Installation & Configuration d'un DNS, DHCP, Firewall et protocole CARP sous pfSense avec redondance.

Table des matières

1) Introduction

PfSense est un système d'exploitation à part entière, open source, utilisé pour mettre en œuvre un pare-feu, un routeur ou une solution permettant la fourniture d'autres services réseaux. PfSense est une distribution FreeBSD 1 personnalisée, et basée initialement sur le projet m0n0wall, distribution de pare-feu puissant mais léger. PfSense s'appuie sur le principe de base de m0n0wall et reprend la plupart de ses fonctions, en prenant soin de mieux les faire cohabiter, de les sécuriser, de les stabiliser, tout en favorisant la compatibilité du système afin d'y ajouter une variété d'autres services liés essentiellement aux réseaux.

Ce compte-rendu, explique la configuration de base et nécessaires à la quasi-totalité des déploiement, nous verrons les configuration des différents servie, tout en respectant les bonne pratiques.

A son niveau de base, un pfSense peut être utilisé pour remplacer le routeur d'un réseau domestique et pour fournir des fonctionnalités supplémentaires.

Une fois celui-ci installer et configuré, il existe 2 de façons d'y accéder à l'*OS :

- *Par Interface web : http://@IP
- Par SSH : @IP : *22

---

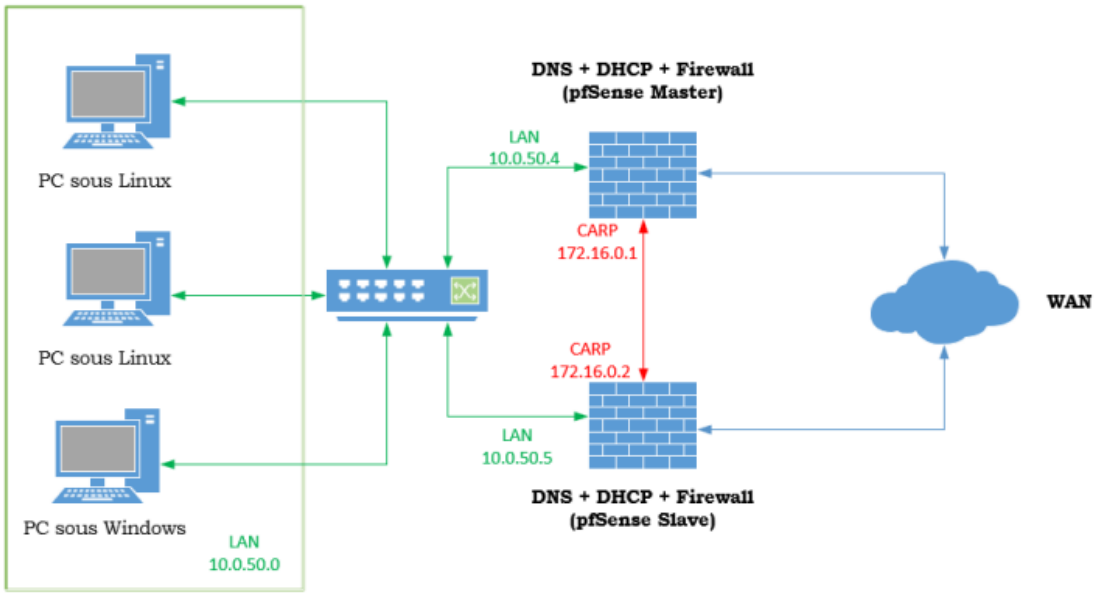
*OS : Operating System ou Système d'exploitation en Français.

*22 : Port par défaut de SSH.

*Interface Web : On verra que par défaut, on accède à l'interface par le protocole http (:80) qui n'est pas sécurisé. Pour des questions de bonne pratiques, nous verrons que ce port sera changer enfin d'y accéder via https (:443).

1.1) Prérequis

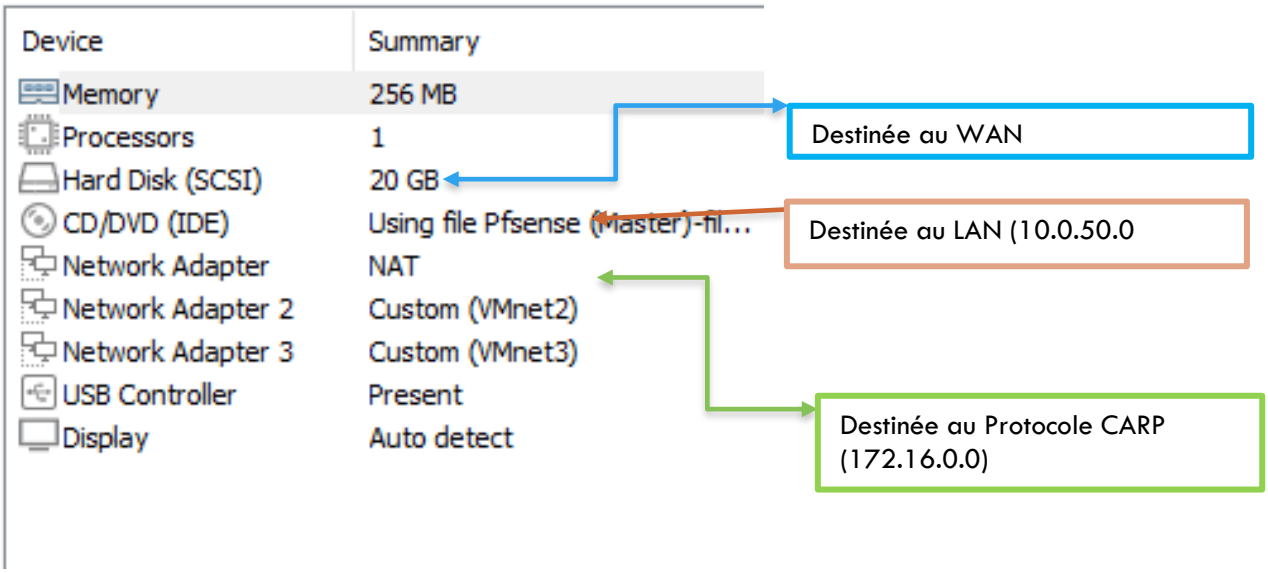
Pour réaliser cette installation nous avons besoin d'une infrastructure virtuelle sous l'applicatif VMware ou VirtualBox ou encore EXsi.



SCHEMA DE NOTRE INFRASTRUCTURE

1.2) Installation de pfSense

Pour l'installation de pfSense, Il faudra configurer notre VM de cette façon (Réalisé sous VMWare Workstation 17) :



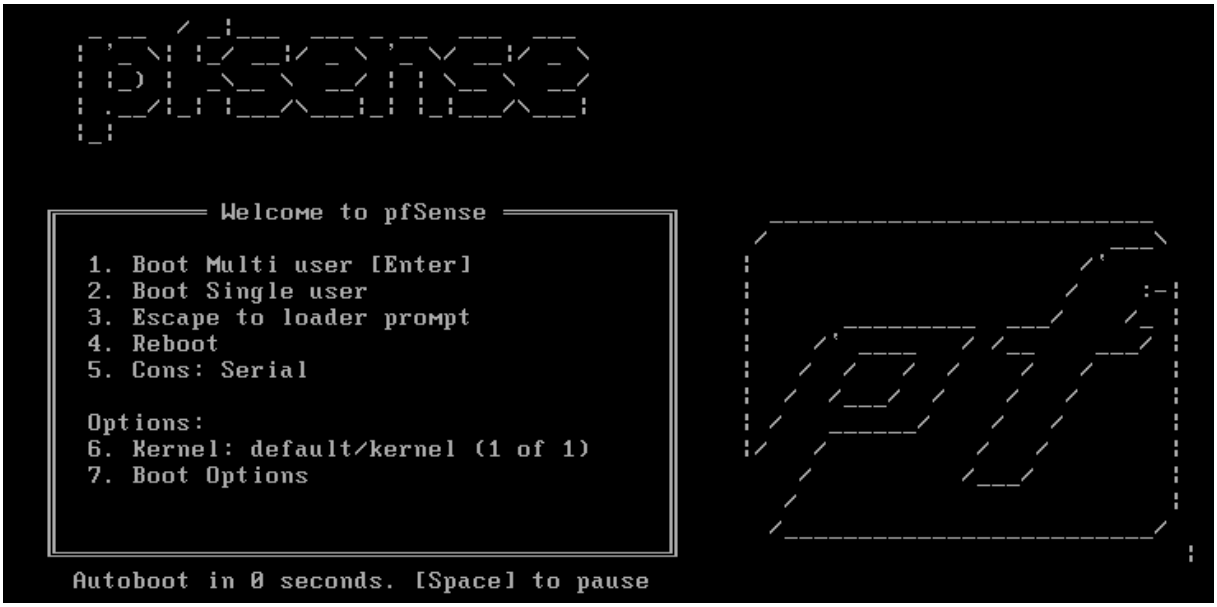
INFO : Pas Besoin d'une grosse configuration matérielle, on peut donc mettre le minimum requis (256MB).

.FREESD (=

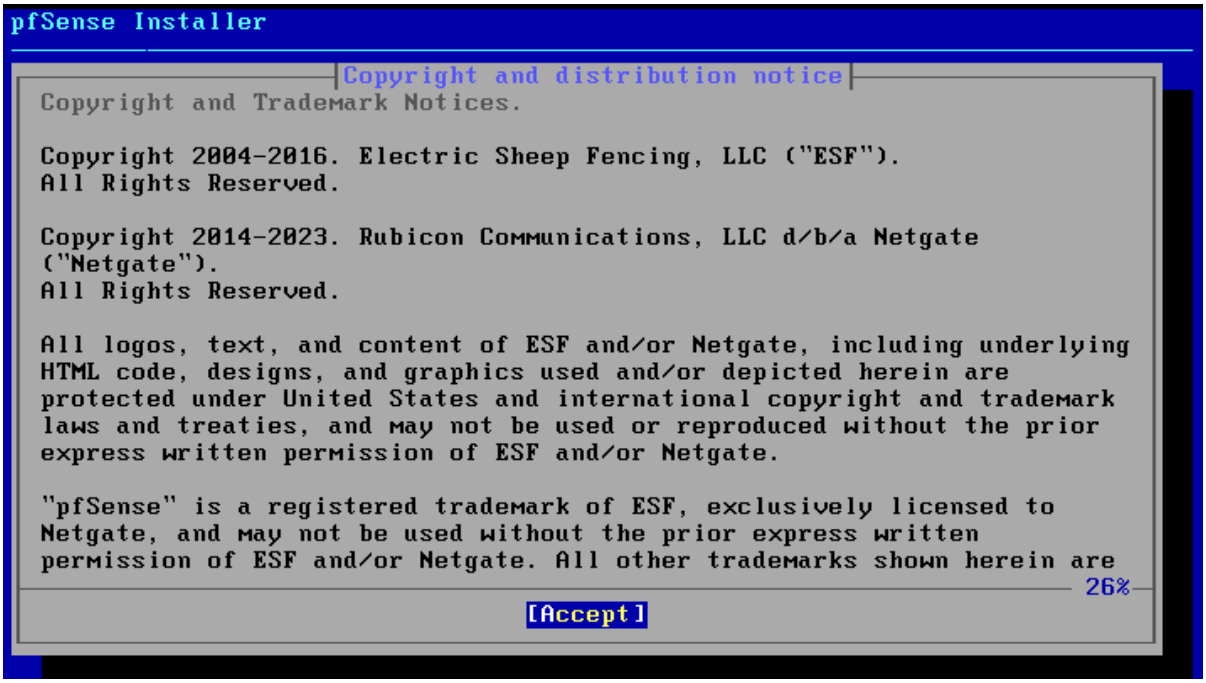
Pour l'ISO de pfSense, il suffit de se rendre sur :
https://www.pfsense.org/download/

(Version actuelle de mon installation : 2.7.2)

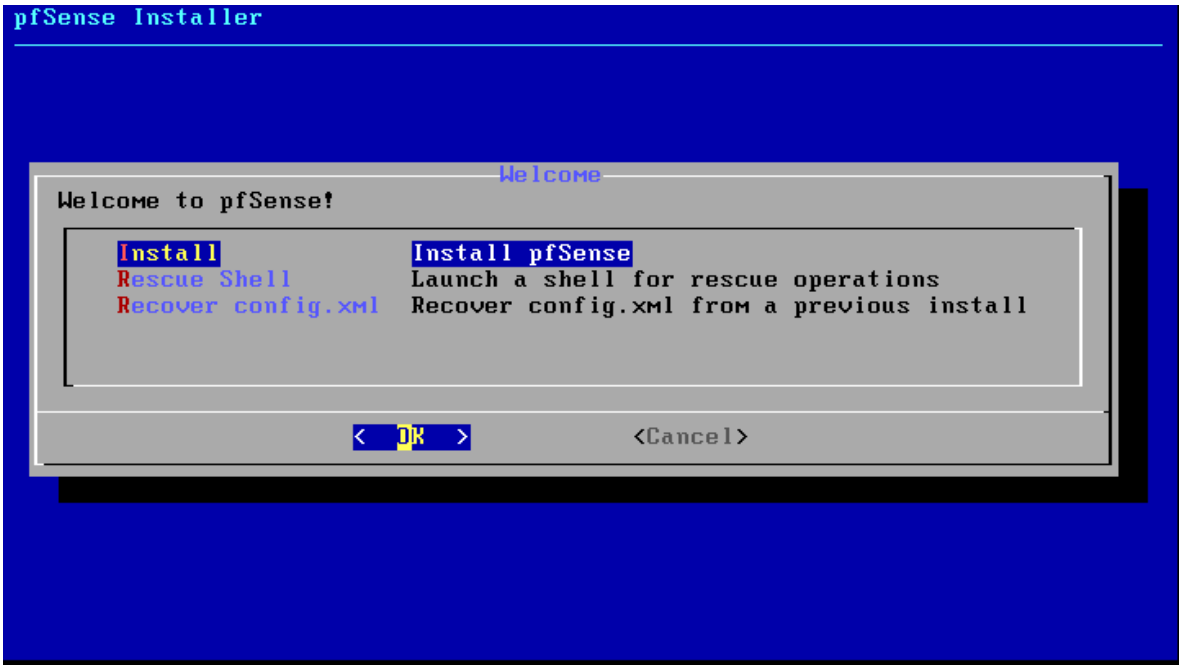
Après avoir insérer l'ISO, nous pouvons démarrer la machine, le setup va démarrer automatiquement après quelques secondes.



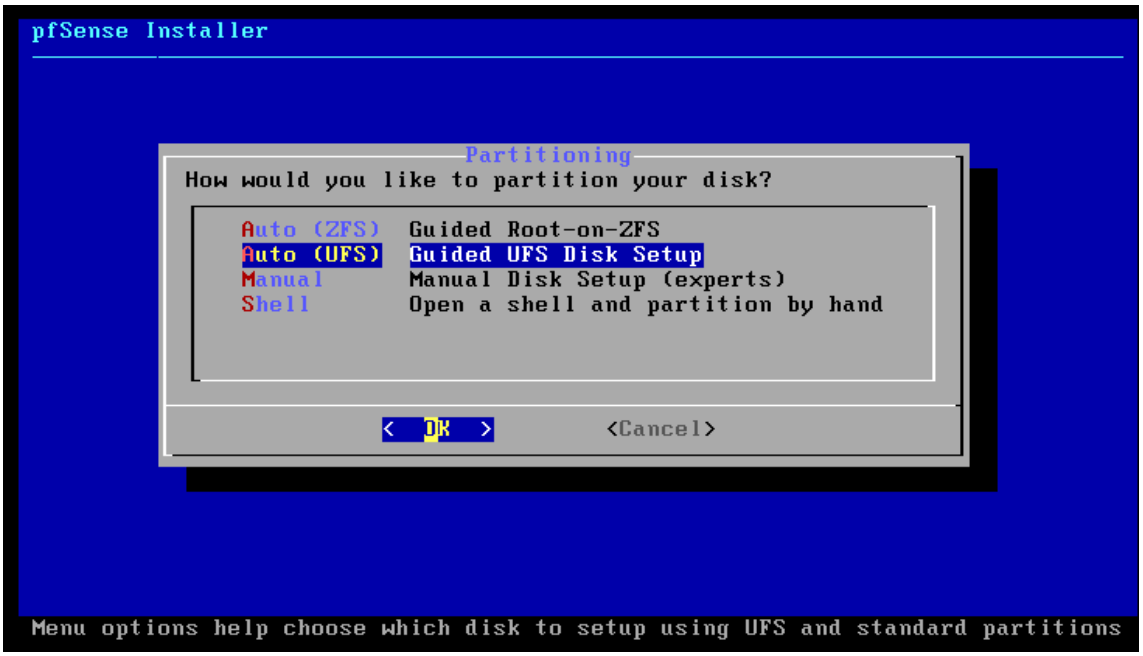
⚠ Important : L'installation va s'effectuer au clavier. Appuyez sur la touche Entrée pour Accepter.



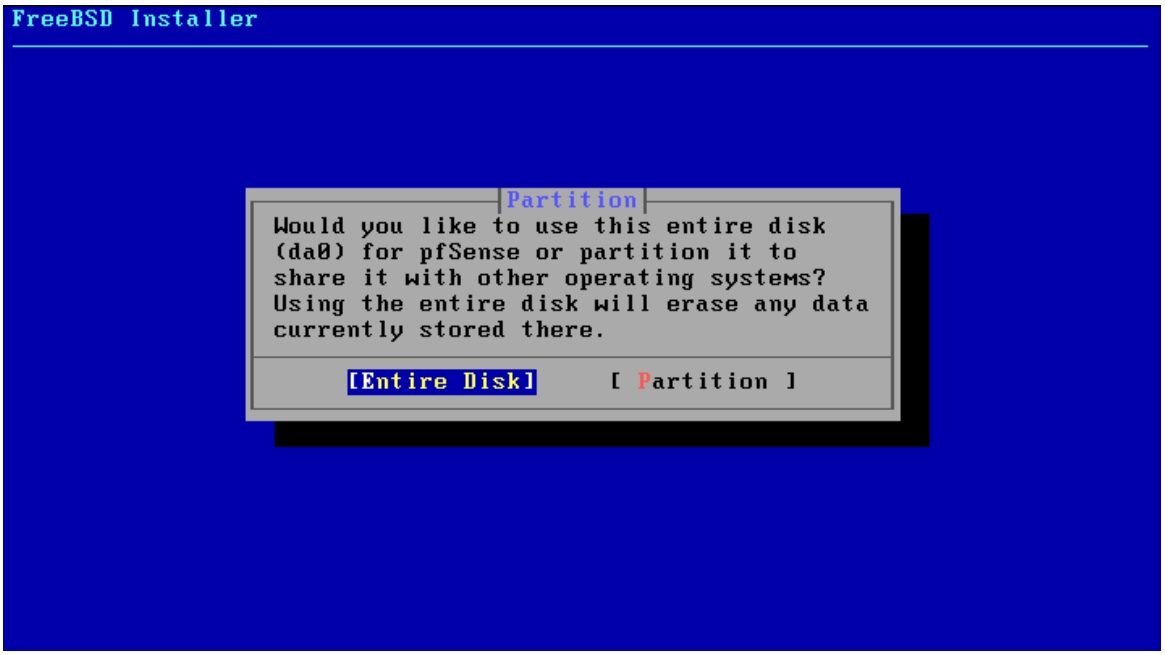
Vérifier que vous êtes bien sur l'onglet **Install,** sinon déplacez vous avec les flèches de votre clavier « ↑↓ » et appuyez sur **Entrée pour faire OK.**

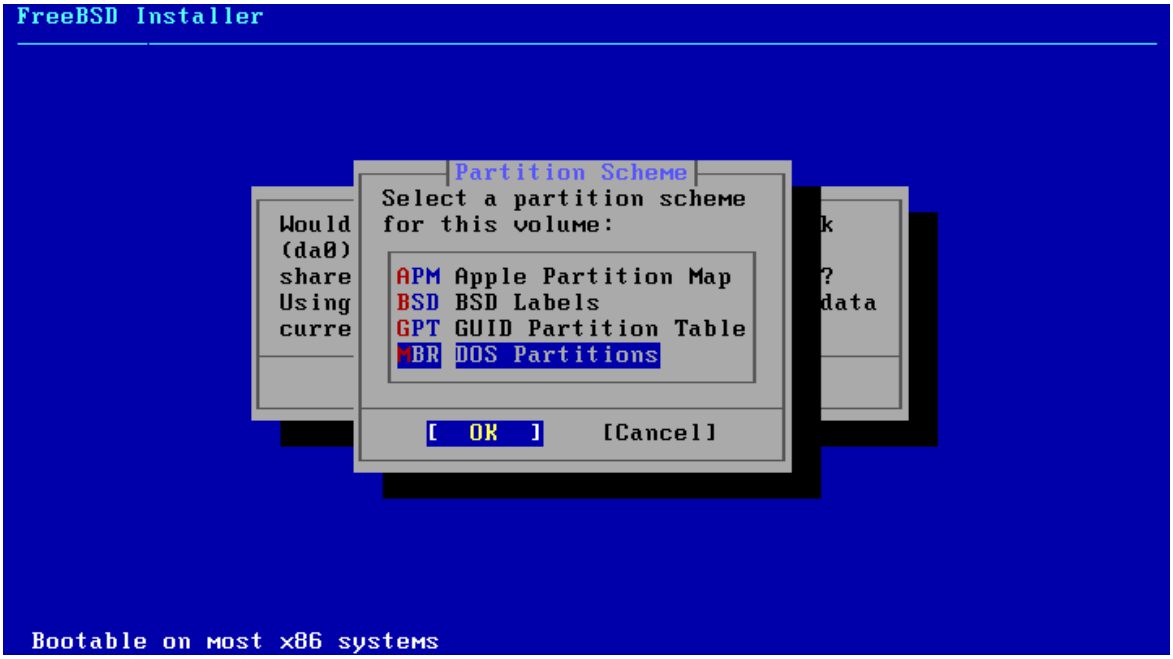


Le setup va vous demander de **partitionner le disque** de stockage de la machine. Avec les touches fléchées de votre clavier, allez sur **« Auto (UFS) » et appuyez sur Entrée.**

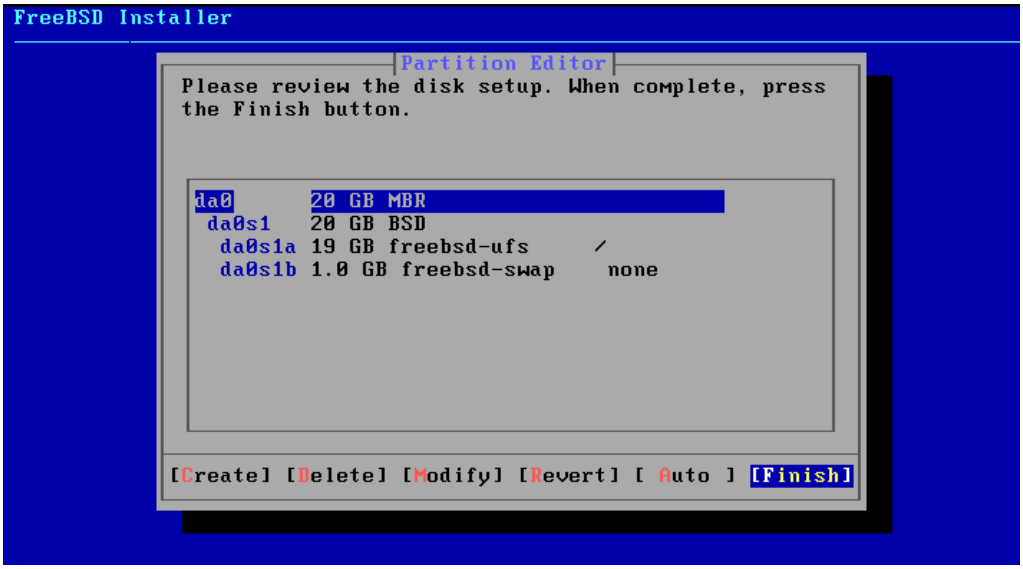


Séléctionner [Entire Disk] ou [Partitions] (nécessite des connaissances)



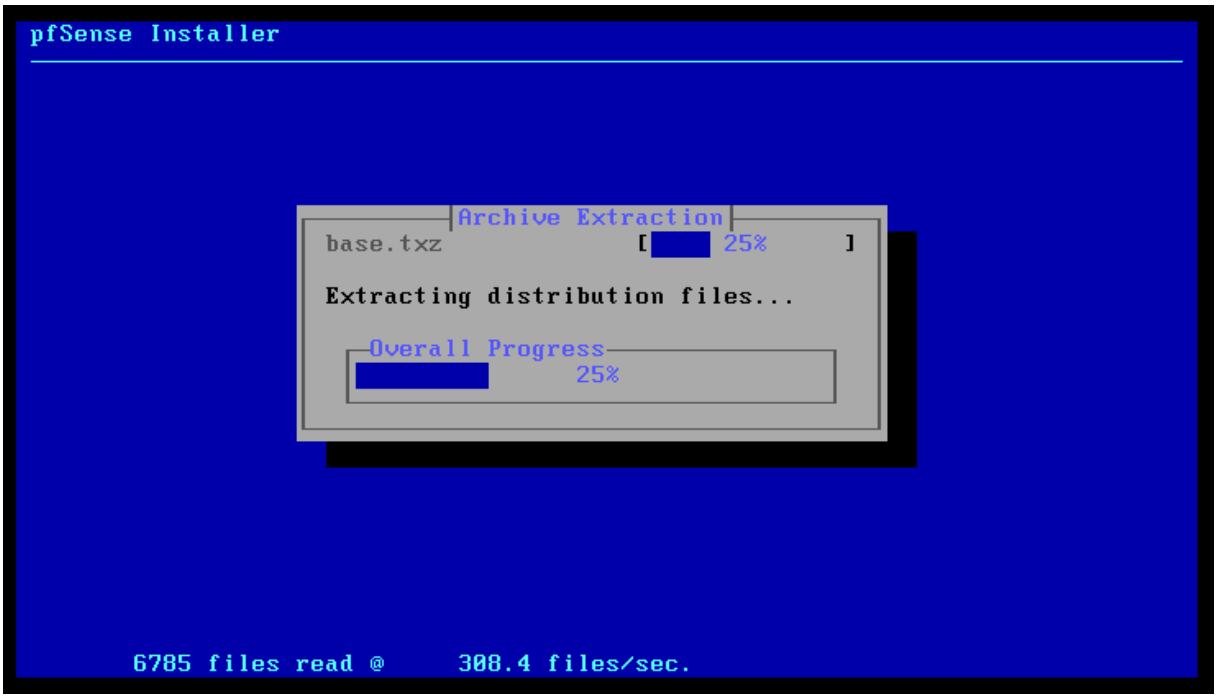


Installateur nous propose un découpage sur le disque 0 (nommé ici da0), nul besoin de modifier celle-ci, sélectionner Finish puis Entrée.

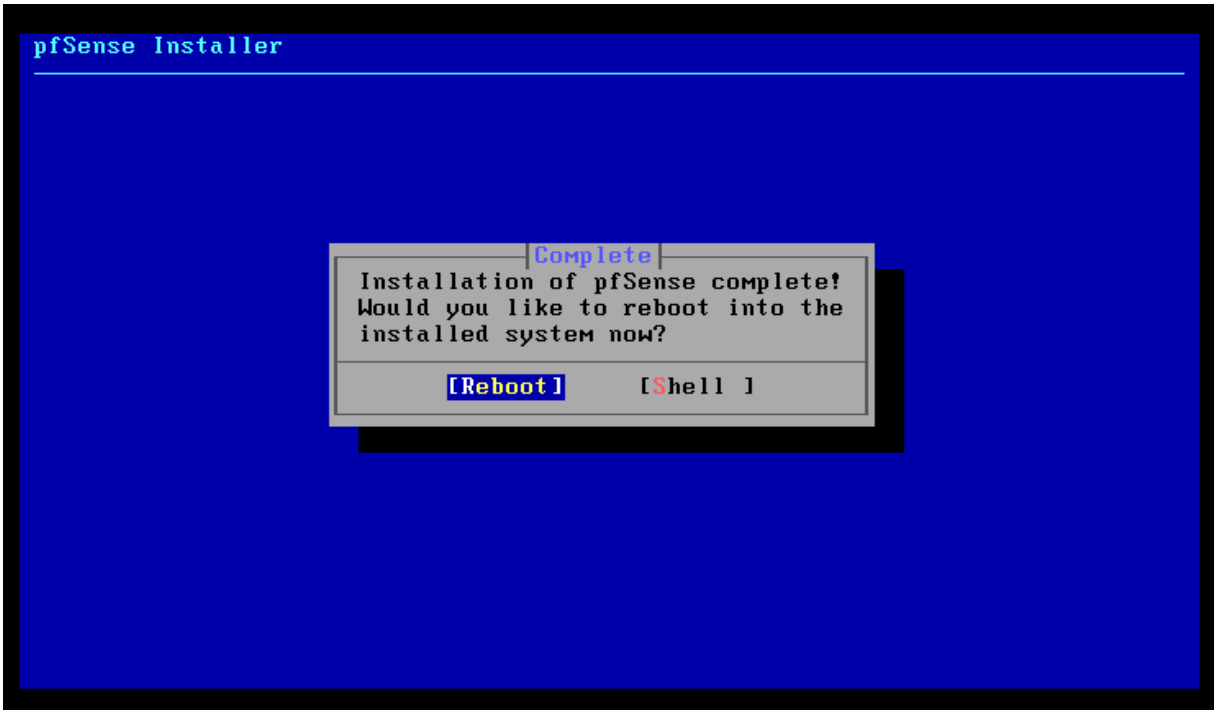


Un dernier avertissement pour demander si on est sûr que le disque sera effacé pour l'installation de pfSense.

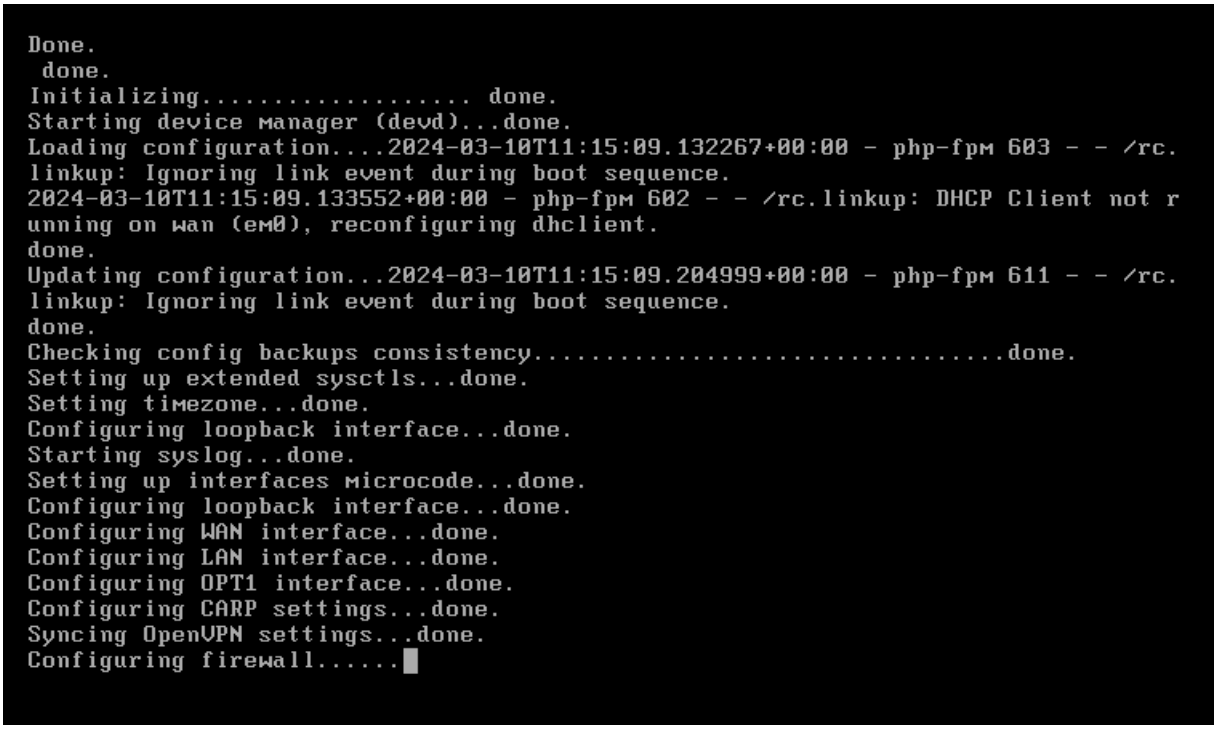
L'Installation est en cours……



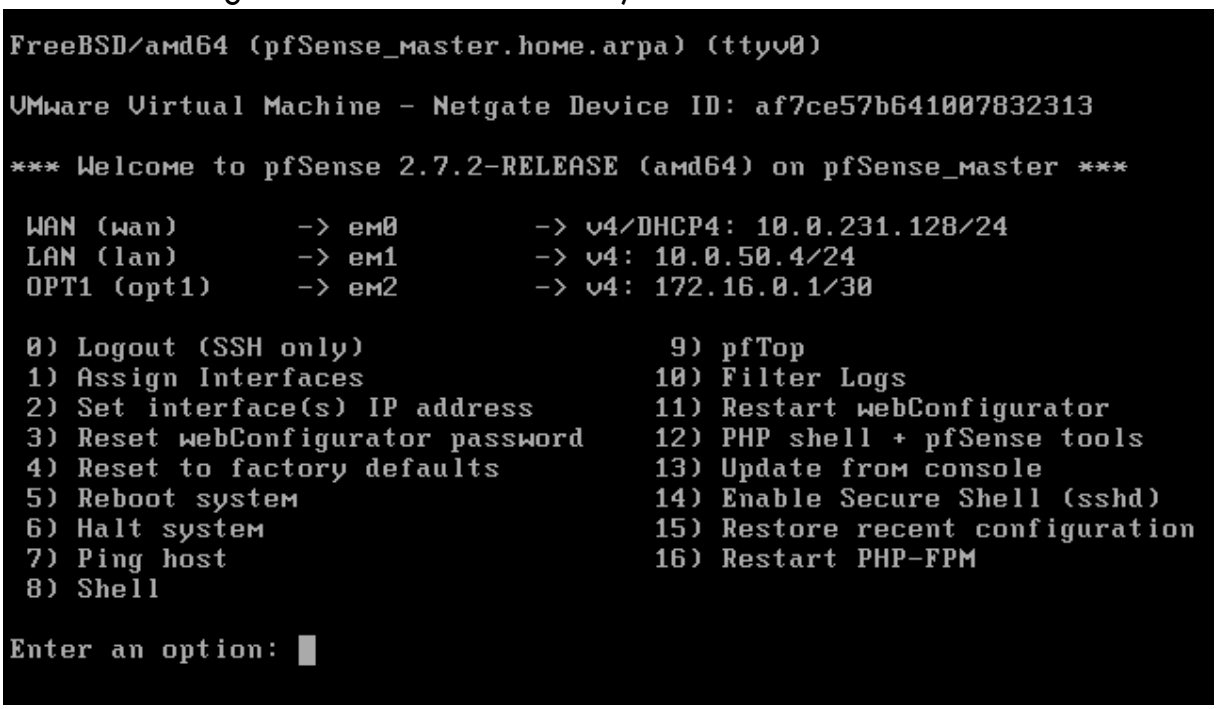
Sélectionner Reboot ou Shell (si vous souhaitez apporter des modifications)



A son lancement, pfSense va charger ce qu'il a besoin pour son fonctionnement. (Services)



Une fois le démarrage fini, on obtiendra ceci (Configuration qu'on doit obtenir à la fin des configurations de nos interfaces) :



⚠ Important : Le clavier est par défaut en qwerty !

Pour la configuration de nos interfaces on sélectionne option 2 **« Set interface(s) IP address »**

```
 0) Logout (SSH only)
 1) Assign Interfaces
 2) Set interface(s) IP address
 3) Reset webConfigurator passw
 4) Reset to factory defaults
 5) Reboot system
 6) Halt system
 7) Ping host
 8) Shell
```

On me demande quelle interface je souhaite configurer (2 – LAN).

```
Available interfaces:

1 - WAN (em0 - dhcp)
2 - LAN (em1 - static)
3 - OPT1 (em2 - static)

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

Em0 -> Network Adapter

Em1 -> Network Adapter 2 (10.0.50.0)

Em2 -> Network Adapter 3 (172.16.0.1-2)

qu'on va l'attribuer manuellement, on sélectionne « n » pour répondre Non et on appuie sur Entrée.

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

Ensuite on saisit l'adresse IP qu'on souhaite attribuer à cette interface qui sera la passerelle de sortie de notre réseau local (LAN). Une fois l'adresse IP saisi on appuie sur Entrée pour passer à la suite.

```
Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 10.0.50.4
```

On définit le masque du sous-réseau en notation CIDR, 24 pour notre infrastructure.

⚠ Important : Tout dépend du nombre d'IP qu'on souhaite, en sélectionnant /24, j'ai 256 IP dont 256-2 = 254 hôtes (Réseau – Broadcast). 2^8-2 = **254**

Défini par le « Calcul de sous-réseaux »

```
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
```

On nous demande ensuite si le réseau dispose d'une passerelle vers laquelle renvoyer les flux. Ce n'est notre cas, l'interface WAN fait déjà son travail et je n'ai pas d'autre routeur dans mon réseau donc j'appuie sur Entrée pour laisser vide « none ».

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

Je ne souhaite pas configurer d'adresse en IPv6, je réponds donc « n »

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

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

On souhaite activer le DHCP pour le réseau local donc on saisit « y » pour répondre Oui puis Entrée.

INFORMATION : Le service DHCP peut être activé et configuré plus simplement via l'interface WEB.

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

On nous demande à partir de quand commence l'adressage IP : 10.0.50.10

Puis Quand elle se termine : 10.0.50.30

```
Enter the start address of the IPv4 client address range: 10.0.50.10
Enter the end address of the IPv4 client address range: 10.0.50.30
```

On se rend sur nos machine client (Windows ou Linux) :

Windows :

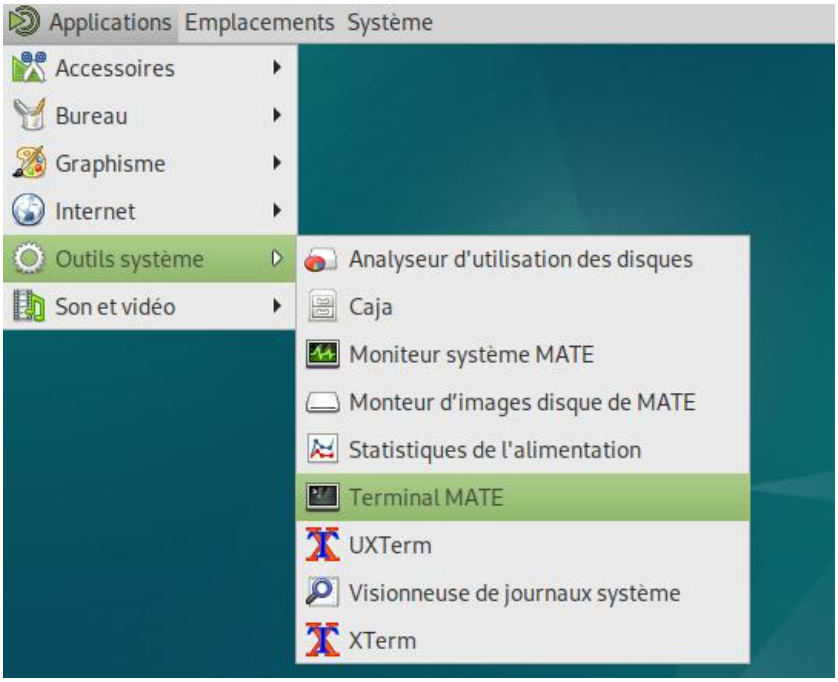
On tape simultanément sur les touches Windows+R puis on saisit « cmd » et sélectionne Entrée

Taper la commande « ipconfig »

```
C:\Users\CLIENTMK>ipconfig

Configuration IP de Windows


Carte Ethernet Ethernet0 :

   Suffixe DNS propre à la connexion. . . : home.arpa
   Adresse IPv6 de liaison locale. . . . .: fe80::fc36:71df:da75:9f04%14
   Adresse IPv4. . . . . . . . . . . . . .: 10.0.50.18
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 10.0.50.4

C:\Users\CLIENTMK>
```

On obtient bien une adresse IP !

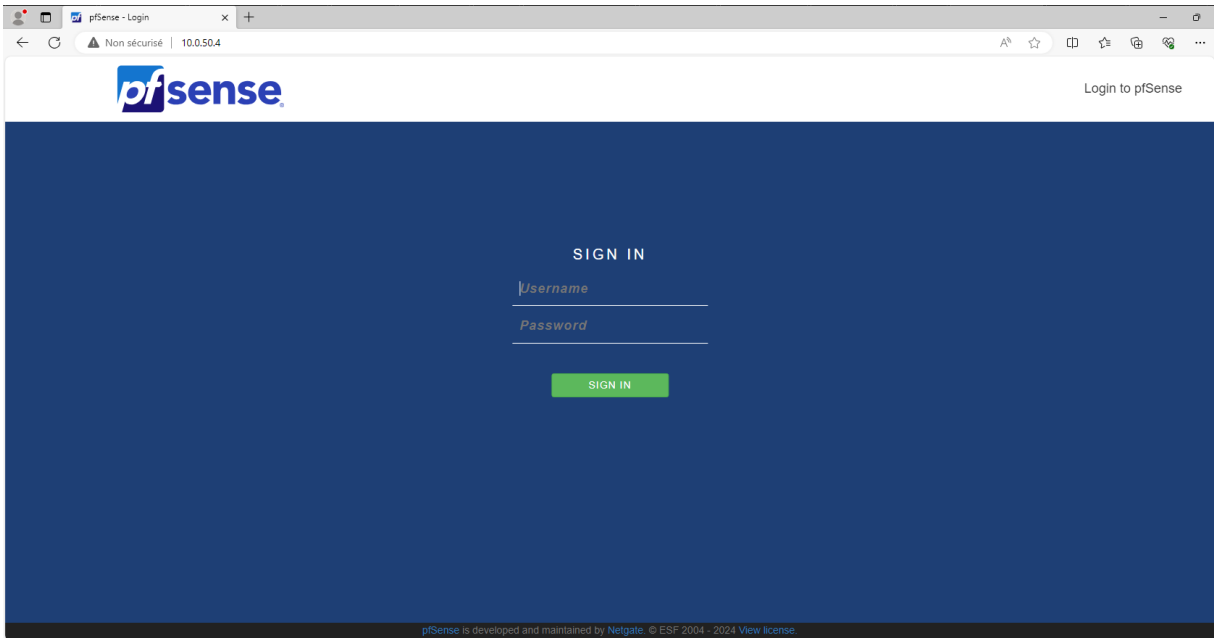
Linux :



Puis arriver sur le terminal on saisit « ip a »

```
root@debian:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether 00:0c:29:d7:2e:41 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 10.0.50.16/24 brd 10.0.50.255 scope global dynamic noprefixroute ens33
       valid_lft 7144sec preferred_lft 7144sec
    inet6 fe80::20c:29ff:fed7:2e41/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
root@debian:~#
```

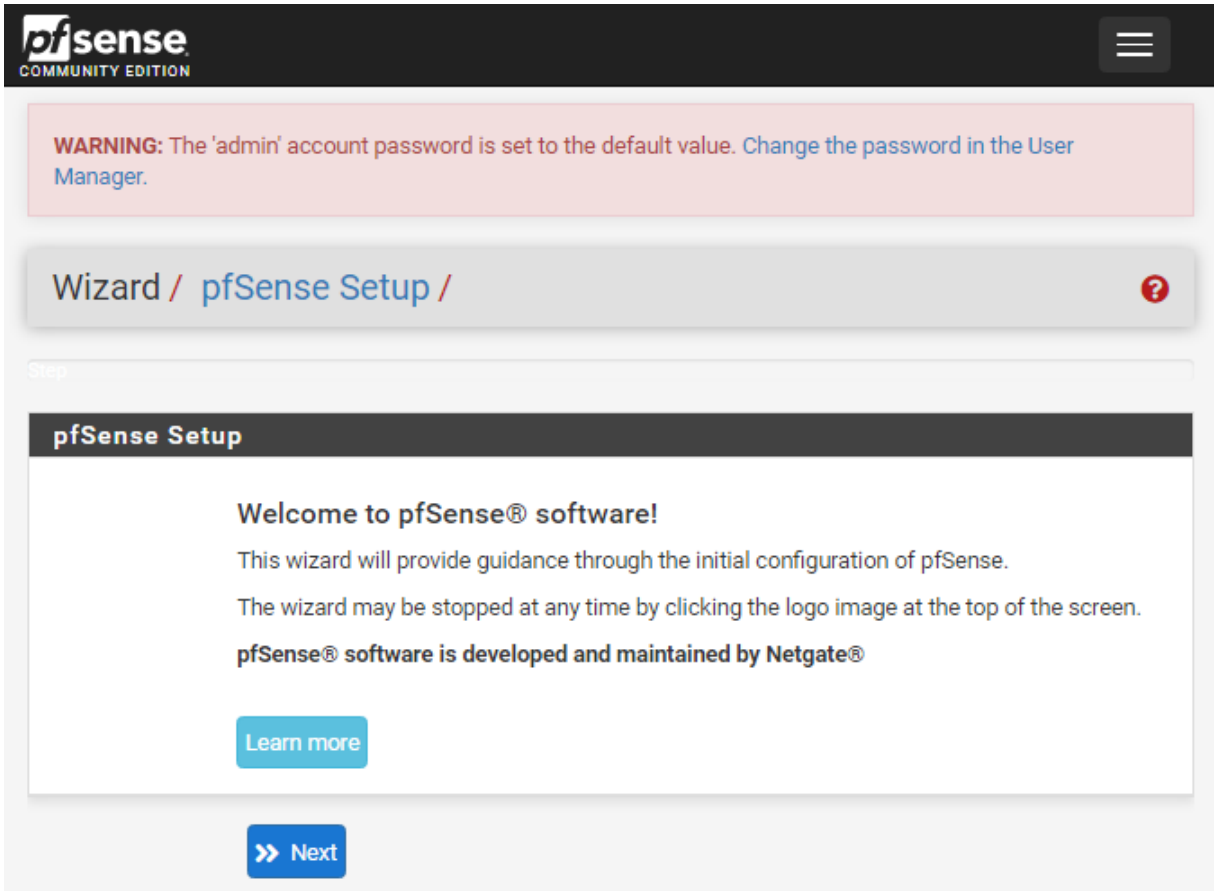
On ouvre le navigateur internet et saisi l'IP donner précédemment pour accéder à notre pfsense.



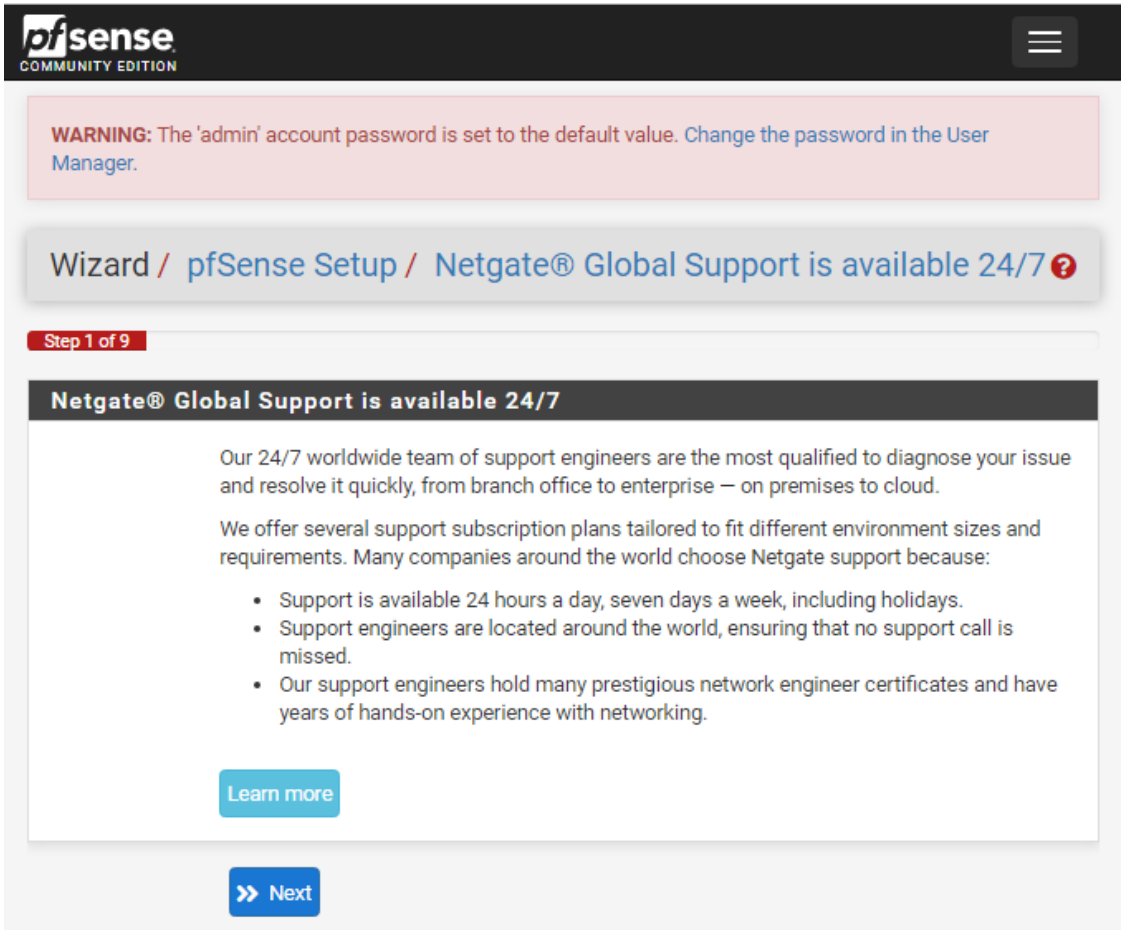
Les identifiants par défaut de pfsense sont les suivants :

- Login : admin
- Mot de passe : pfsense

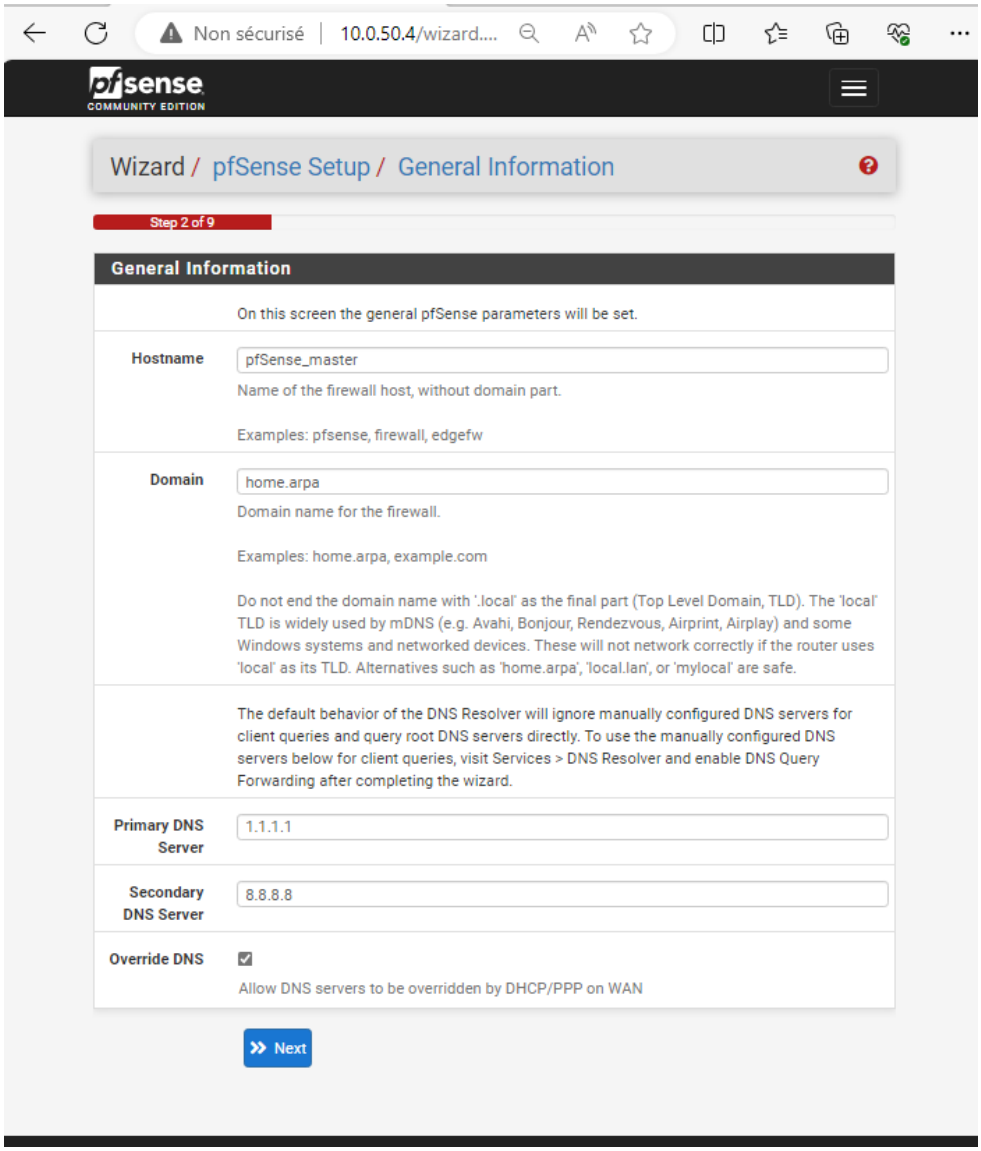
On arrive sur l'assistant de configuration de pfSense qui va nous permettre de finaliser l'installation de notre firewall.



L'Assistant nous informe qu'il est possible d'avoir un support technique sous condition de souscrire à un contrat (💰) Sélectionner « Next »

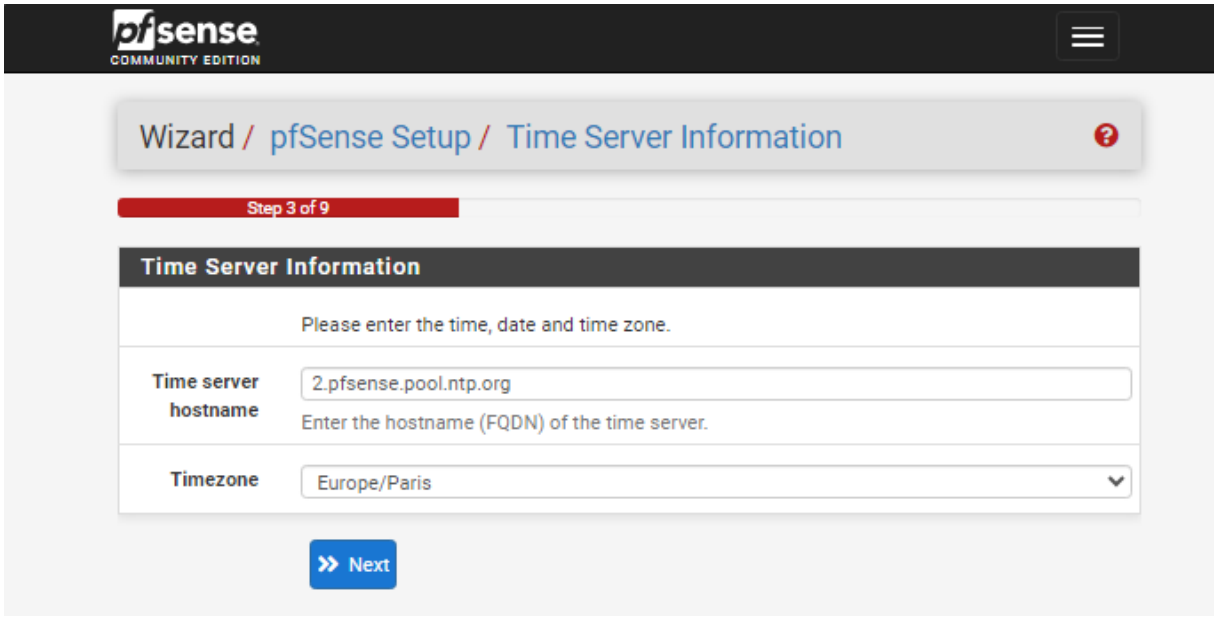


On peut choisir le nom du firewall et déclarer notre nom de Domain si on en possède un dans notre réseau. On peut également déclarer un serveur DNS local.

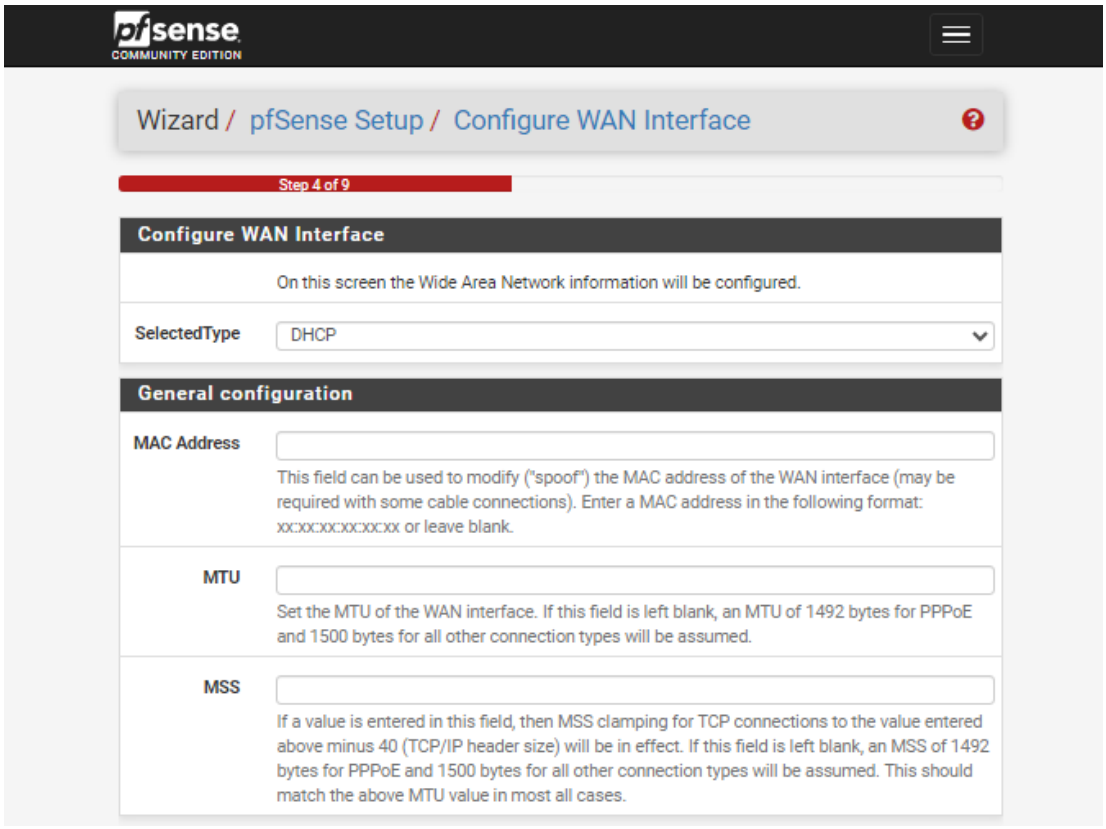


1.1.1.1- DNS de CloudFlare
8.8.8.8 - DNS de Google

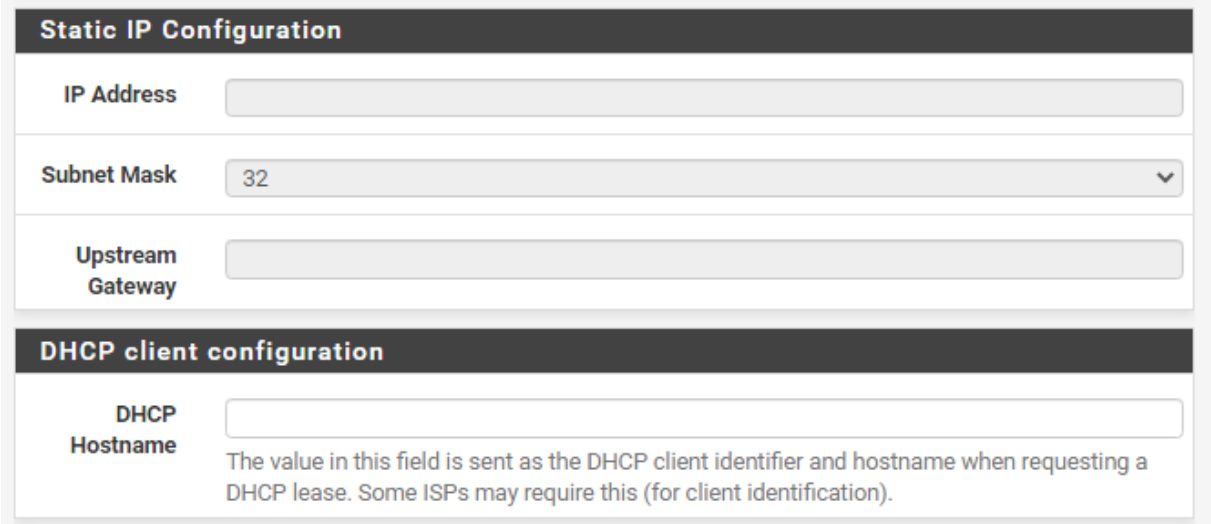
Choisissez « **Europe/Paris** » dans la **Timezone** et on poursuit.



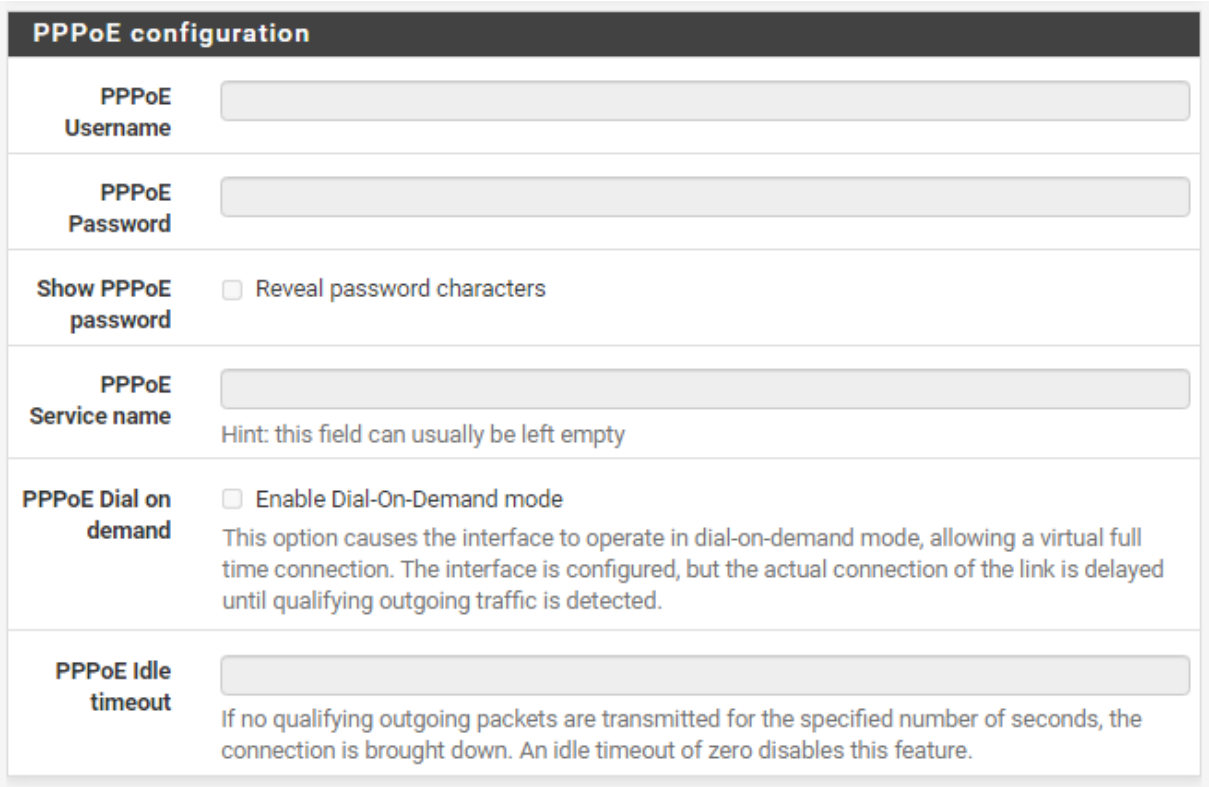
Ensuite nous arrivons à la configuration de l'interface WAN. Elle est configurée automatiquement par DHCP, je n'y touche pas.



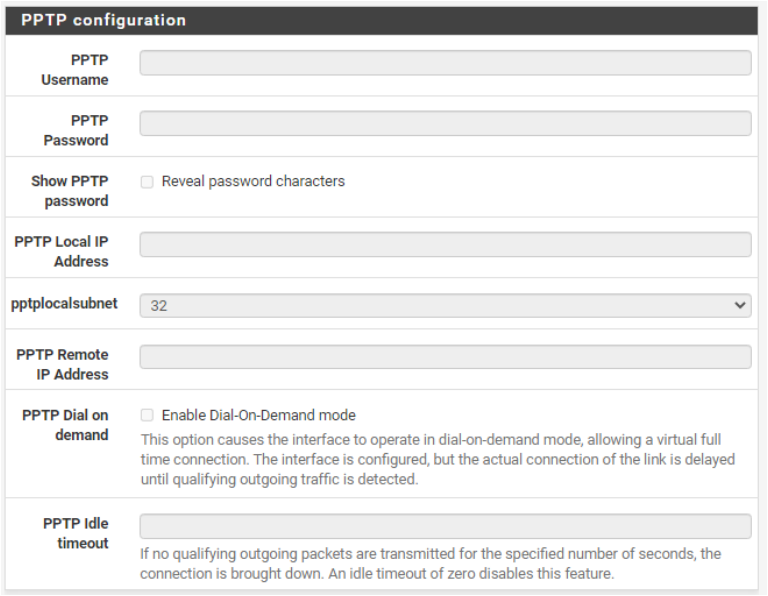
Si on a besoin d'attribuer une IP fixe à cette interface WAN, c'est dans cette partie que ça se définit, sinon, on continue.



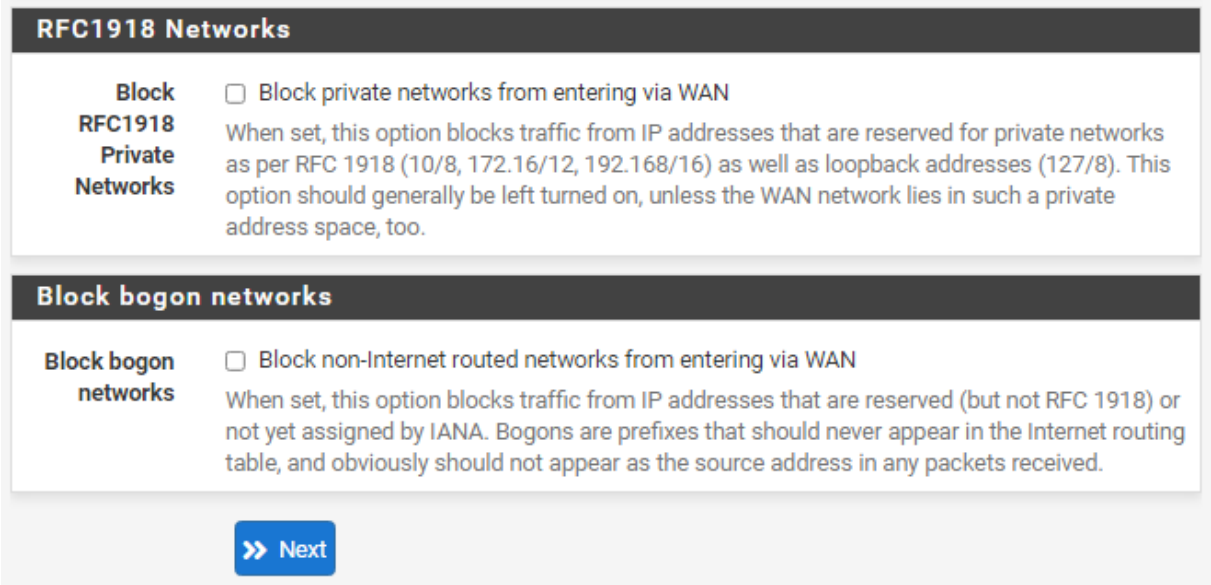
La partie « **PPPoE configuration** » sert en général à mettre les **identifiants fournis par votre FAI**. Ce sont ces identifiants qui sont définis dans votre box internet actuellement. Si vous souhaitez placer un firewall à la place de la box, il sera nécessaire de remplir cette partie.



La partie suivante « **PPTP configuration** » servira plutôt au **montage d'un VPN point à point** *(Protocole de tunnel point-à-point, à éviter car peu sécurisé, plutôt privilégier son petit frère IPSEC)*.

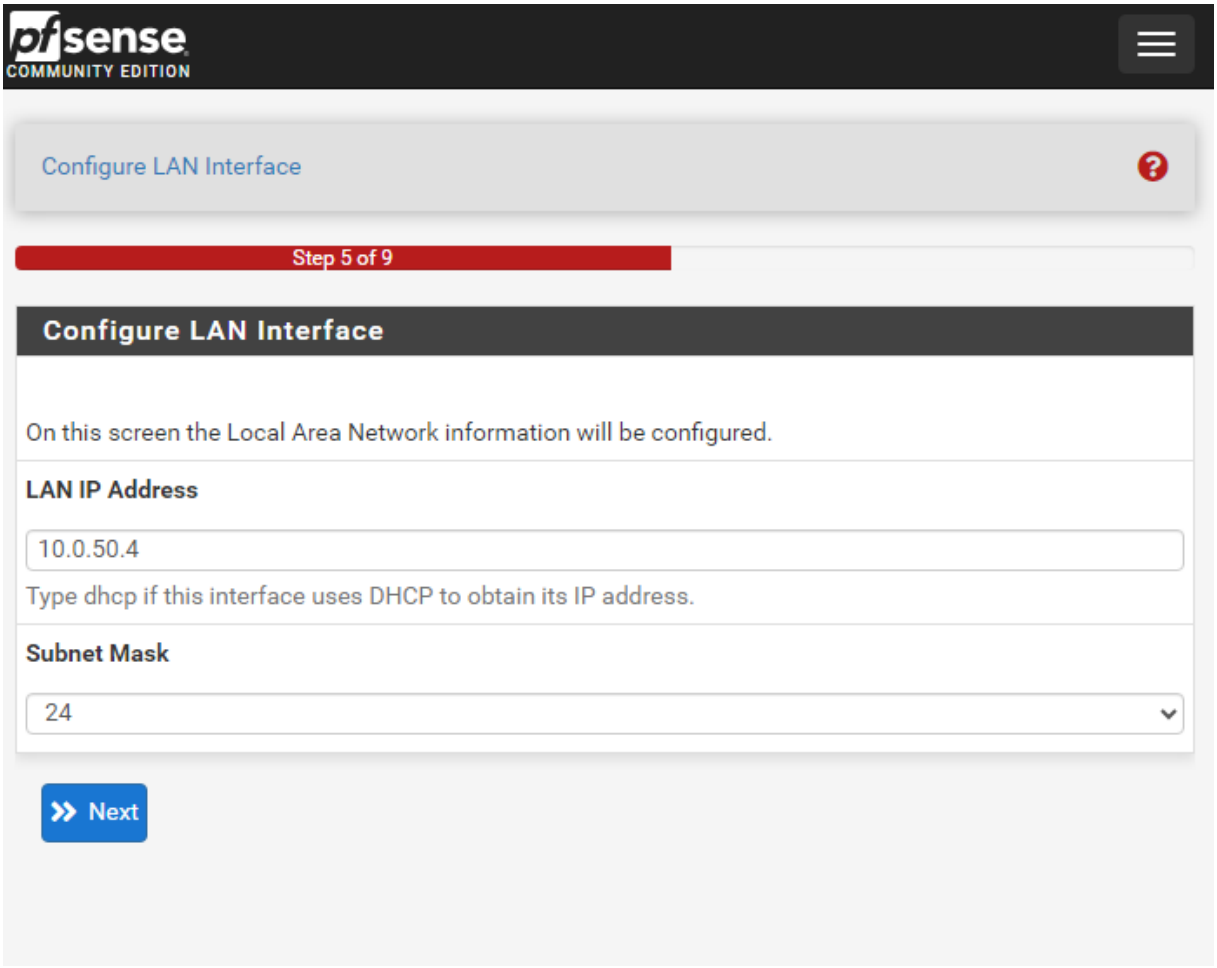


Les deux dernières options de cette page définissent que tout trafic entrant sur l'interface WAN et venant d'une classe d'adresse réseau privé est automatiquement bloqué. ***Comme notre infra est ici virtuelle, on veut obligatoirement faire communiquer des réseaux privés, on n'utilise pas réellement une adresse publique***. Il est donc ***nécessaire dans le cadre d'un labo de décocher ces 2 cases*** sinon on peut avoir des petits soucis (; .

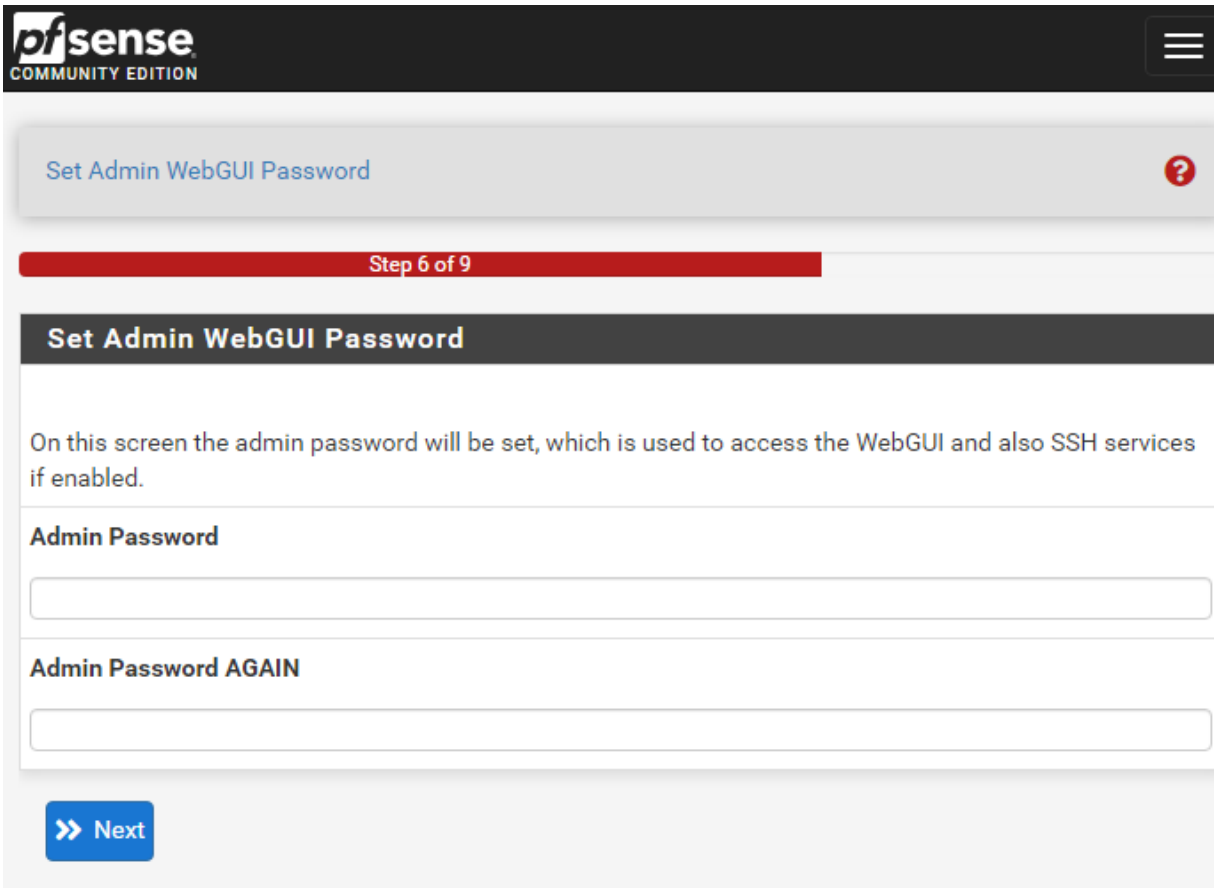


Nous n'avons donc rien modifier de spécial sur notre interface WAN ici, vous pouvez poursuivre.

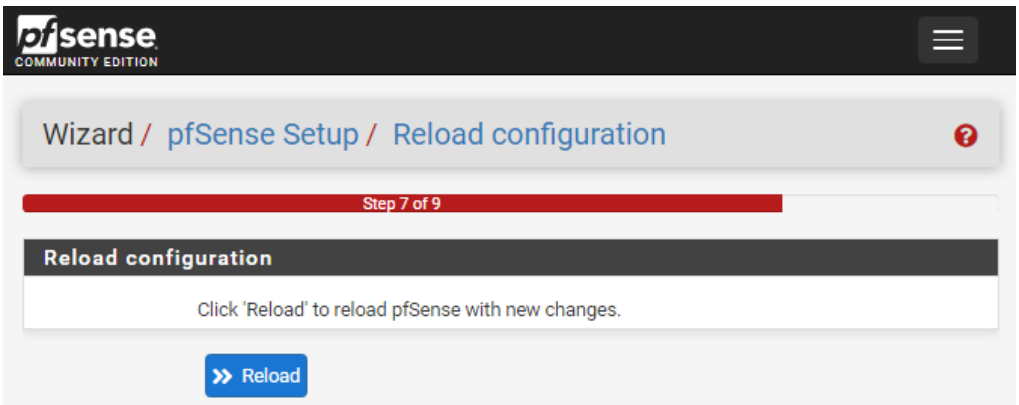
L'assistant de pfsense passe donc cette fois-ci à l'**interface côté LAN**. Vous pouvez changer ici l'adresse IP de l'interface LAN de pfSense *(nous l'avons déjà fait en amont)*.



Durant la phase de configuration, il est également nécessaire de changer les identifiants par défaut du compte admin de pfsense.

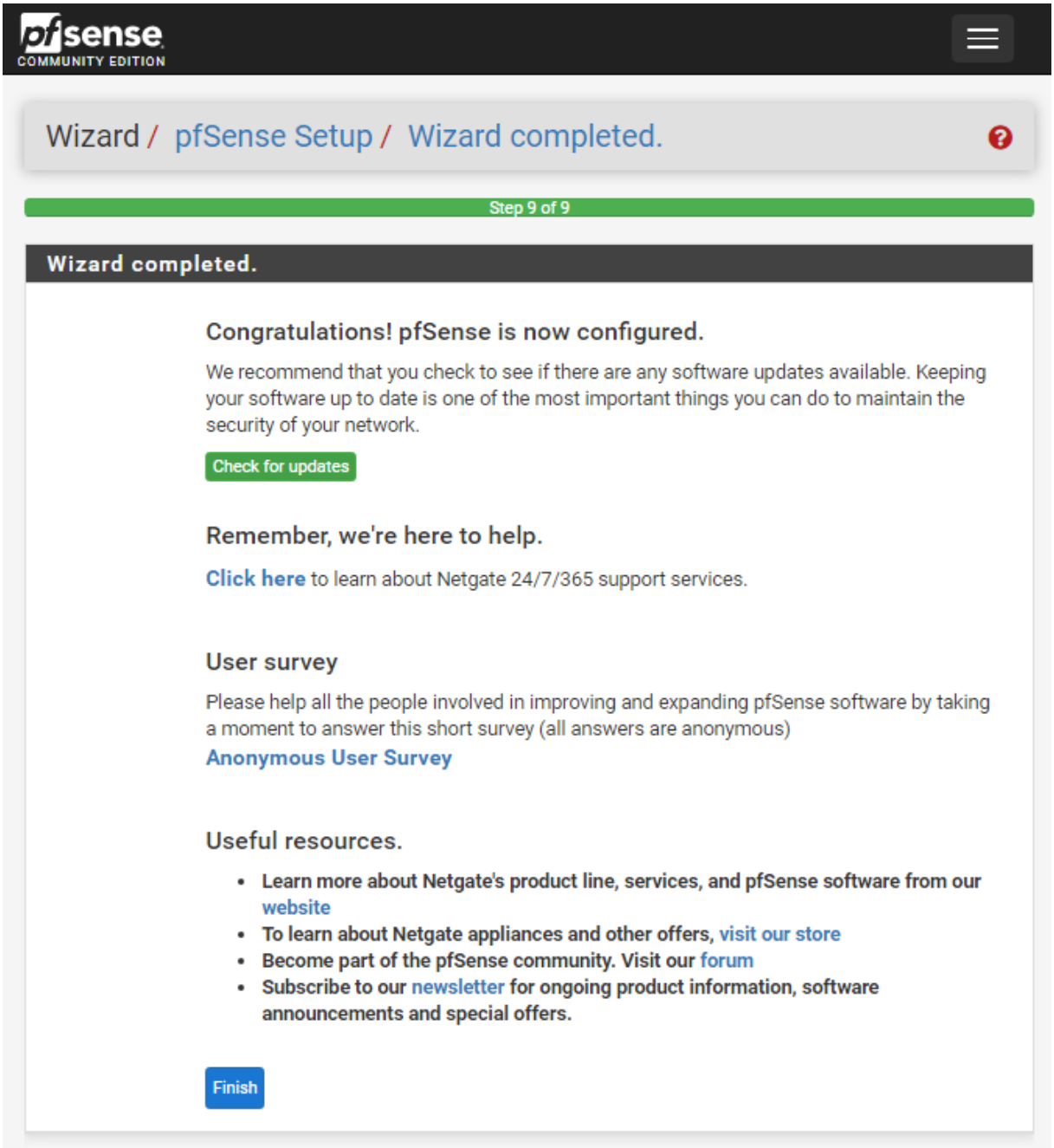


La phase finale de l'installation de pfsense est terminée. Cliquez sur **Reload** pour recharger pfsense.



Patientez quelques secondes, la page va se recharger d'elle-même.

A la fenêtre suivante, cliquez sur le bouton **Finish**.



Cliquez sur le bouton « **Accept »** pour valider les points législatifs divers.

Copyright and Trademark Notices.

Copyright© 2004-2016. Electric Sheep Fencing, LLC ("ESF"). All Rights Reserved.
Copyright© 2014-2023. Rubicon Communications, LLC d/b/a Netgate ("Netgate"). All Rights Reserved.

All logos, text, and content of ESF and/or Netgate, including underlying HTML code, designs, and graphics used and/or depicted herein are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of ESF and/or Netgate.

"pfSense" is a registered trademark of ESF, exclusively licensed to Netgate, and may not be used without the prior express written permission of ESF and/or Netgate. All other trademarks shown herein are owned by the respective companies or persons indicated.

pfSense© software is open source and distributed under the Apache 2.0 license. However, no commercial distribution of ESF and/or Netgate software is allowed without the prior written consent of ESF and/or Netgate.

ESF and/or Netgate make no warranty of any kind, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. ESF and/or Netgate shall not be liable for errors contained herein or for any direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of any software, information, or material.

Restricted Rights Legend.

No part of ESF and/or Netgate's information or materials may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of ESF and/or Netgate. The information contained herein is subject to change without notice.

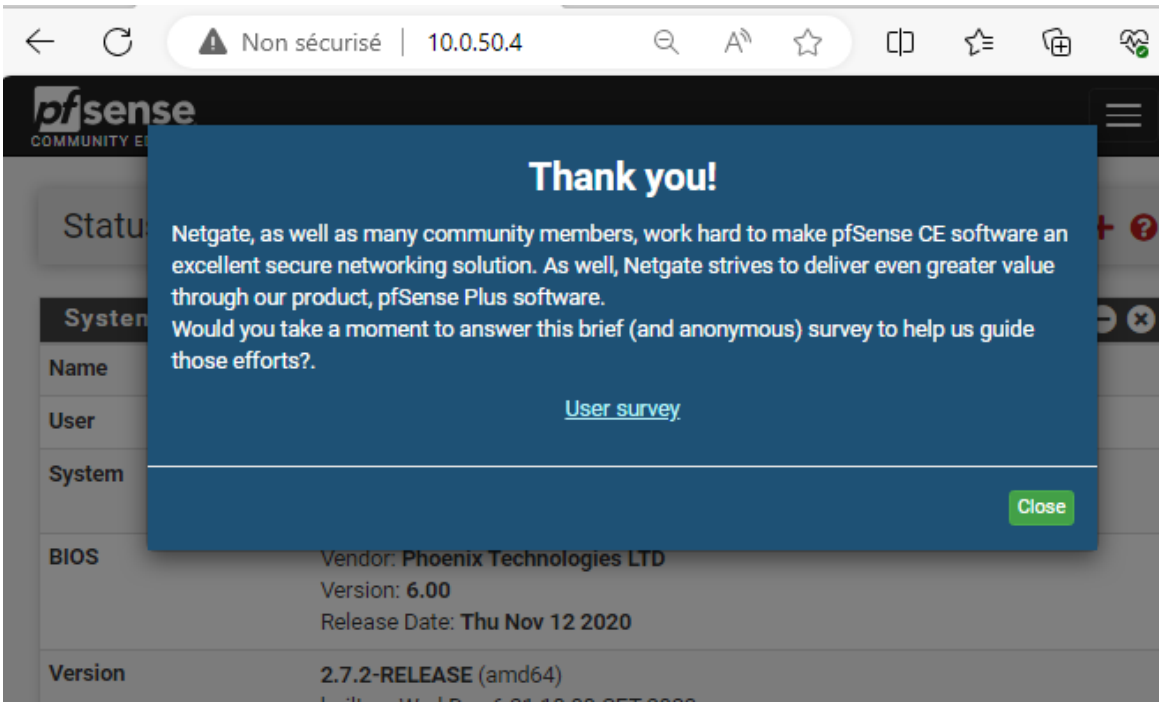
Use, duplication or disclosure by the U.S. Government may be subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance.

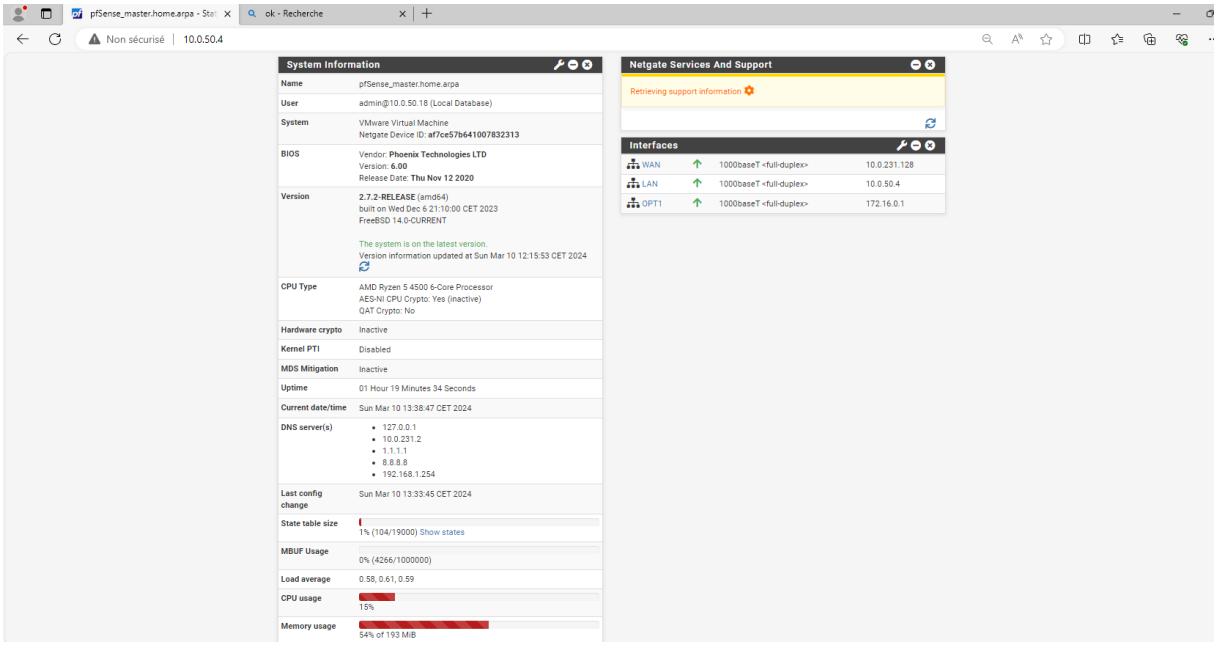
The export and re-export of software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, Licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Government's Enemies List; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that Licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

Accept

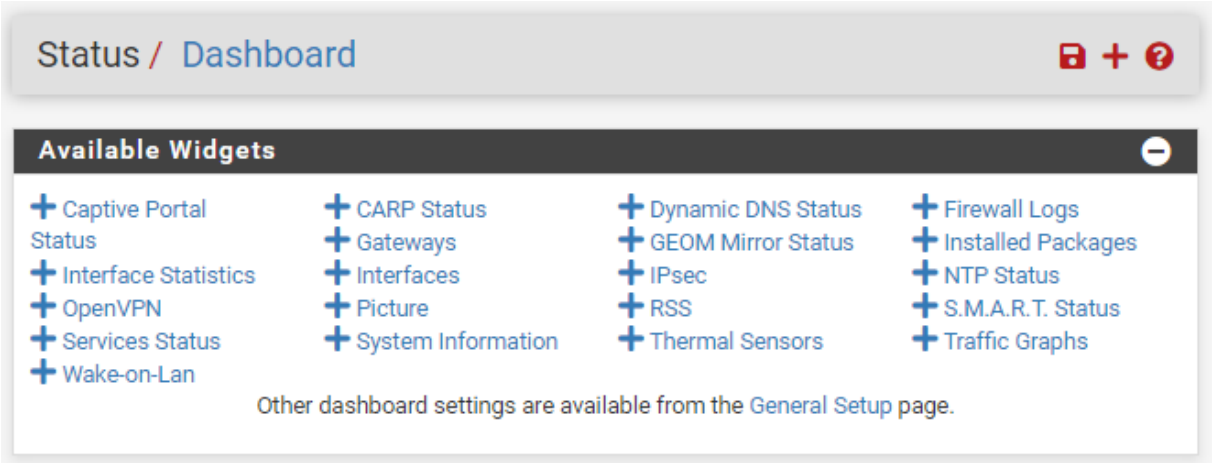
On nous demande si on souhaite répondre à un sondage, on clique sur close.



On arrive sur le tableau de bord de notre pfSense. Où on retrouvera les infos sur l'utilisation des ressources de la machine elle-même, ses différentes adresses IP, version & mises à jour.



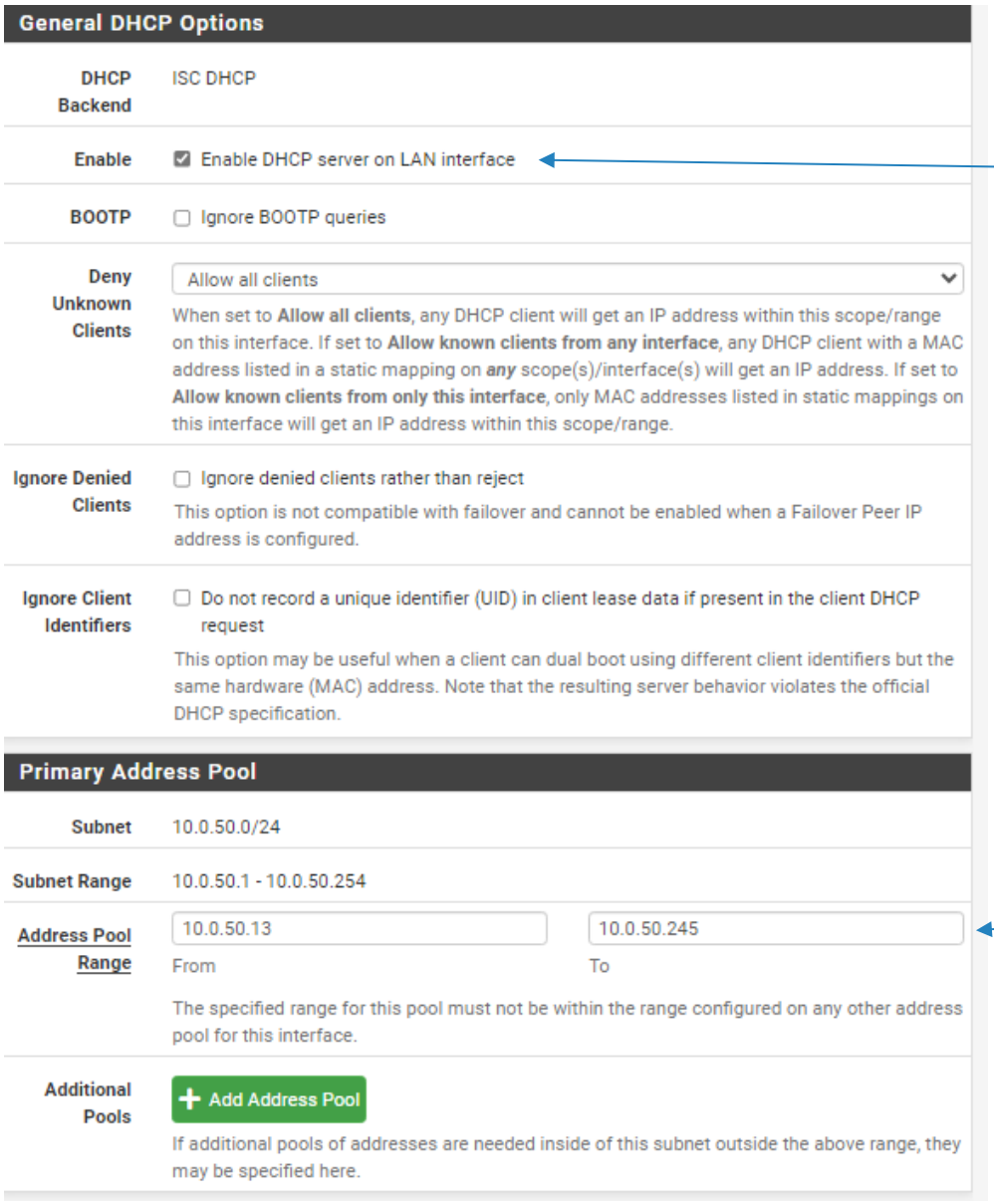
Cette **vue est personnalisable** est cliquant sur le **petit + en haut à droite** dans la barre de titre.



2) Service Requis

1.1 Configuration du DHCP serveur :

Pour configurer le DHCP via l'interface WEB, on se rend dans **l'onglet Services -> DHCP Server**



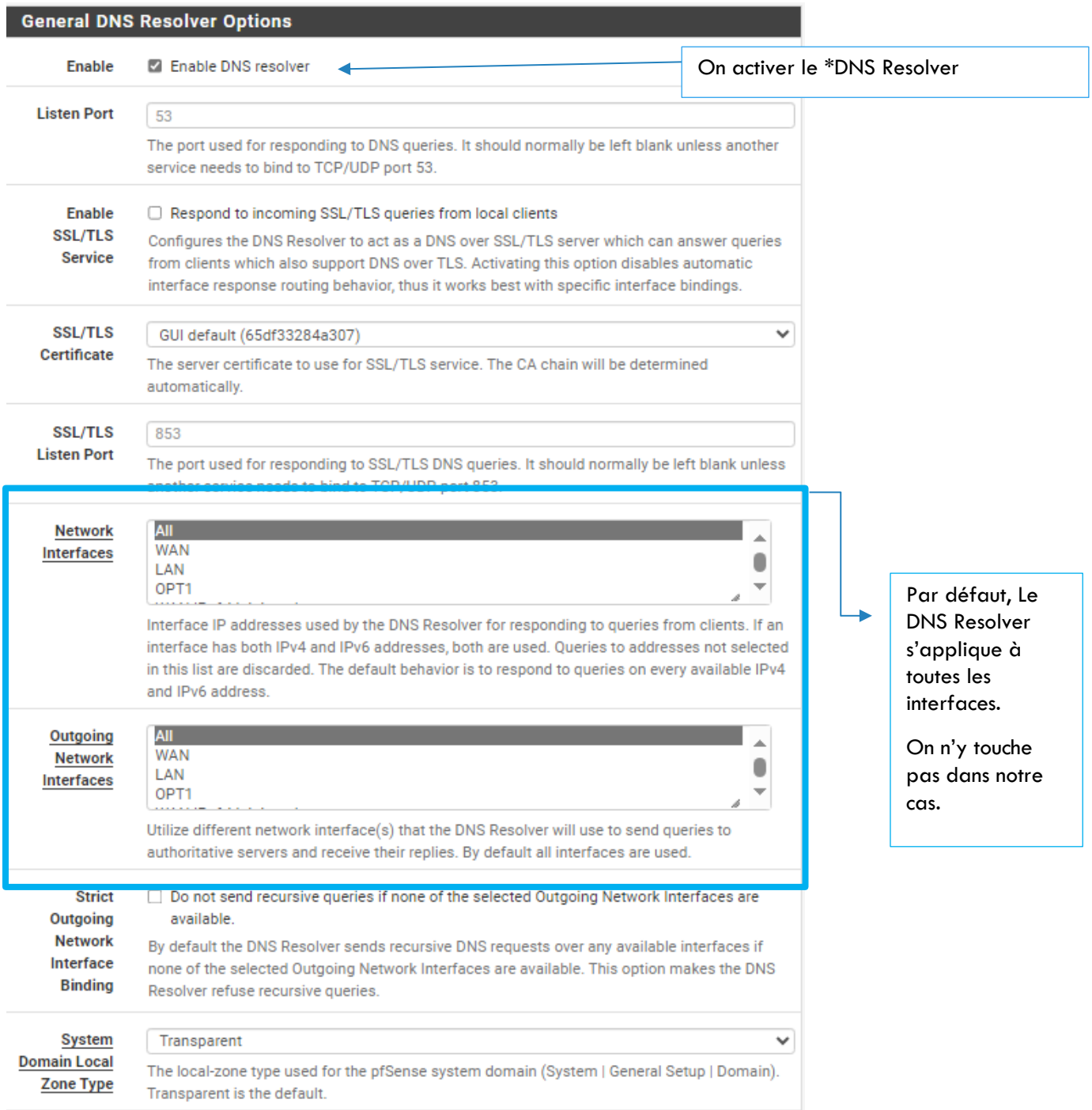
On active le DHCP

On saisi à partir de quand commence notre @IP et jusqu'à où elle s'arrête.

⚠ Important : N'oublier pas de Cliquer sur « Save » !

1.2 Configuration du DNS serveur :

Pour configurer le DNS, on se rend dans **l'onglet Services -> DNS Resolver -> General Settings**



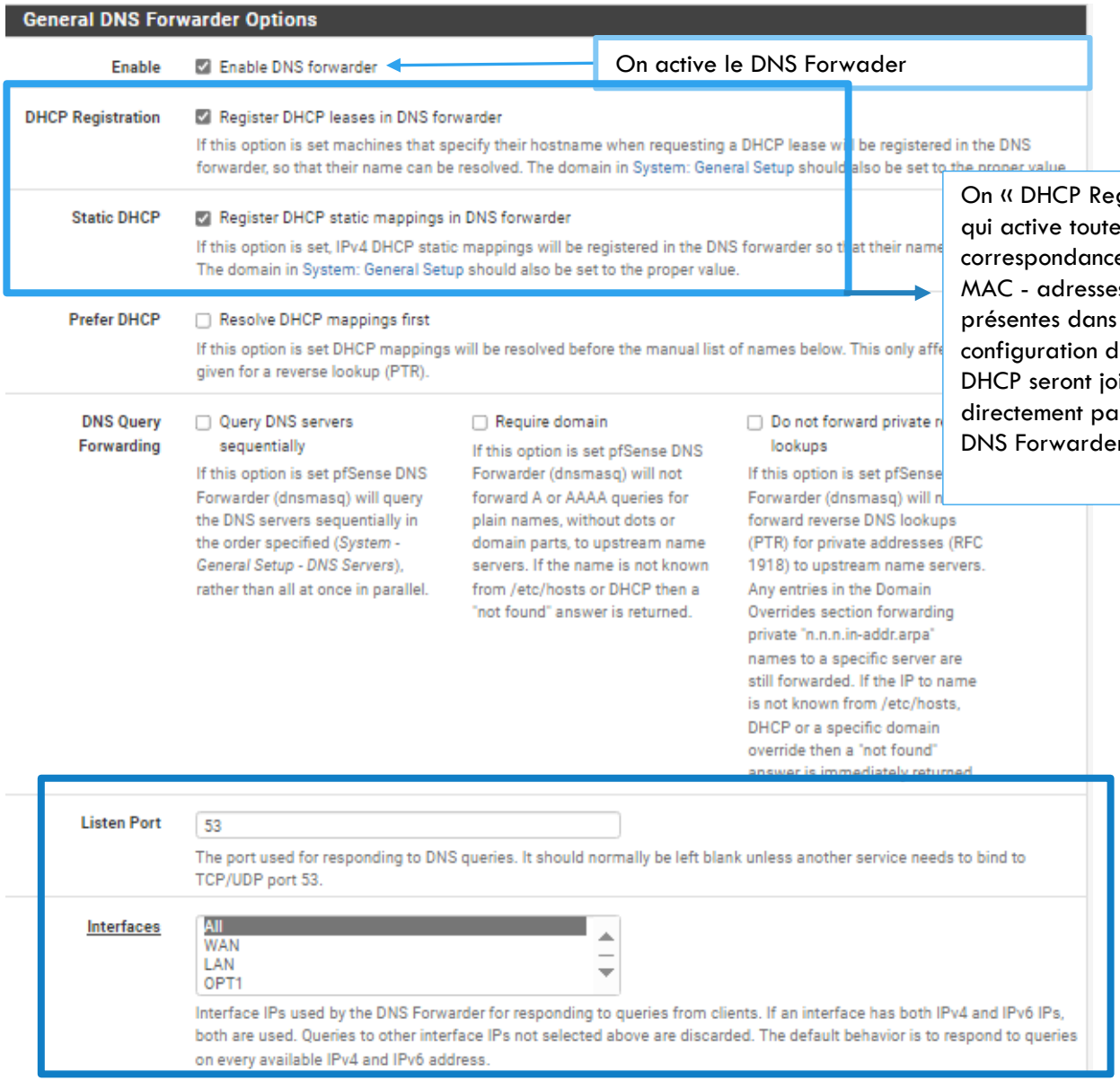
« SAVE »

Définition **DNS RESOLVER** : Les résolveurs DNS sont un composant essentiel du Domain Name System (DNS). Ils agissent en tant que contrepartie interrogative aux serveurs de noms DNS qui leur répondent. Du point de vue de l'utilisateur, un DNS resolver sert d'interface de transmission entre l'utilisateur ou l'application et les serveurs de noms.

3) Activer le DNS Forwader

Le DNS forwarder de pfSense permet de résoudre les requêtes DNS des clients DHCP (mappés ou non) ainsi que des entrées DNS saisies manuellement. Le DNS forwarder permet également de renvoyer les requêtes DNS des clients pour un domaine particulier.

On se rend sur **Services -> DNS Forwader**

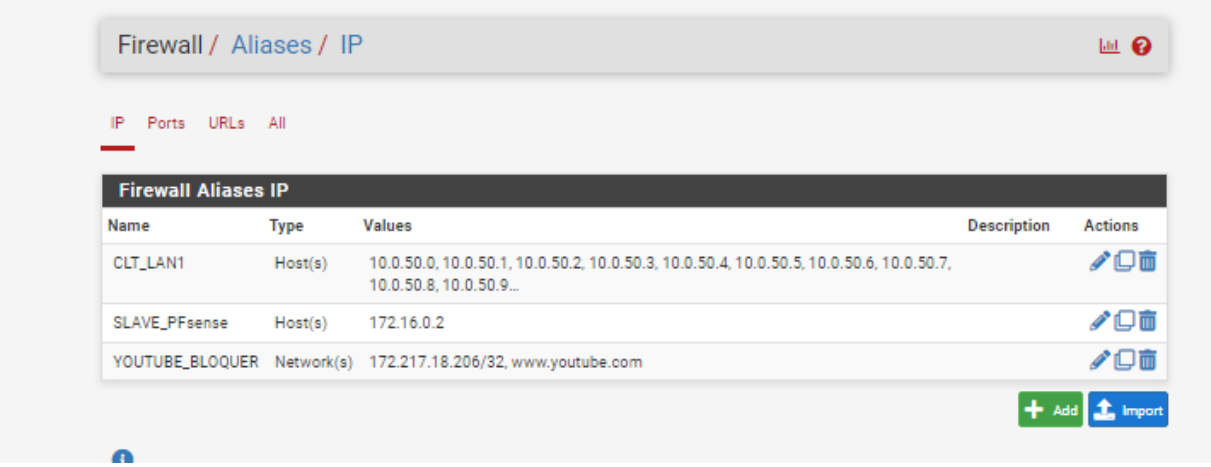


4) Configuration générale

1.1) Les Alias

Les alias définissent un groupe de ports, d'hôtes ou de réseaux. Les alias peuvent être référencés par des règles de pare-feu, des transferts de port, des règles NAT sortantes et d'autres endroits du pare-feu. L'utilisation d'alias donne lieu à des ensembles de règles nettement plus courts, auto-documentés et plus gérables.

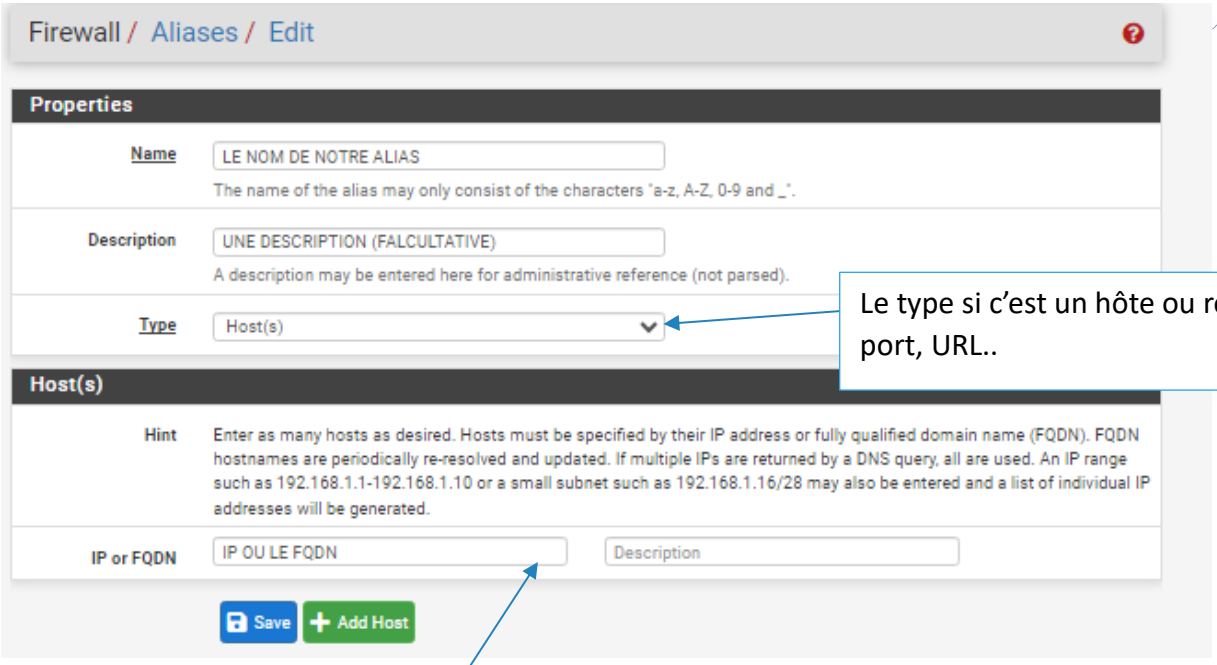
On se rend dans Firewall > Aliases



On voit les Aliases que j'ai configuré.

Pour Ajouter un Alias, on procède comme ceci :

- On clique sur +ADD



Le type si c'est un hôte ou réseau, port, URL..

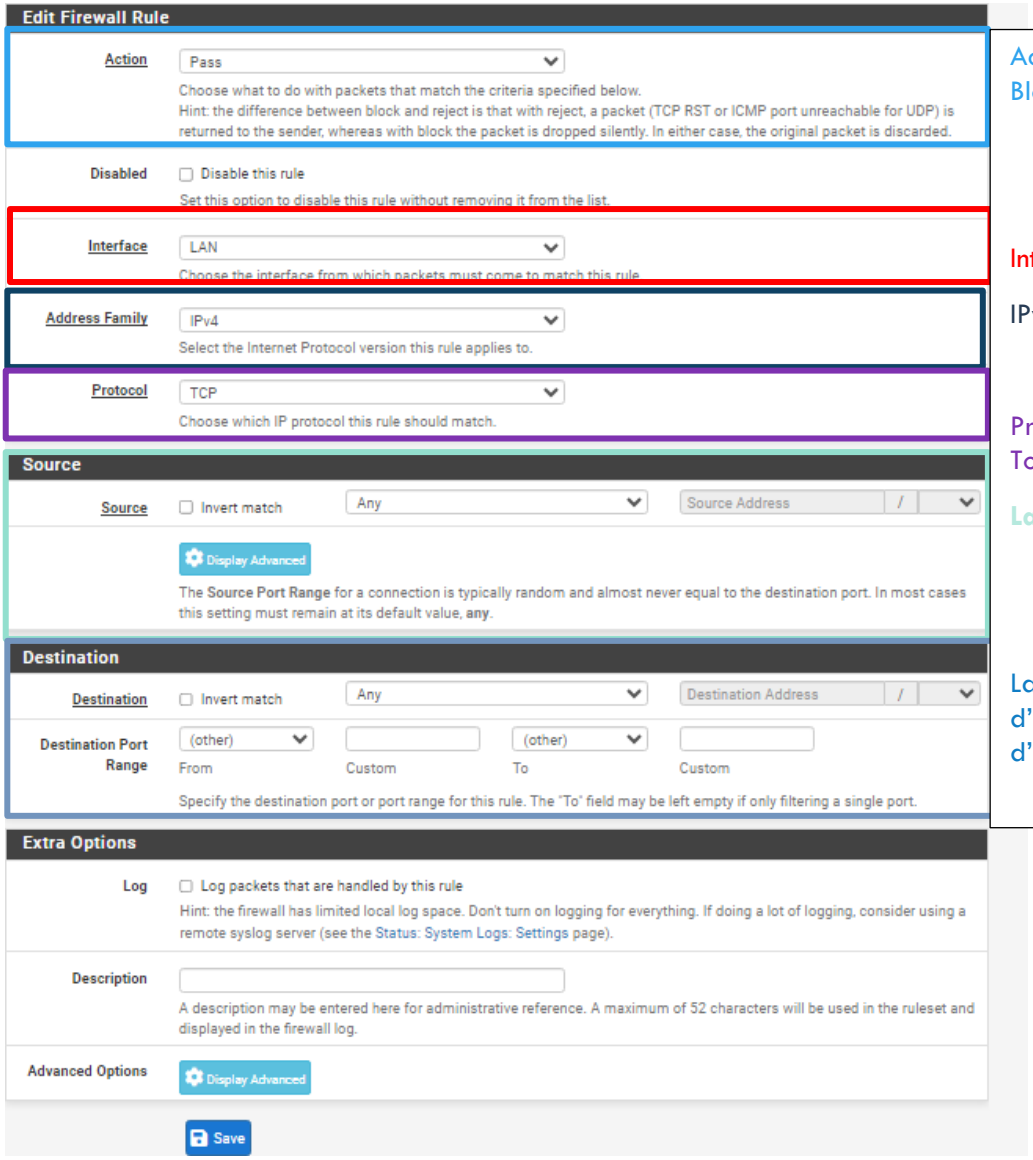
Définition FQDN (Full Qualifed Domain Name) : désigne l'adresse complète et unique d'un site Internet.

Exemple : https://btssio.org.

1.2) Création d'une règle de FireWall

On se rend dans **FireWall -> Rules puis on sélectionne l'interfaces (WAN, LAN, OPT1)**

Puis ***↑ADD*** *pour ajouter une règle.*



Action : Bloquer,Autoriser,Refuser

Interface LAN,WAN,OPT1

IPv4/IPv6 ou IPv4+IPv6

Protocol TCP,UDP,ICMP.. ou Tous

La source -> ex : LAN

La Destination -> ex : @IP d'un serveur d'administration.

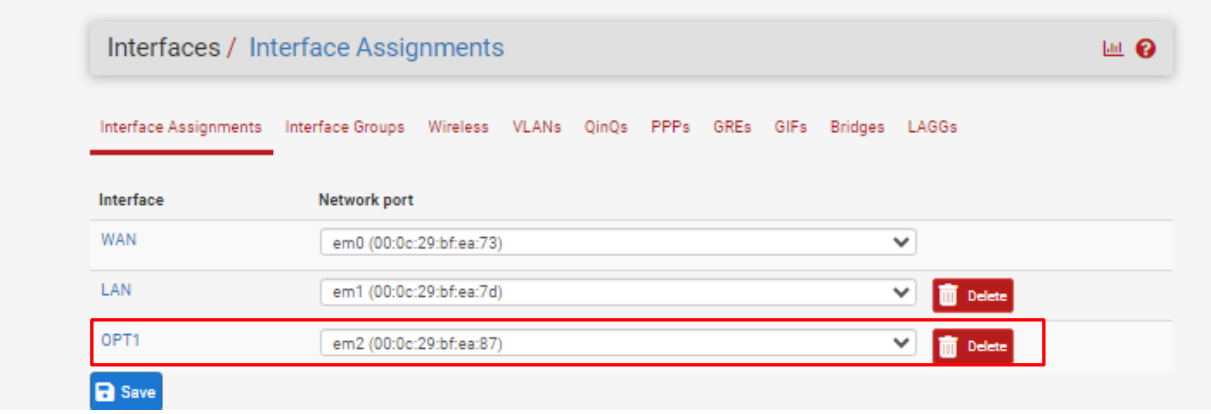
1.3) Configuration de CARP

Le protocole CARP (Common Address Redundancy Protocol) permet à plusieurs équipements réseaux de partager une même adresse IP. C'est une alternative libre au protocole propriétaire HSRP de CISCO, par exemple. Les machines partageant cette IP font parties du groupe de redondance. On y trouve un équipement « maitre » et les autres « esclaves ». Ces derniers sont destinés à prendre le relais en cas de défaillance du premier équipement.

Dans notre cas, nous allons utiliser CARP pour créer un routeur / pare-feu redondant, avec serveurs DNS + DHCP. Nos clients prendront l'IP virtuelle comme passerelle par défaut. Ainsi, en cas de panne de notre routeur principal, le second répondra aux requêtes de nos clients en toute transparence et sans coupures.

Nous avons laissé une interface disponible «Network Adapter 3 »

Pour la configurer, il suffit d'aller dans **Interfaces -> Assign**



On clique sur « OPT1 »

Le choix du CIDR /30 est une question de bonnes pratiques et de sécurité, On sait qu'on doit lier 2 servers (Master & SLAVE) via CARP donc 2 IP alors il suffit de faire le calcul 2n>@IP.

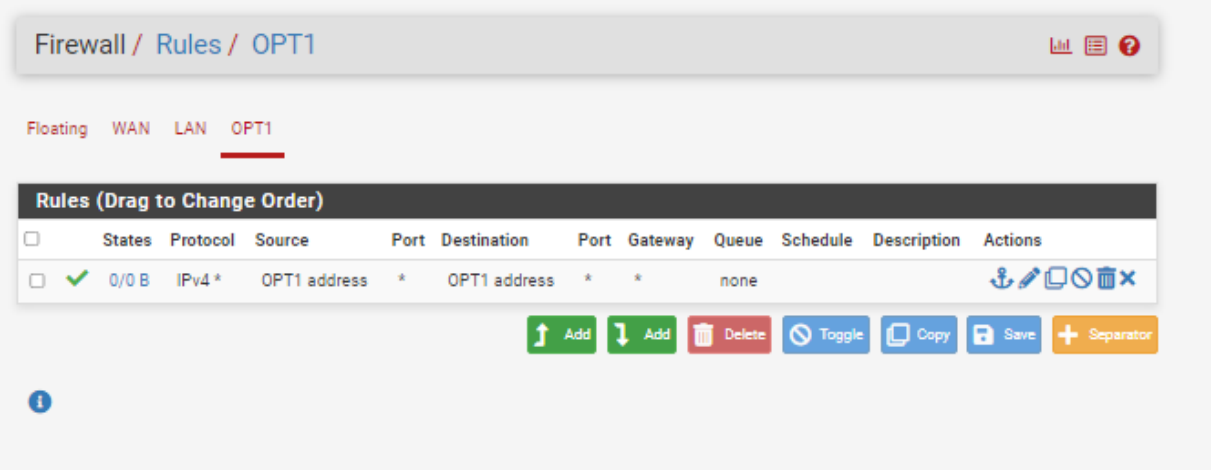
(2^32-30) -2 = 2 IP

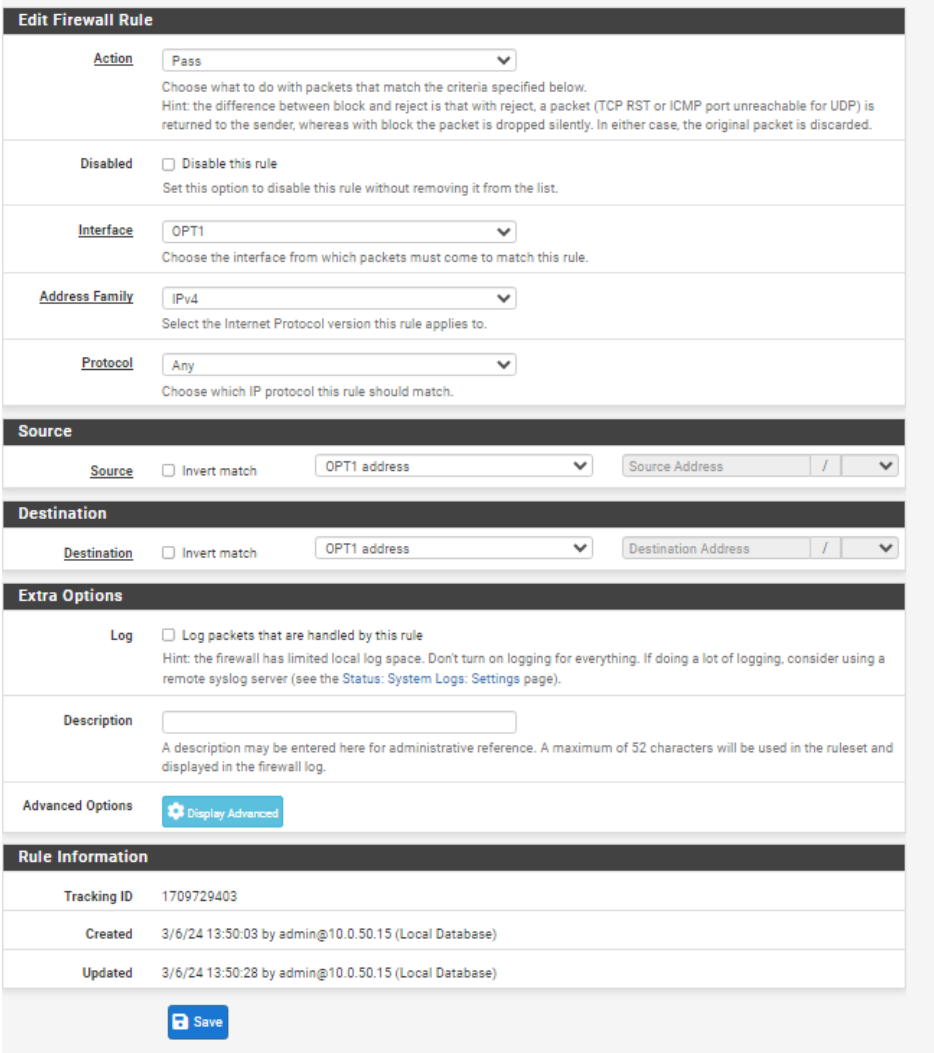
172.16.0.1 = Serveur Maître

172.16.0.2 = Serveur Slave

Ensuite, sur le serveur Maître nous, devons lui indiquer une règle de firewall autorisant le trafics sur l'interface CARP.

FireWall -> Rules -> CARP, puis on insère la règle suivante :

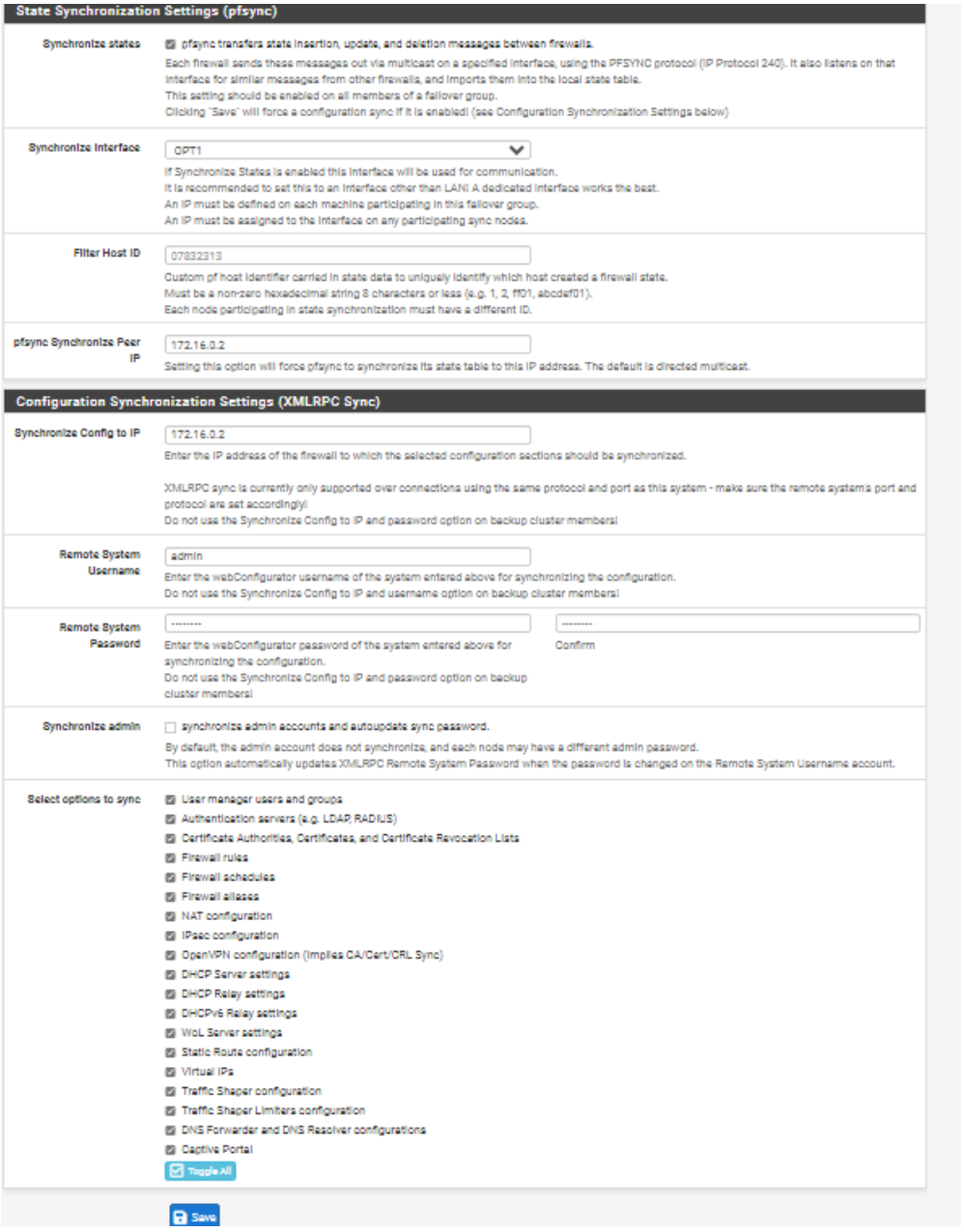




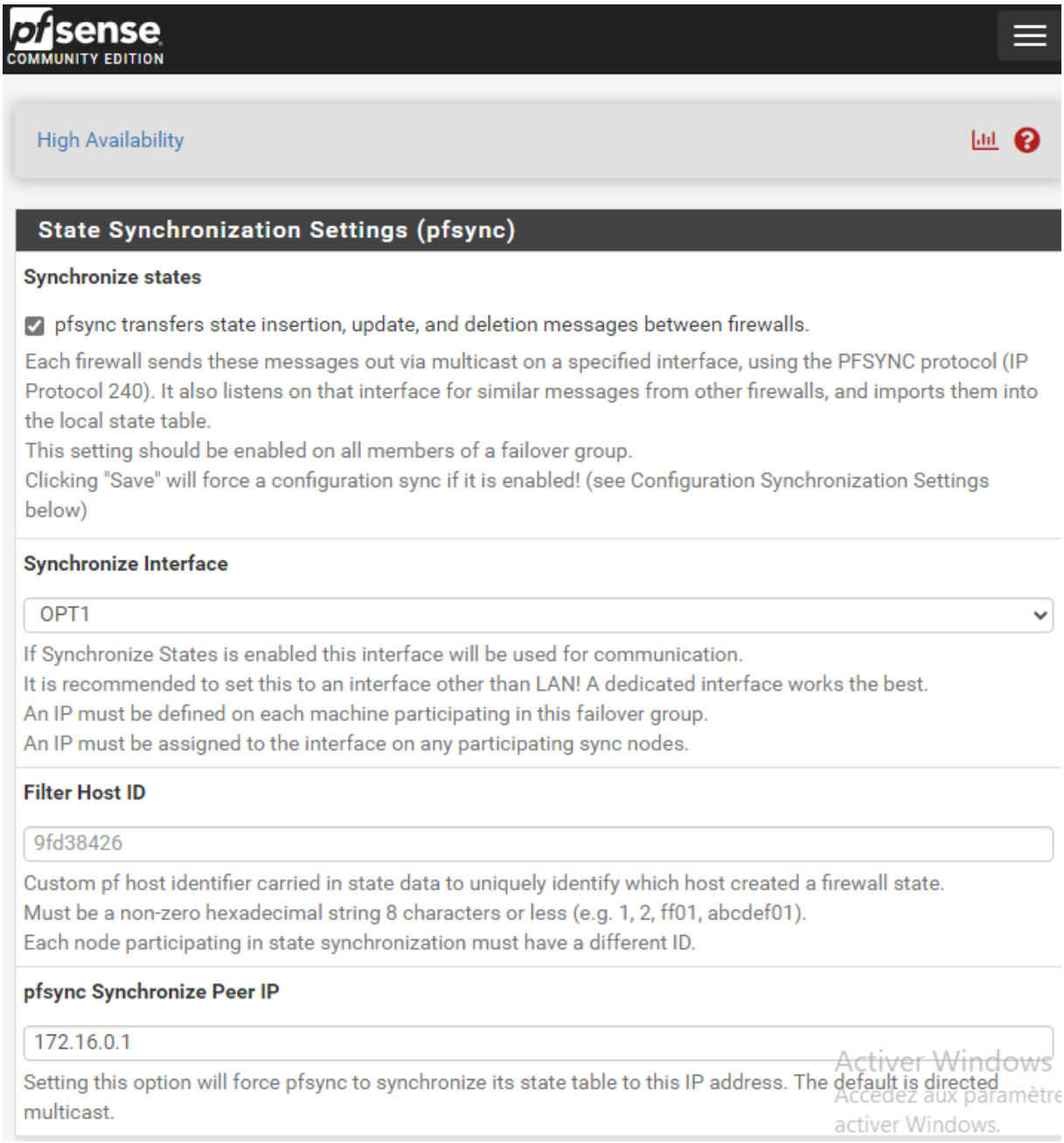
Ensuite nous allons activer la réplication entre les deux routeurs.

On va dans **System -> High Availability Sync.**

Sur le pfSense maître, On configure la partie pfsync en choisissant l'interface CARP, et l'@IP de notre pfSense Slave (172.16.0.2) dans notre cas, Puis dans la partie XMLRPC Sync), on saisit l'IP et Login de notre slave ainsi que la configuration à répliquer. Il est conseillé de cocher toutes les cases pour éviter tout problème.

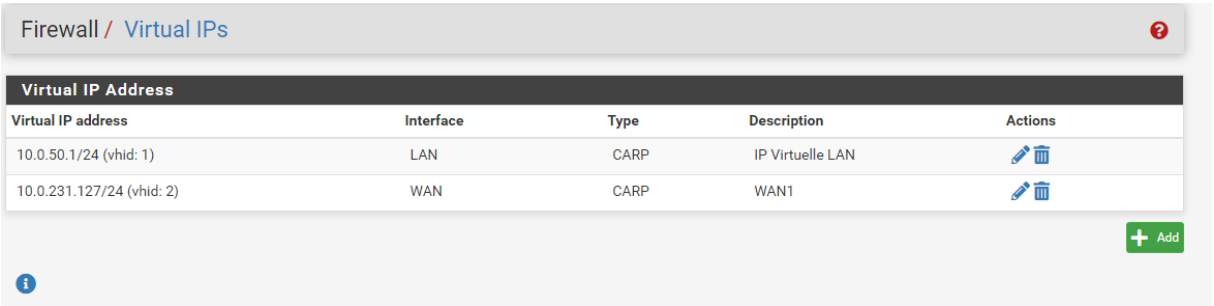


On va sur l'interface de notre pfSense Slave, cette fois-ci **seulement** la partie pfsync est à configurer :

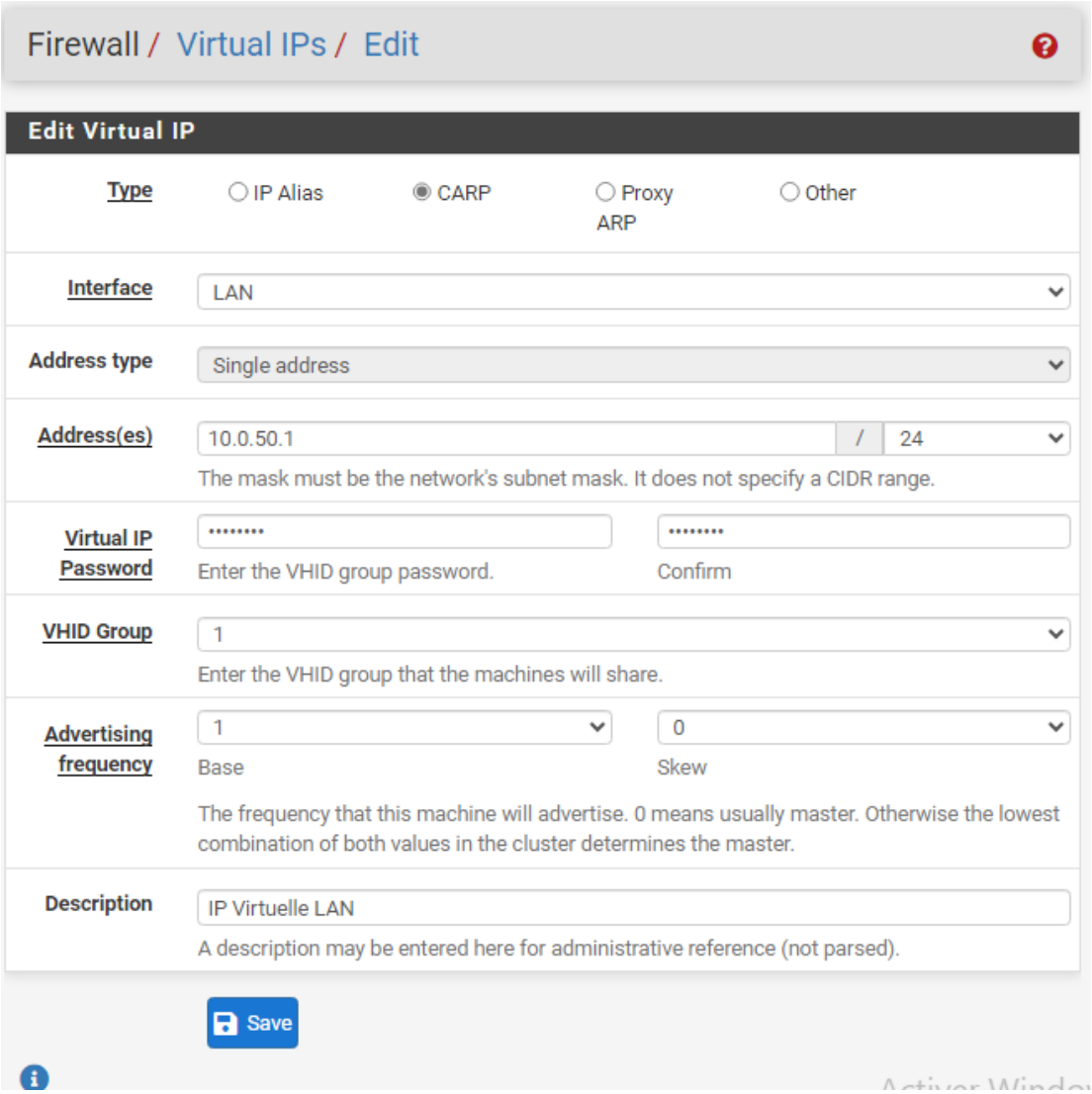


Dans Firewall / Virtual IPs on déclare cette nouvelle IP sur l'interface LAN.

Il est également possible de déclarer une IP pour le WAN ou une éventuelle DMZ. Il faudra simplement changer le VHID Group qui est à 1 par défaut.



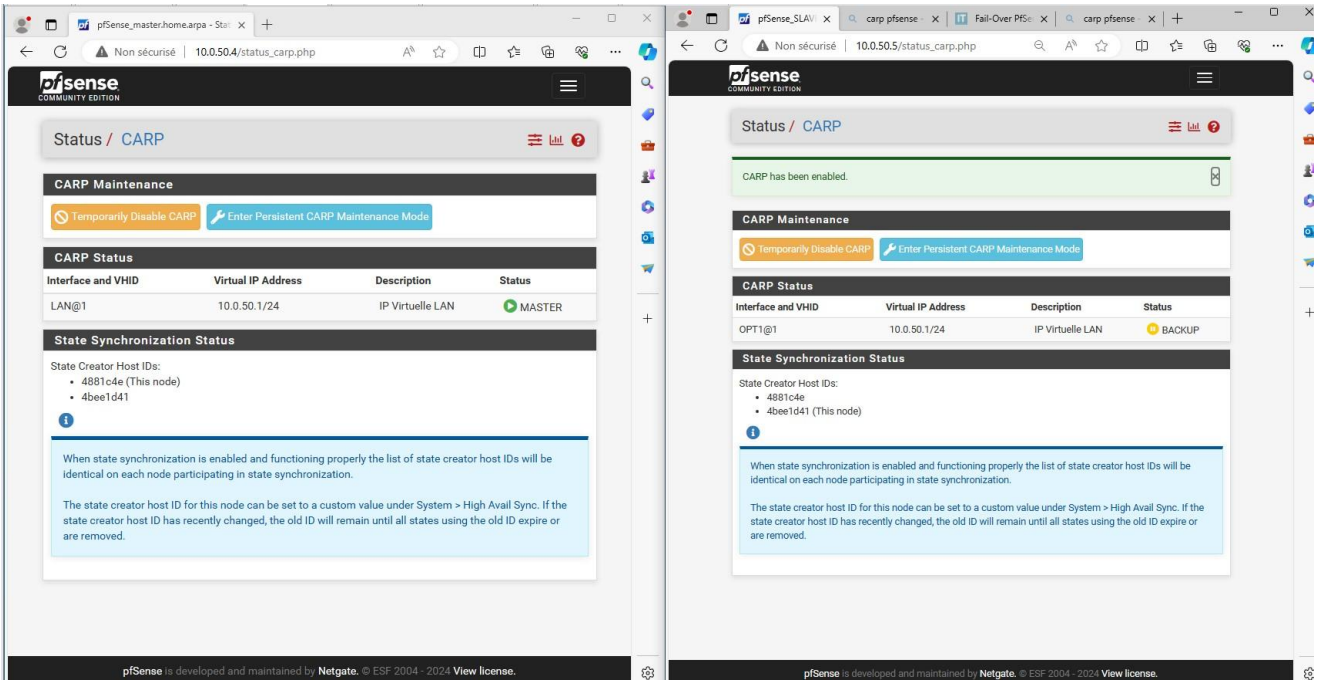
Configuration de l'IP virtuelle LAN :



Enfin, il faut modifier notre serveur DHCP du LAN pour déclarer cette IP en tant que passerelle par défaut.

5) Synchronisation des Interfaces et Test de basculement

Nous allons commencer par vérifier l'état de la synchronisation entre nos deux servers pfSense Master et pfSense Slave.



En prenant un client du LAN, nous allons pinger la Gateway (ou une IP externe) et éteindre le pfSense Master principal.
On constate le moment de la bascule avec deux paquets dupliqués (les deux routeurs répondent à ce moment-là) ou une perte d'un paquet. Il n'y a pas eu d'interruption de service, et le second routeur est passé avec le statut MASTER.
Les services rebasculeront sur le routeur principal lorsqu'il sera de nouveau opérationnel.

```
C:\Users\CLIENTMK>ping 10.0.50.1 -t

Envoi d’une requête 'Ping'  10.0.50.1 avec 32 octets de données :
Délai d’attente de la demande dépassé.
Délai d’attente de la demande dépassé.
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.50.1 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 10.0.50.1:
    Paquets : envoyés = 15, reçus = 13, perdus = 2 (perte 13%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

```
icrosoft Windows [version 10.0.19045.2006]
(c) Microsoft Corporation. Tous droits réservés.

:\Users\CLIENTMK>ping 8.8.8.8 -t

nvoi d’une requête 'Ping'  8.8.8.8 avec 32 octets de données :
éponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
éponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
éponse de 8.8.8.8 : octets=32 temps=7 ms TTL=127
éponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
élai d’attente de la demande dépassé.
élai d’attente de la demande dépassé.
élai d’attente de la demande dépassé.
éponse de 10.0.50.18 : Impossible de joindre l’hôte de destination.
éponse de 10.0.50.18 : Impossible de joindre l’hôte de destination.
éponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
éponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
éponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
éponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
éponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
éponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
éponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
éponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
éponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127
éponse de 8.8.8.8 : octets=32 temps=9 ms TTL=127

tatistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 19, reçus = 16, perdus = 3 (perte 15%),
urée approximative des boucles en millisecondes :
    Minimum = 7ms, Maximum = 9ms, Moyenne = 8ms
```

```
onfiguration IP de Windows


arte Ethernet Ethernet0 :

   Suffixe DNS propre à la connexion. . . : home.arpa
   Adresse IPv6 de liaison locale. . . . .: fe80::fc36:71df:da75:9f04%14
   Adresse IPv4. . . . . . . . . . . . . .: 10.0.50.18
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 10.0.50.4

arte Ethernet Connexion réseau Bluetooth :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :
```

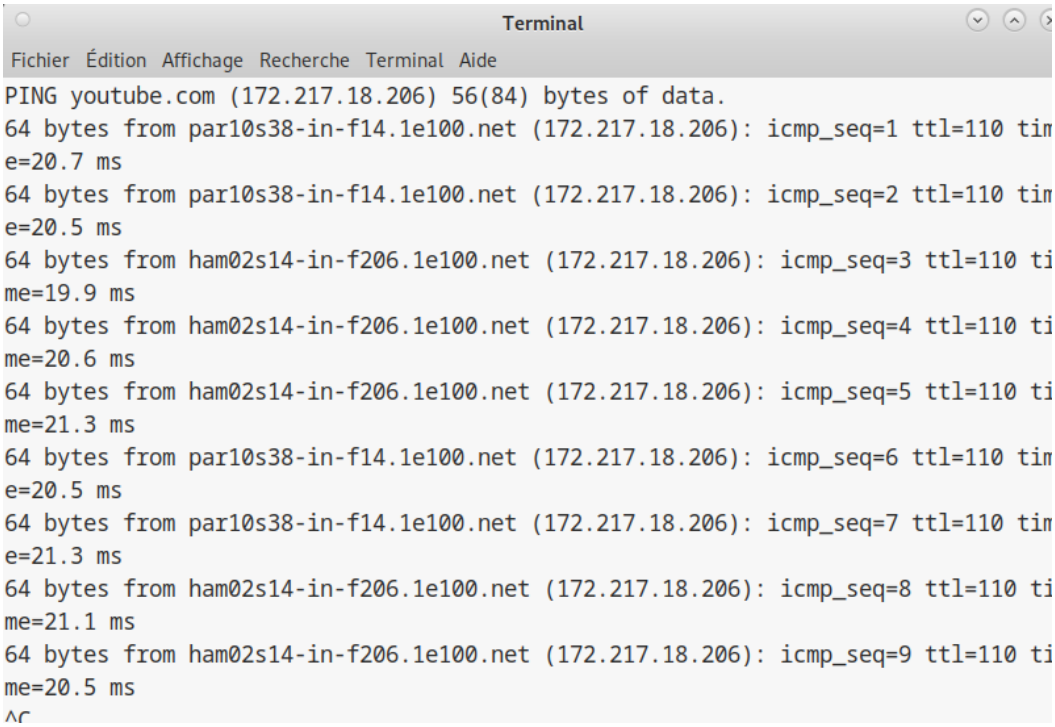
```
C:\Users\CLIENTMK>ipconfig

Configuration IP de Windows


Carte Ethernet Ethernet0 :

   Suffixe DNS propre à la connexion. . . : home_slave.arpa
   Adresse IPv6 de liaison locale. . . . .: fe80::fc36:71df:da75:9f04%14
   Adresse IPv4. . . . . . . . . . . . . .: 10.0.50.18
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 10.0.50.1

Carte Ethernet Connexion réseau Bluetooth :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :
```

BONUS

1.1/Bloquer YouTube

Pour bloquer un site, dans notre cas « YouTube », on va aller dans **Firewall -> Aliases -> Add**

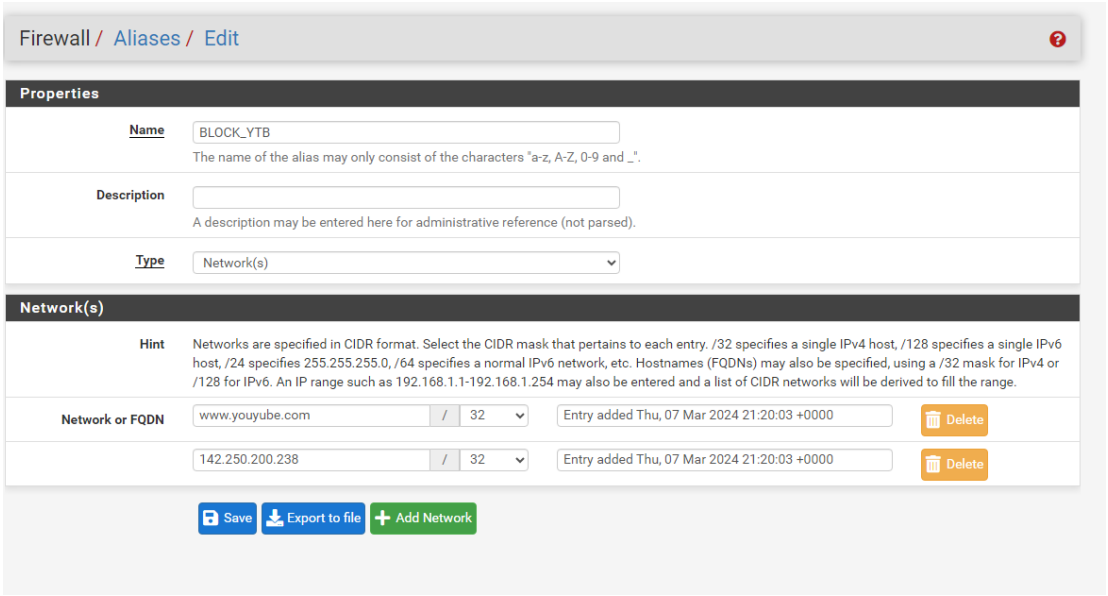
Pour trouver son IP, il suffit de faire un ping de www.youtube.fr.



On connaît maintenant l'adresse @IP de YouTube.

On ajouter un site en tant Aliasses, dans notre cas « YouTube », on va aller dans **Firewall -> Aliases -> Add**

On inclut le **FQDN.**



Firewall Aliases IP

Name	Type	Values	Description	Actions
CLT_LAN1	Host(s)	10.0.50.0, 10.0.50.1, 10.0.50.2, 10.0.50.3, 10.0.50.4, 10.0.50.5, 10.0.50.6, 10.0.50.7, 10.0.50.8, 10.0.50.9...		
SLAVE_PFsense	Host(s)	172.16.0.2		
YOUTUBE_BLOQUER	Network(s)	172.217.18.206/32, www.youtube.com		

Add

Nos Aliases avec Notre réseau @IP,

Youtube

Firewall / Rules / Edit

Edit Firewall Rule

Action — Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled — ☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface — LAN

Choose the interface from which packets must come to match this rule.

Address Family — IPv4

Select the Internet Protocol version this rule applies to.

Protocol — Any

Choose which IP protocol this rule should match.

Source

Source — ☐ Invert match | Address or Alias | CLT_LAN1 | /

Destination

Destination — ☐ Invert match | Address or Alias | YOUTUBE_BLOQUER | /

Extra Options

Log — ☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description — bloquer youtube site

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options — Display Advanced

Rule Information

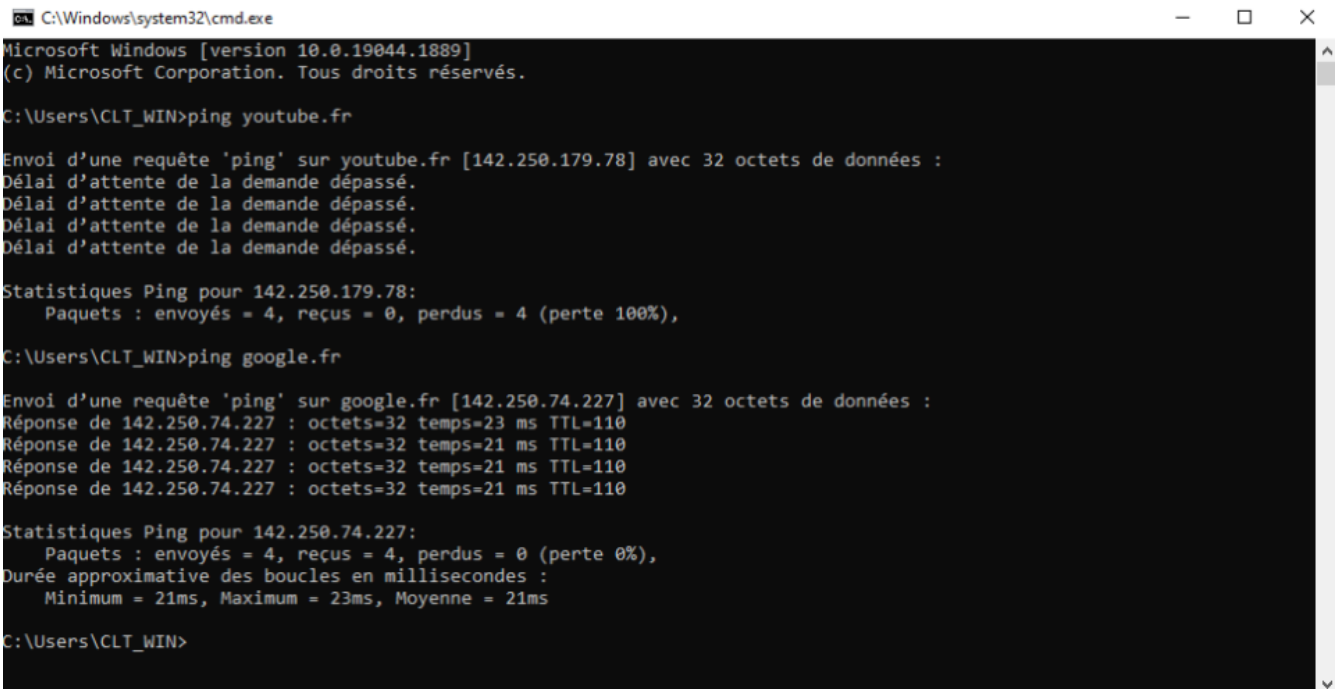
Tracking ID — 1709128905

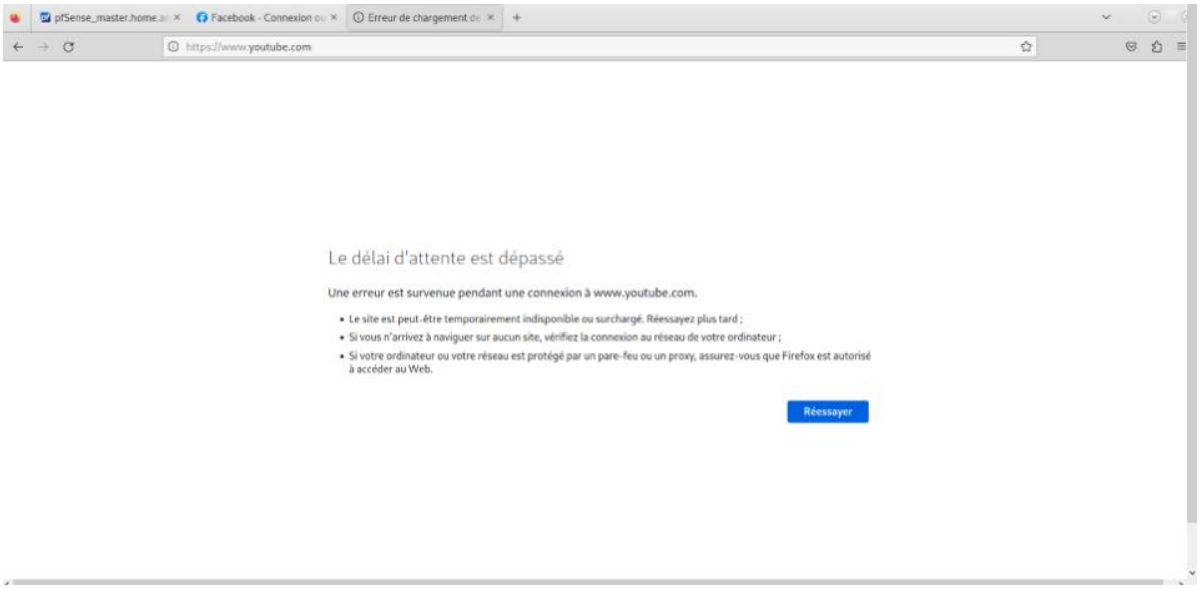
Created — 2/28/24 15:01:45 by admin@10.0.50.13 (Local Database)

Updated — 3/7/24 21:30:45 by admin@10.0.50.18 (Local Database)

Save

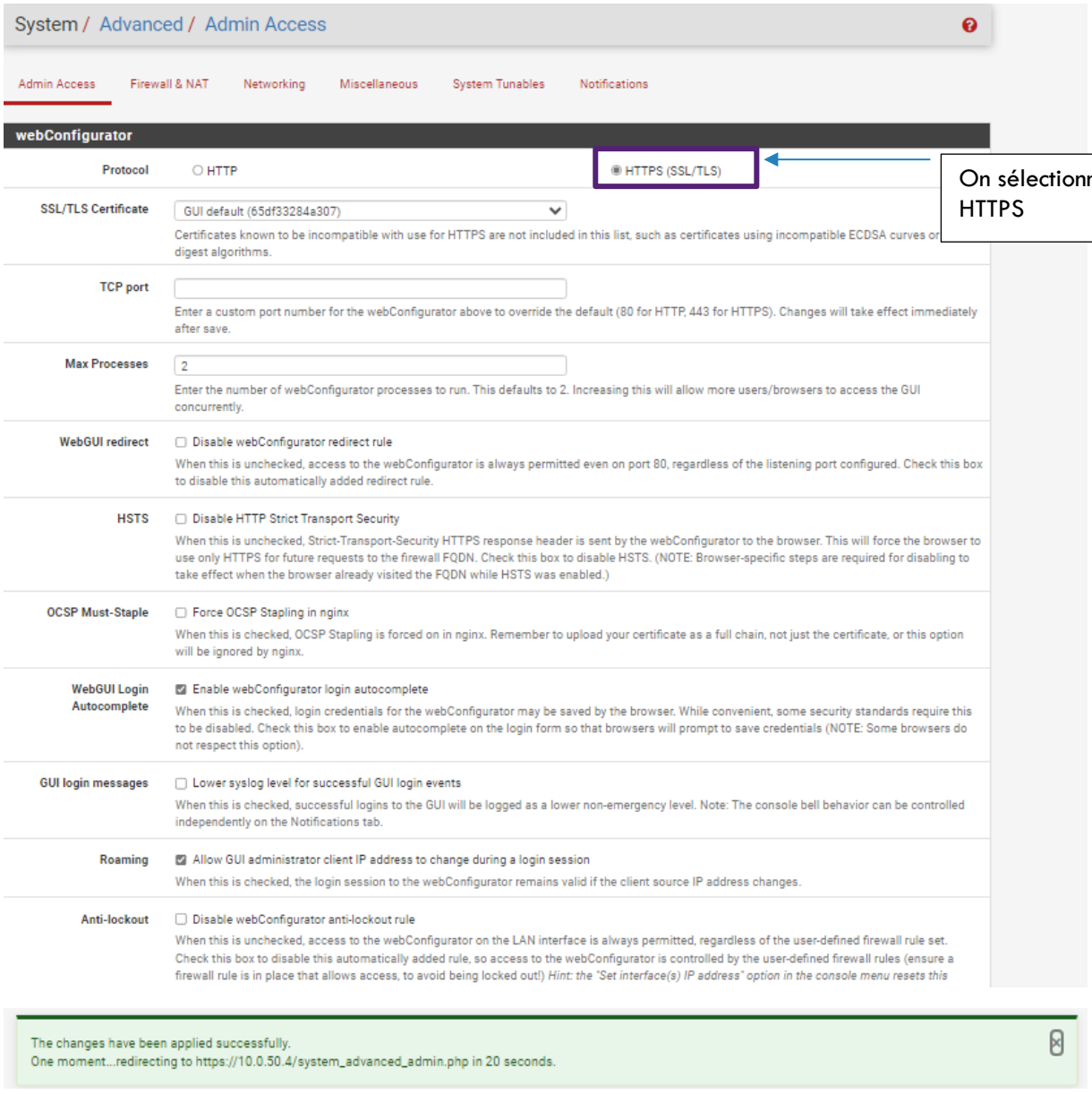
Test du blocage de YouTube



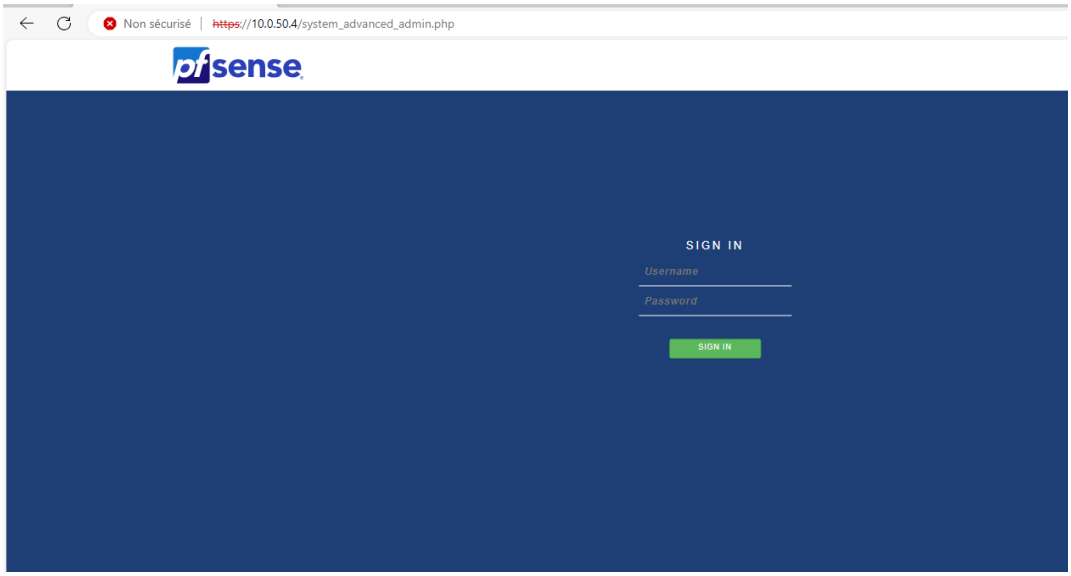


HTTPS)

Aller dans **System -> Advanced -> Admin Access**



On « Save »



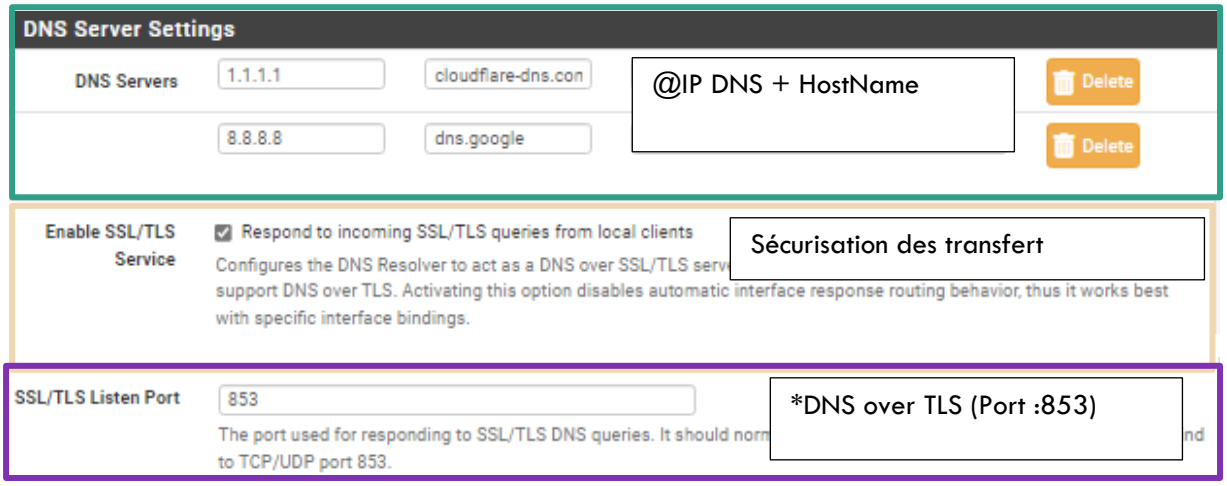
Nous voici sur notre interface en HTTPS !

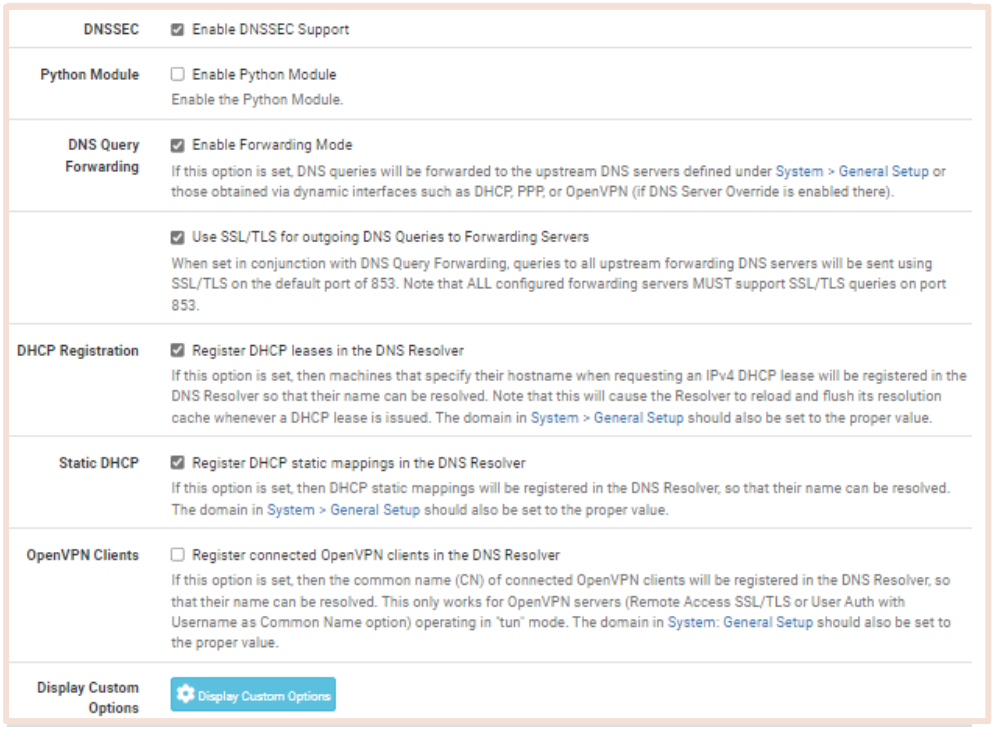
DNSSEC)

Le DNSSEC (Domain Name System Security Extensions, extensions de sécurité du système de noms de domaine) est une signature cryptographique qui est ajoutée aux enregistrements DNS afin de sécuriser les données transmises sur les réseaux IP (protocole Internet).

System -> General Setup

On saisit le HostName DNS de Cloud Flare et Google.





On active DNSSEC

SSL

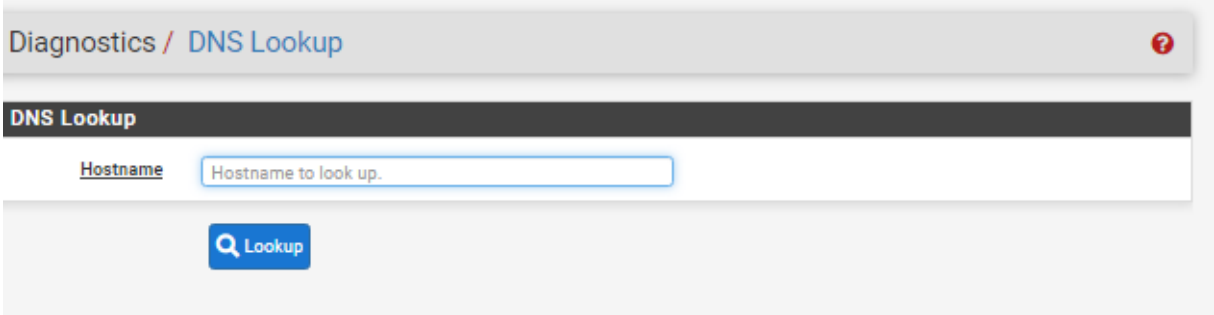
On l'inclue Dans le DHCP

Définition DNS over TLS : **DNS over TLS (DoT)** est un protocole de sécurité pour le chiffrement et l'encapsulation des requêtes et des réponses DNS via le protocole TLS. Le but de la méthode est d'augmenter la confidentialité et la sécurité des utilisateurs en empêchant les écoutes et la manipulation des données DNS

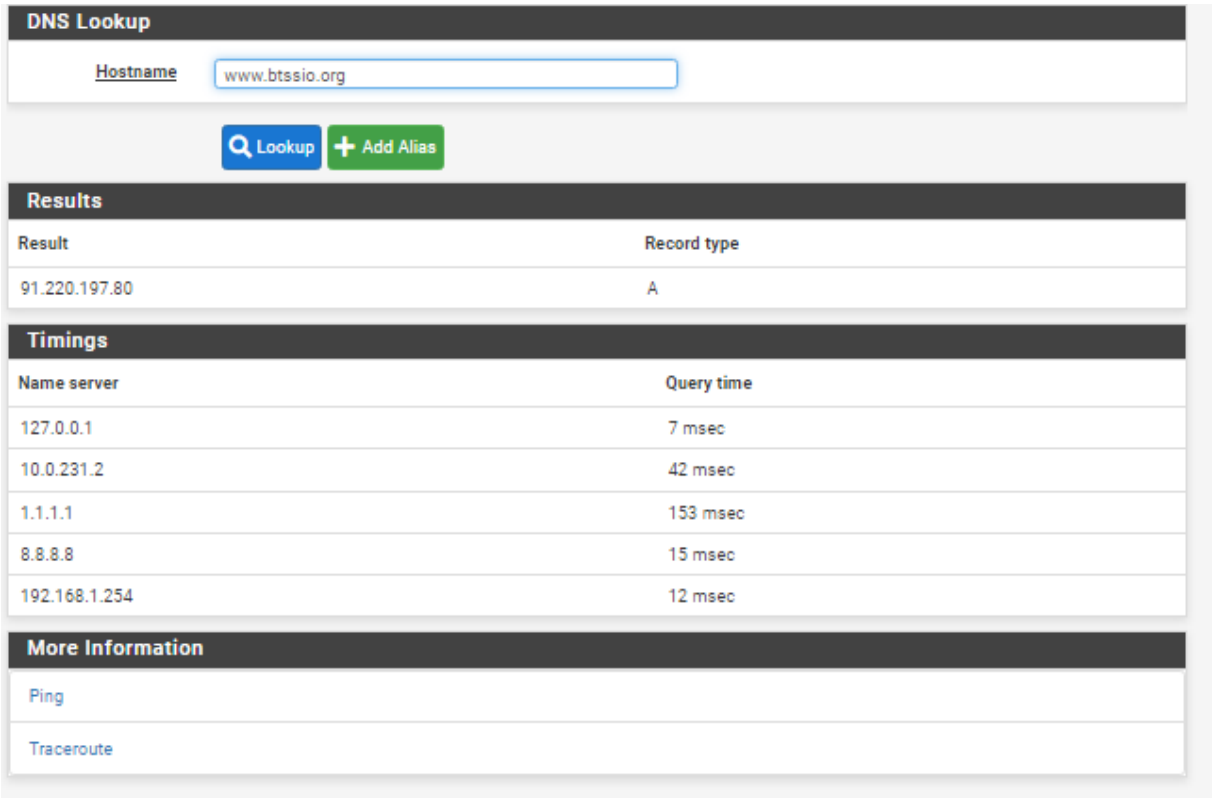
Test du fonctionnement DNSSEC

On va dans **Diagnostics -> DNS Lookup**

On saisit une adresse, dans mon cas j'ai choisi « **www.btssio.org** »

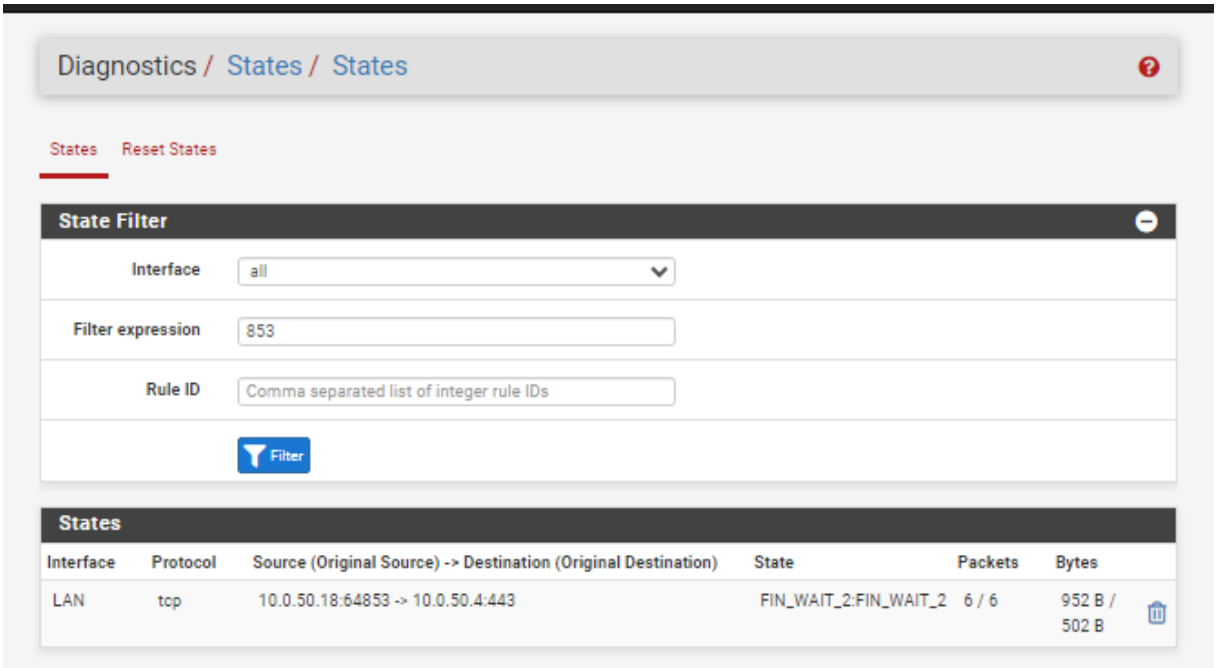


Puis on obtient ceci :



On va dans **Diagnostics -> States -> States**

Puis on saisit à **Filter expression 853** qui correspond au **port DoT**



Conclusion Générale

Avantage de pfSense :

- Gratuit, même si la machine ou la vm qui hébergera Pfsense ne l'est pas, la solution en elle-même ne coûte rien.

-Les évolutions d'un logiciel libre, comme ses mises à jour, dépendent d'une communauté de développeurs et non pas d'un éditeur unique.

-La communauté développe chaque partie des logiciels libres et Open Source. Le développement communautaire favorise la réactivité lorsqu'il s'agit de corriger un bug ou une faille de sécurité.

Désavantages de pfSense :

- Parce que c'est libre, tout le monde peut étudier son fonctionnement et trouver des failles.

-Un firewall matériel est plus stable qu'un firewall logiciel comme pfsense, le vendeur "contrôle" son hardware et à conçu son firewall autour de cette hardware.

- Vous n'avez aucune garantie si vous avez un problème matériel ou logiciel, vous devez vous débrouiller ou alors payer pour du support.

- L'interface peut en rebuter plus d’un, elle peut paraître peut intuitive et trop fournis.

Avis Globale sur cette installation :

- J’ai trouvé cette installation, intéressante on peut voir qu’avec pfsense on peut à peu près tout faire et tout ça gratuit, il ne demande pas beaucoup de ressources parfaites pour un petit réseau d’entreprises qui tourne avec un serveur pas tout récent. Pas trop de difficulté rencontrée, j’ai aimé le concept de management de pfSense et le re-utiliserai dès que j’en aurai l’occasion. J’ai continué à chercher d’autres solutions qui pourront notamment être utilisées prochainement.

ANNEXE :

Liste des masques de sous-reseaux

CIDR	bits disponibles	Masque de sous-réseau	Nombre d'hôtes par sous-réseau
/1	31	128.0.0.0	2^{31}-2 = 2 147 483 646
/2	30	192.0.0.0	2^{30}-2 = 1 073 741 822
/3	29	224.0.0.0	2^{29}-2 = 536 870 910
/4	28	240.0.0.0	2^{28}-2 = 268 435 454
/5	27	248.0.0.0	2^{27}-2 = 134 217 726
/6	26	252.0.0.0	2^{26}-2 = 67 108 862
/7	25	254.0.0.0	2^{25}-2 = 33 554 430
/8	24	255.0.0.0	2^{24}-2 = 16 777 214
/9	23	255.128.0.0	2^{23}-2 = 8 388 606
/10	22	255.192.0.0	2^{22}-2 = 4 194 302
/11	21	255.224.0.0	2^{21}-2 = 2 097 150
/12	20	255.240.0.0	2^{20}-2 = 1 048 574
/13	19	255.248.0.0	2^{19}-2 = 524 286
/14	18	255.252.0.0	2^{18}-2 = 262 142
/15	17	255.254.0.0	2^{17}-2 = 131 070
/16	16	255.255.0.0	2^{16}-2 = 65 534
/17	15	255.255.128.0	2^{15}-2 = 32 766
/18	14	255.255.192.0	2^{14}-2 = 16 382
/19	13	255.255.224.0	2^{13}-2 = 8 190
/20	12	255.255.240.0	2^{12}-2 = 4 094
/21	11	255.255.248.0	2^{11}-2 = 2 046
/22	10	255.255.252.0	2^{10}-2 = 1 022
/23	9	255.255.254.0	2^{9}-2 = 510
/24	8	255.255.255.0	2^{8}-2 = 254
/25	7	255.255.255.128	2^{7}-2 = 126
/26	6	255.255.255.192	2^{6}-2 = 62
/27	5	255.255.255.224	2^{5}-2 = 30
/28	4	255.255.255.240	2^{4}-2 = 14
/29	3	255.255.255.248	2^{3}-2 = 6
/30	2	255.255.255.252	2^{2}-2 = 2
/31	1	255.255.255.254	2^{1}-0 =2
/32	0	255.255.255.255	2^{0}-0 =1

Services	Ports
Modbus	502
Telnet	23
FTP	21
SMTP	25
NTP	123
BOOTP	67
DHCP	67
HTTP	80
DNS	53
POP	110
SNMP	161