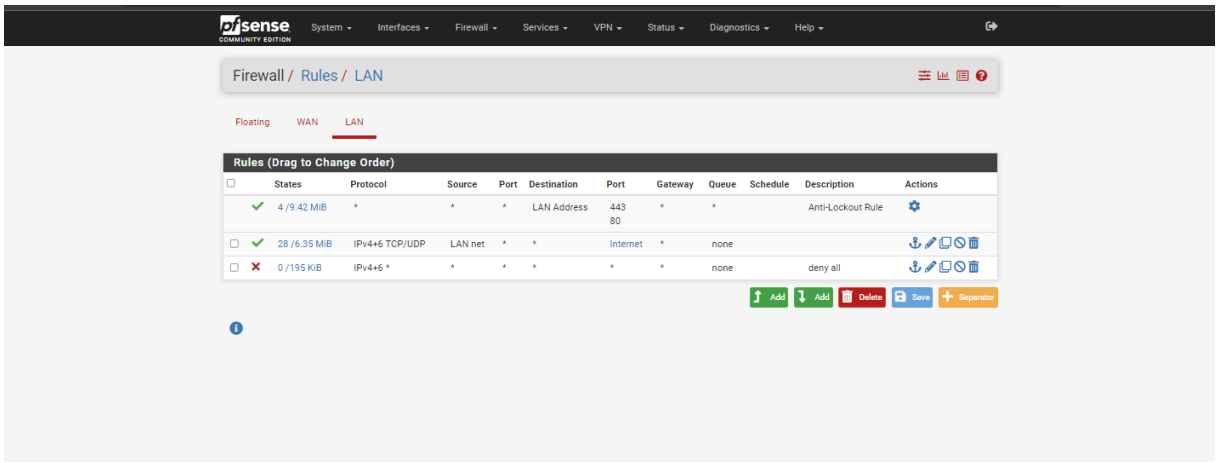
III. Règle internet :

Pour compléter la règle précédente qui bloque tout les connexions, nous allons autoriser l'accès à internet uniquement avec une autre règles.

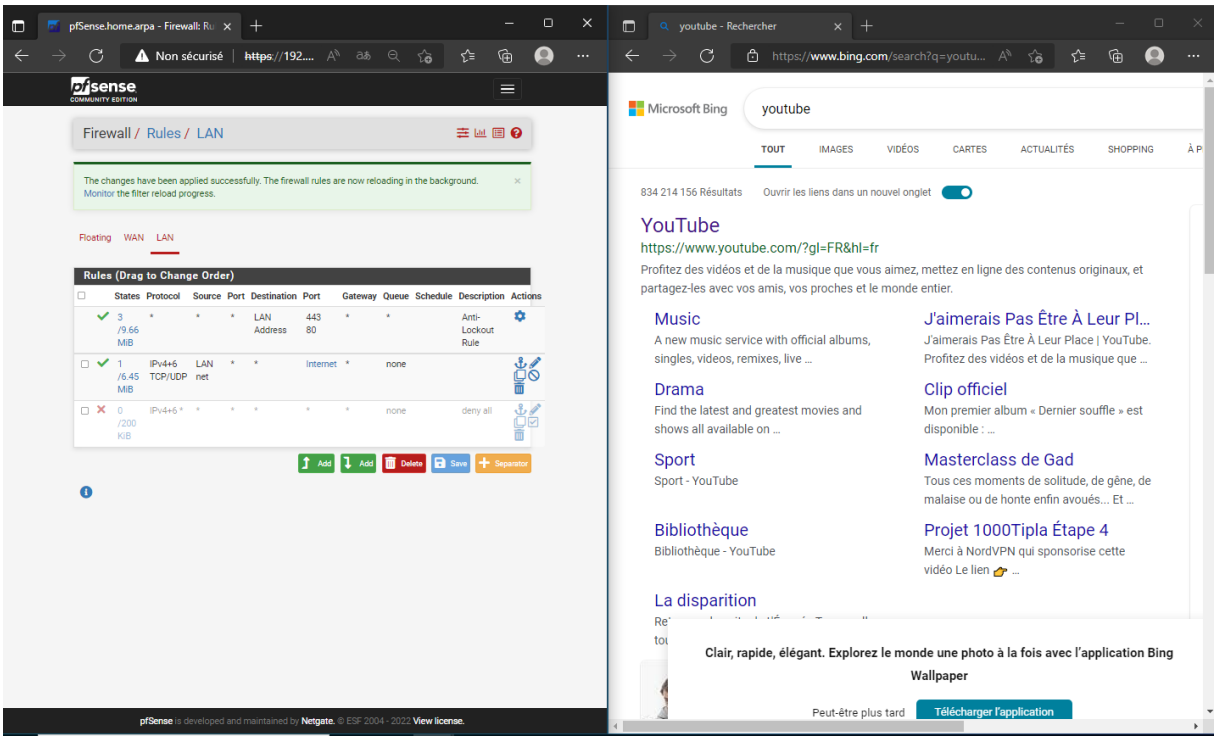
Pour commencer il faut crée un Aliases qui va comprendre les ports que l'on autorise :







Nous avons donc maintenant de nouveau accès à internet tout en ayant bloquer les connexions indésirables



IV. Captive portail :

Dans un premier temps nous devons activer le portail captive en remplissant les paramètres sur les image ci-contre :

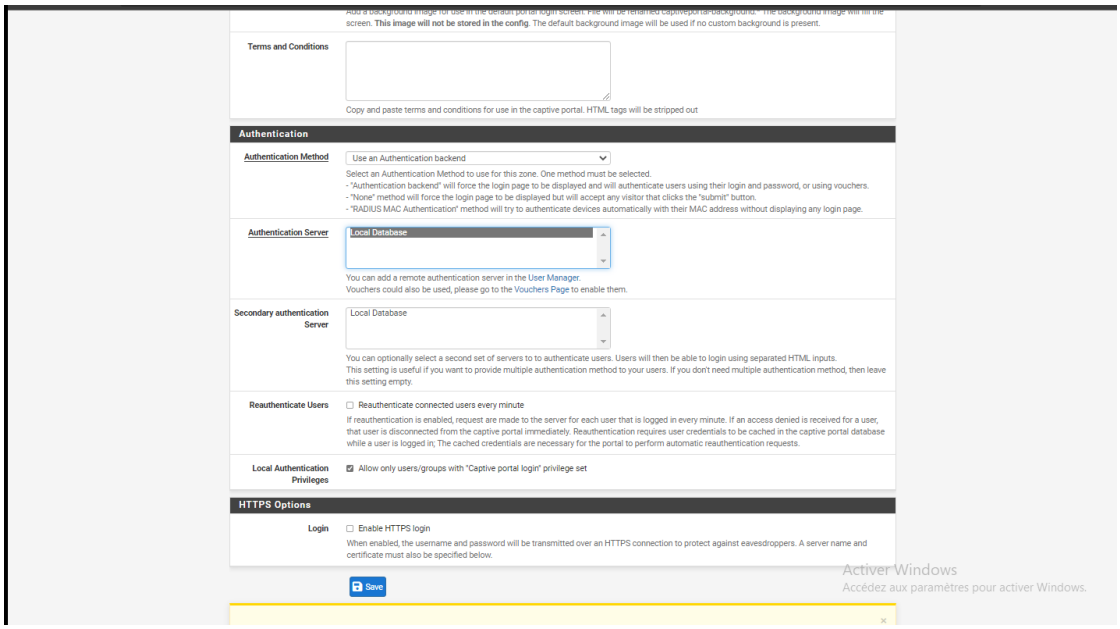
Captive Portal Configuration

Enable	☑ Enable Captive Portal
Description	portail captif A description may be entered here for administrative reference (not parsed).
Interfaces	WAN LAN Select the interface(s) to enable for captive portal.
Maximum concurrent connections	1 Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.
Idle timeout (Minutes)	5 Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.
Hard timeout (Minutes)	Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).
Traffic quota (Megabytes)	Clients will be disconnected after exceeding this amount of traffic, inclusive of both downloads and uploads. They may log in again immediately, though. Leave this field blank for no traffic quota.
Pass-through credits per MAC address.	Allows passing through the captive portal without authentication a limited number of times per MAC address. Once used up, the client can only log in with valid credentials until the waiting period specified below has expired. Recommended to set a hard timeout and/or idle timeout when using this for it to be effective.
Waiting period to restore pass-through credits. (Hours)	Clients will have their available pass-through credits restored to the original count after this amount of time since using the first one. This must be above 0 hours if pass-through credits are enabled.
Reset waiting period	☐ Enable waiting period reset on attempted access If enabled, the waiting period is reset to the original duration if access is attempted when all pass-through credits have already been exhausted.
Logout popup window	☑ Enable logout popup window If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.
Pre-authentication	

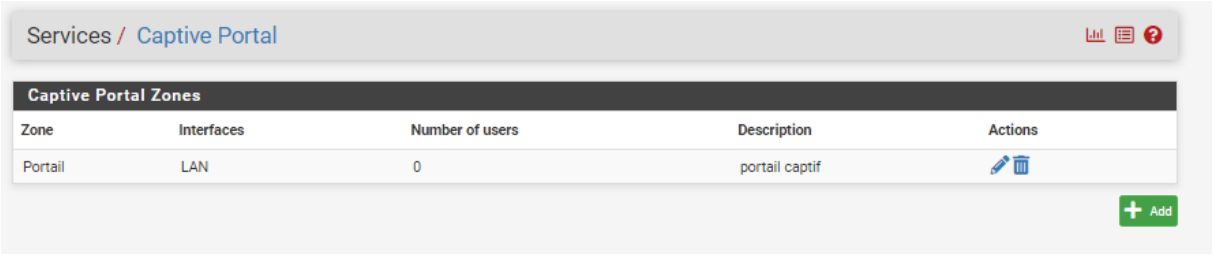
pass-through credits. (Hours)	Clients will have their available pass-through credits restored to the original count after this amount of time since using the first one. This must be above 0 hours if pass-through credits are enabled.
Reset waiting period	☐ Enable waiting period reset on attempted access If enabled, the waiting period is reset to the original duration if access is attempted when all pass-through credits have already been exhausted.
Logout popup window	☑ Enable logout popup window If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.

Pre-authentication redirect URL	http://google.fr/ Set a default redirection URL. Visitors will be redirected to this URL after authentication only if the captive portal doesn't know where to redirect them. This field will be accessible through $PORTAL_REDIRURL$ variable in captiveportal's HTML pages.
After authentication Redirection URL	http://google.fr Set a forced redirection URL. Clients will be redirected to this URL instead of the one they initially tried to access after they've authenticated.
Blocked MAC address redirect URL	Blocked MAC addresses will be redirected to this URL when attempting access.
Preserve users database	☑ Preserve connected users across reboot If enabled, connected users won't be disconnected during a pfSense reboot.
Concurrent user logins	Multiple Disabled: Do not allow concurrent logins per username or voucher. Multiple: No restrictions to the number of logins per username or voucher will be applied. Last login: Only the most recent login per username or voucher will be granted. Previous logins will be disconnected. First login: Only the first login per username or voucher will be granted. Further login attempts using the username or voucher will not be possible while an initial user is already active.
MAC filtering	☑ Disable MAC filtering If enabled no attempts will be made to ensure that the MAC address of clients stays the same while they are logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between pfSense and the clients). If this is enabled, RADIUS MAC authentication cannot be used.
Pass-through MAC Auto Entry	☐ Enable Pass-through MAC automatic additions When enabled, a MAC passthrough entry is automatically added after the user has successfully authenticated. Users of that MAC address will never have to authenticate again. To remove the passthrough MAC entry either log in and remove it manually from the MAC tab or send a POST from another system. If this is enabled, the logout window will not be shown.
Per-user bandwidth restriction	☐ Enable per-user bandwidth restriction
Use custom captive portal page	☐ Enable to use a custom captive portal login page If set a portal.html page must be created and uploaded. If unchecked the default template will be used

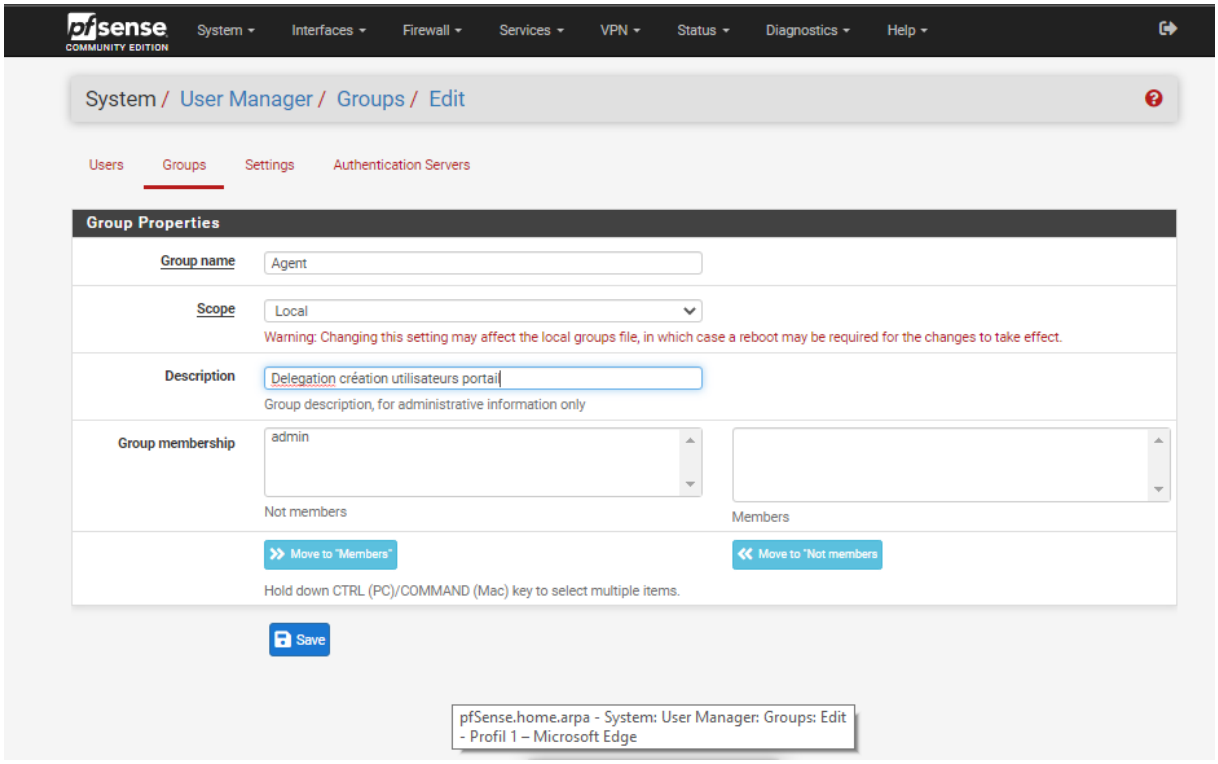
Captive Portal Login Page



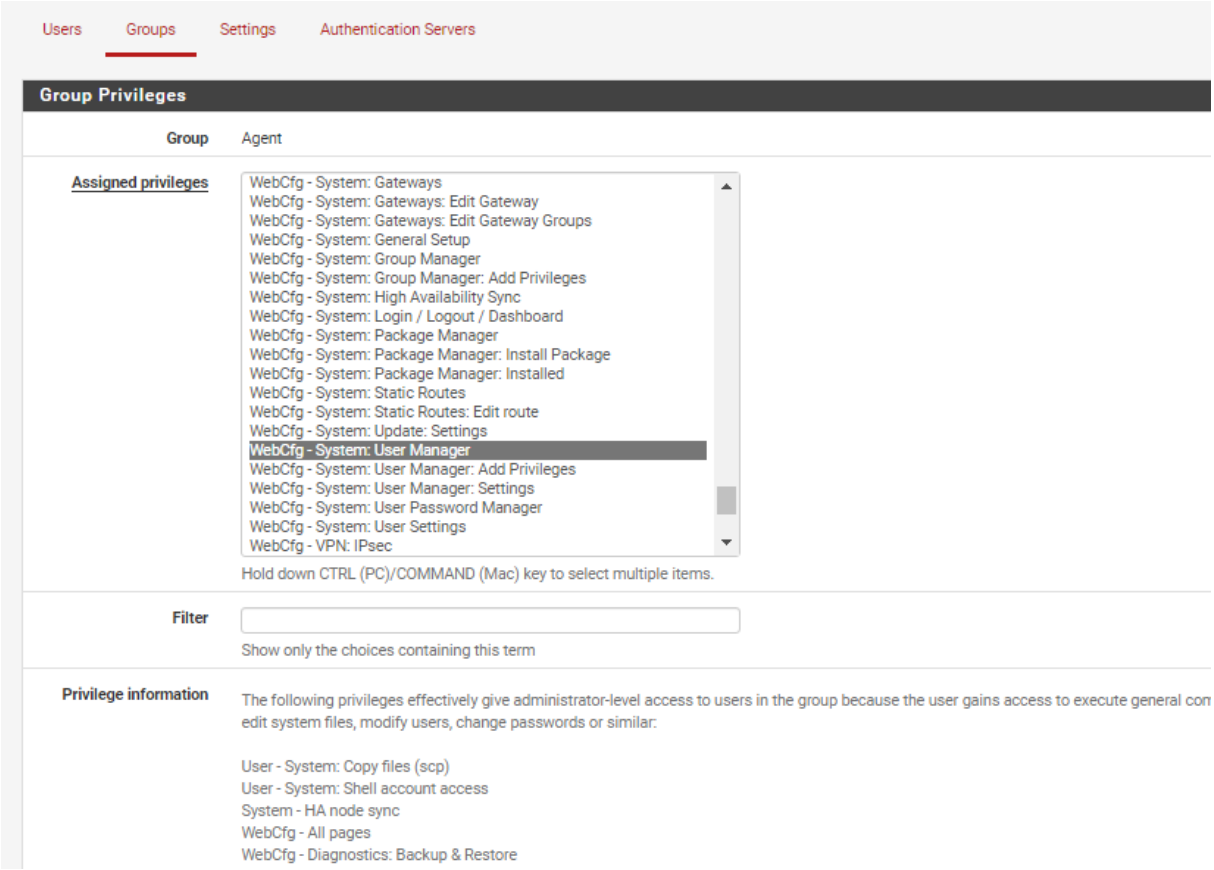
Une fois celui-ci sauvegarder avec le bouton save, vous le retrouverez dans votre liste de captive portail

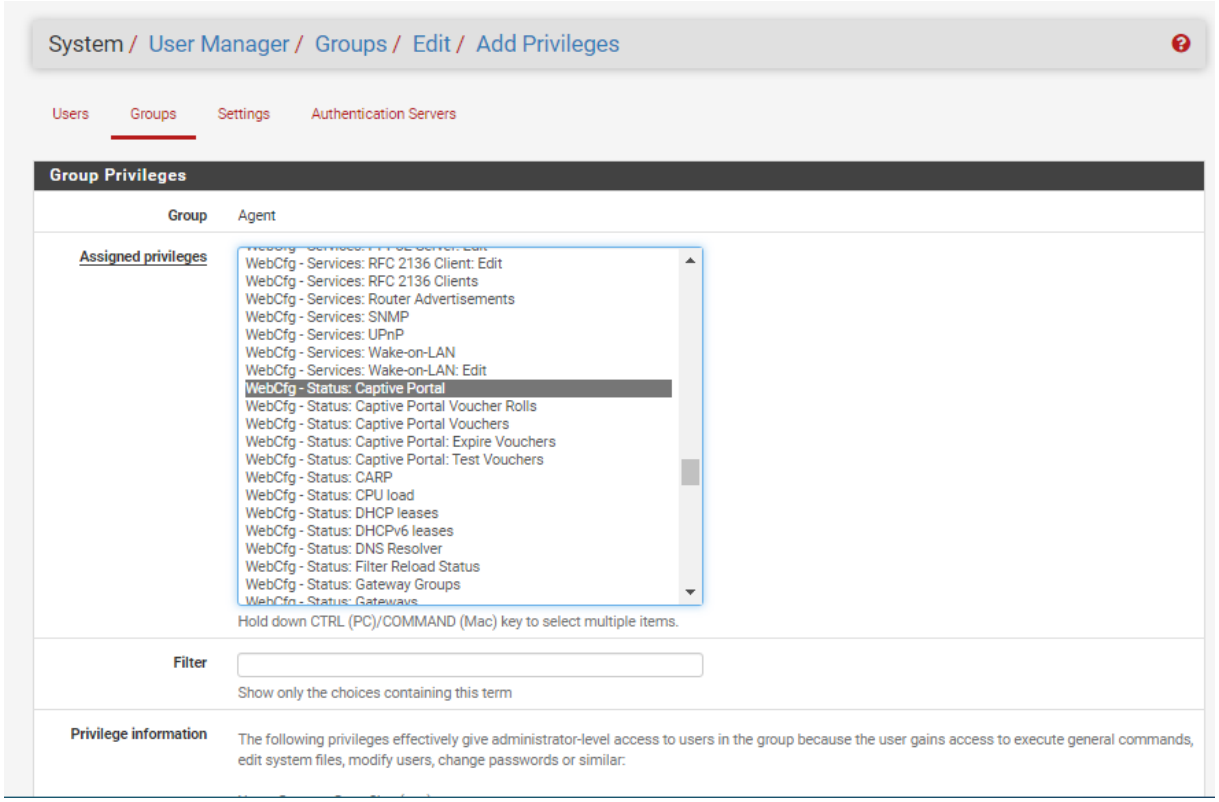


Nous allons maintenant crée notre premier groupe nommé agent

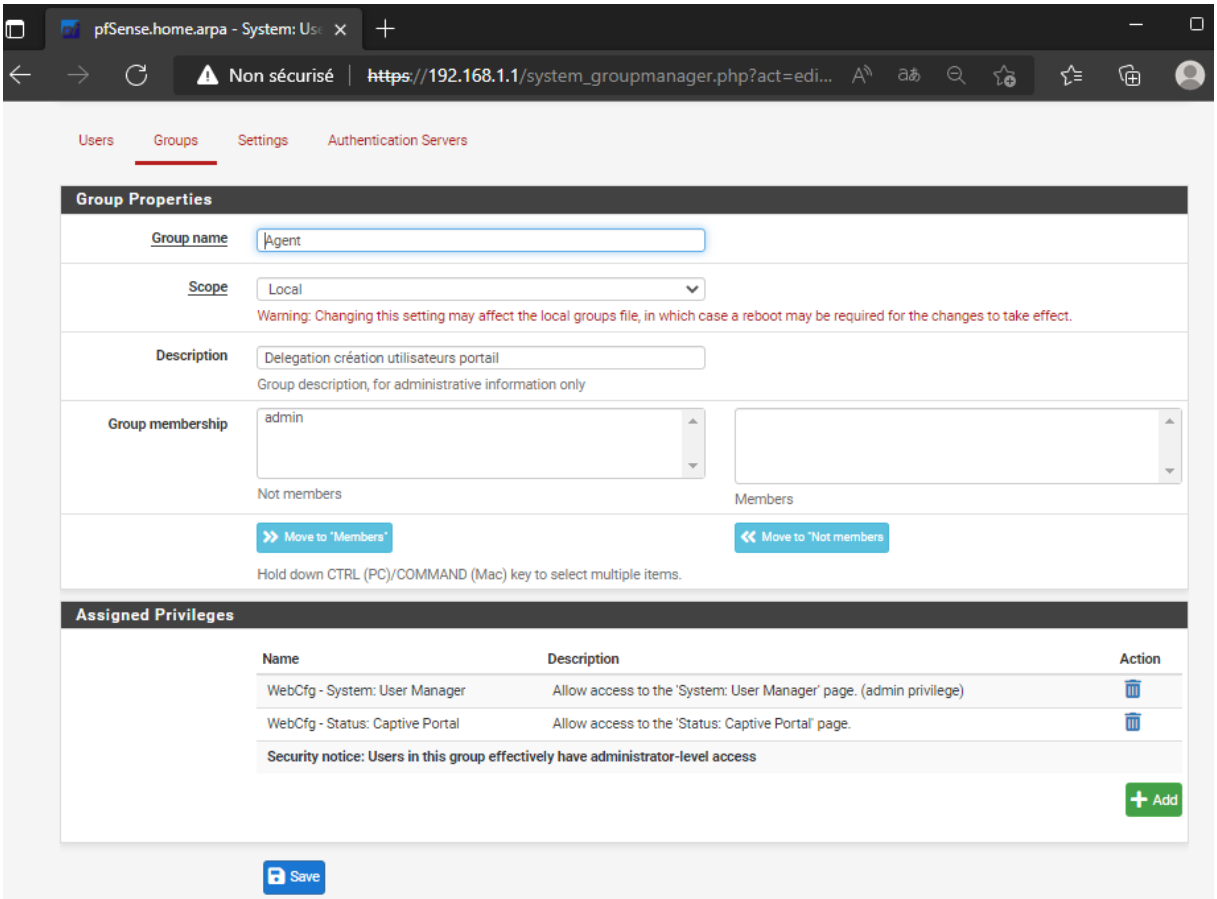


nous lui attribuons les privilèges WebCfg-System : User Manger et WebCfg- statues : captive portalcomme montré en dessous

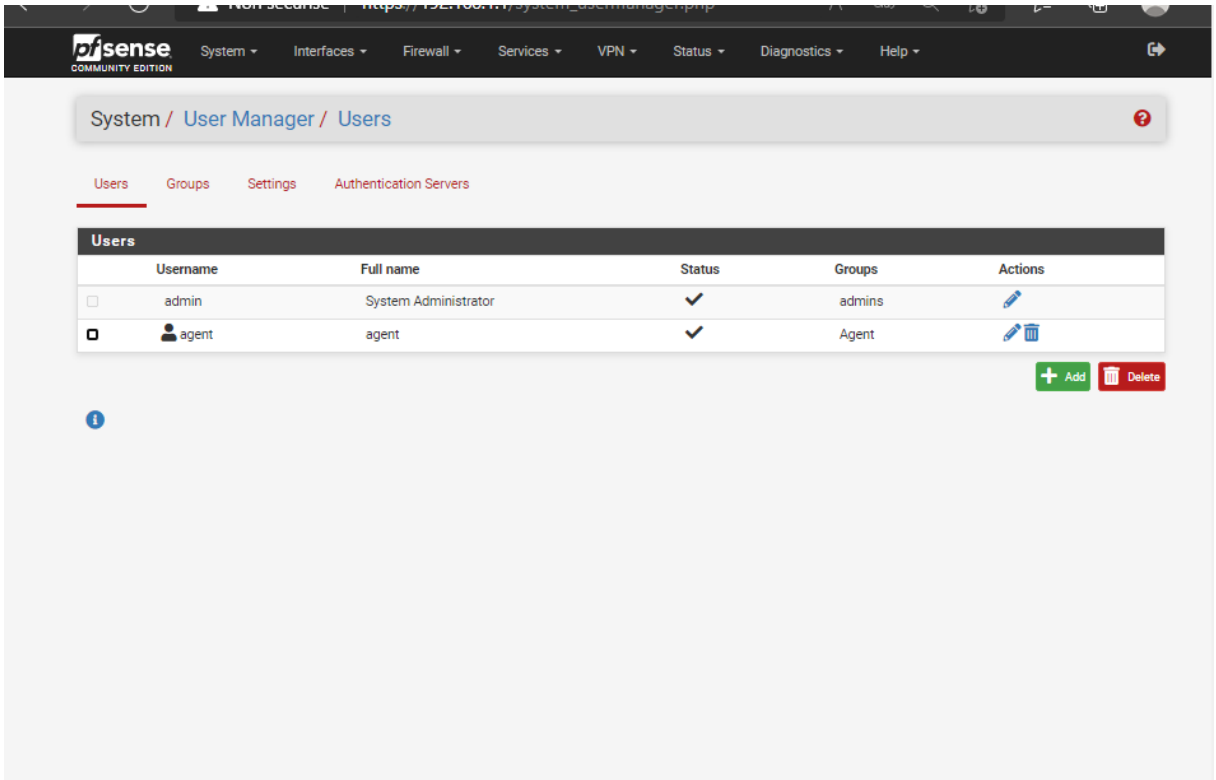




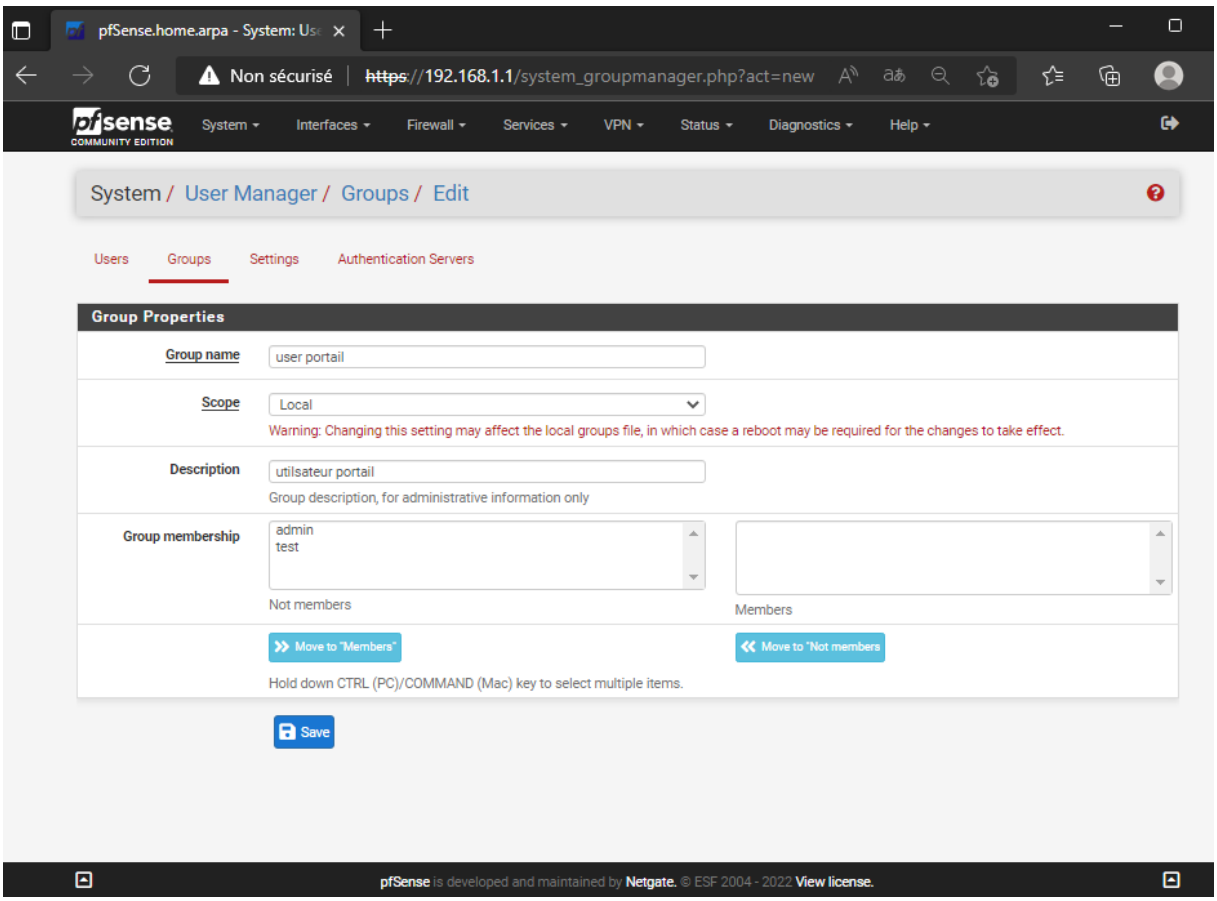
les rôles ont bien été ajouter a notre groupe

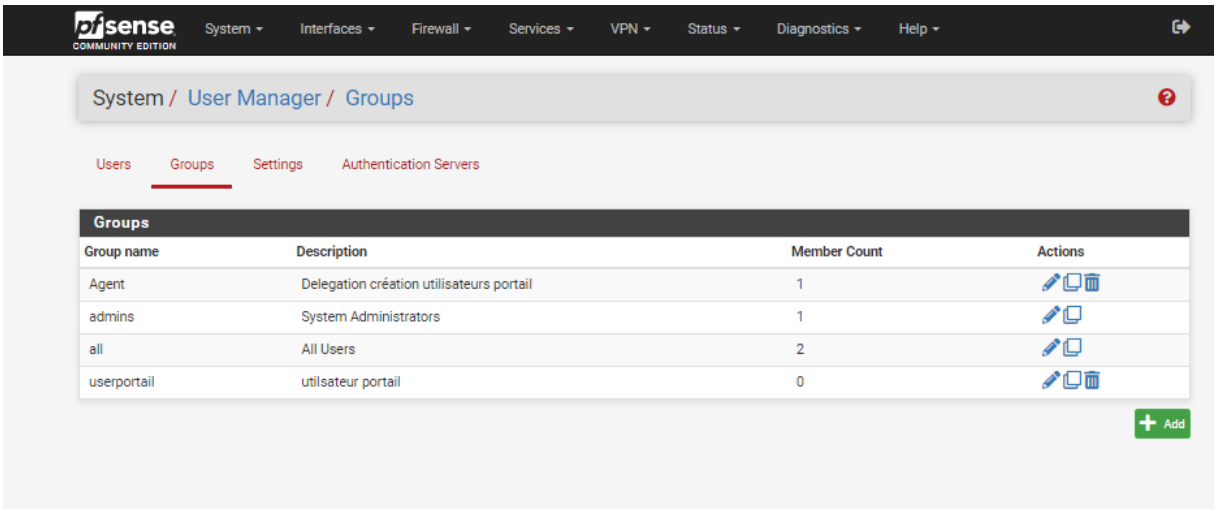


nous créons maintenant un rôles agent et nous l’attribuons au groupe du même nom

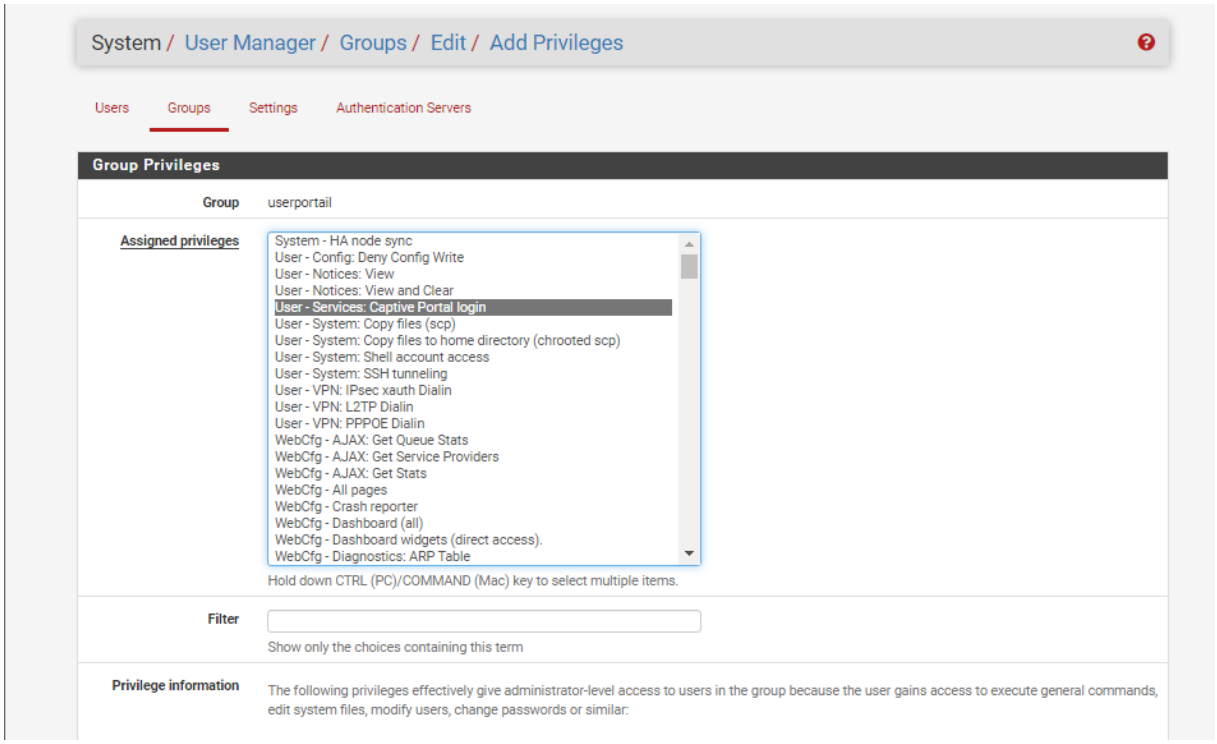


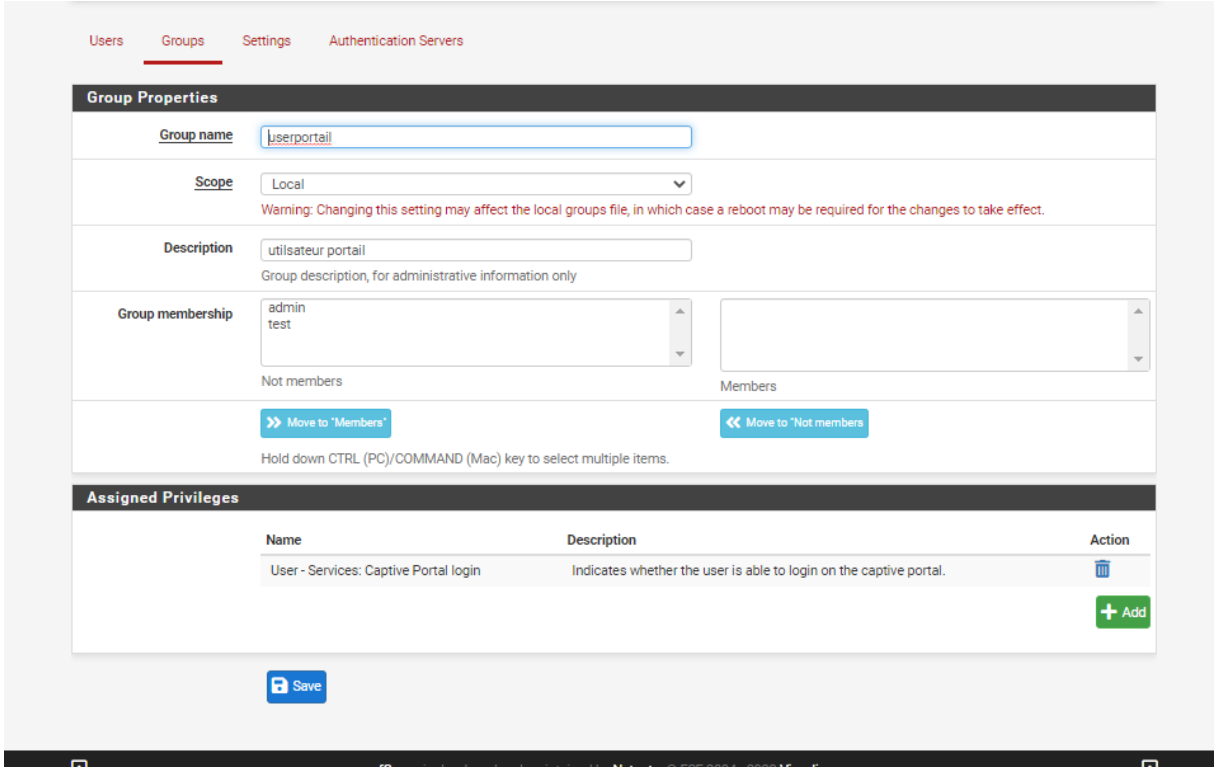
Passons au utilisateur standard, nous créons le groupe userportail



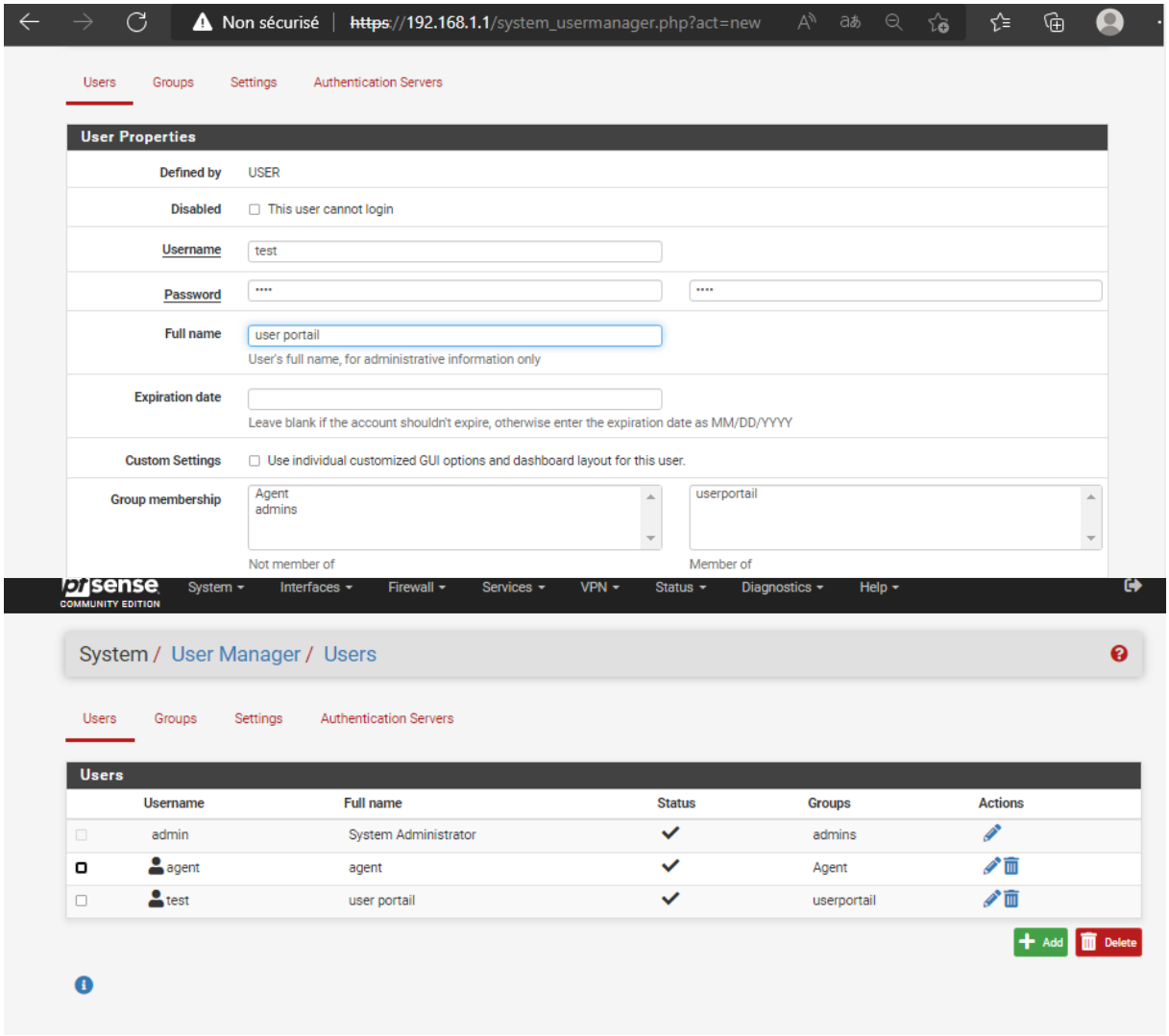


passons au privilège du groupe userportail, nous lui attribuons celle-ci contre :

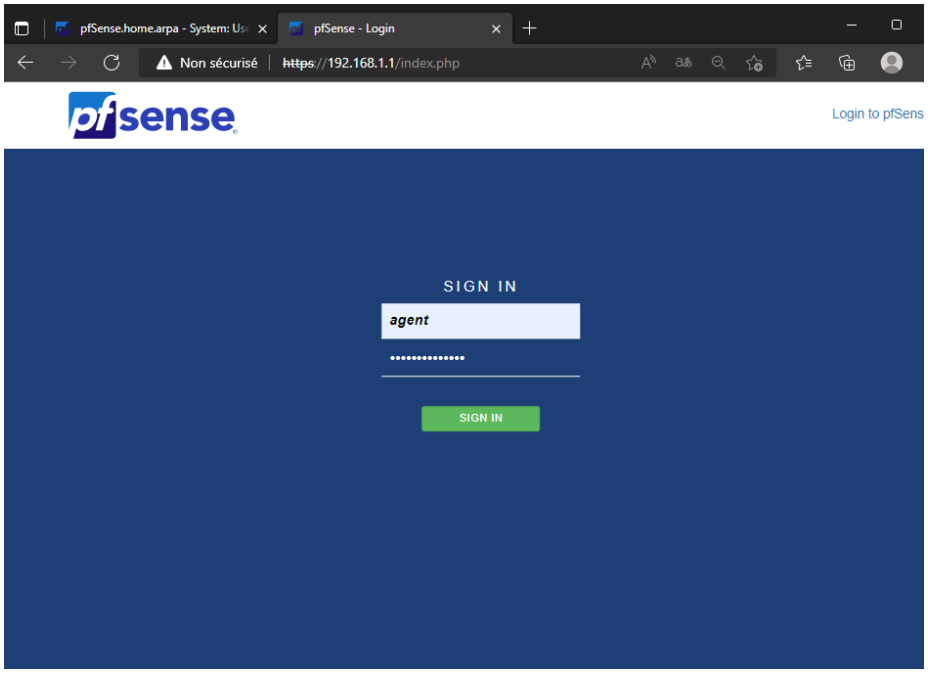




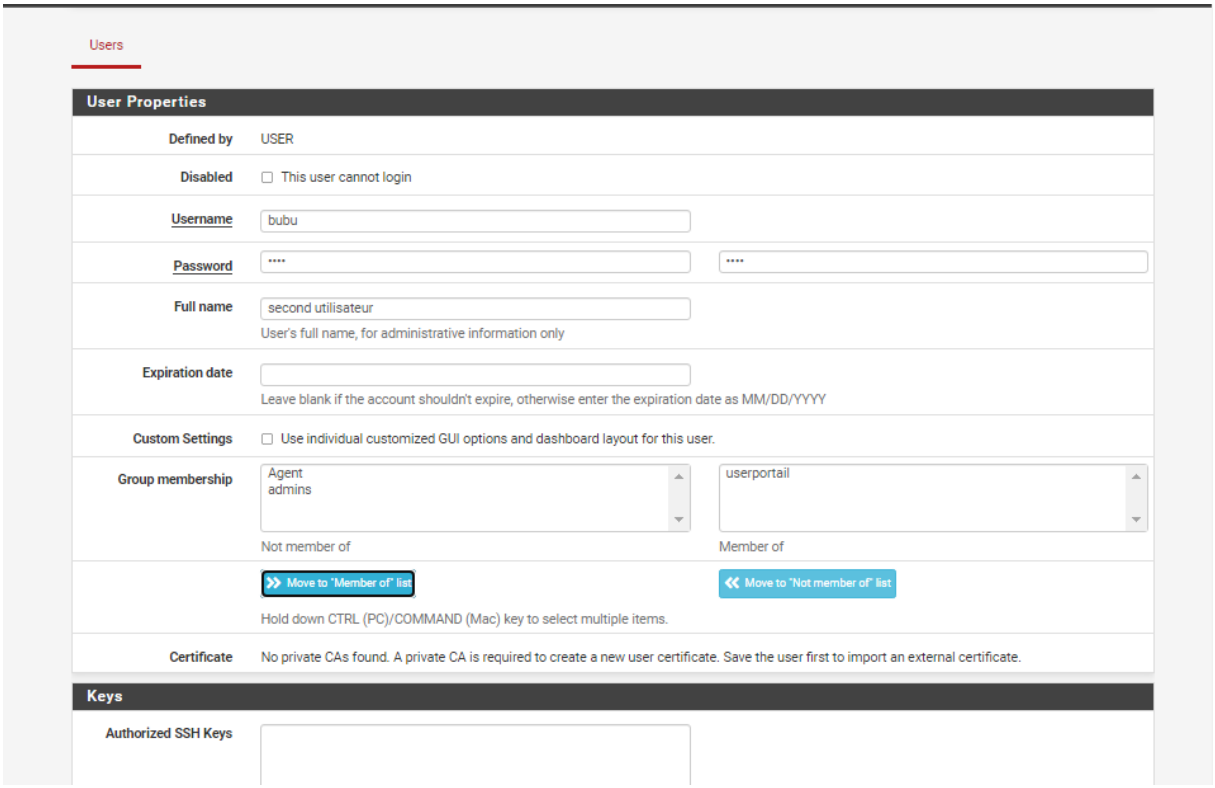
pour faire le test nous allons justement crée un utilisateur test qui va nous servir d'utilisateur lambda

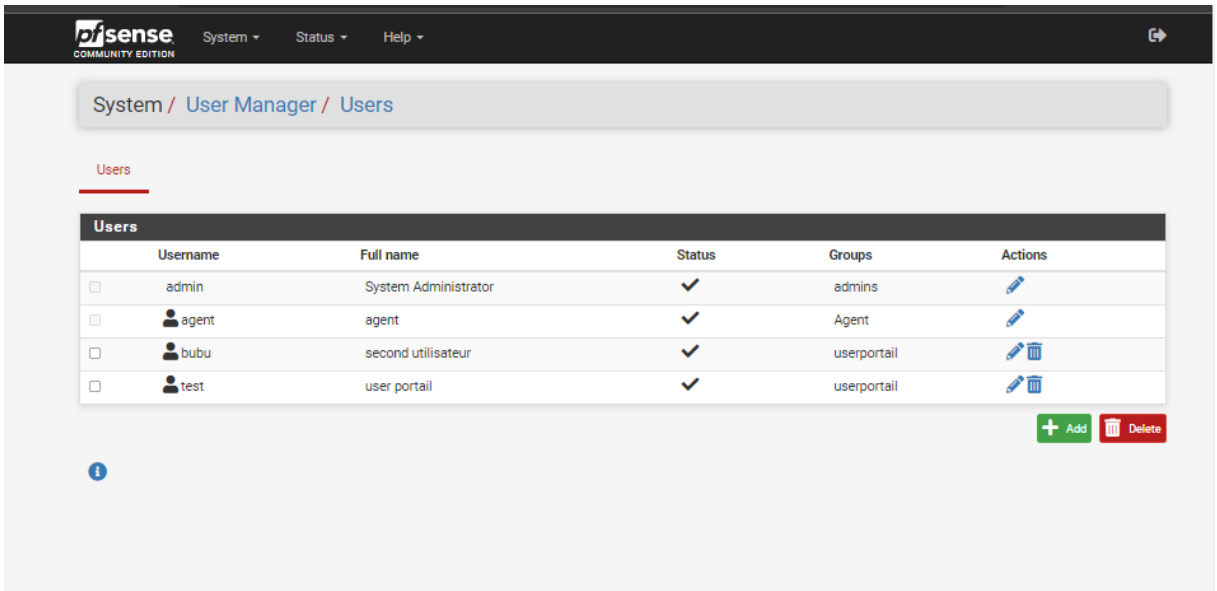


(si besoin nous pouvons maintenant nous connecter avec le compte agent pour faire la gestion des utilisateur inférieur comme l'utilisateur test



Nous allons encore crée un deuxième utilisateurs (pour finir la doc)




pfsense
COMMUNITY EDITION
System
Status
Help
System / User Manager / Users
Users
Users
Username
Full name
Status
Groups
Actions
admin
System Administrator
admins
agent
agent
Agent
bubu
second utilisateur
userportail
test
user portail
userportail
Add
Delete