Mise en place d'un PfSense

Fait en entreprise et dans le cadre de l'épreuve E4 du BTS SIO 2022-2024

Télécharger en PDF

Sommaire

Pour Commencer

Mon entreprise, KNCO, a pris la décision de passer du routeur de notre FAI à un routeur PfSense, afin de pouvoir mieux gérer la sécurisation du réseau et débrider la vitesse de connexion dans les locaux, bridée par la maigre puissance du routeur original, causant des problèmes lors d'interventions à distance mais aussi lors de connexions sur notre serveur SAP, se faisant en Remote Desktop (RDP)
Il a également été demandé de gérer le réseau interne et le réseau du WiFi invité séparément, pour cela nous créeront deux VLAN, un interne et un pour le WiFi invité
Le besoin principal est donc de pouvoir gérer la sécurisation du réseau et de se débarrasser de l'équipement de base de notre fournisseur internet

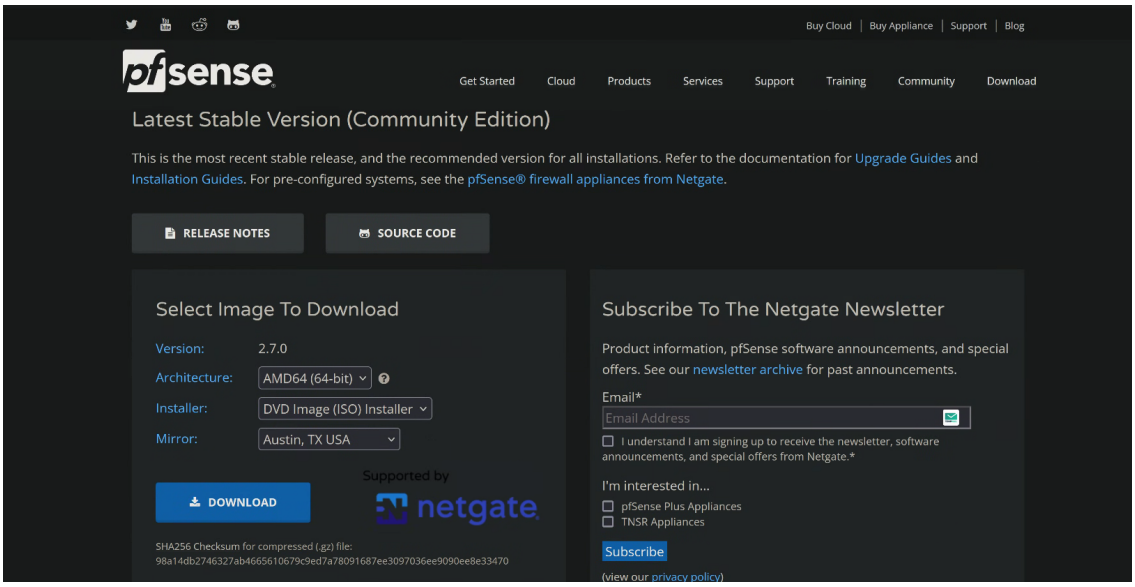
Prérequis

- Rufus, Balena Etcher ou tout autre logiciel du genre
- Clé/Stockage USB de 4Go minimum
- ISO de PfSense
- Un serveur 2 coeurs et 2Go minimum **avec ici, trois cartes réseaux ou plus**

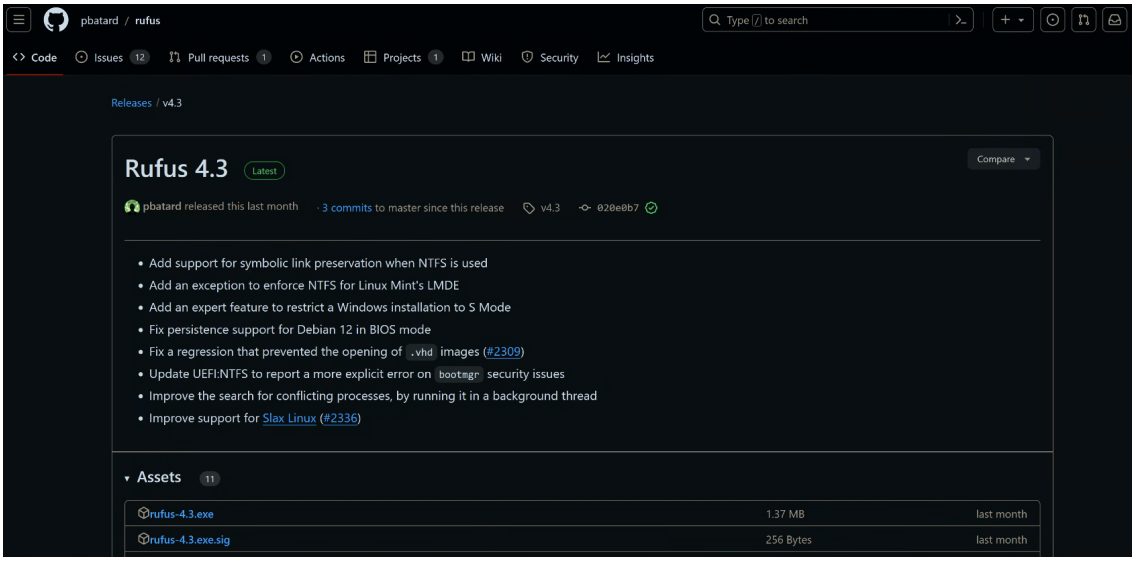
Installation

Formatage de la clé USB

1. Téléchargez l'ISO de PfSense (ici 2.7.0, AMD64, DVD Image)

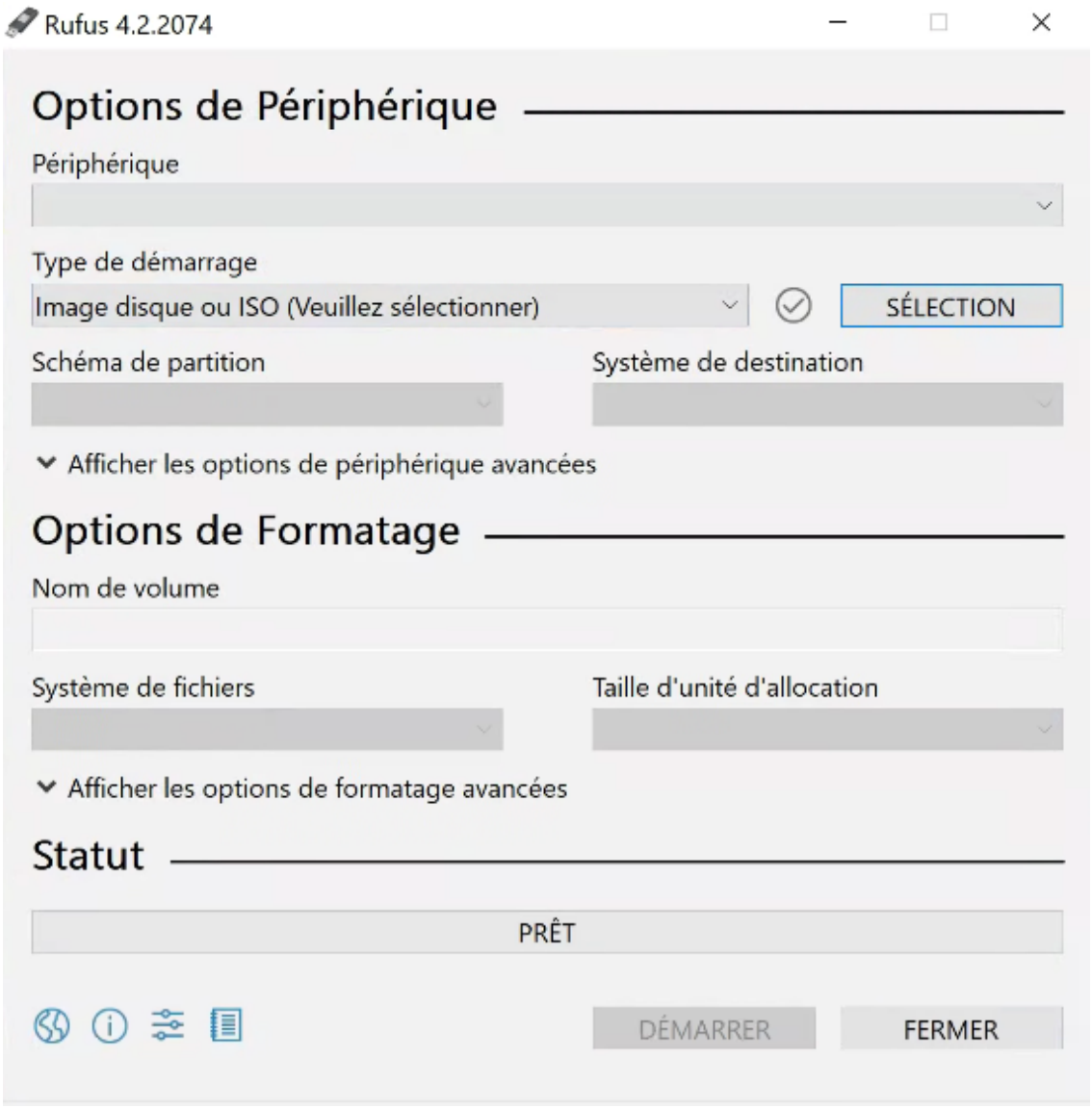


2. Téléchargez Rufus

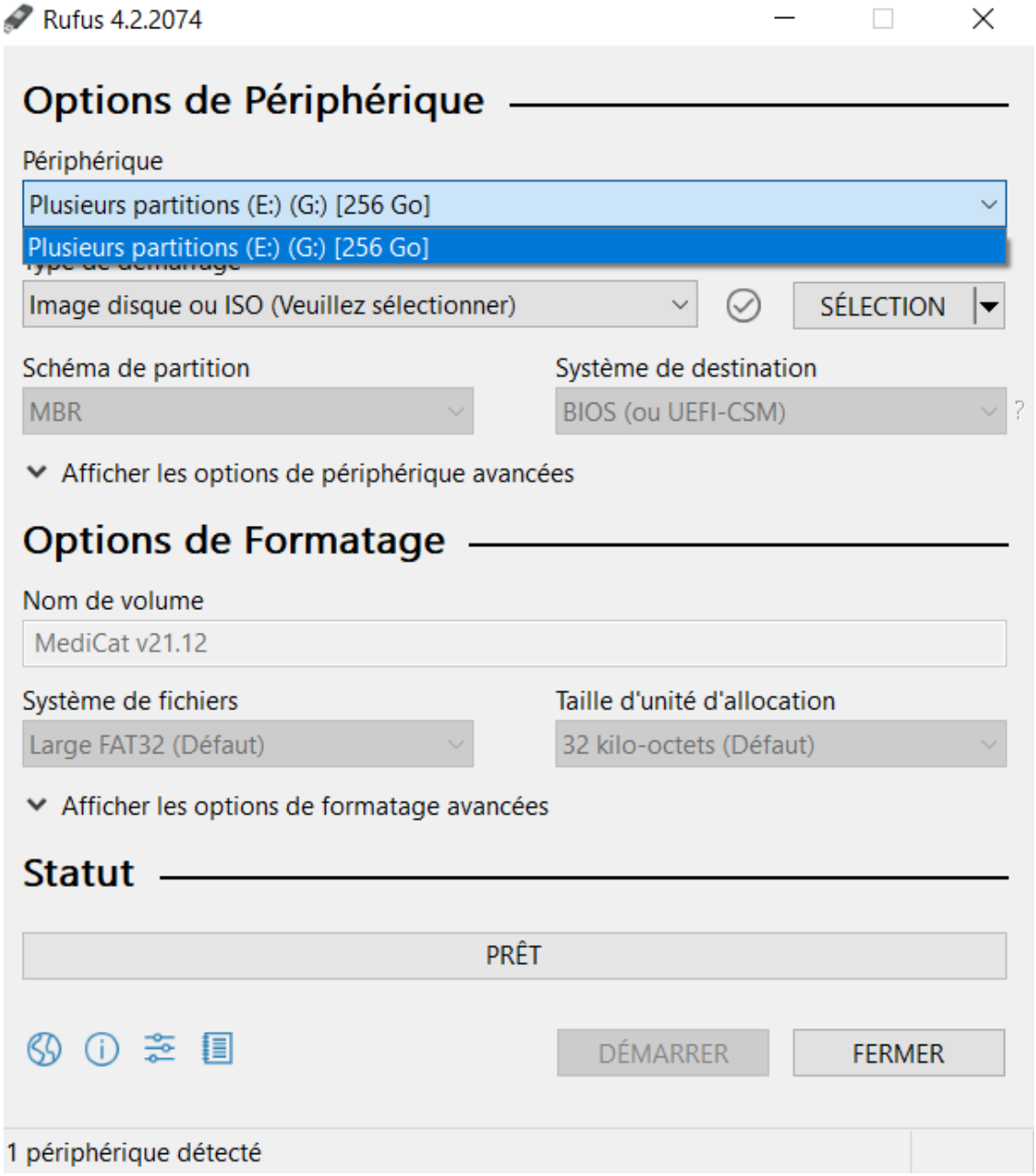


3. Branchez la clé USB sur le PC

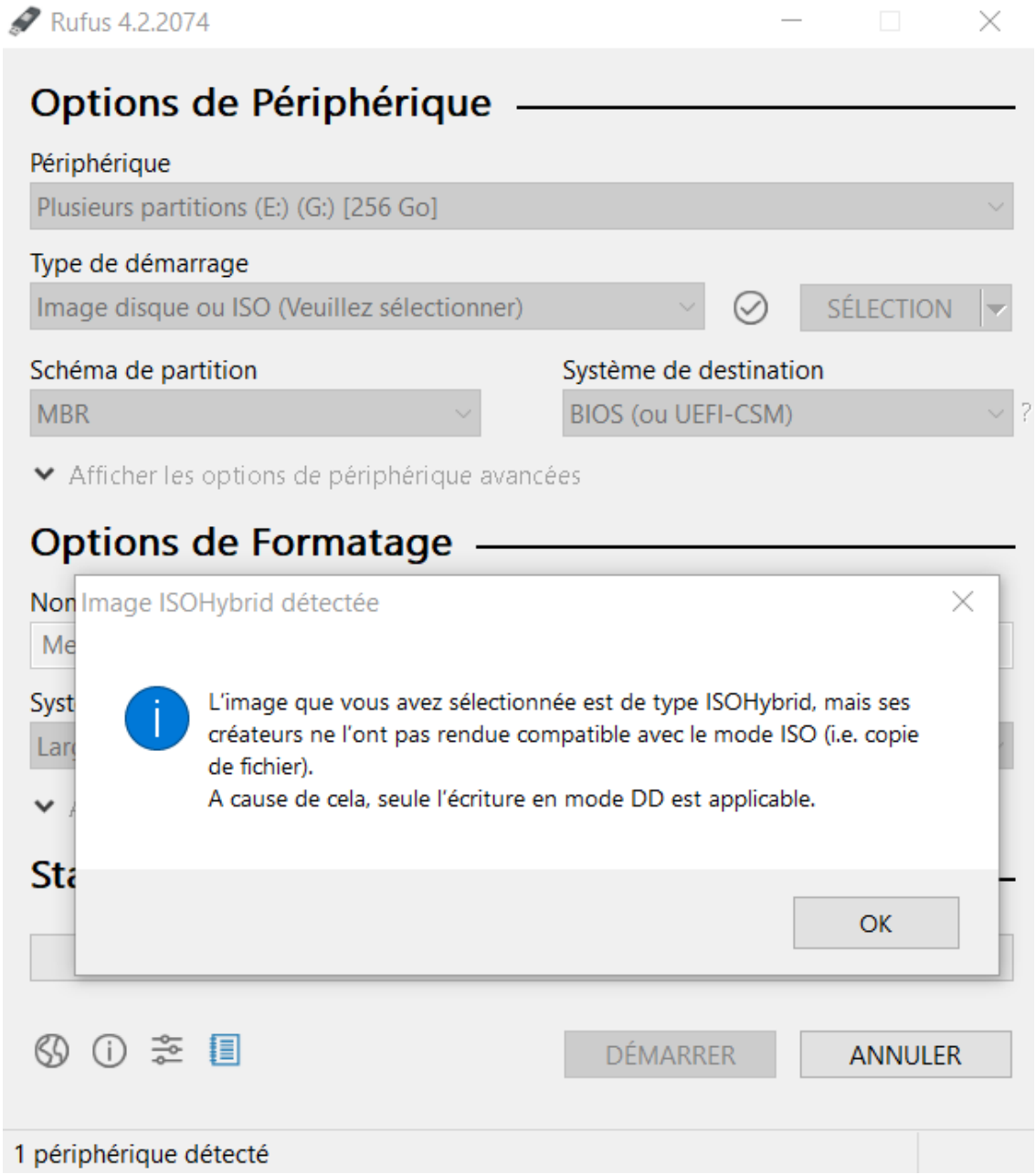
4. Ouvrir Rufus

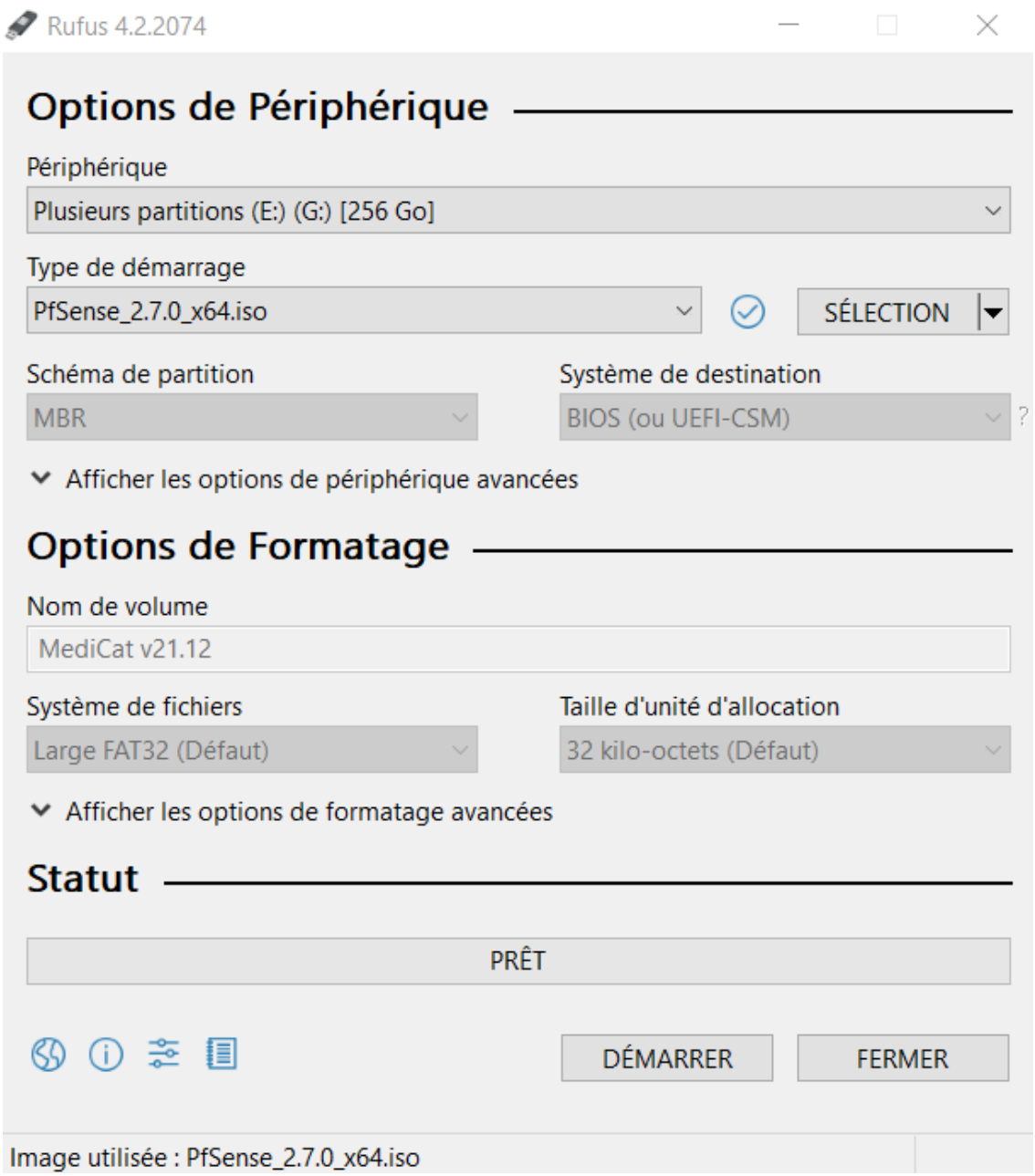


5. Sélectionnez la clé USB



6. Sélectionnez l'ISO de PfSense, continuez si vous avez une erreur "ISOHybrid"



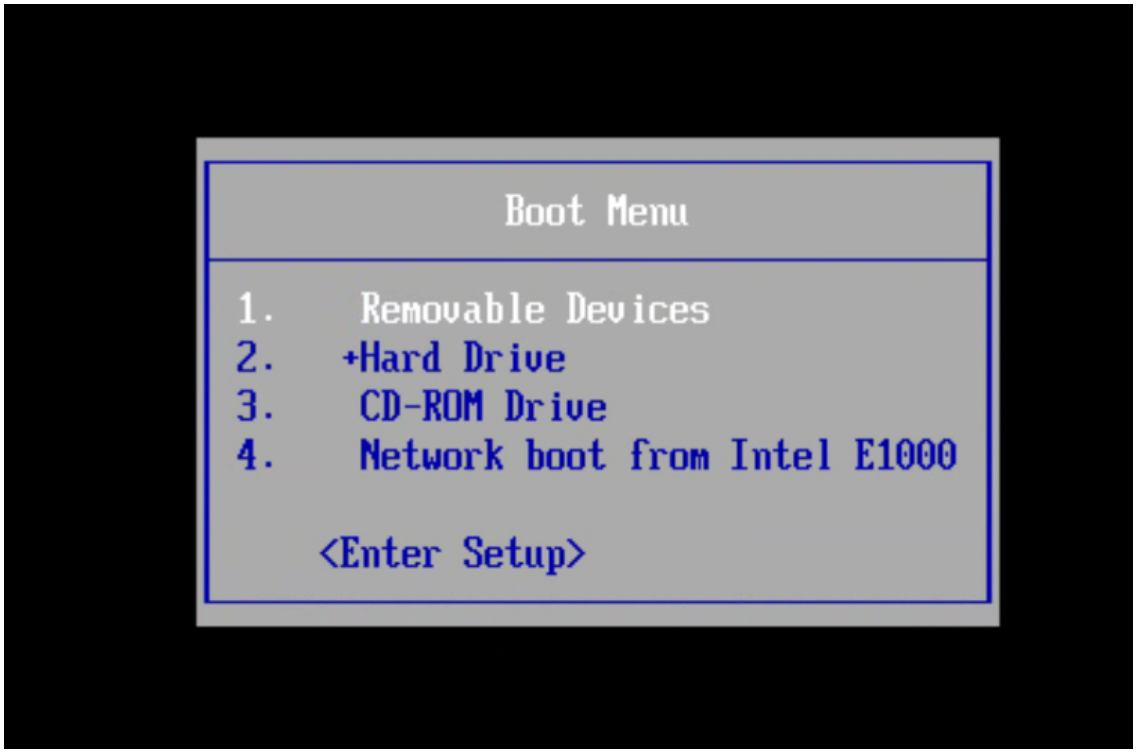


7. Lancez le formatage

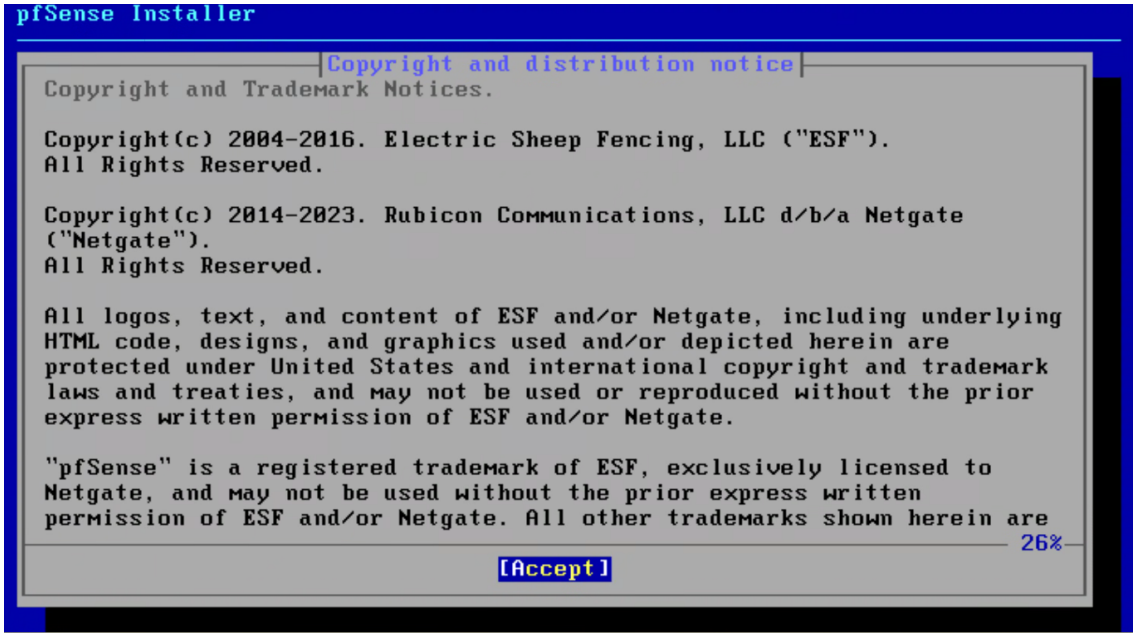
Système

1. Branchez la clé USB sur le serveur
2. Démarrez le serveur
3. Appuyez sur F11 pour accéder au boot menu

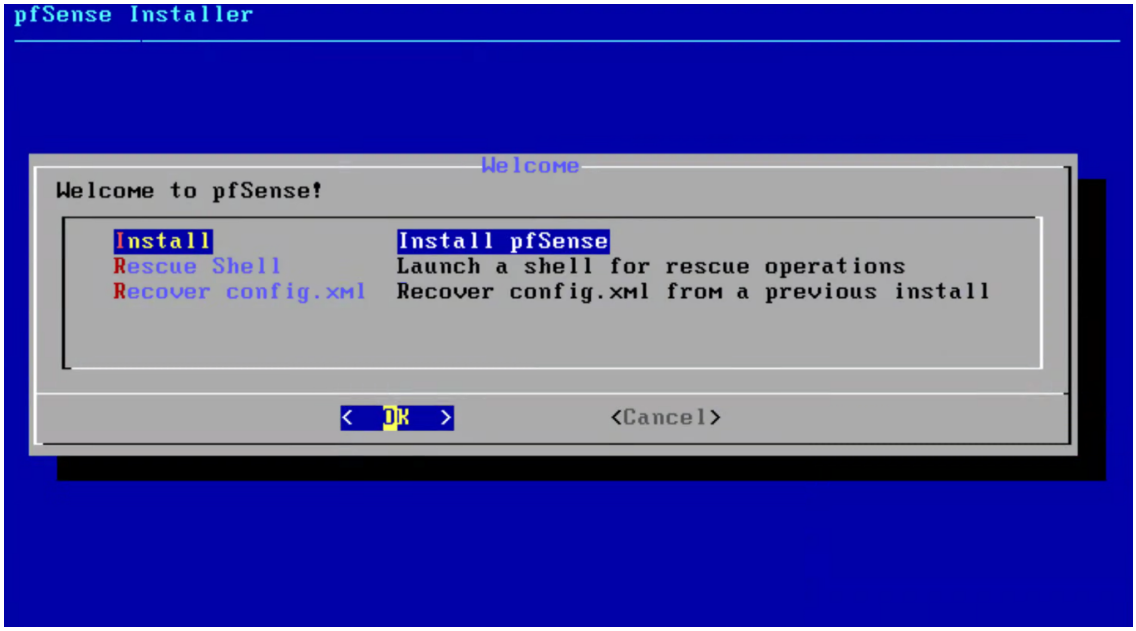
4. Sélectionnez la clé USB



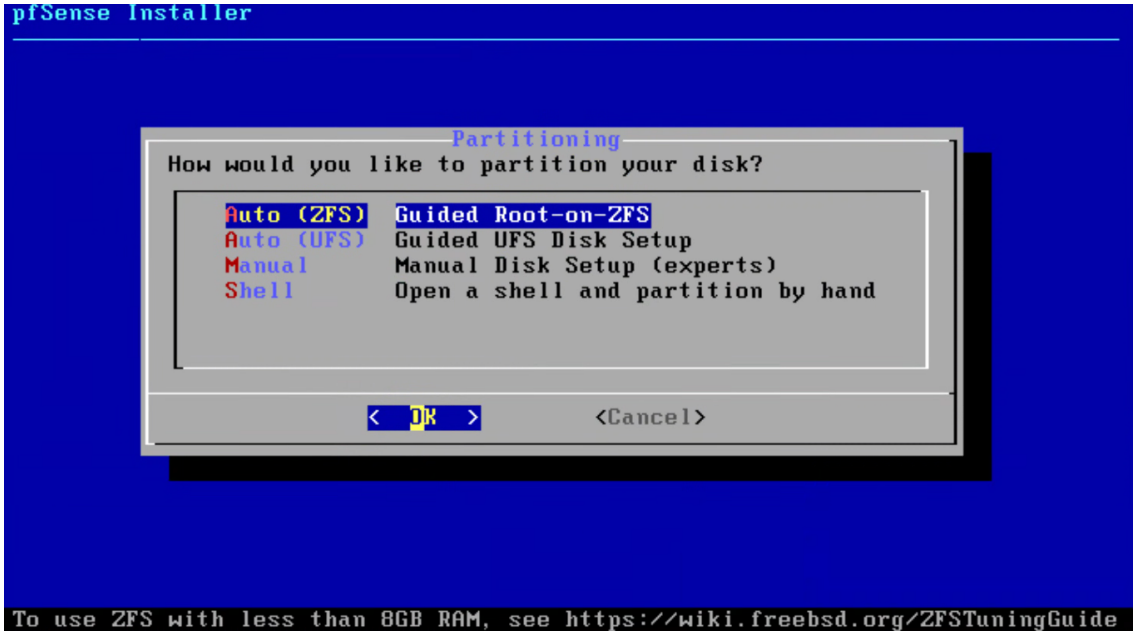
5. Faites entrer pour démarrer l'installation



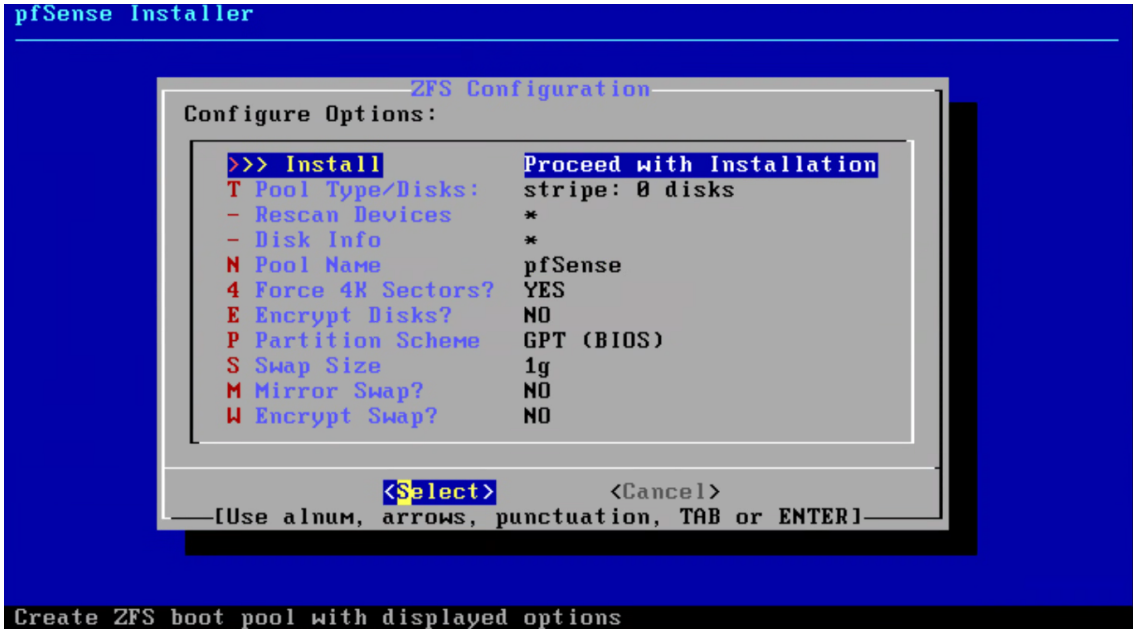
6. Sélectionnez "Install"



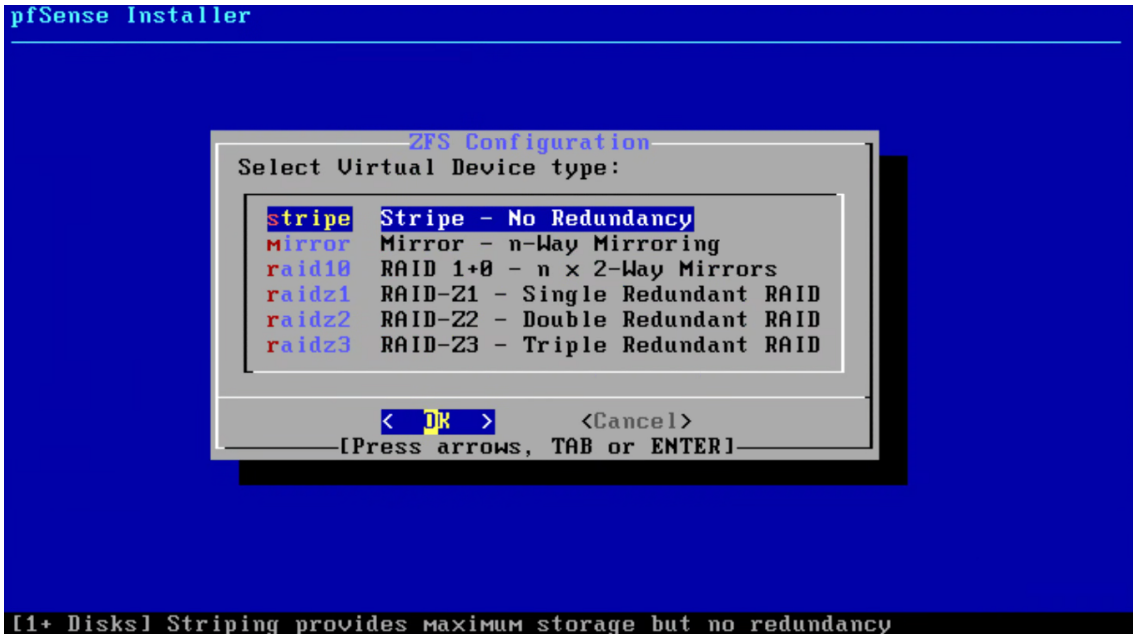
7. Sélectionnez le clavier "Auto (ZFS)"



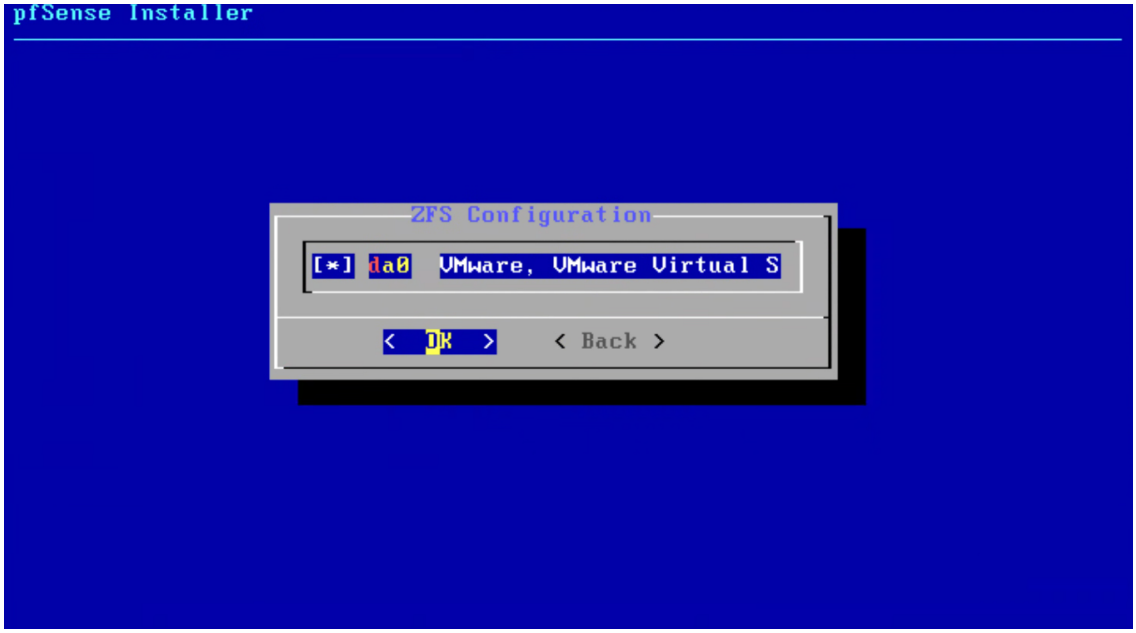
8. Faites entrer pour valider la configuration



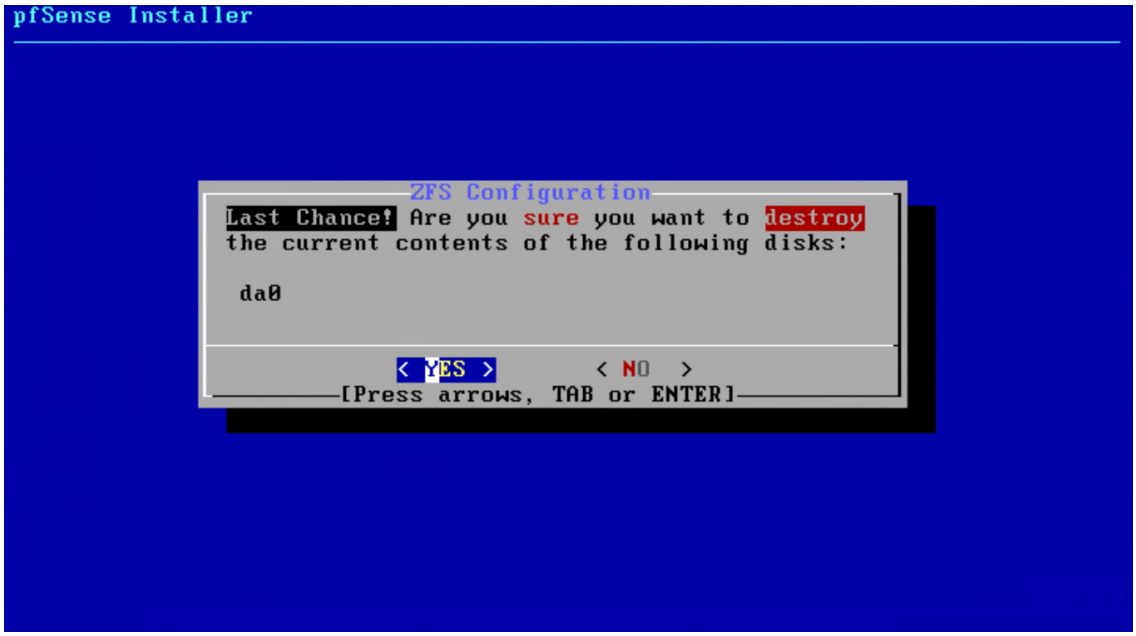
9. Sélectionnez "Stripe"



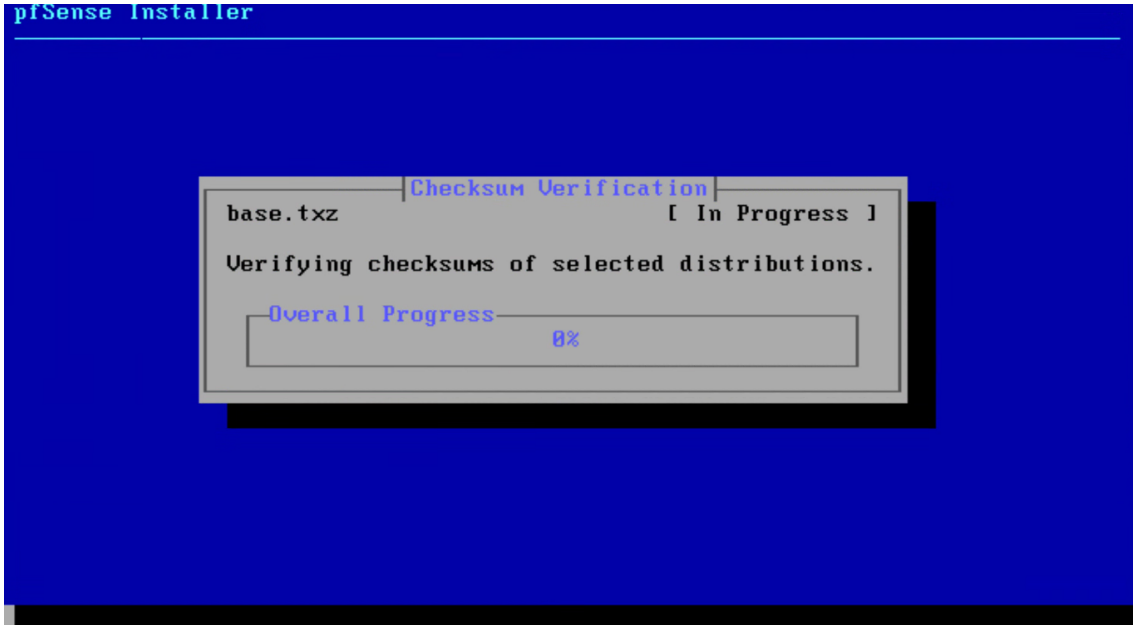
10. Sélectionnez votre disque (touche espace pour sélectionner), ici "da0"

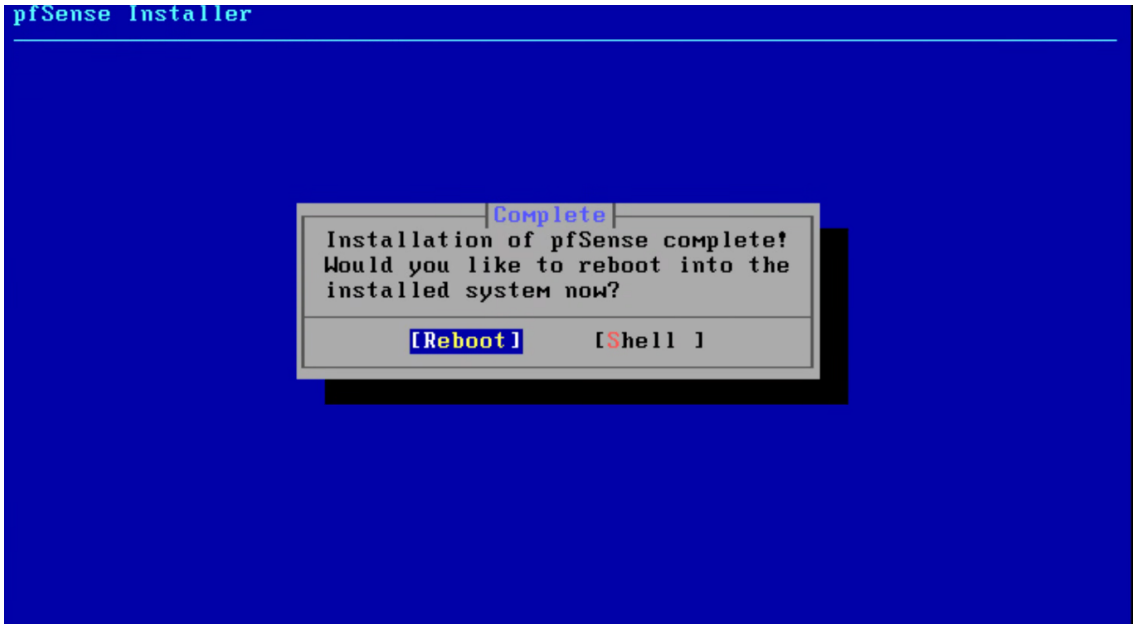


11. Sélectionnez "Yes"



12. L'installation commence, sélectionnez "Reboot" une fois terminé

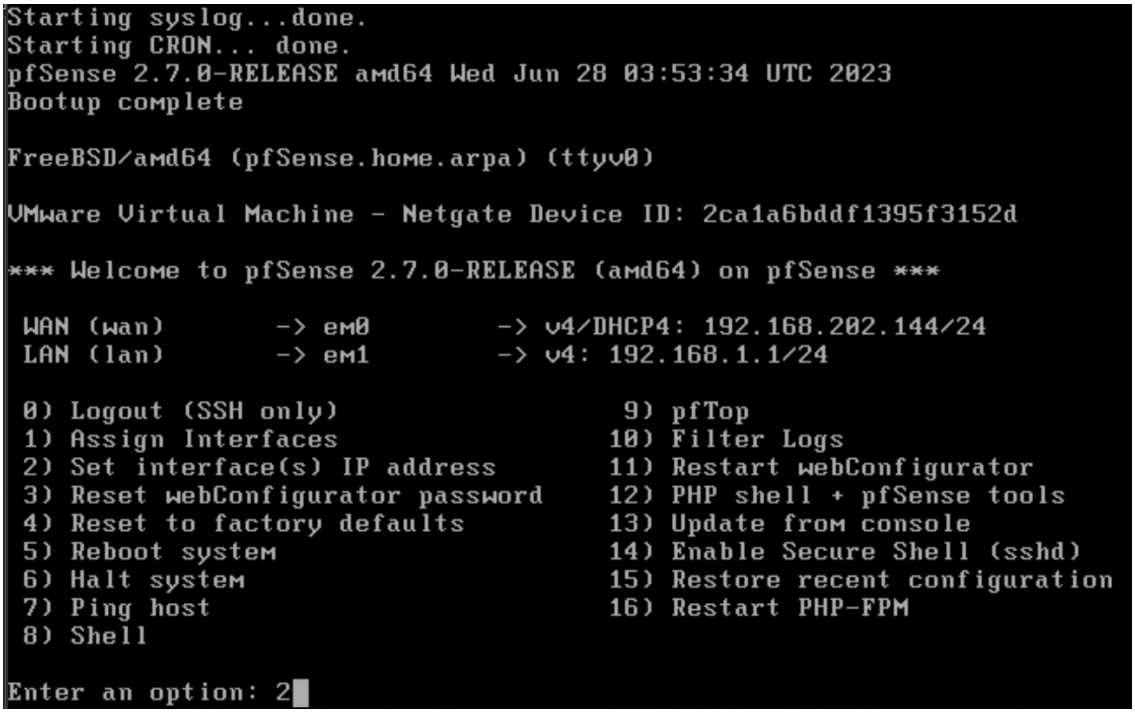




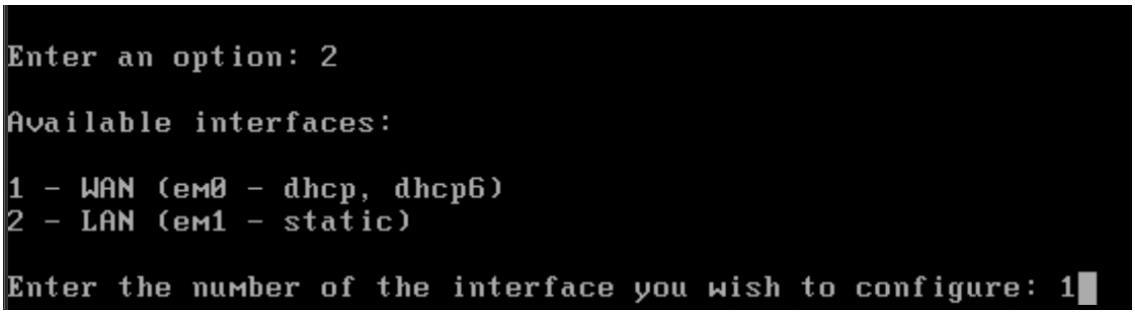
Configuration Interne

0. Laissez le serveur démarrer
1. Faites "a" pour détecter automatiquement l'inteface WAN et LAN, en cas d'erreur, sélectionnez les manuellement

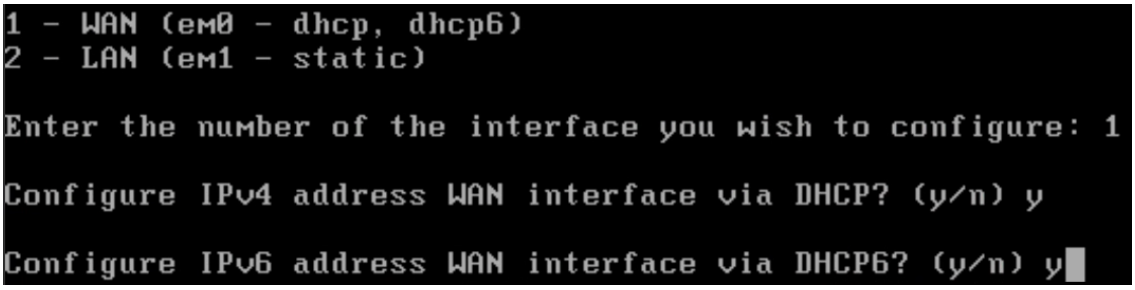
2. Appuyez sur 2 pour configurer l'interface WAN



3. Sélectionnez l'interface WAN avec le numéro correspondant (ici 1)



4. Faites "y" pour configurer l'interface WAN en DHCP pour l'IpV4
5. Faites de même pour l'IpV6



6. Si demandé, refusez l'http pour le webconfigurator

```
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to WAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 WAN address has been set to dhcp


The IPv6 WAN address has been set to dhcp6

Press <ENTER> to continue.
```

7. Faites "Entrer" pour valider la configuration
8. Appuyez sur 2 pour configurer l'interface LAN
9. Sélectionnez l'interface LAN avec le numéro correspondant (ici 2)

```
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.202.144/24
 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: 2
```

10. Faites "n" pour configurer l'interface LAN en statique pour l'IpV4
11. L'adresse LAN est 192.168.1.1
12. Le masque est 24

13. Faites "Entrer" pour la Gateway car c'est le serveur PfSense lui-même

```
Available interfaces:

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

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

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.1.1

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 32):
> 24

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

14. Faites "y" pour configurer l'interface LAN en DHCP pour l'IpV6, la raison étant que nous n'en avons pas besoin en LAN dans cette infrastructure
15. Faites "y" pour configurer le serveur DHCP pour l'IpV4

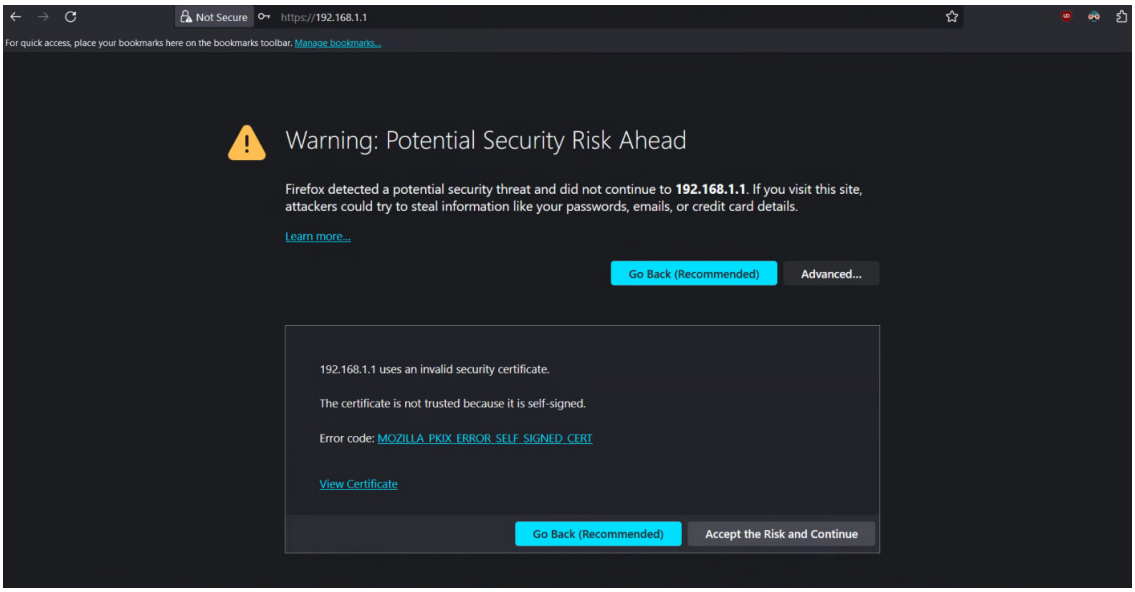
```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>



Configure IPv6 address LAN interface via DHCP6? (y/n) y

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

16. L'adresse de départ est 192.168.1.2
17. L'adresse de fin est 192.168.1.2
18. Nous gardons cette IP dans le cas où nous aurions besoin d'accéder au serveur PfSense en direct
19. Faites "Entrer" pour valider la configuration

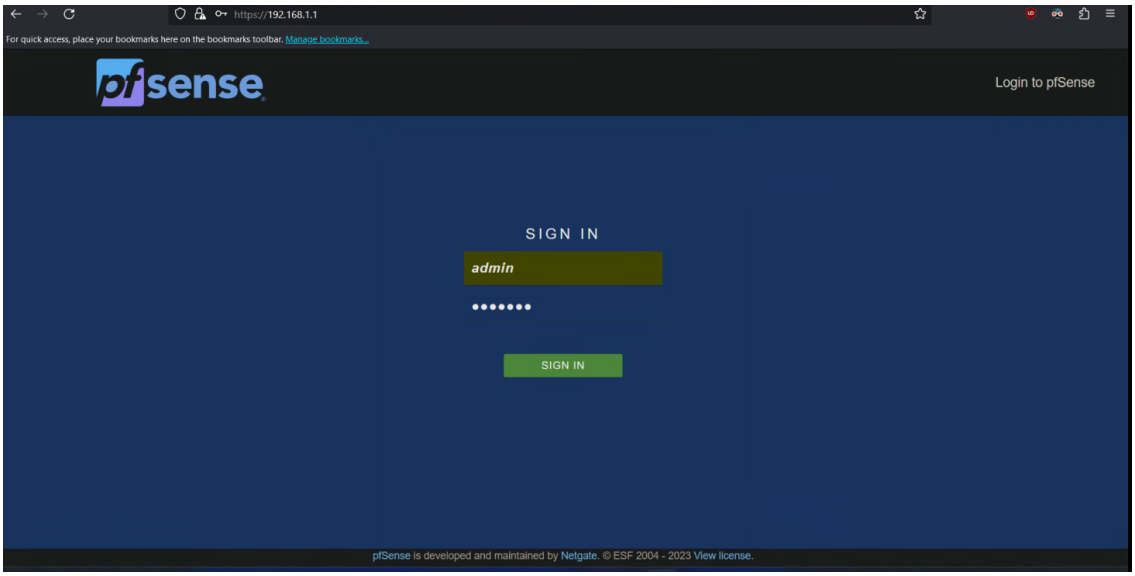
```
Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.1.2
Enter the end address of the IPv4 client address range: 192.168.1.5
Disabling IPv6 DHCPD...

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 LAN address has been set to 192.168.1.1/24


The IPv6 LAN address has been set to dhcp6

Press <ENTER> to continue.
```

Configuration GUI

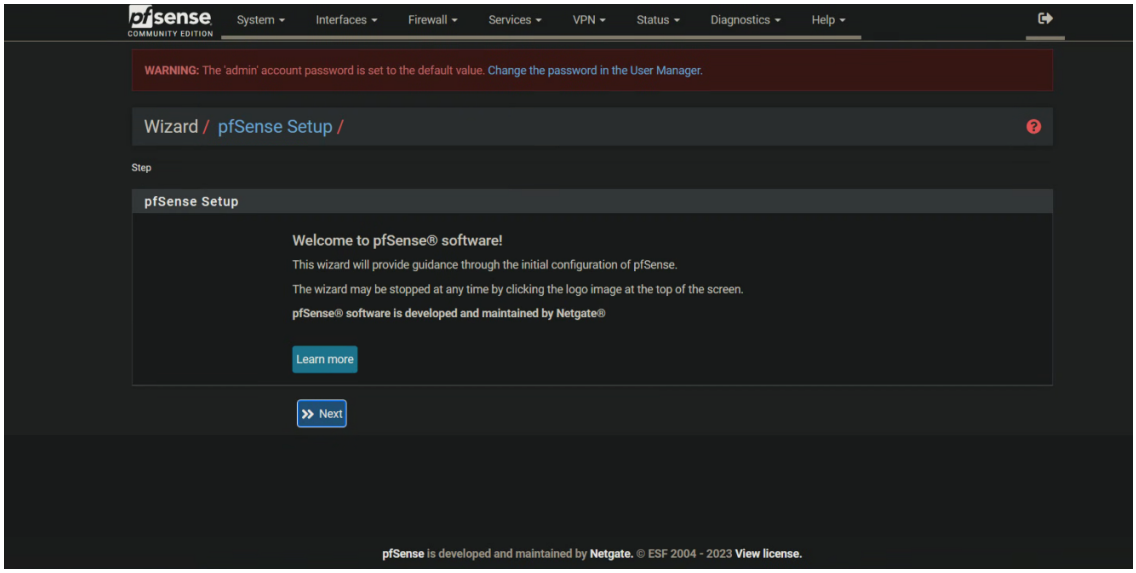
1. Connectez un ordinateur au port LAN du serveur, vous devriez ainsi obtenir l'adresse 192.168.1.2
2. Ouvrez un navigateur
3. Allez sur l'adresse https://192.168.1.1/
4. Acceptez et continuez malgré le certificat invalide



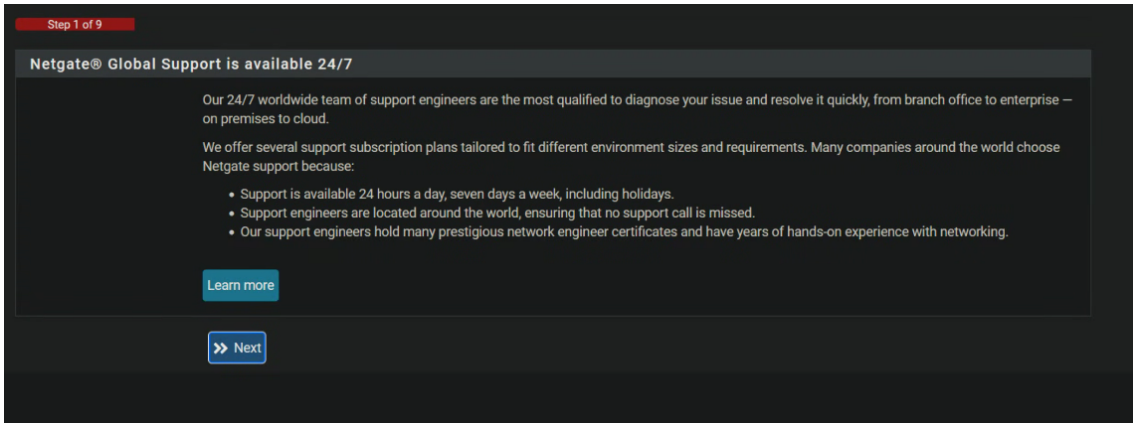
5. Connectez-vous avec les identifiants par défaut (admin/pfsense)



6. Faites "Next"



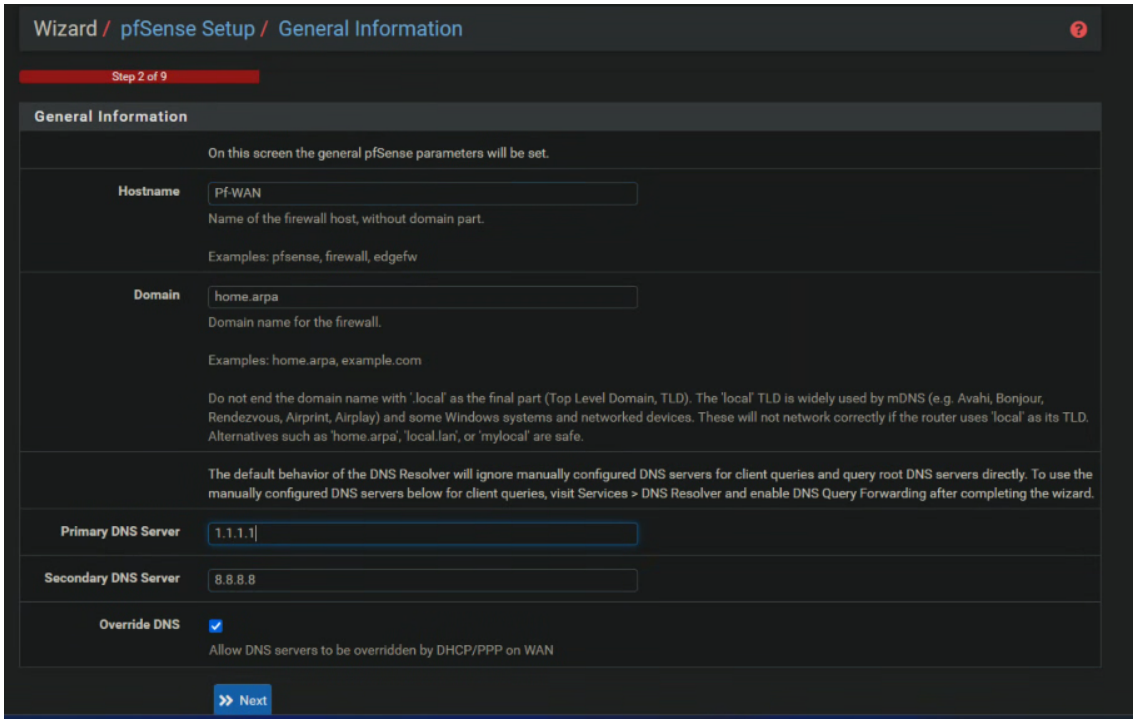
7. Faites "Next"



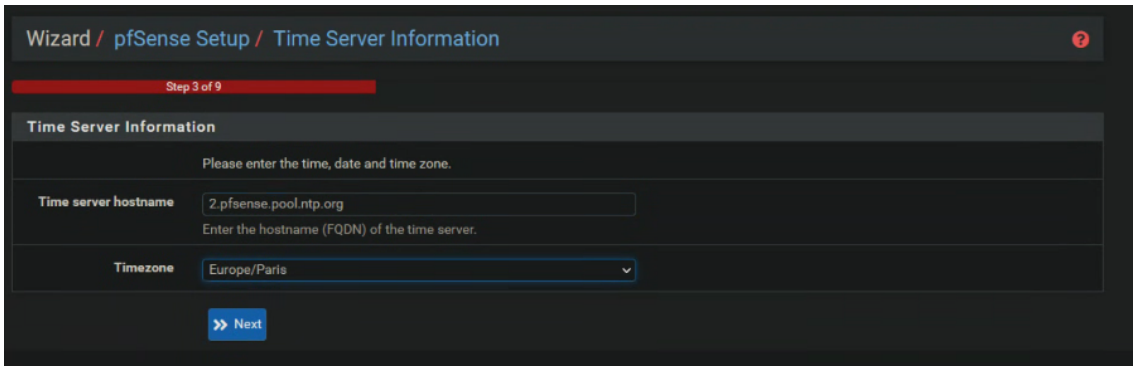
8. Remplissez les informations :

- "Pf-Entreprise" pour le hostname
- "1.1.1.1" pour le DNS principal
- "8.8.8.8" pour le DNS secondaire

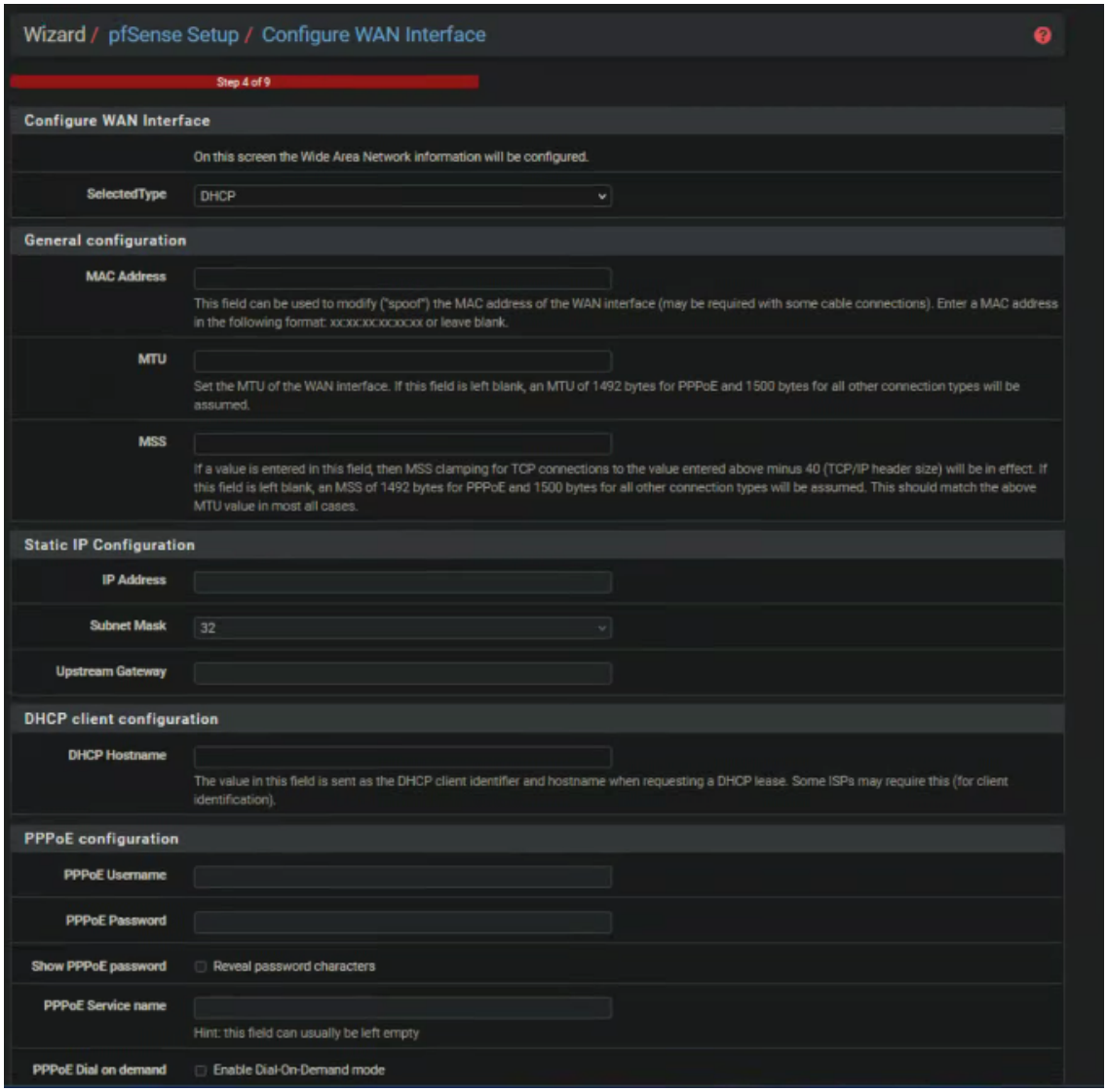
8. Faites "Next"

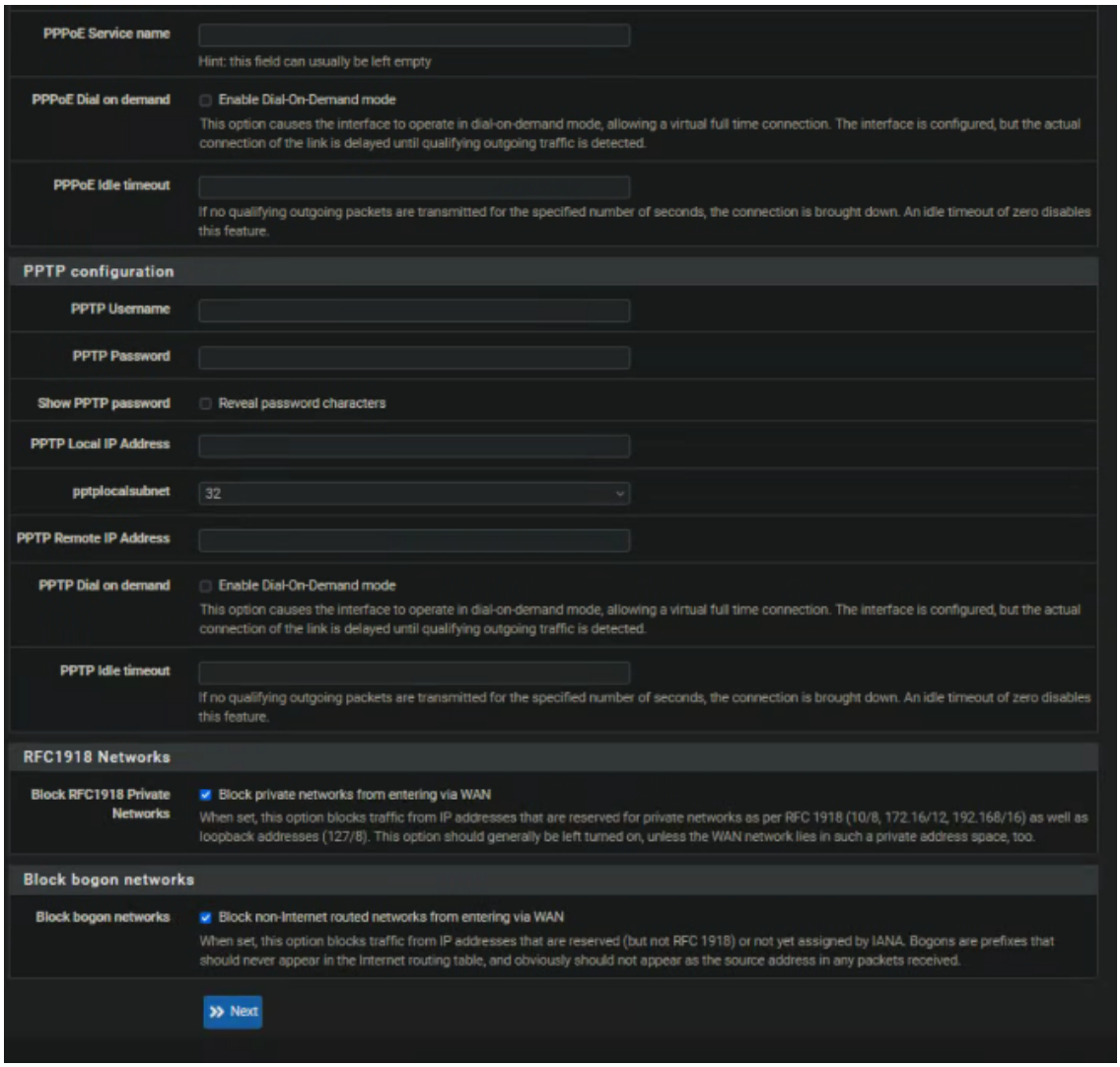


9. Séléctionnez votre fuseau horaire (ici Europe/Paris)
10. Faites "Next"

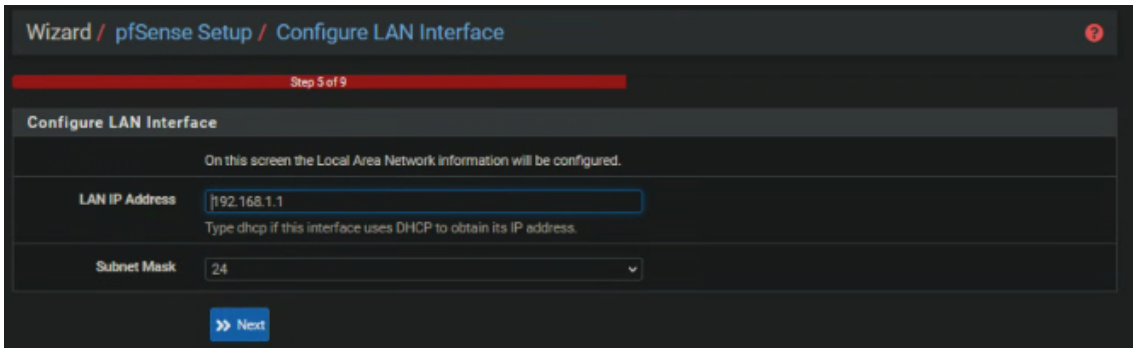


11. Faites "Next", aucune modification n'est nécessaire pour le WAN

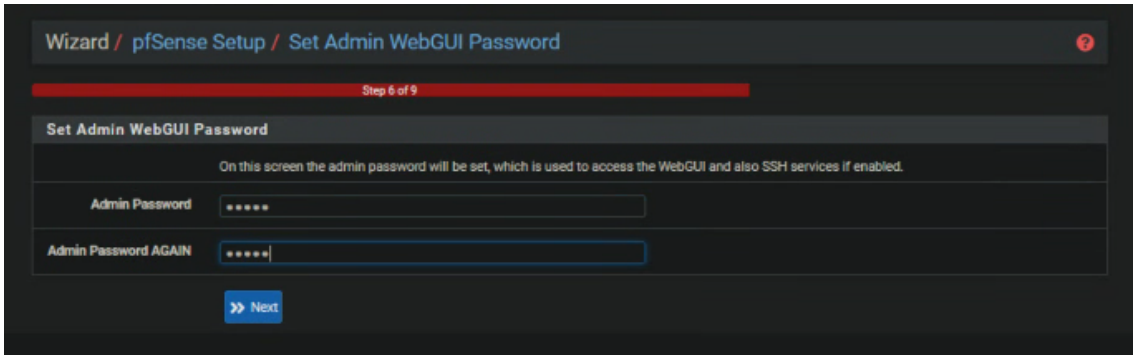




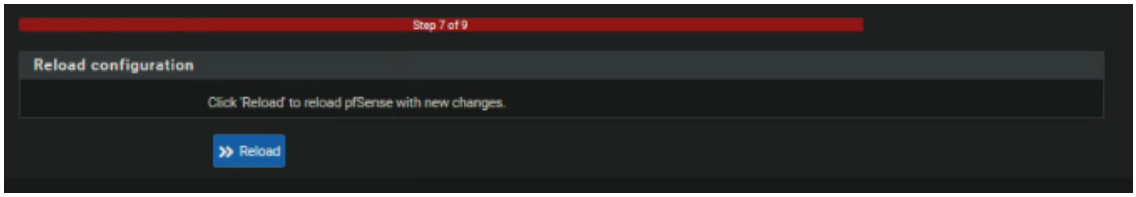
12. Faites "Next", aucune modification n'est nécessaire pour le LAN



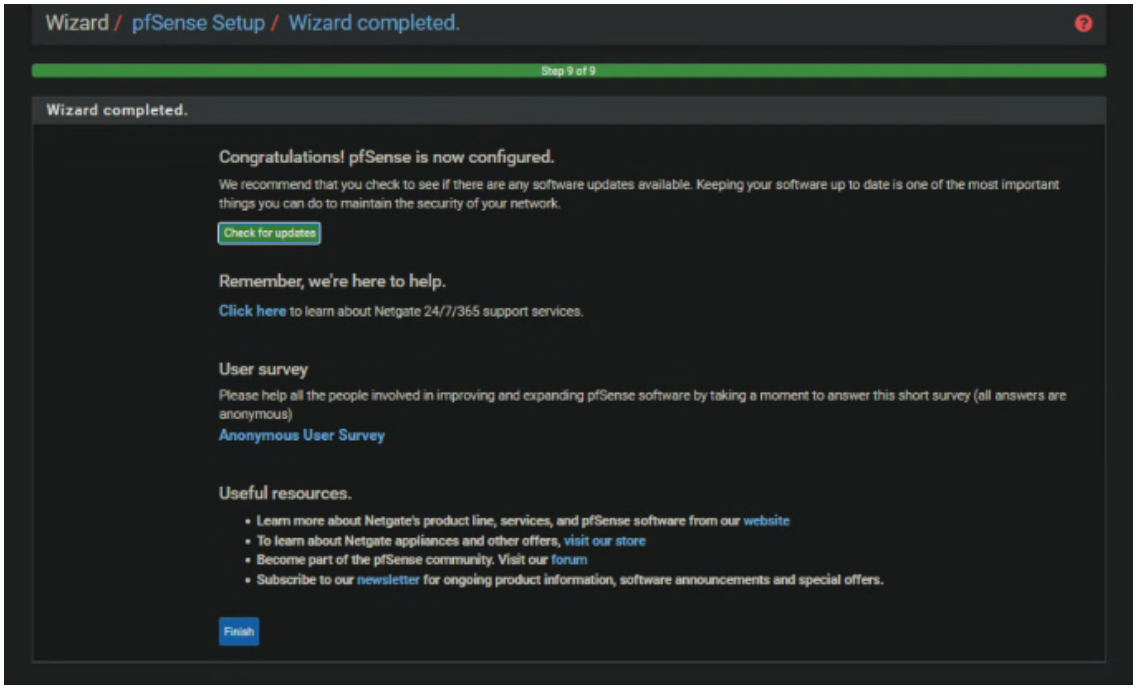
13. Changez le mot de passe de l'admin ("admin" pour l'exemple, mais il se doit d'être sécurisé)
14. Faites "Next"



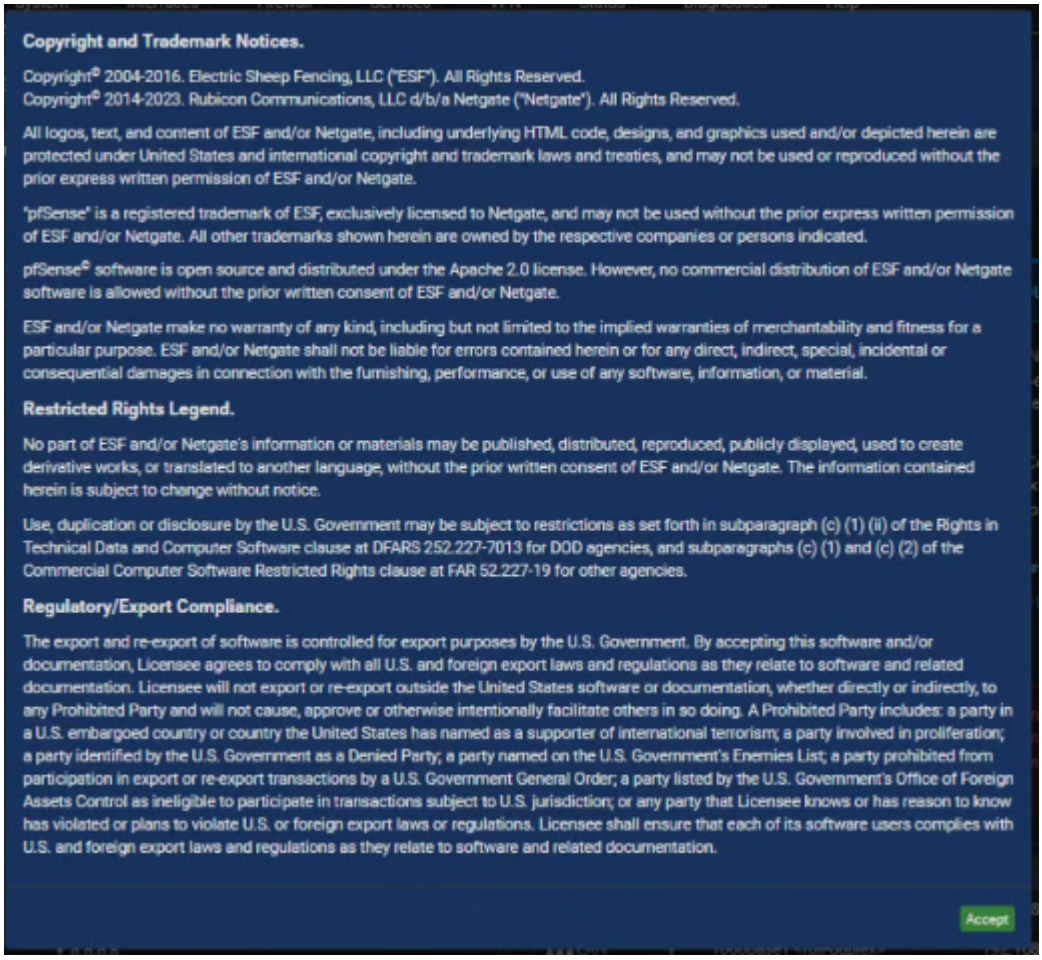
15. Faites "Reload" et attendez que le serveur redémarre



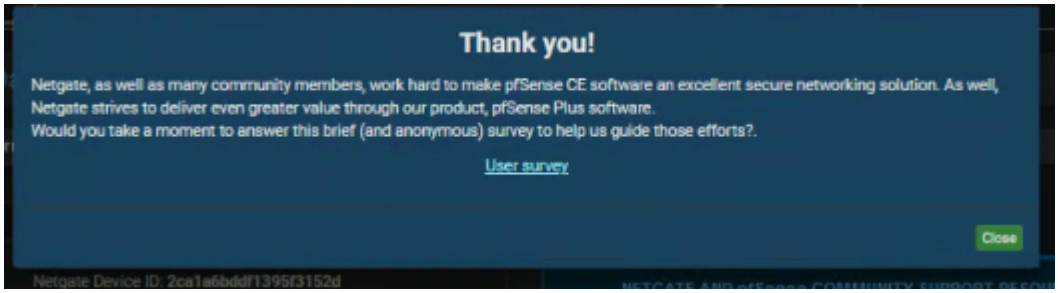
16. Une fois la page rechargée, faites "Check for updates" si l'ISO utilisée est ancienne, sinon faites "Finish"



17. Acceptez les conditions d'utilisation



18. Faites "Close"

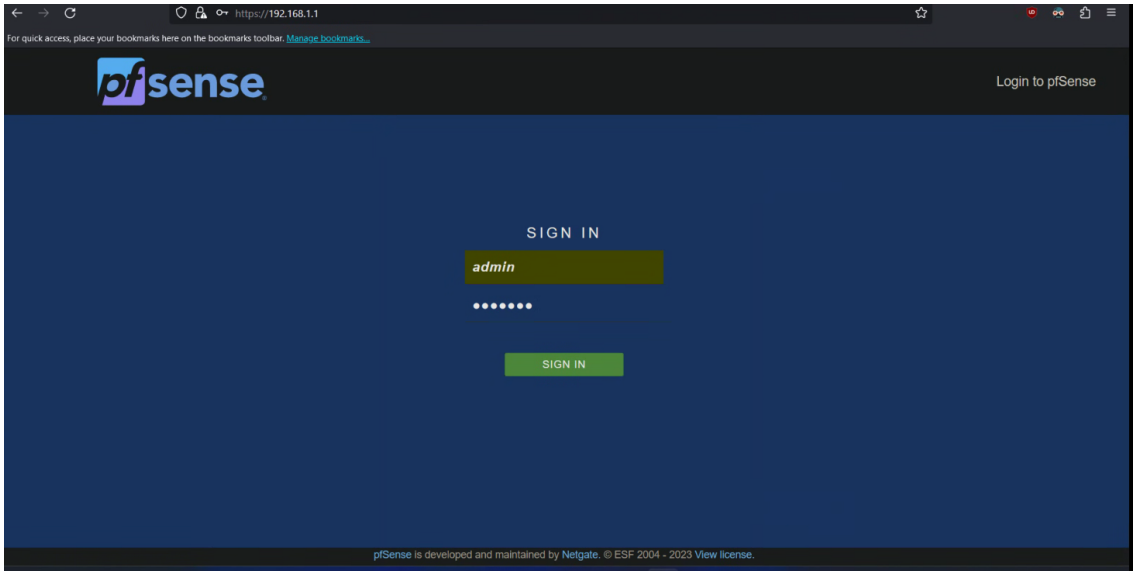


Configuration Interfaces

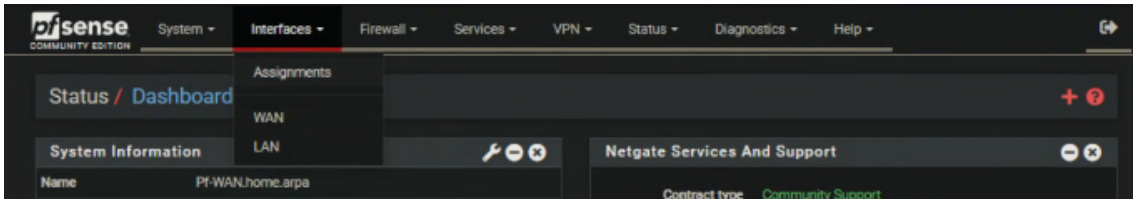
Configuration VLANs

1. Connectez un ordinateur au port LAN du serveur, vous devriez ainsi obtenir l'adresse 192.168.1.2
2. Ouvrez un navigateur
3. Allez sur l'adresse https://192.168.1.1/

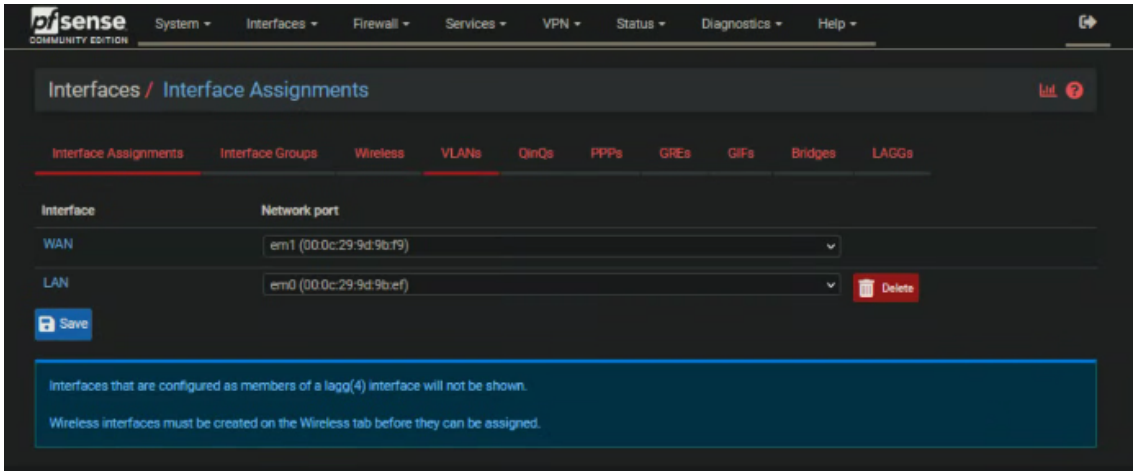
4. Connectez-vous avec les identifiants défini (ici admin/admin)



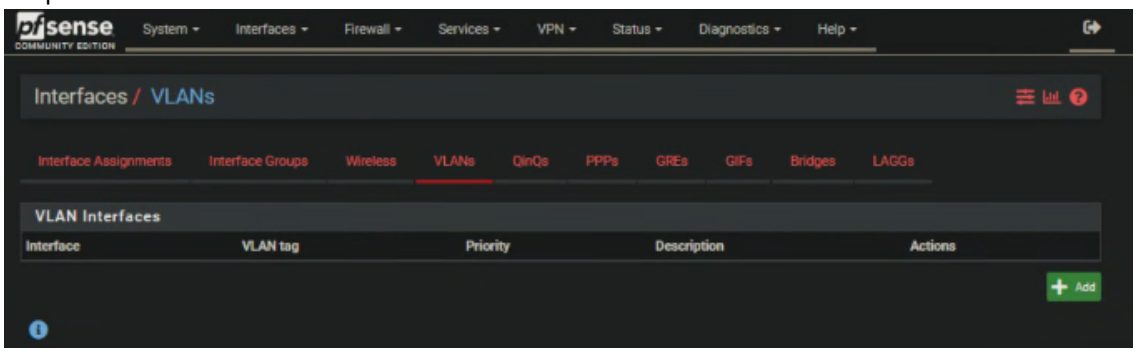
5. Allez dans "Interfaces" > "Assignments"



6. Allez dans "VLANs"

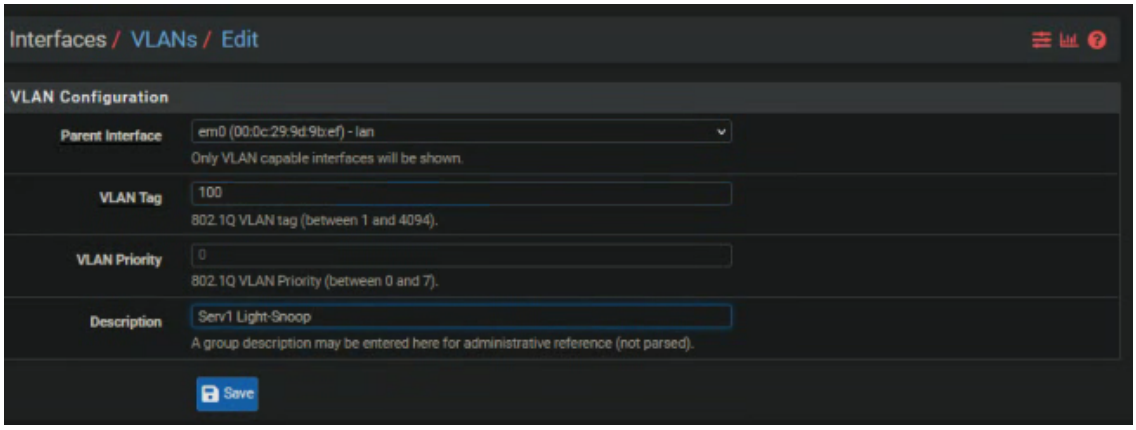


7. Cliquez sur "Add"

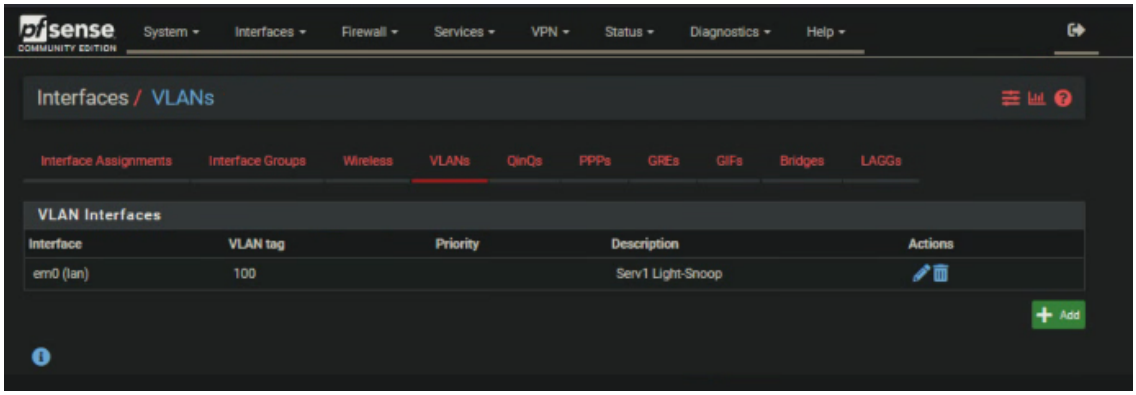


8. Sélectionnez l'interface LAN (ici em0)
9. Entrez le VLAN (ici 100)
10. Entrez une description (ici "Ethernet + Wifi")

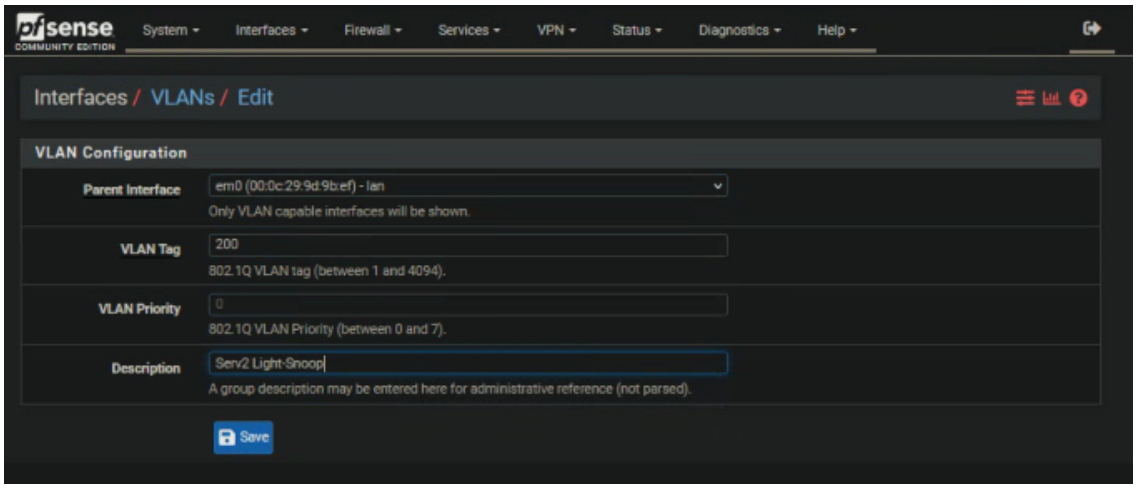
11. Faites "Save"



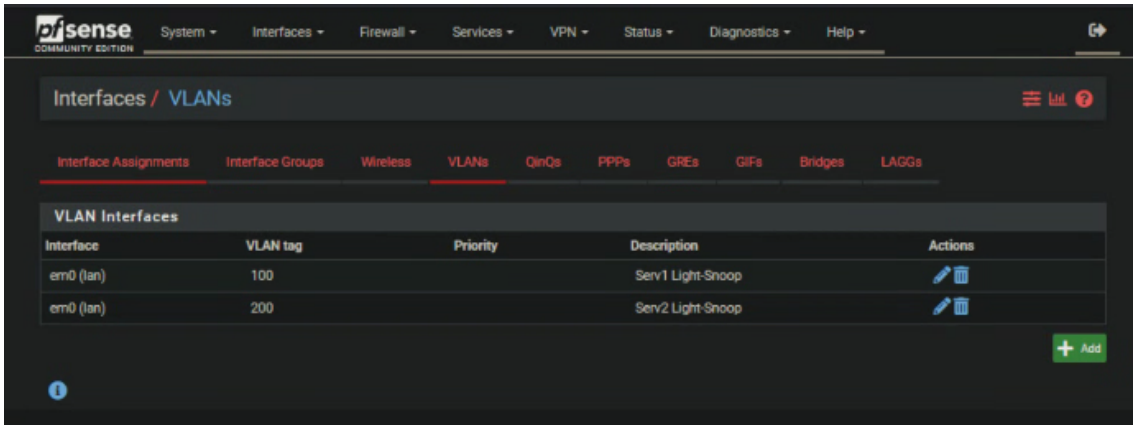
12. Cliquez sur "Add"



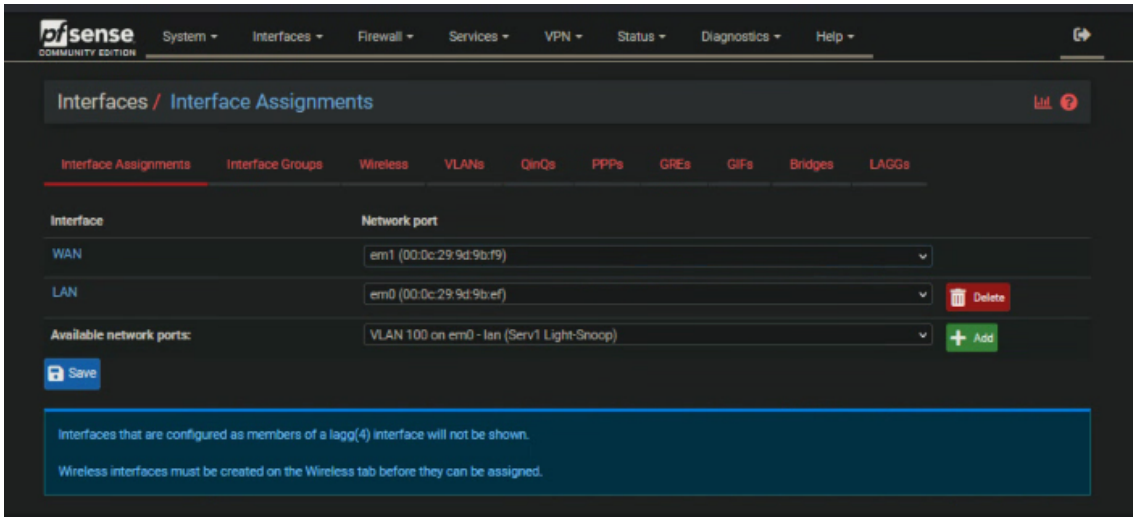
13. Sélectionnez l'interface LAN (ici em0)
14. Entrez le VLAN (ici 200)
15. Entrez une description (ici "Wifi Invité")
16. Faites "Save"



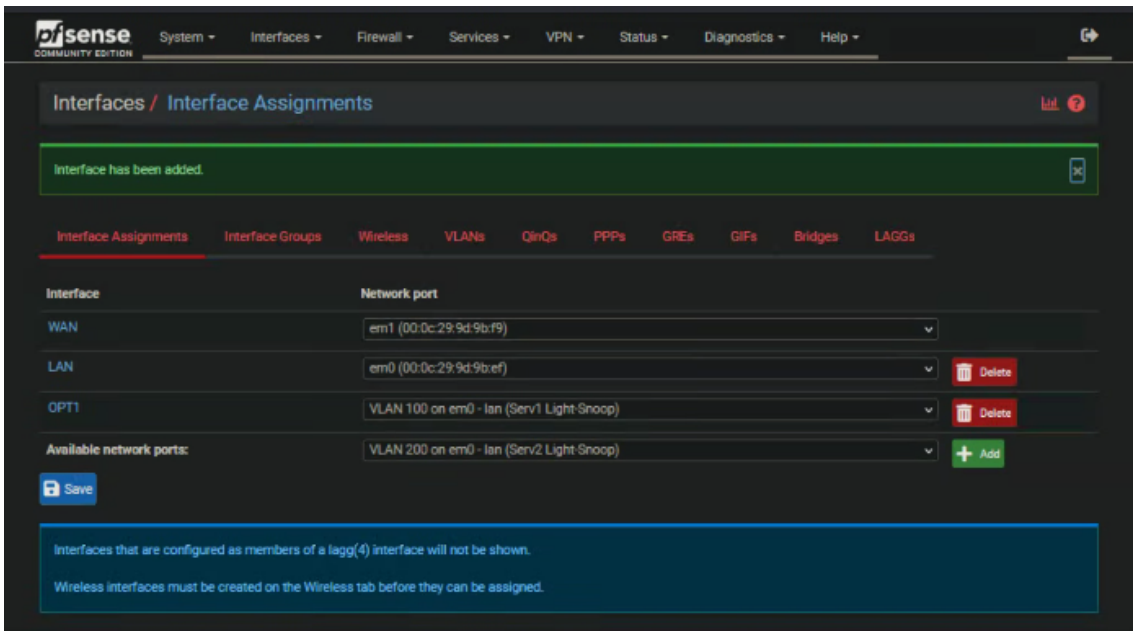
17. Allez dans "Interfaces Assignments"



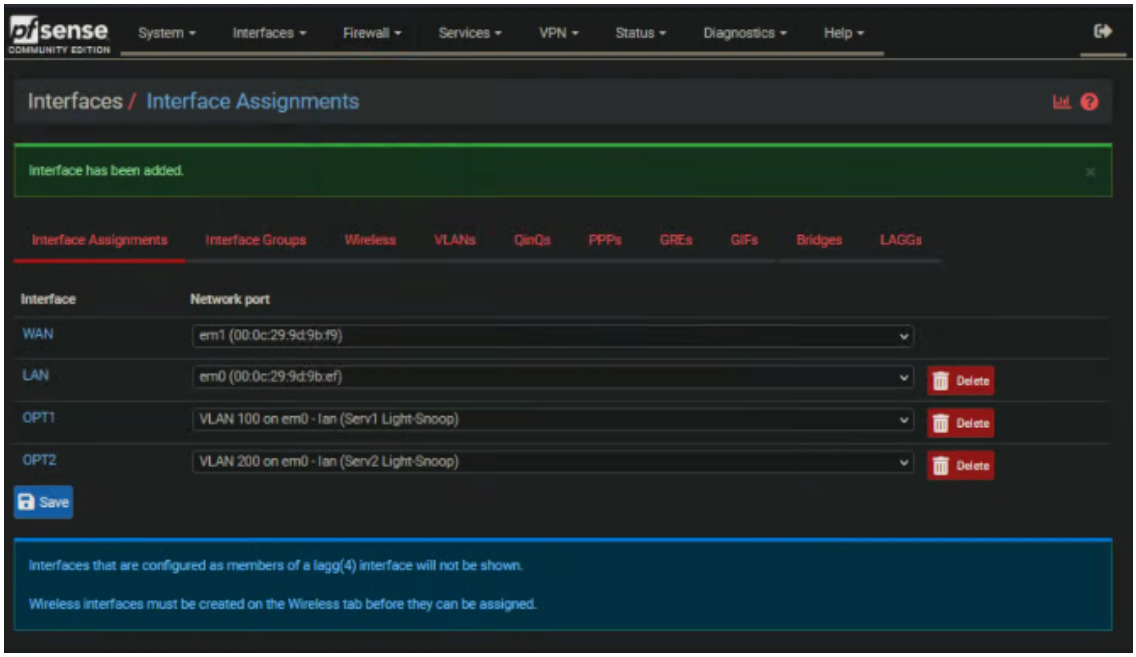
18. Faites "Add"



19. Faites à nouveau "Add"

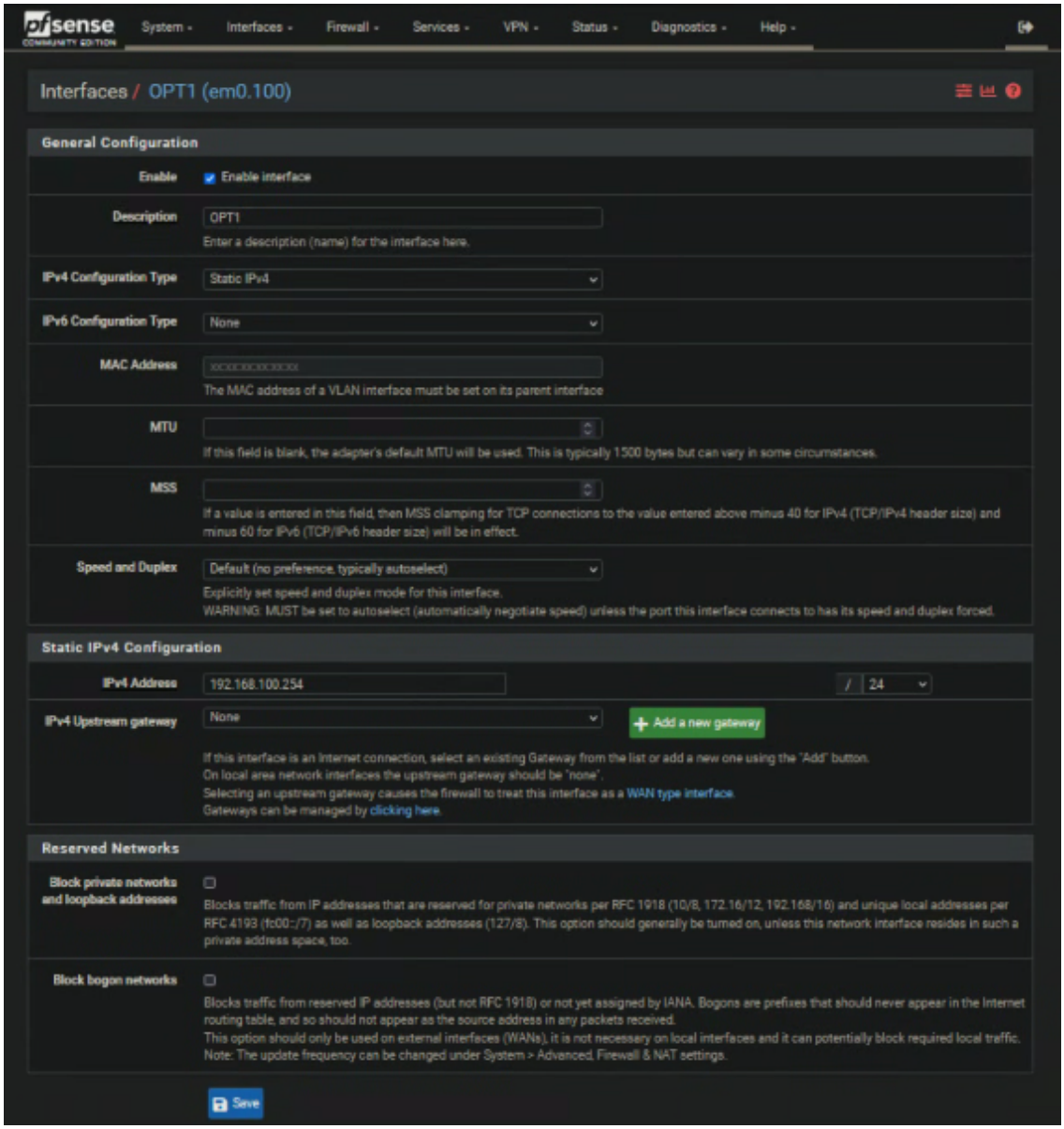


20. Cliquez sur l'interface OPT1 (VLAN 100)

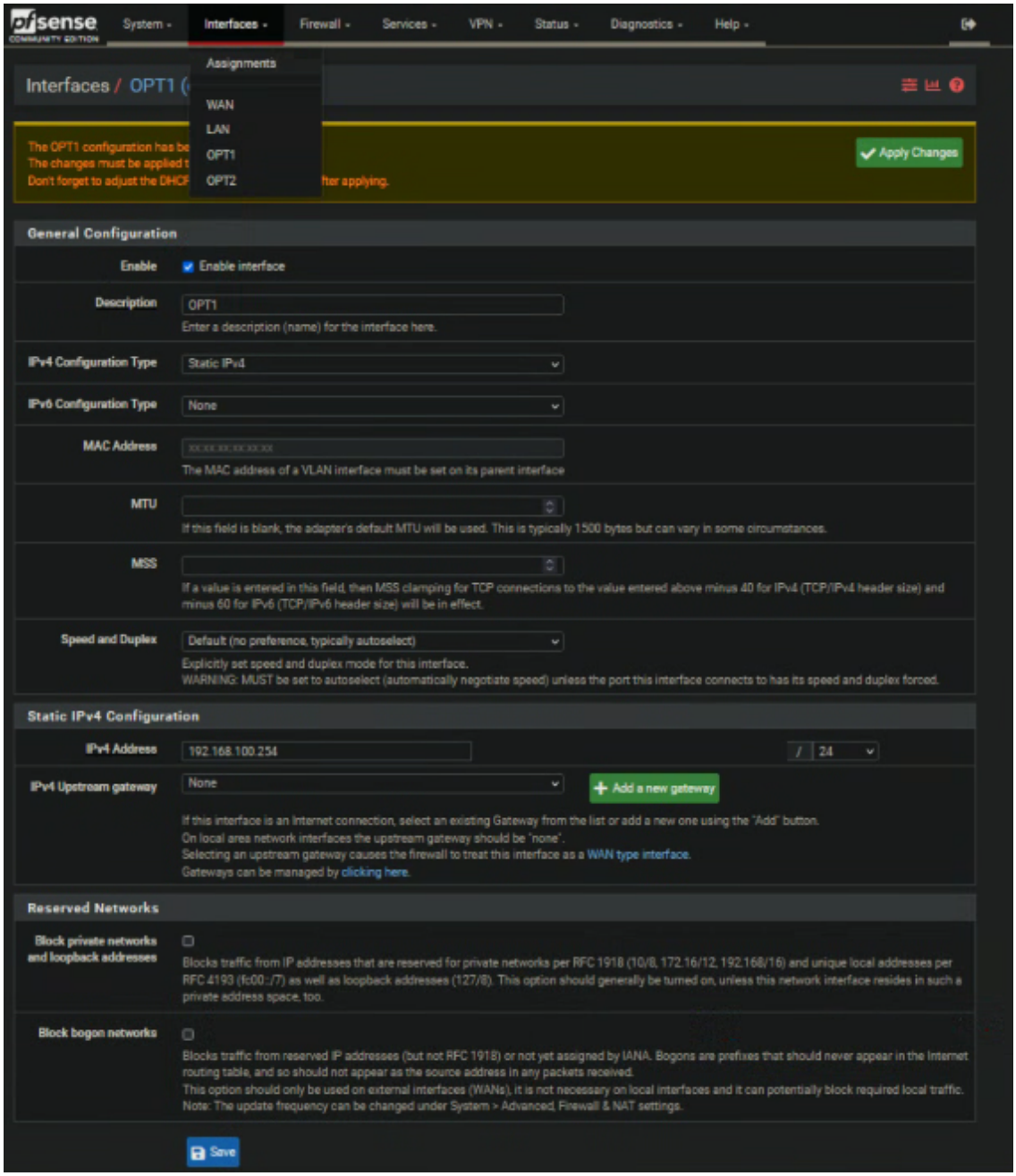


21. Activez l'interface
22. Passez l'IPv4 en statique
23. Entrez l'adresse IP (ici 192.168.100.254)
24. Précisez le masque (ici 24)

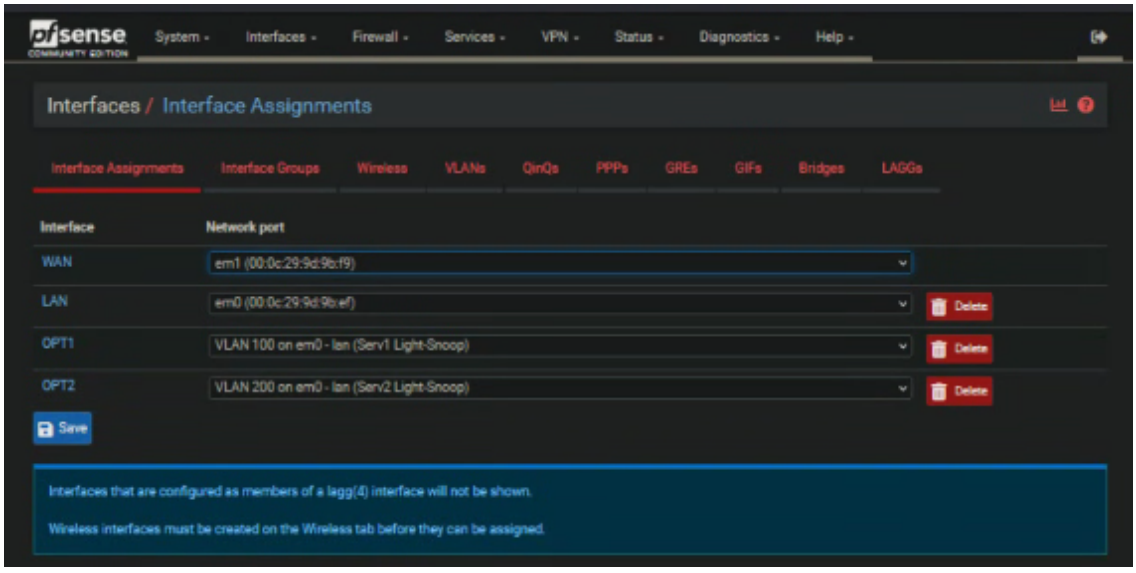
25. Faites "Save"



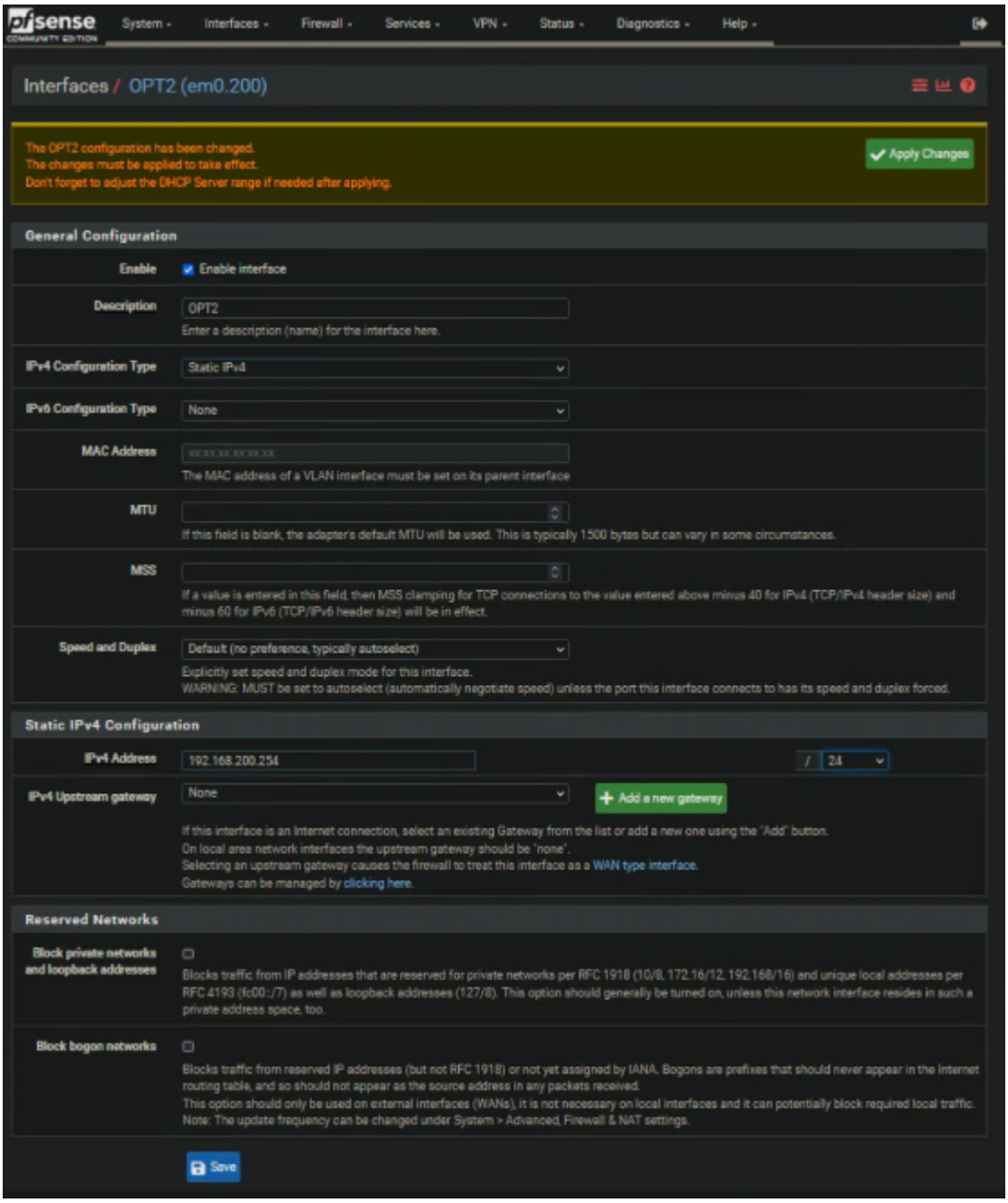
26. Retournez dans "Interfaces" > "Assignments"



27. Cliquez sur l'interface OPT2 (VLAN 200)

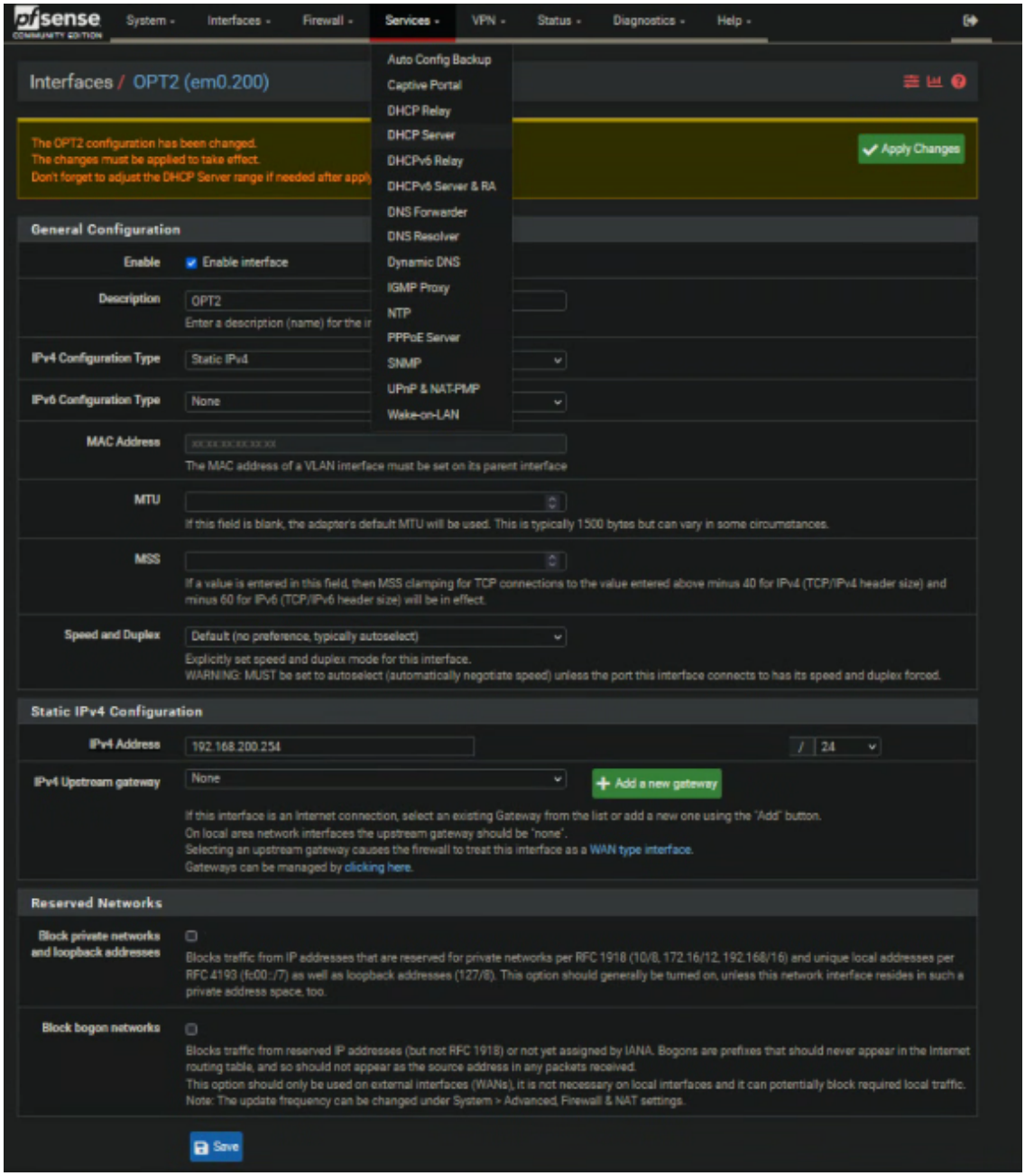


28. Activez l'interface
29. Passez l'IPv4 en statique
30. Entrez l'adresse IP (ici 192.168.200.254)
31. Précisez le masque (ici 24)
32. Faites "Save"

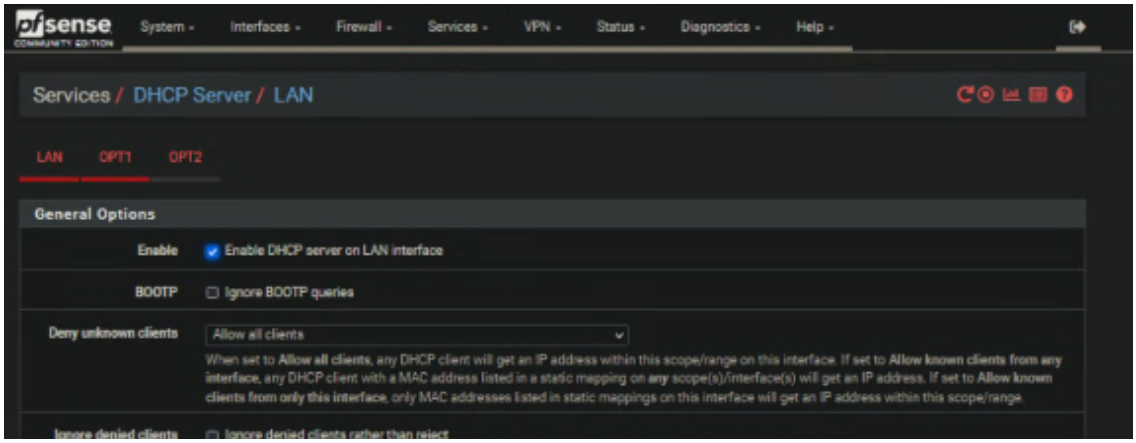


Configuration DHCP

1. Allez dans "Services" > "DHCP Server"



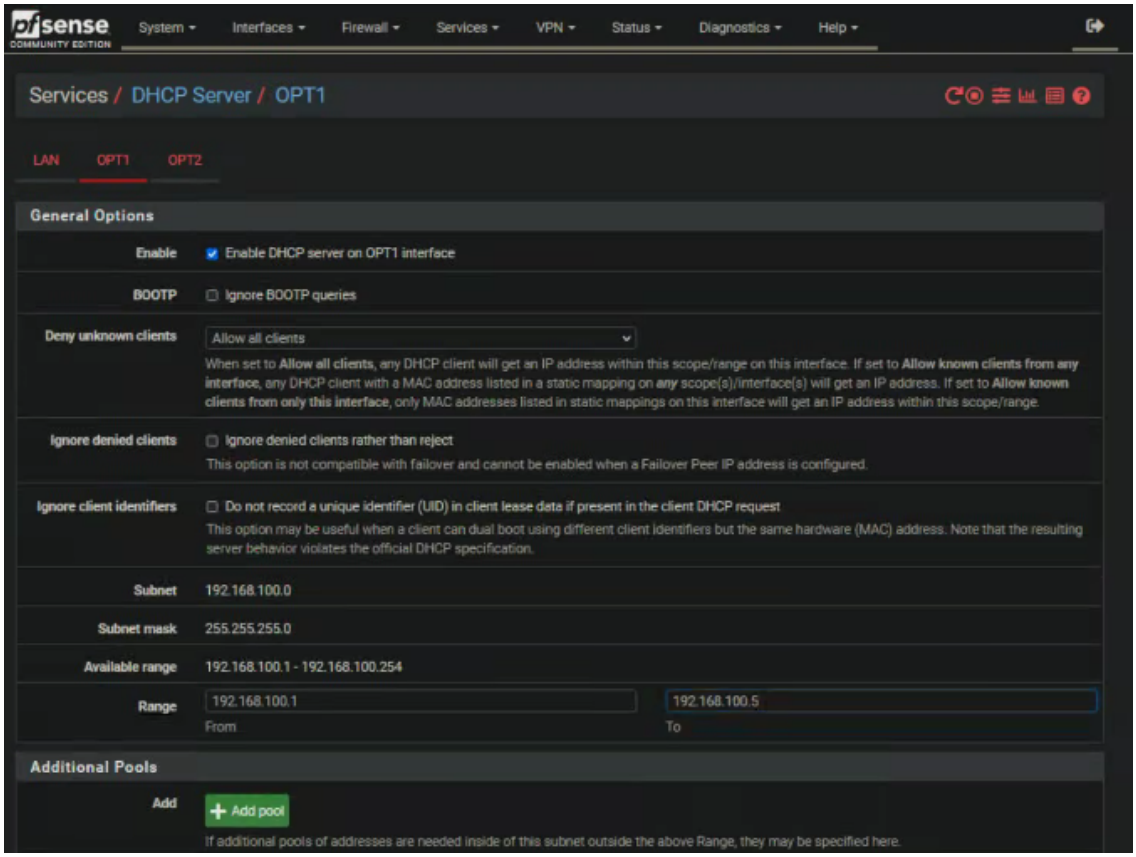
2. Allez dans "OPT1"



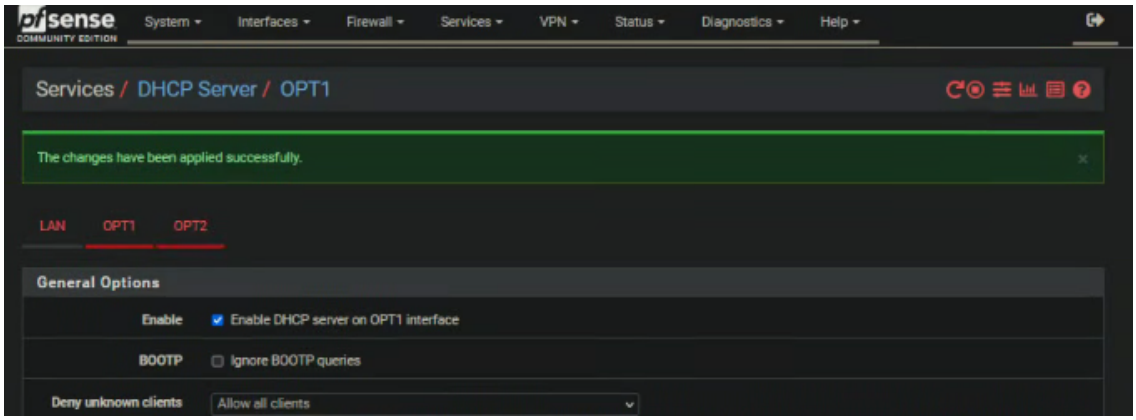
3. Activez le serveur DHCP
4. Entrez le range d'adresse (ici 192.168.100.1 - 192.168.100.5, adaptez en fonction de vos besoins, si vous avez plus d'ordinateurs et autres appareils ou que vous allez augmenter

votre parc, augmentez le range. Préférez prendre une range adaptée avec une petite marge pour minimiser les risques)

5. Faites "Save"

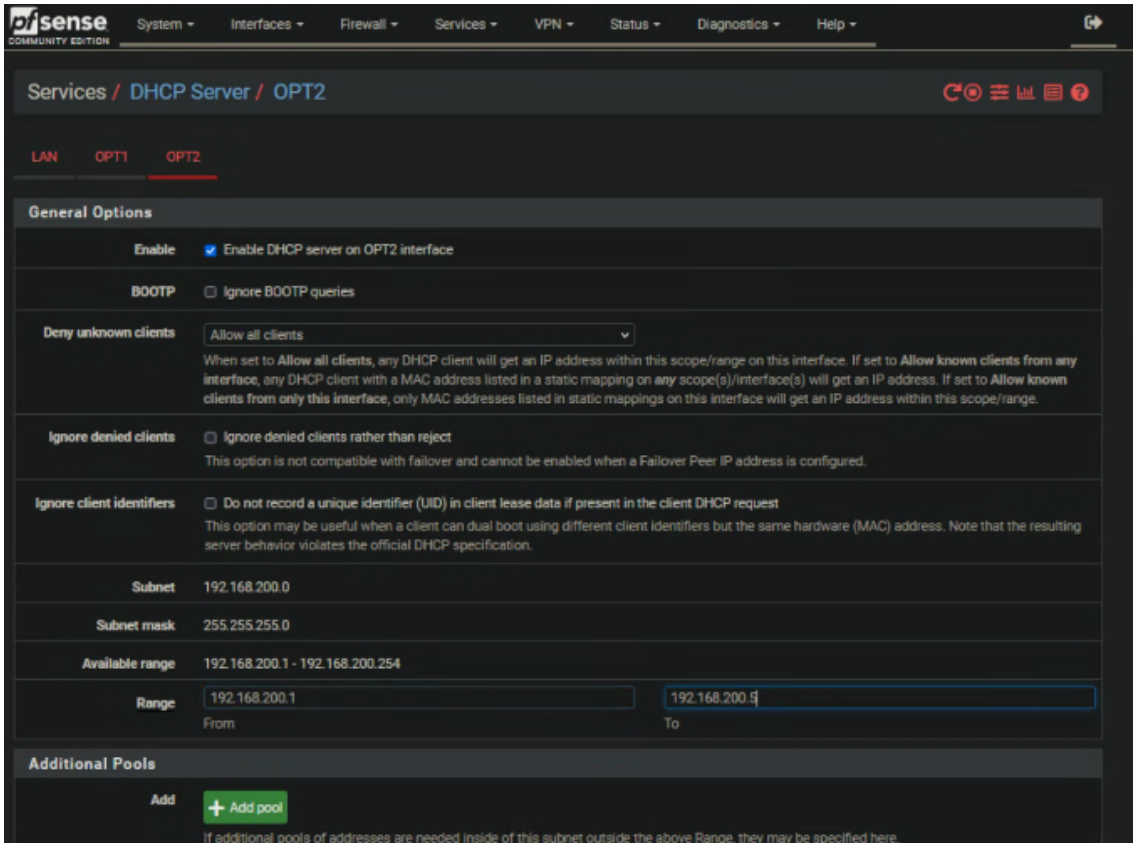


6. Allez dans "OPT2"



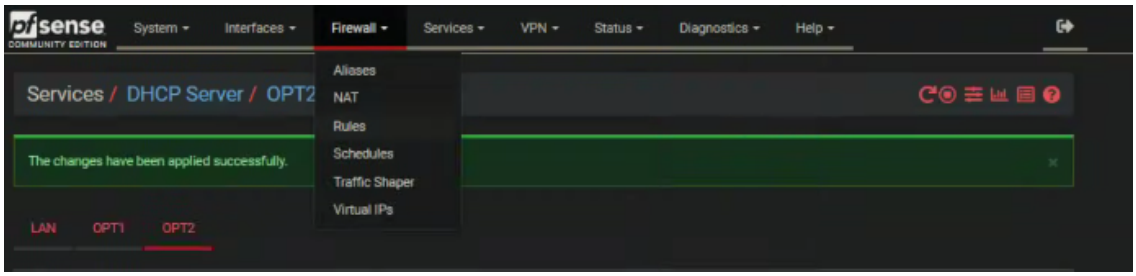
7. Activez le serveur DHCP
8. Entrez le range d'adresse (ici 192.168.200.1 - 192.168.200.254, la range est plus grande car nous ne savons pas combien d'appareils vont se connecter au Wifi invité et que celui-ci sera plus contrôlé)

9. Faites "Save"

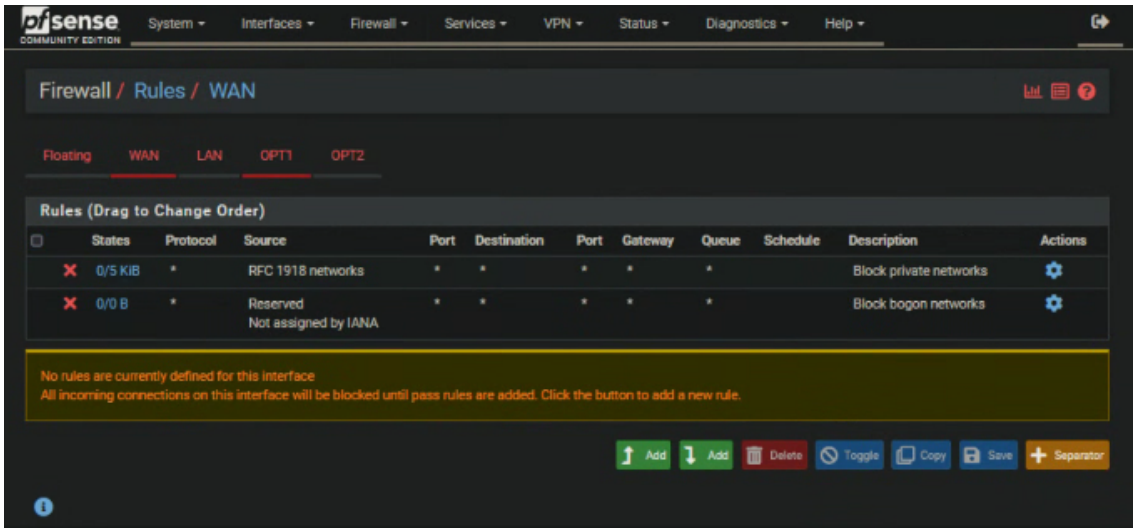


Configuration Firewall

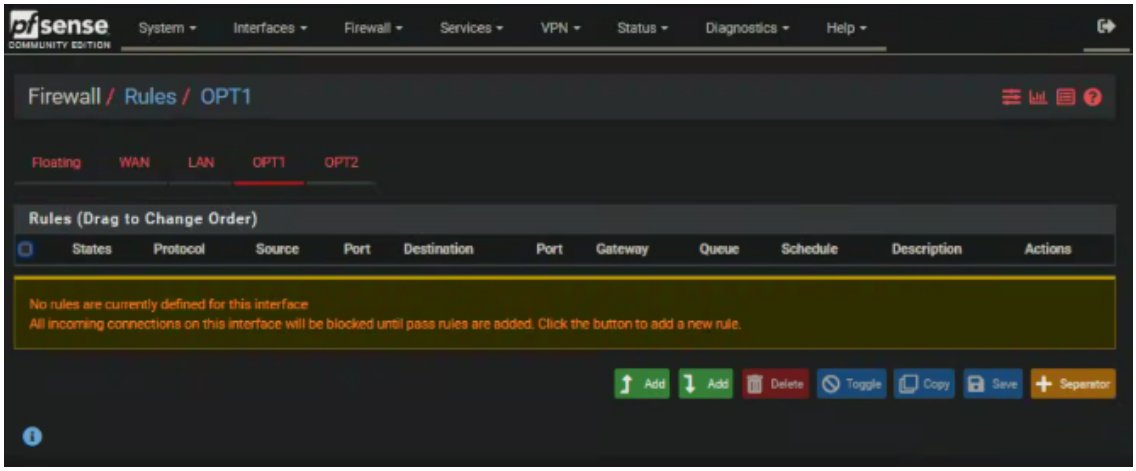
1. Allez dans "Firewall" > "Rules"



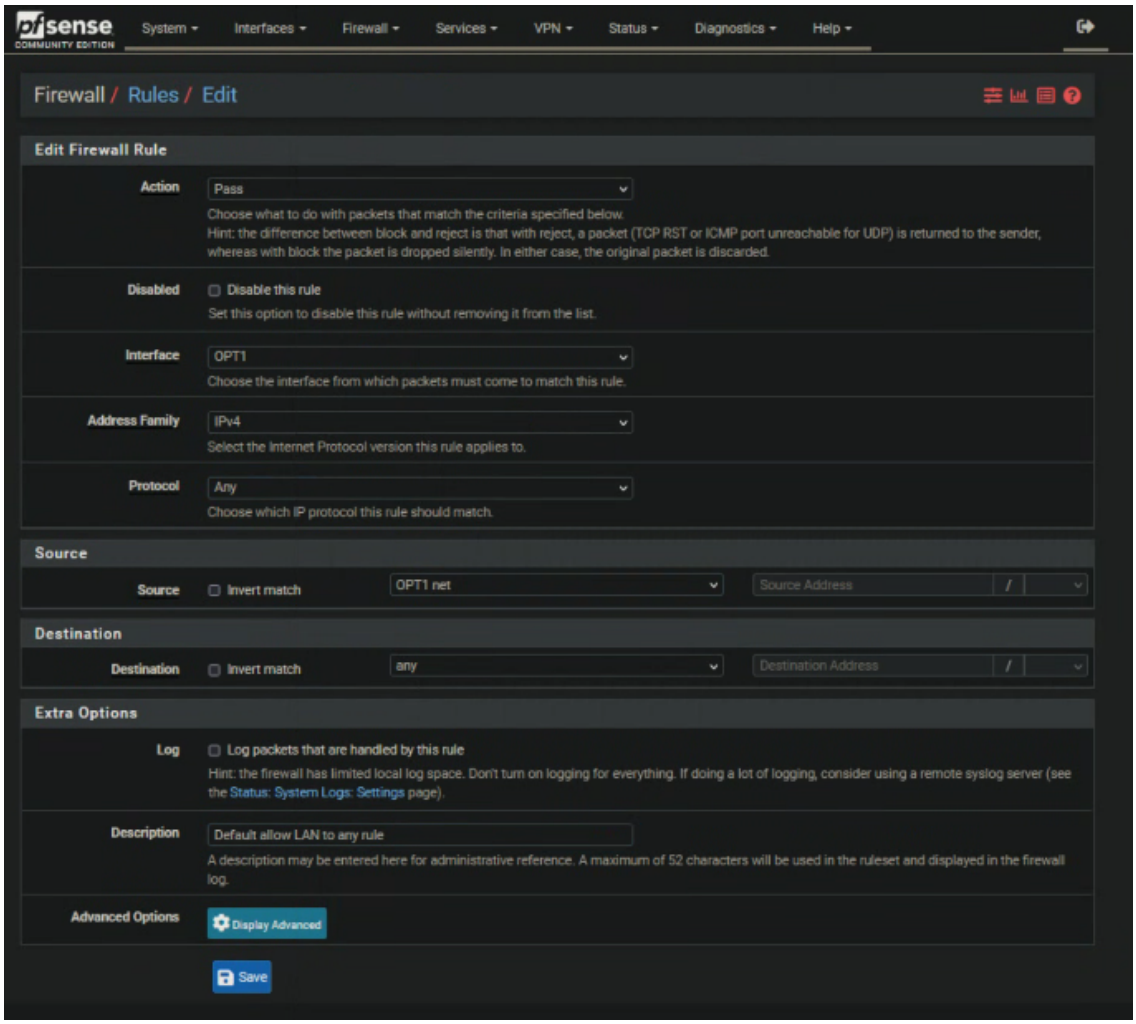
2. Allez dans "OPT1"



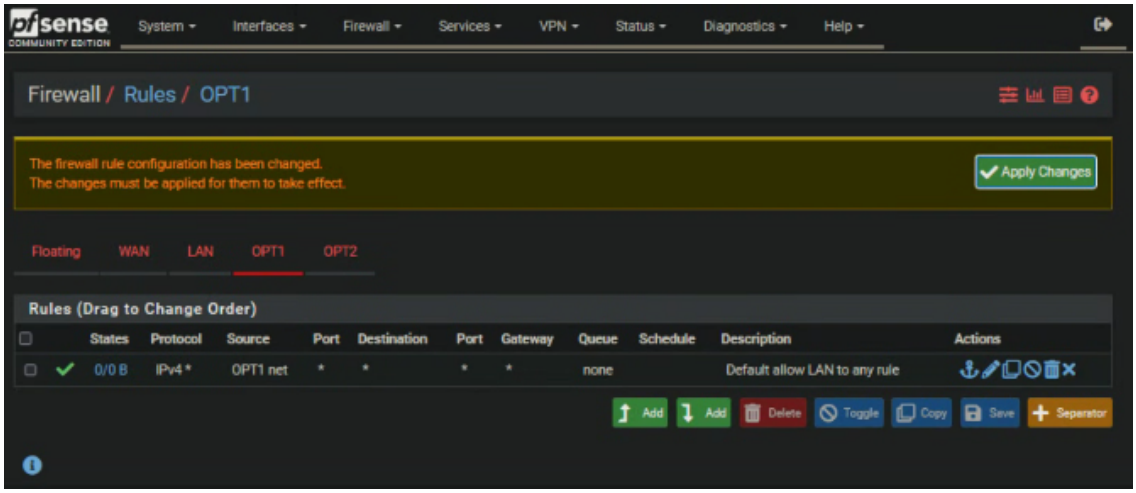
3. Faites "Add"



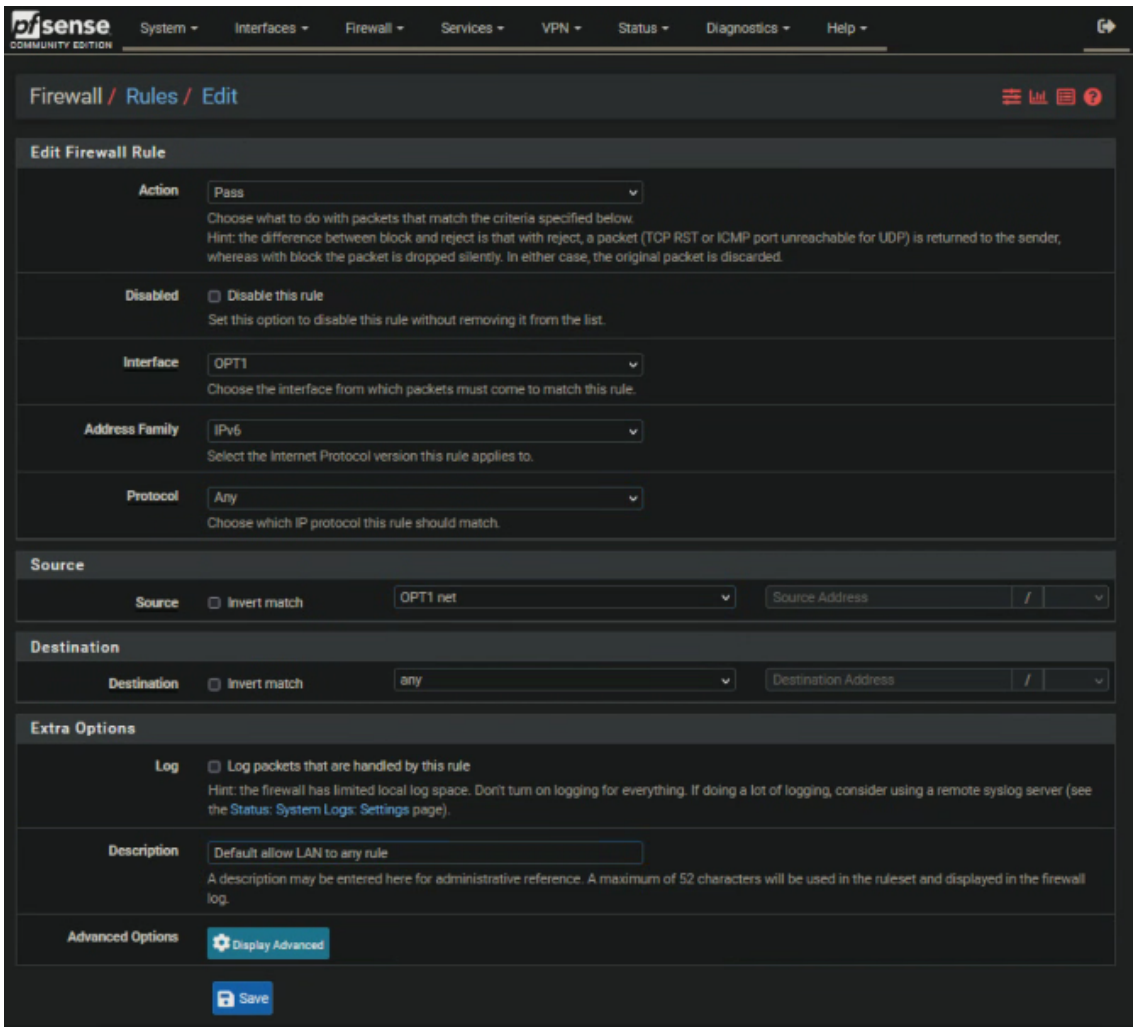
4. Changer le "Protocol" en "Any"
5. Changer la "Source" en "OPT1 net"
6. Mettez "Default allow LAN to any rule" en description
7. Faites "Save"



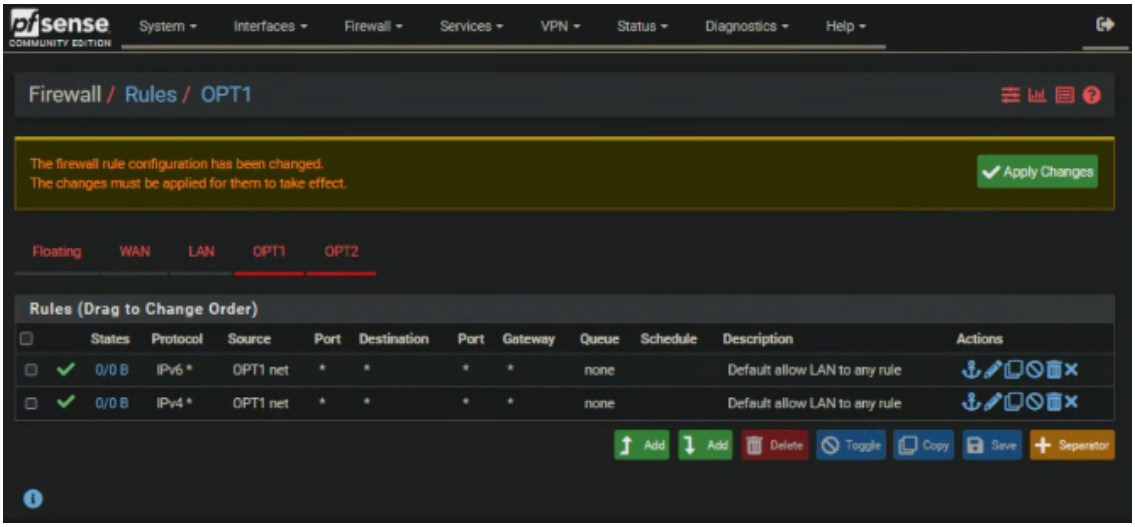
8. Faites "Add"



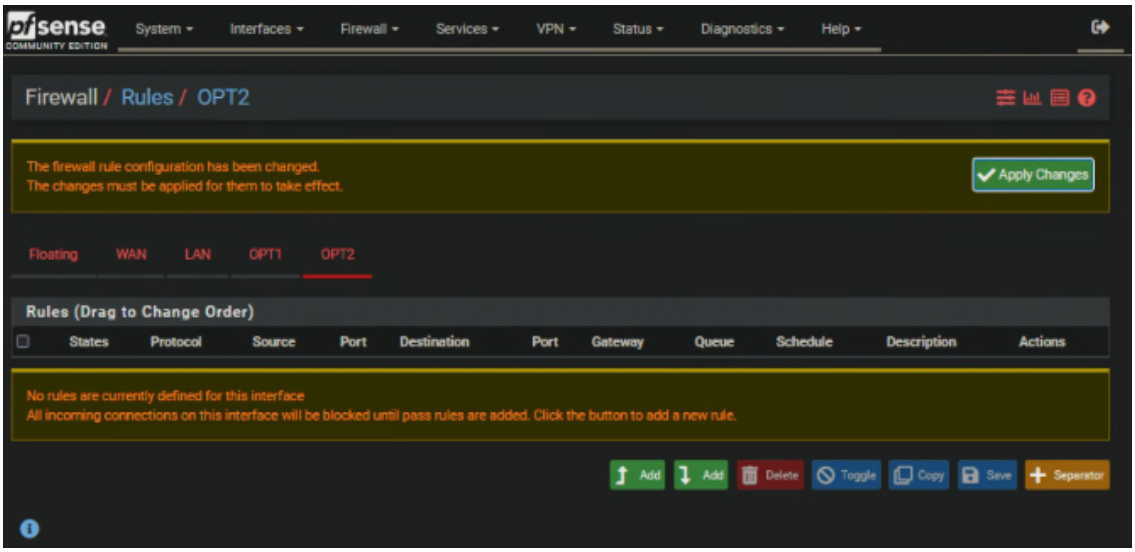
9. Changer l' "Address Family" en "IPv6"
10. Changer le "Protocol" en "Any"
11. Changer la "Source" en "OPT1 net"
12. Mettez "Default allow LAN to any rule" en description
13. Faites "Save"



14. Allez dans "OPT2"

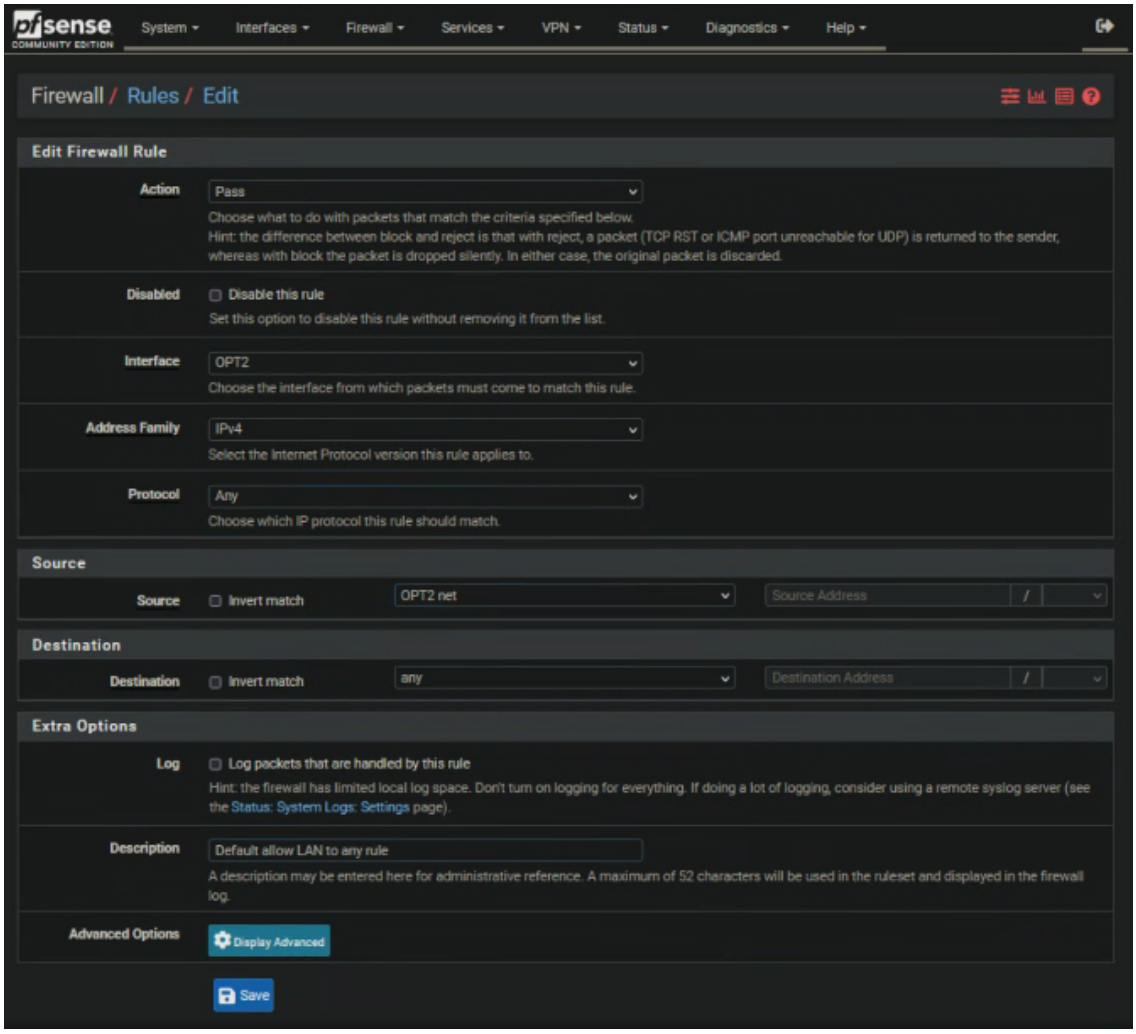


15. Faites "Add"

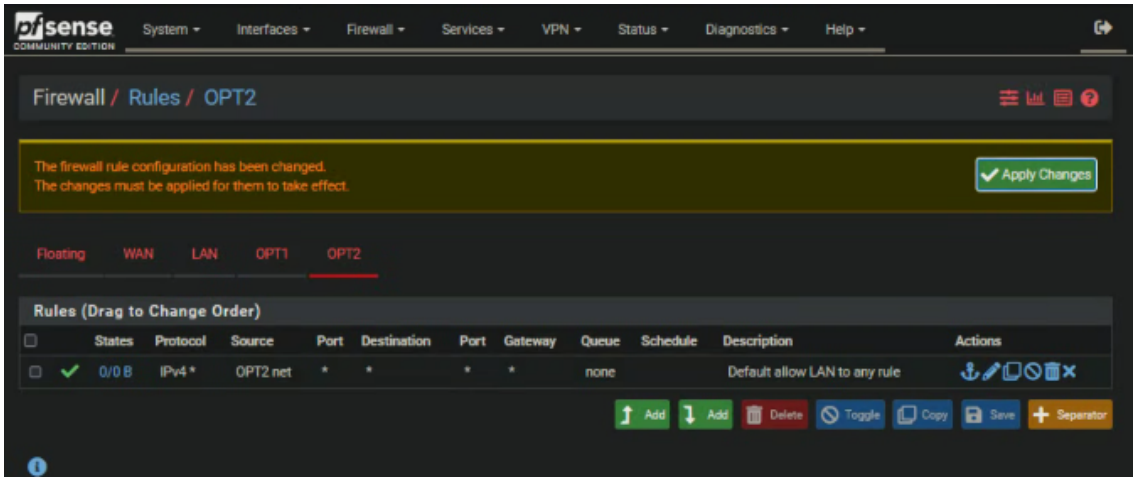


16. Changer le "Protocol" en "Any"
17. Changer la "Source" en "OPT2 net"
18. Mettez "Default allow LAN to any rule" en description

19. Faites "Save"

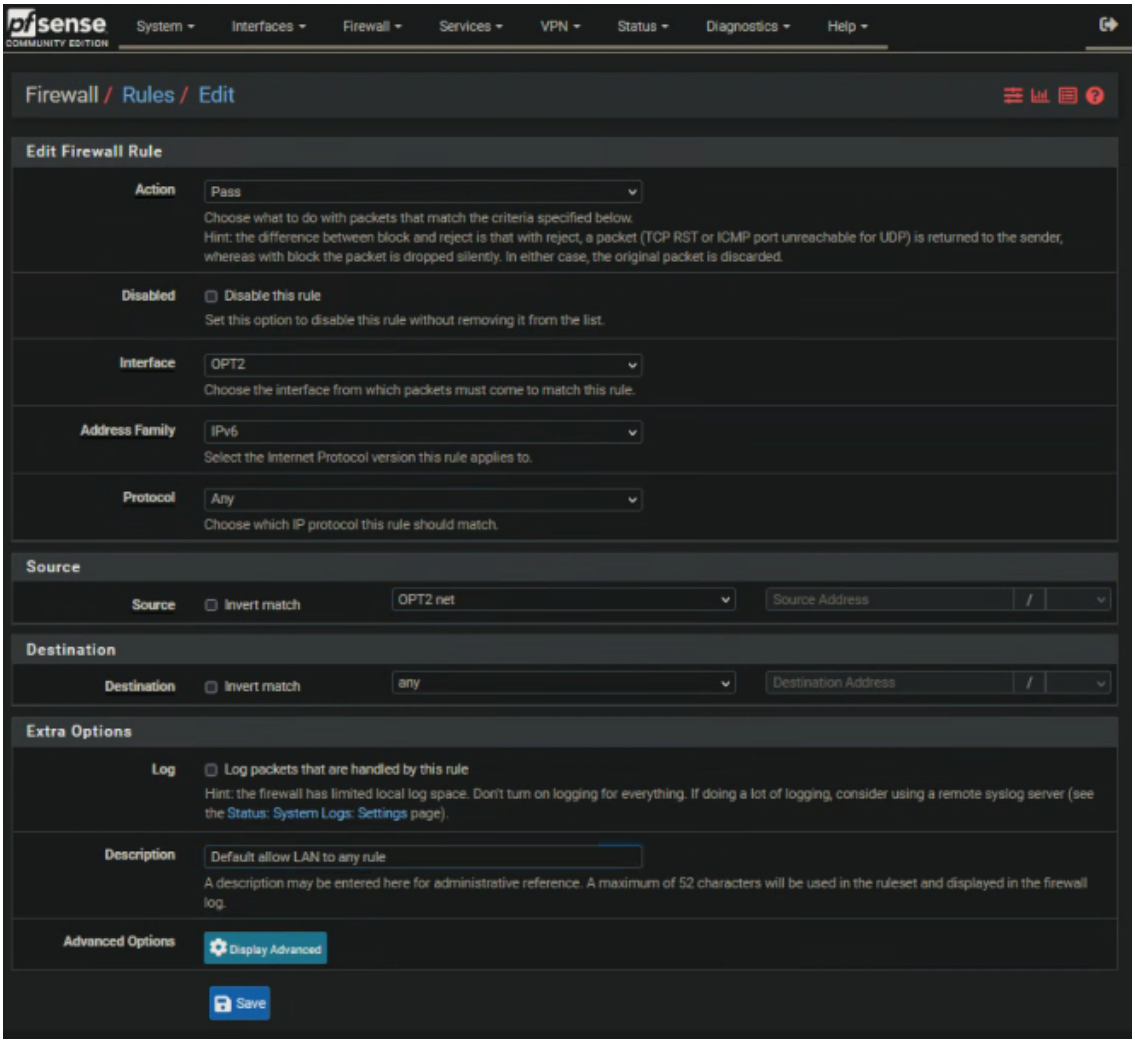


20. Faites "Add"

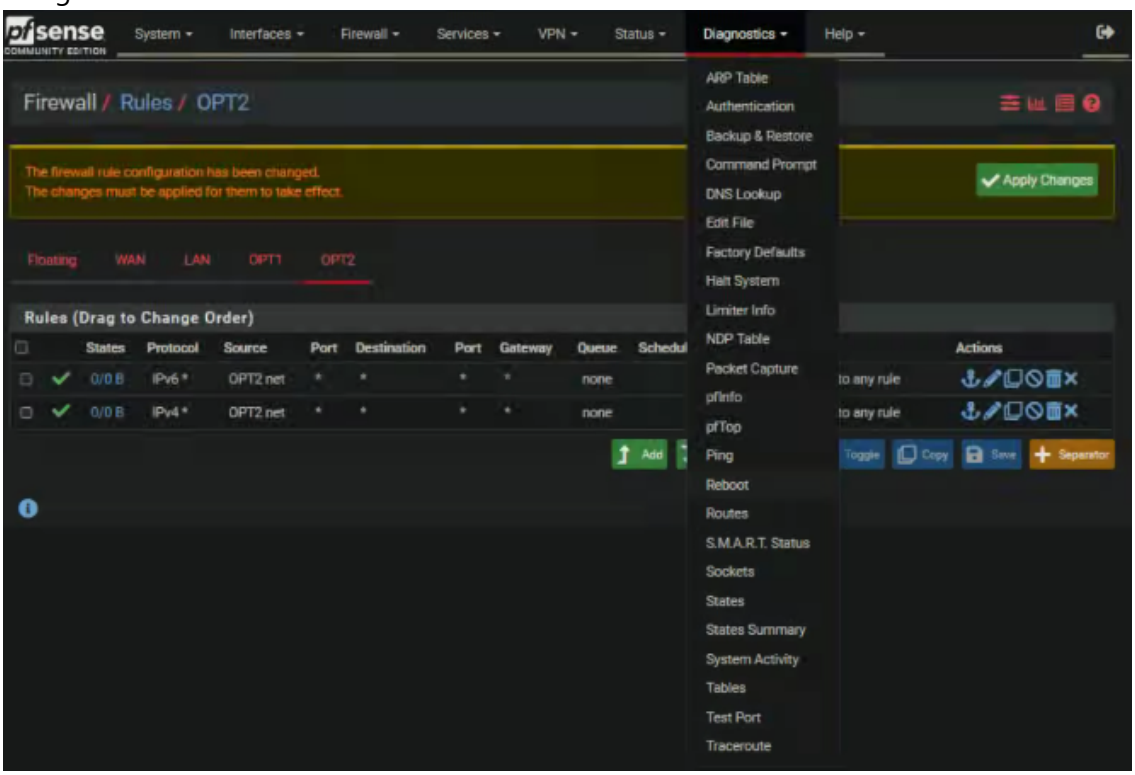


21. Changer l' "Address Family" en "IPv6"
22. Changer le "Protocol" en "Any"
23. Changer la "Source" en "OPT2 net"
24. Mettez "Default allow LAN to any rule" en description

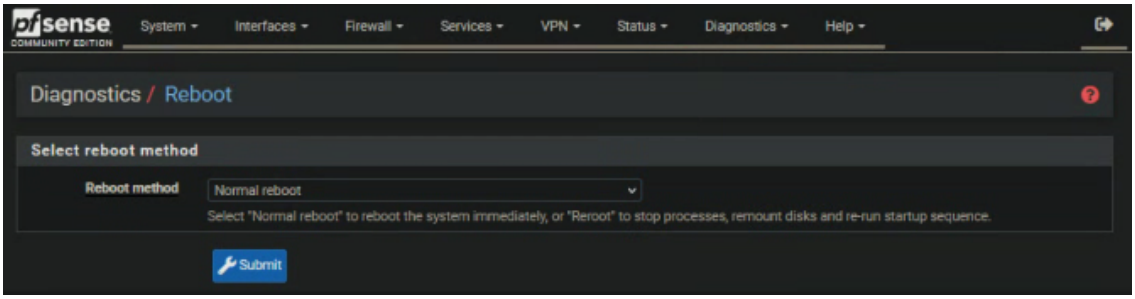
25. Faites "Save"



26. Redémarrez le serveur PfSense pour que tout les changements soient pris en compte : "Diagnostics" > "Reboot"



27. Faites "Submit" pour confirmer le redémarrage

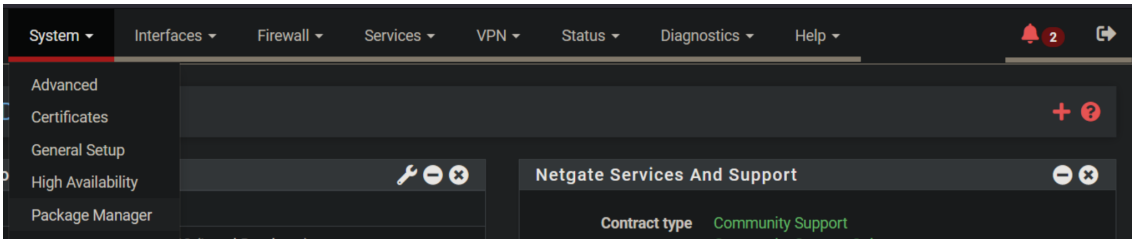


Configuration Applications

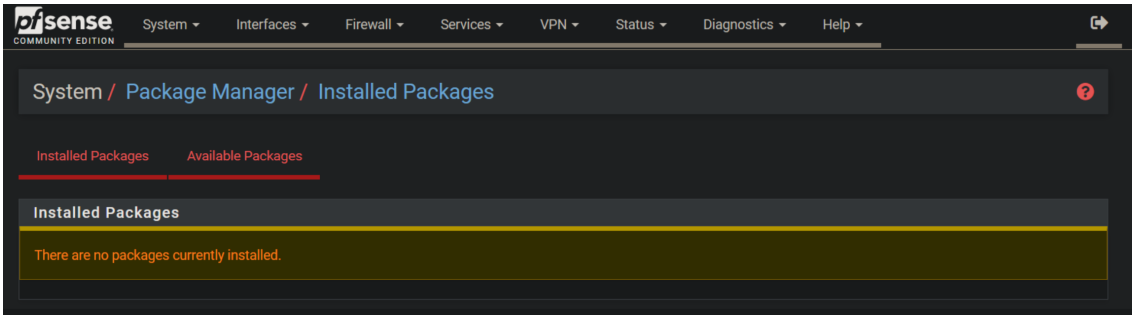
Il nous faut un packet qui puisse gérer la sécurisation du réseau, nous utilisons ici Suricata
Afin de pouvoir intervenir en CLI sur le PfSense à distance, il nous faut un accès SSH

Suricata

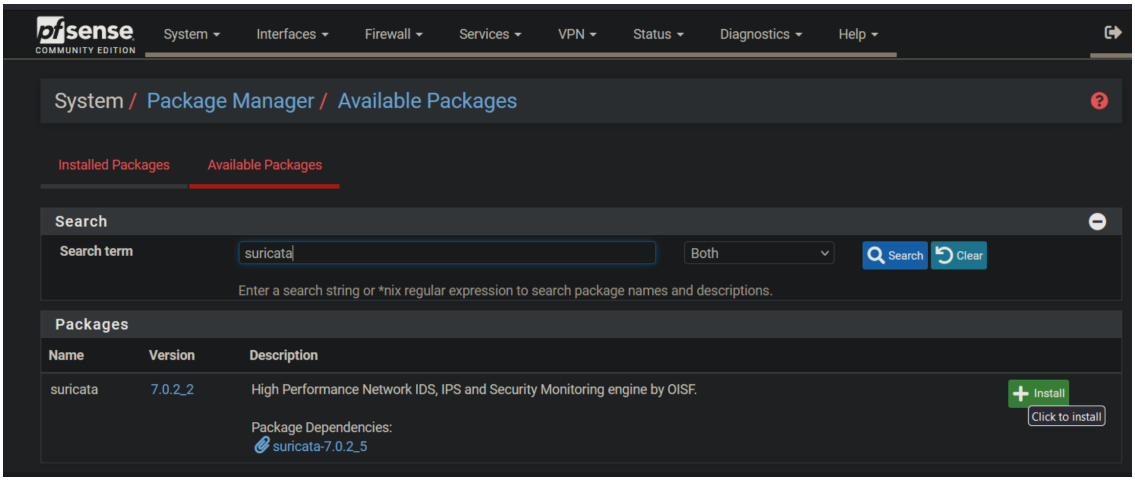
1. Allez dans "System" > "Package Manager"



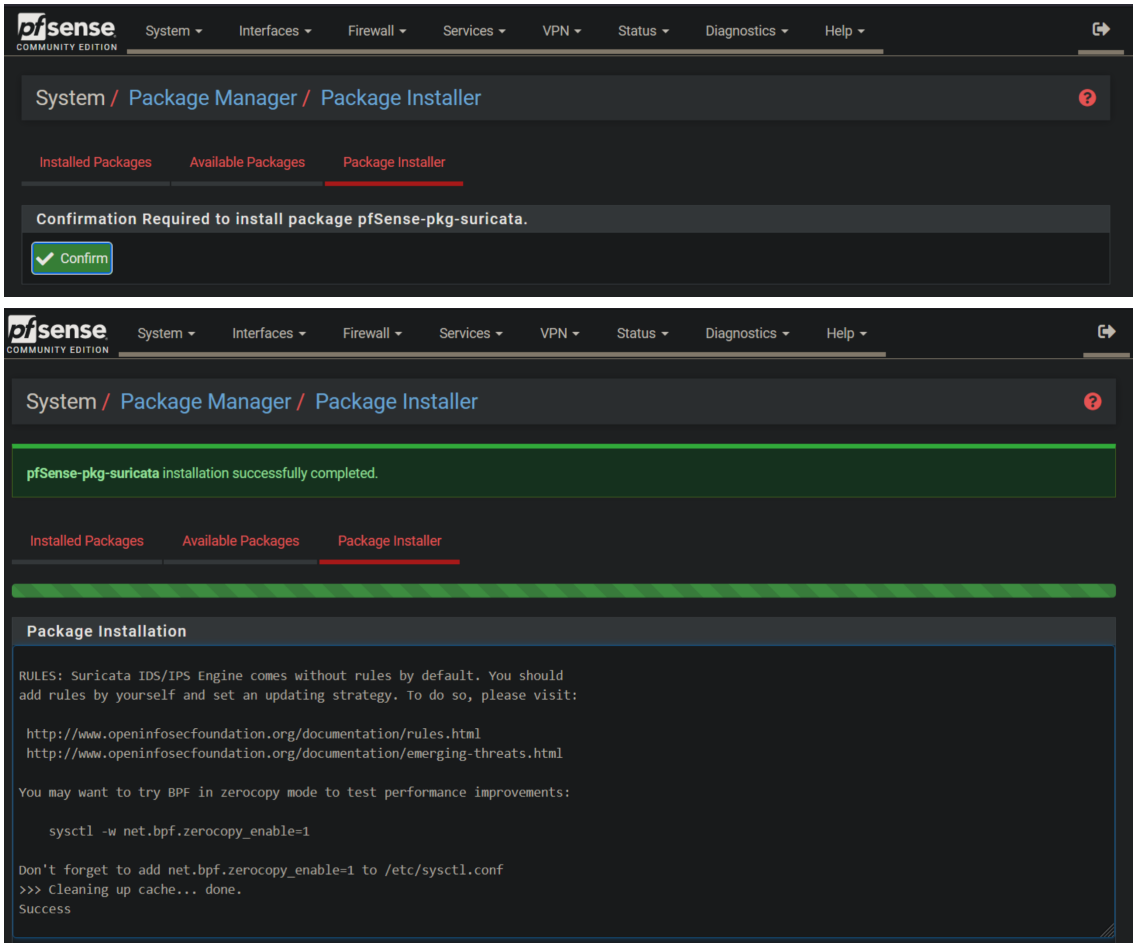
2. Allez dans "Available Packages"



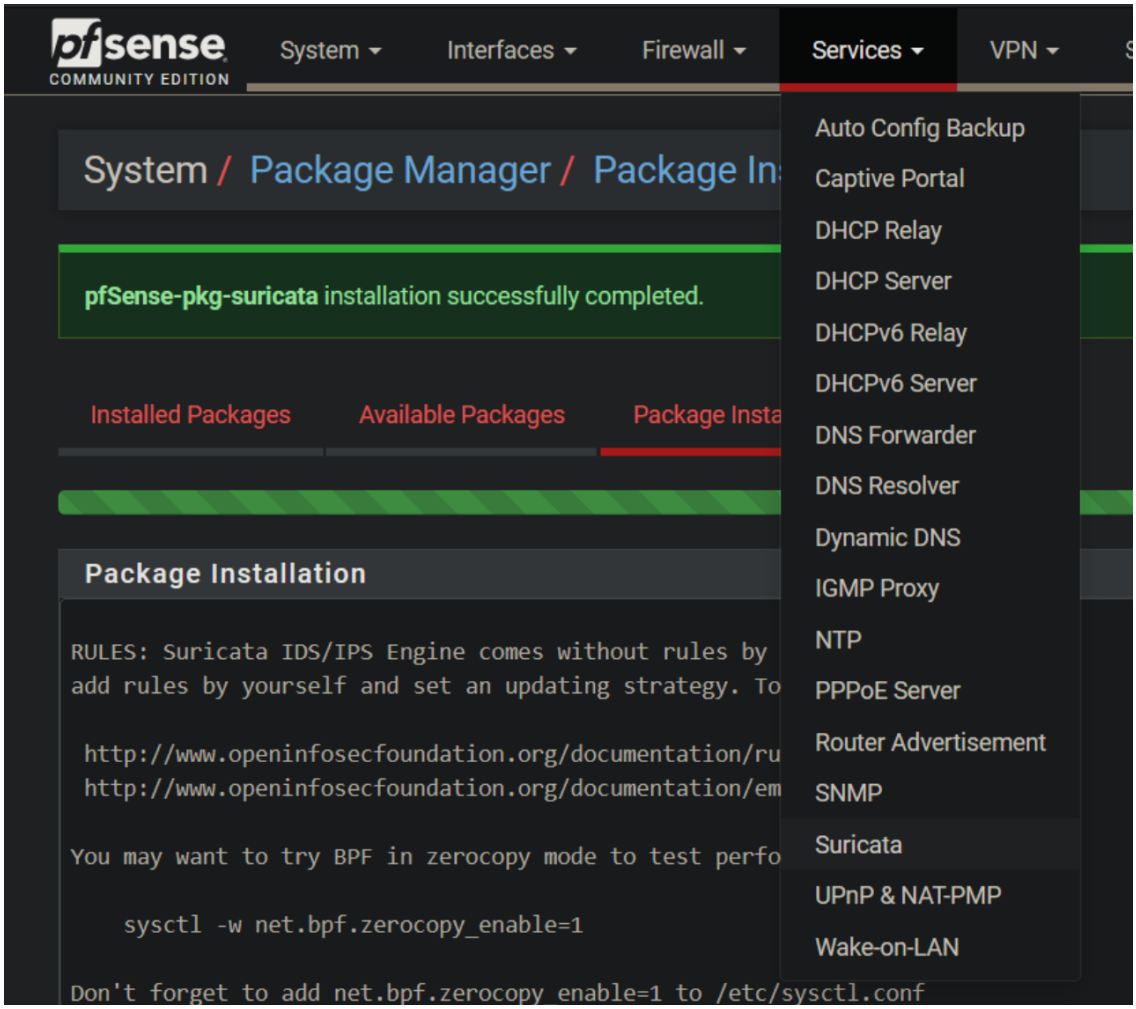
3. Cherchez "Suricata" puis faites "Install"



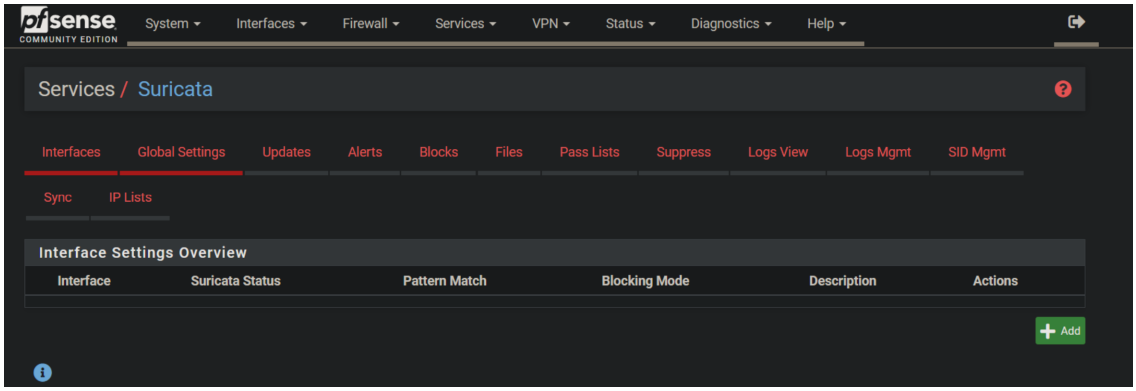
4. Faites "Confirm" pour lancer l'installation et attendez la fin de celle-ci



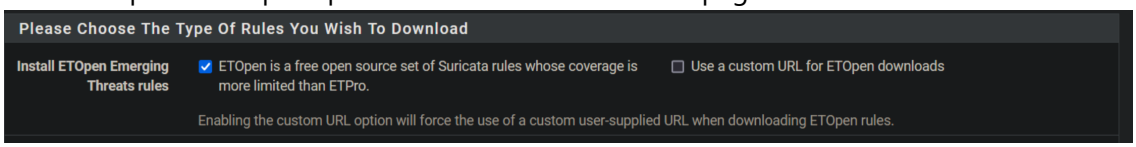
5. Allez dans "Services" > "Suricata"



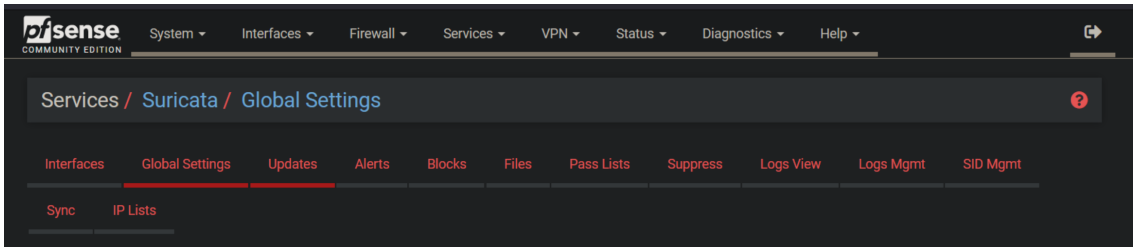
6. Allez dans "Global Settings"

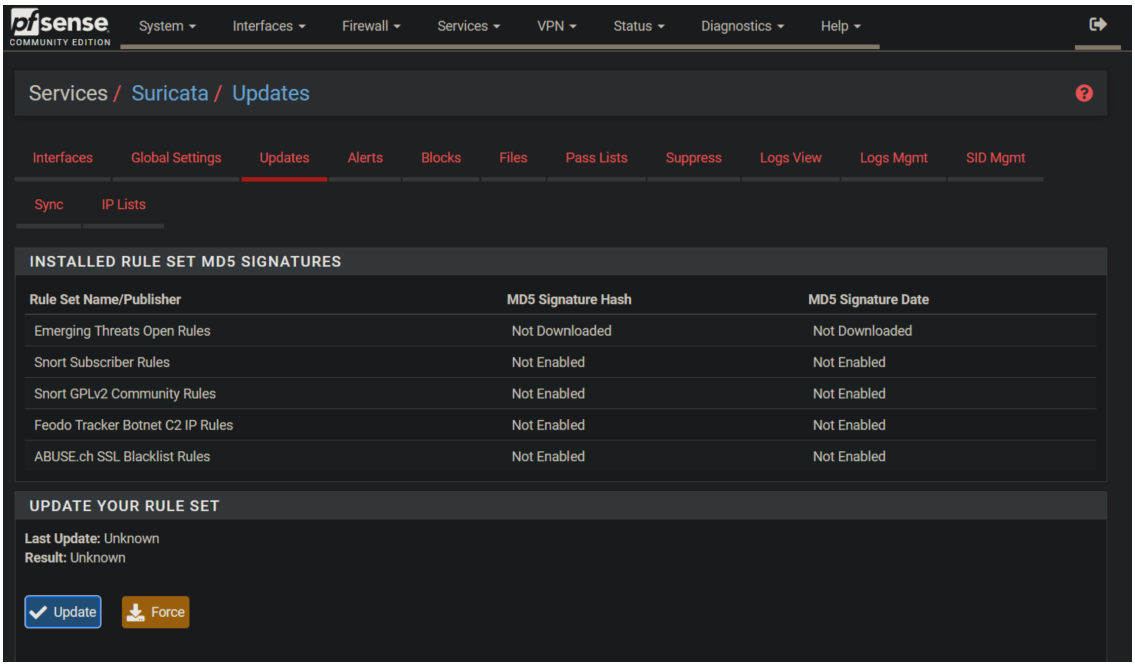


7. Activez l'option "ETOpen" puis faites "Save" en bas de la page

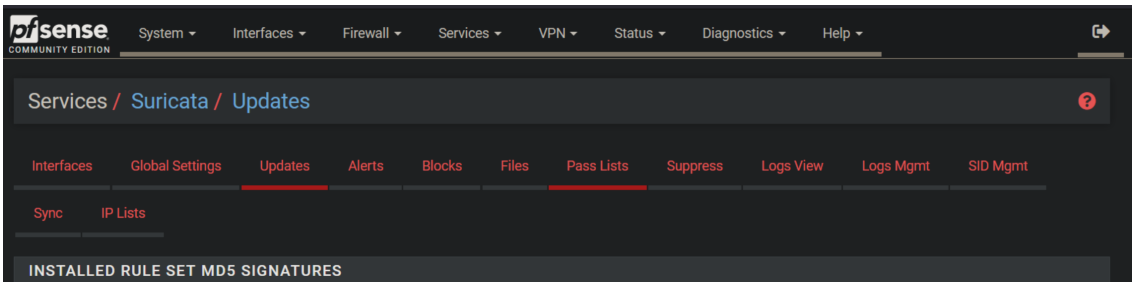


8. Allez ensuite dans "Updates" puis faites "Update"

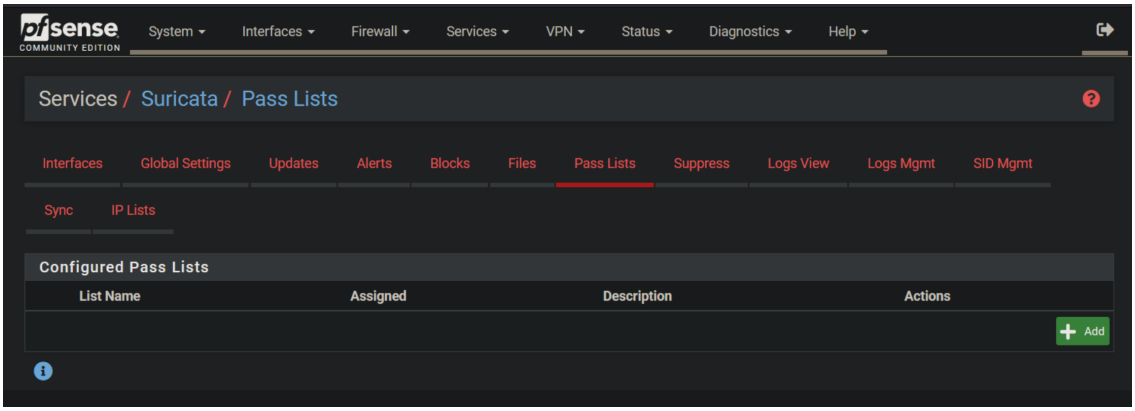




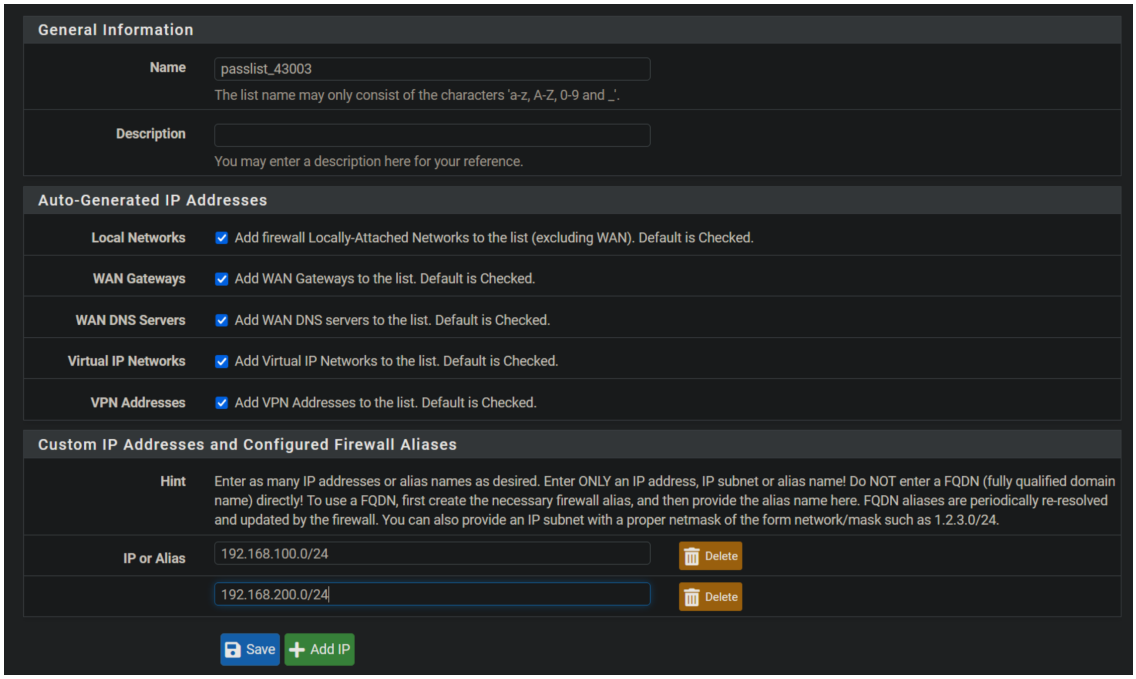
9. Une fois la pop-up fermée automatiquement, allez dans "Pass Lists"



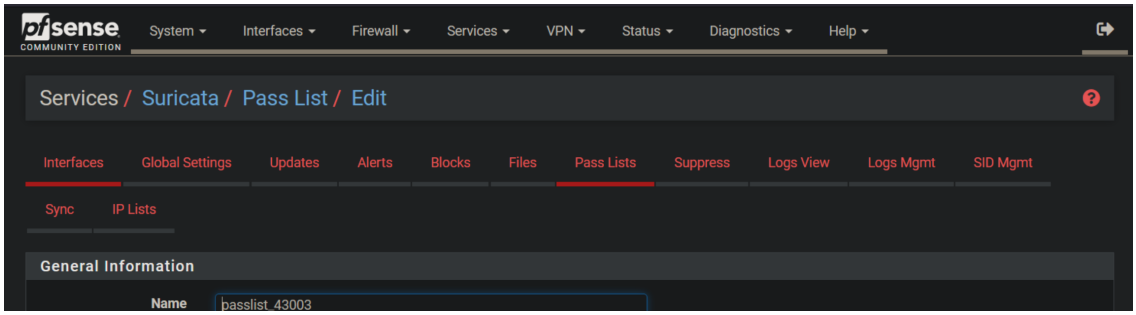
10. Faites "Add"



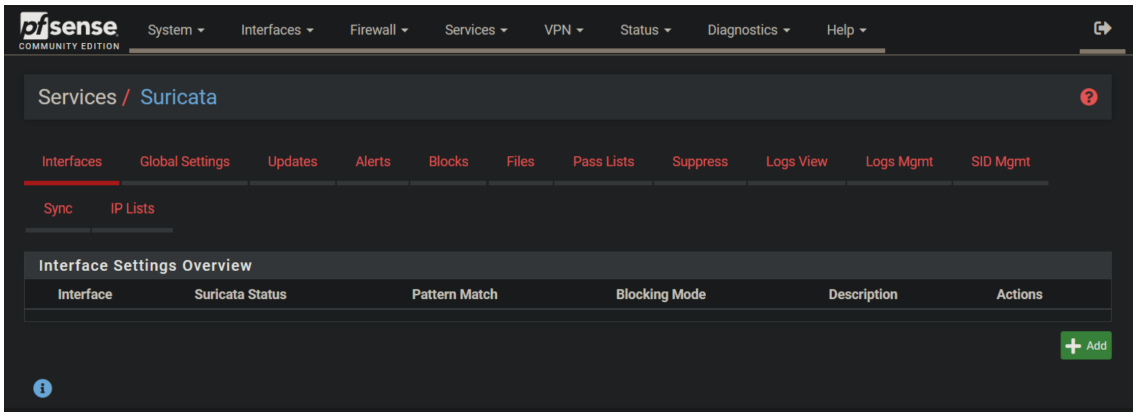
11. Ajoutez les deux réseaux, 192.168.100.0/24 et 192.168.200.0/24 et faites "Save"

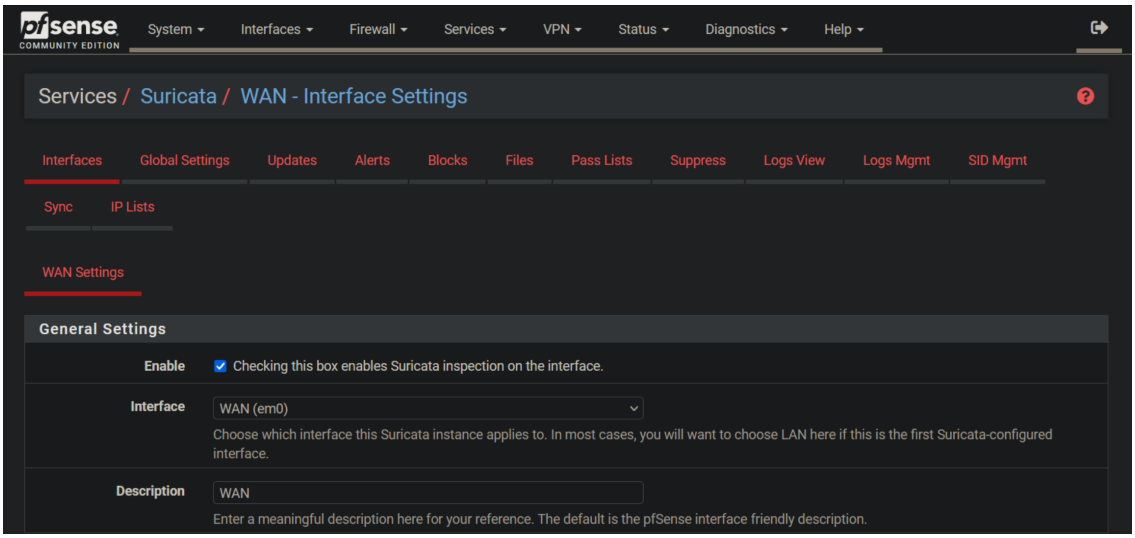


12. Allez dans "Interfaces"



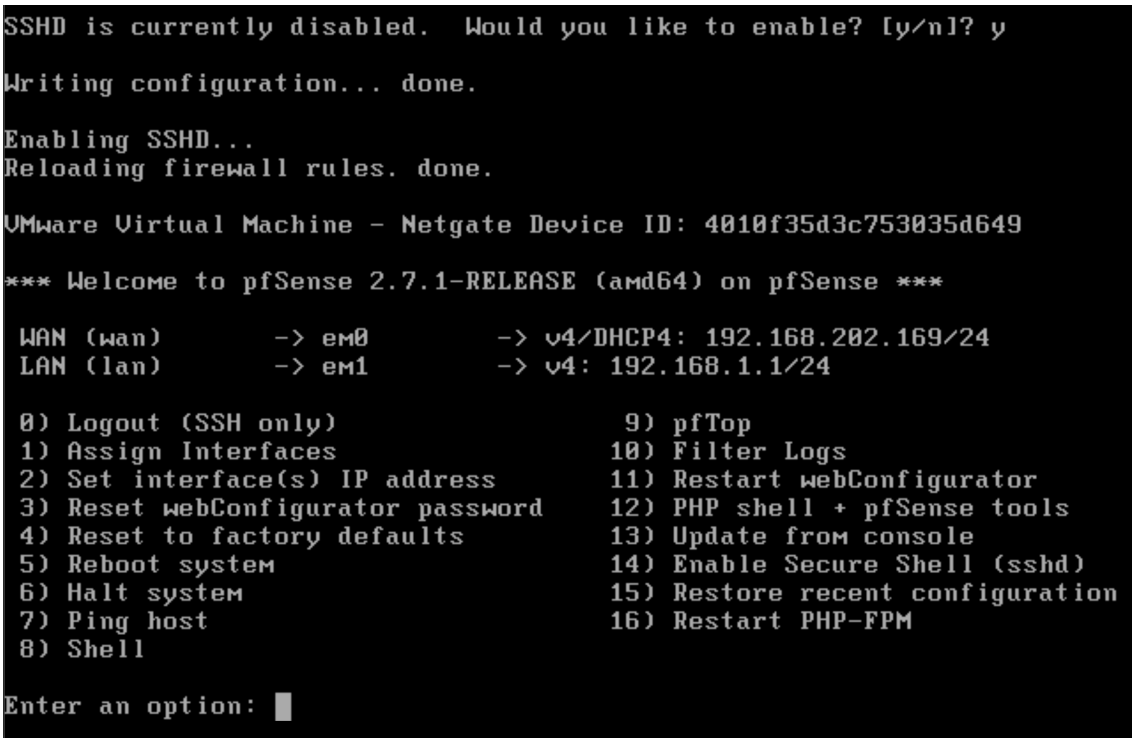
13. Enfin, faites "Add" puis allez en bas de la page et faites "Save"



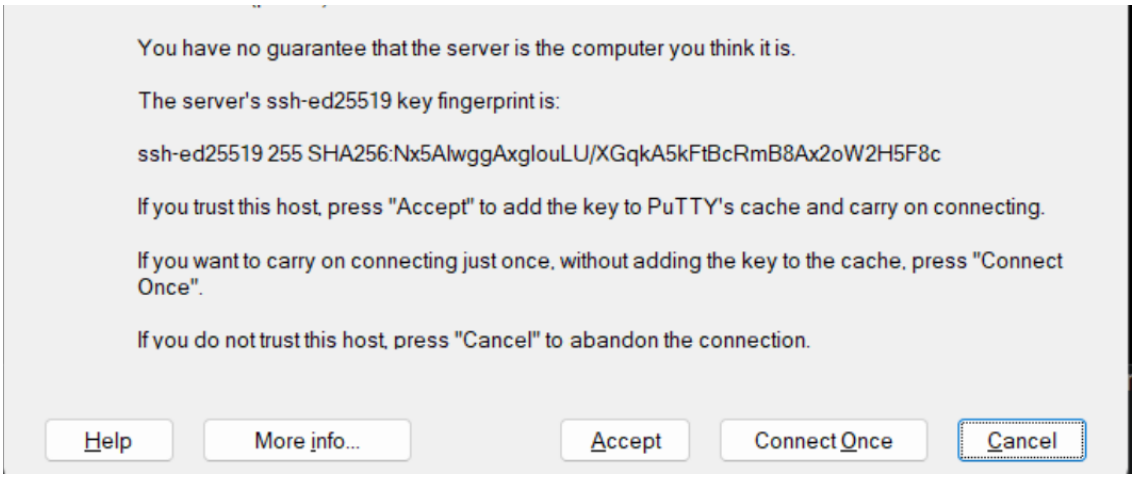


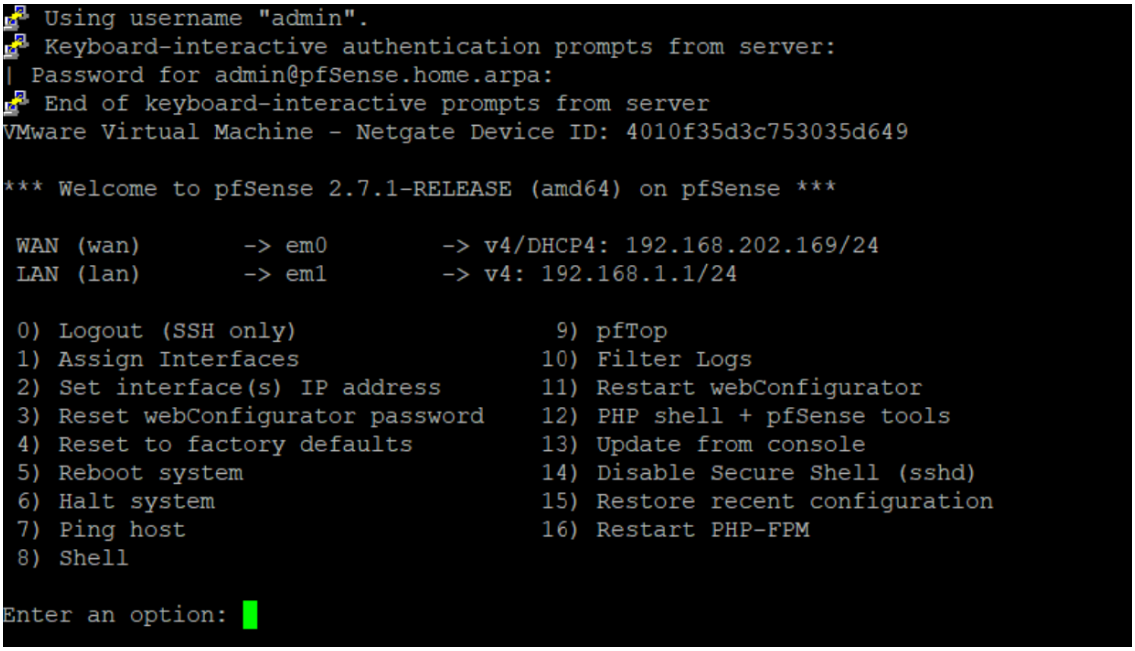
SSH

1. Connectez vous sur le PfSense physiquement
2. Tapez "14"



3. Il est désormais possible de se connecter en SSH par l'adresse 192.168.100.254 avec les identifiants du PfSense, acceptez la clé SSH pour vous connecter


You have no guarantee that the server is the computer you think it is.
The server's ssh-ed25519 key fingerprint is:
ssh-ed25519 255 SHA256:Nx5AlwggAxglouLU/XGqkA5kFtBcRmB8Ax2oW2H5F8c
If you trust this host, press "Accept" to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, press "Connect Once".
If you do not trust this host, press "Cancel" to abandon the connection.
Help
More info...
Accept
Connect Once
Cancel


Using username "admin".
Keyboard-interactive authentication prompts from server:
Password for admin@pfSense.home.arpa:
End of keyboard-interactive prompts from server
VMware Virtual Machine - Netgate Device ID: 4010f35d3c753035d649
*** Welcome to pfSense 2.7.1-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 192.168.202.169/24
LAN (lan) -> em1 -> v4: 192.168.1.1/24
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Disable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option: