Documentation d'installation

Installation PFSENSE (Redondance, Filtrage, NAT, VPN)

pfsense®

PROXY

18/03/2018 Yohan Fresneau

Sommaire

1. Pourquoi mettre en place PFSENSE

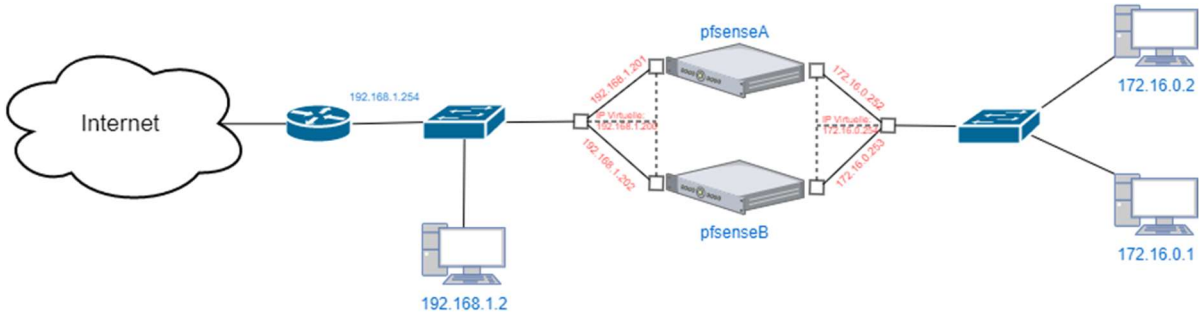
Pfsense est un routeur/pare-feu qui est libre de droit. Il est entièrement configurable par interface web et il a de nombreux service supporter comme :

- Routage
- DNS
- NAT
- Filtrage
- VPN(open vpn, L2TP, IPSec)
- Et plein d'autres services.

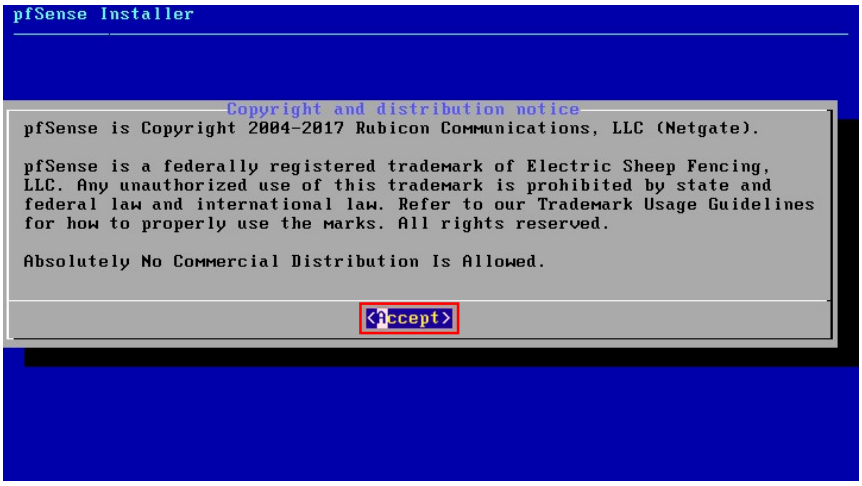
Il y'a aussi la possibilité de faire de la redondance et de la haute disponibilité, et de mettre en place des adresses IP virtuelle.

2. Configuration réseau

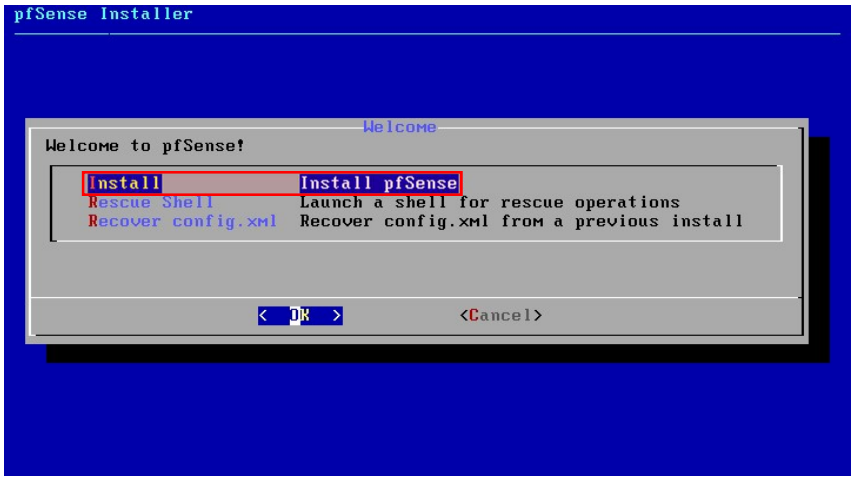
Pour cette installation, nous allons mettre en place 2 serveurs en redondance et avec une haute disponibilité comme sur le schéma suivant :



3. Installation Pfsense

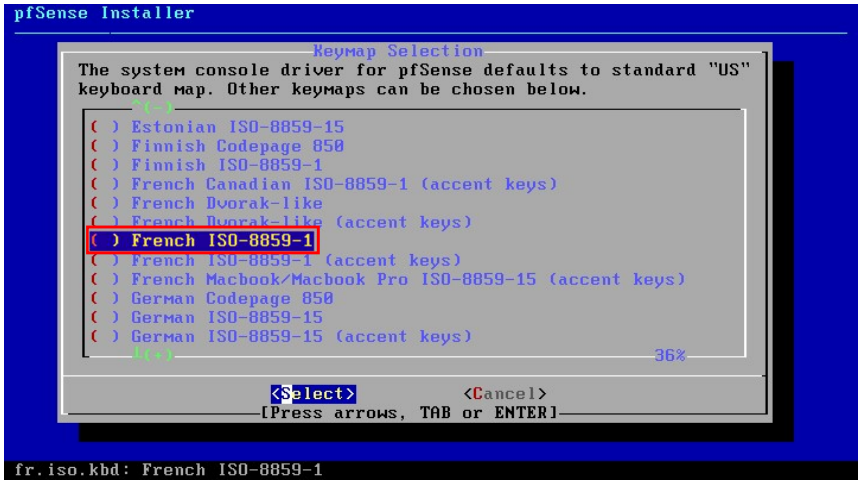


Accepter les termes afin d'installer pfsense

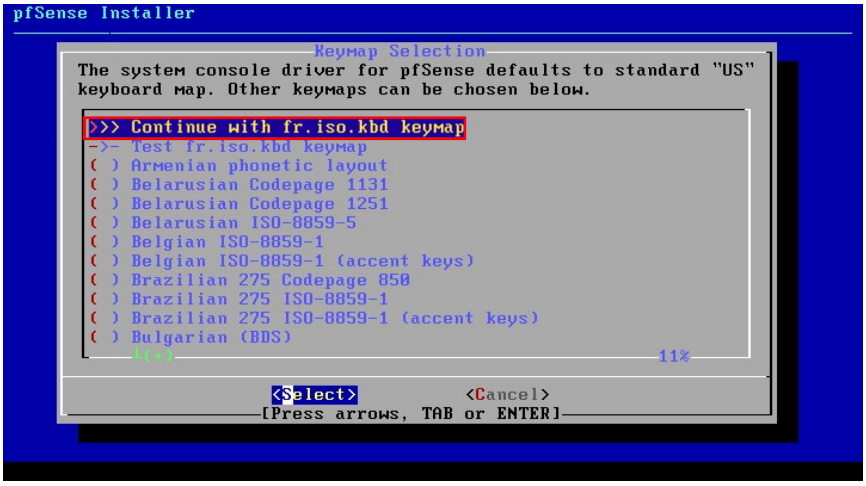


*Sélectionner « **Installer pfsense** »*

Nous allons sélectionner le clavier français en azerty, pour cela effectuer ces actions

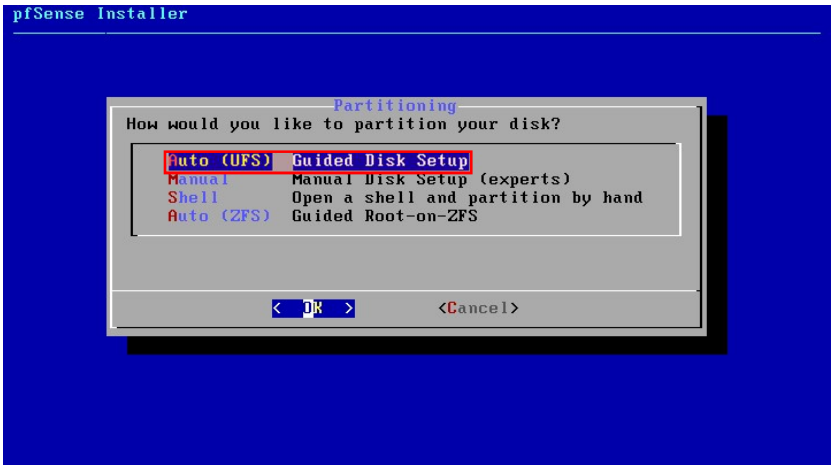


Sélectionner « French ISO-8859-1 »

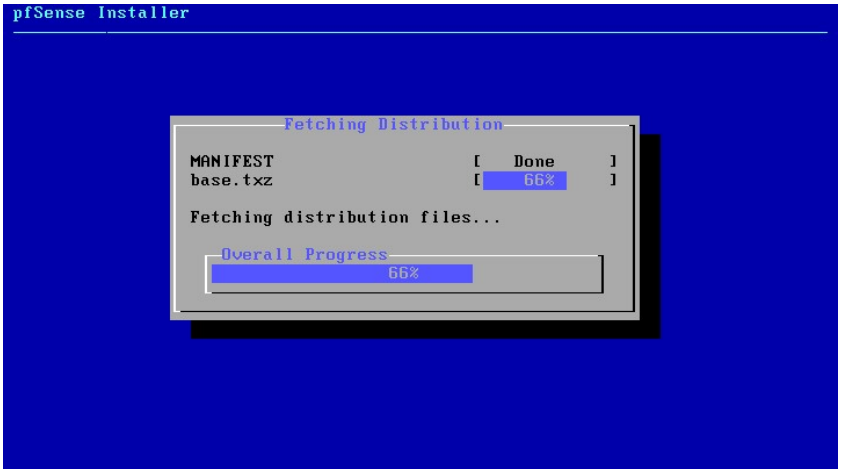


On confirme bien notre choix, choisir Continuer

Une fois le clavier choisi, on installe le système sur le disque

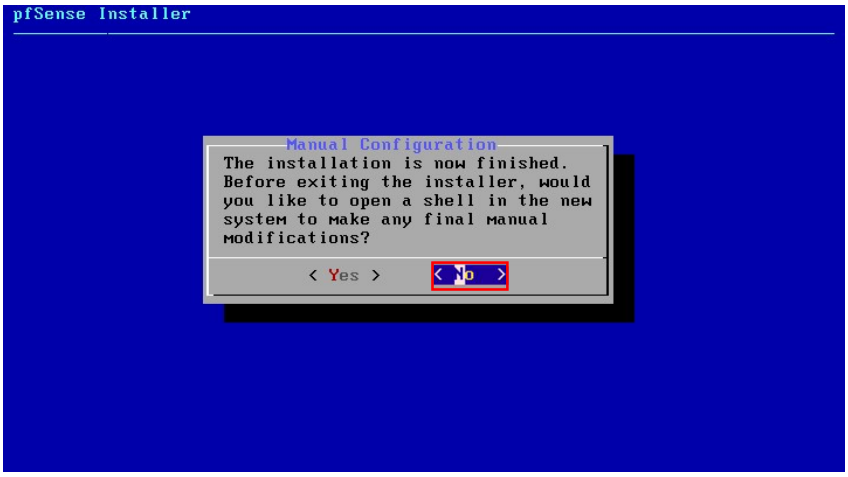


J'ai utilisé le partitionnement automatique, mais cela n'est pas obligé

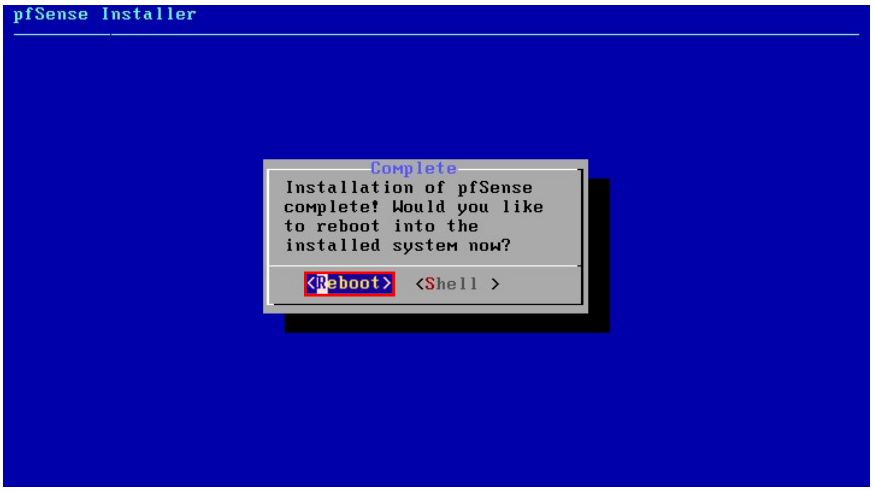


La progression d'installation nous indique son état

Une fois fini, il nous demande si l'on souhaite redémarrer ou bien afficher le « **Shell** »



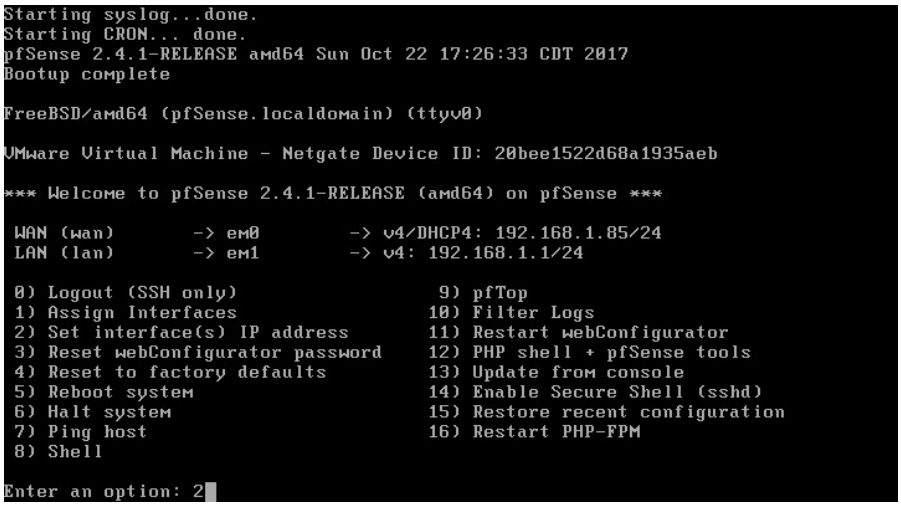
*Sélectionner « No », pour redémarrer et si vous voulez utiliser le « **Shell** » sélectionner « **Yes** »*



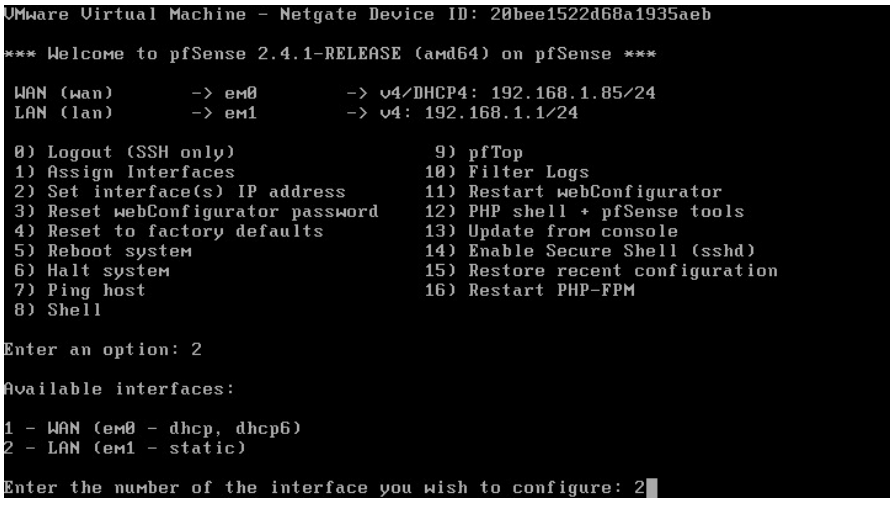
*Confirmation du choix "**Reboot**", pour redémarrer*

4. Configuration du serveur PFSENSE A

Une fois redémarrer, nous avons l'interface de pfsense qui est afficher.



Nous devons changer l'adresses de nos interface « Wan » et « Lan », pour cela sélectionner « 2 »



On sélectionne l'interface « Lan », qui est le choix « 2 »

```
WAN (wan)       -> em0        -> v4/DHCP4: 192.168.1.85/24
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

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 172.16.0.252
```

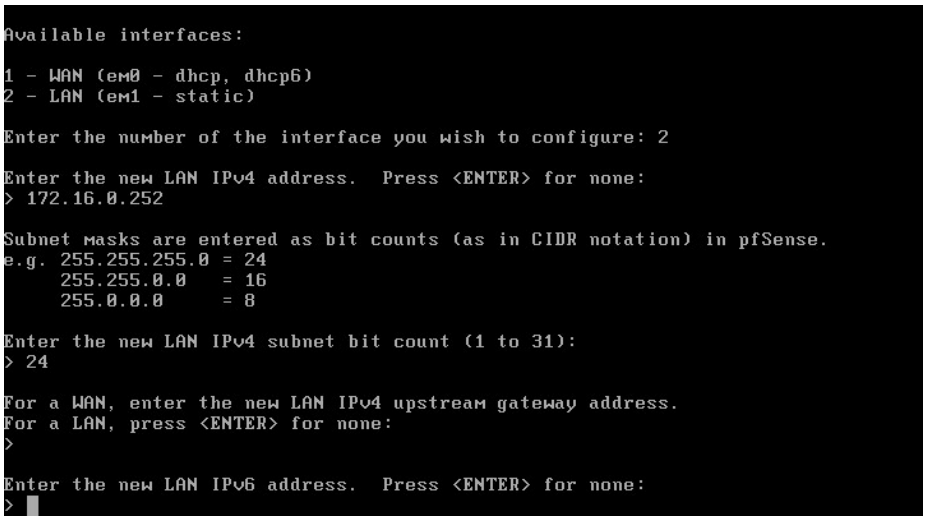
Ont défini l'adresse IP de notre interface

```
 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

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 172.16.0.252

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 31):
> 24
```

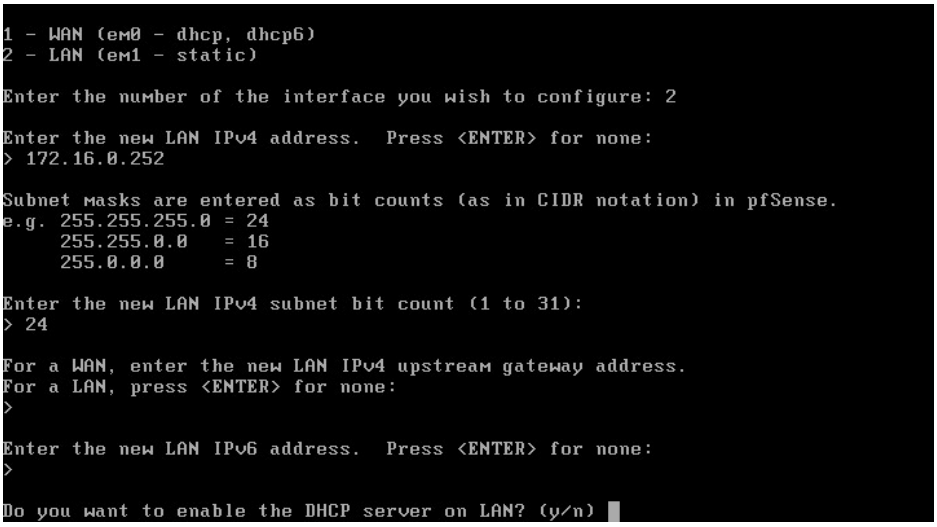
Et l'on indique le masque de sous réseau de notre réseau en « CIDR »

```
 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

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 172.16.0.252

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 31):
> 24

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

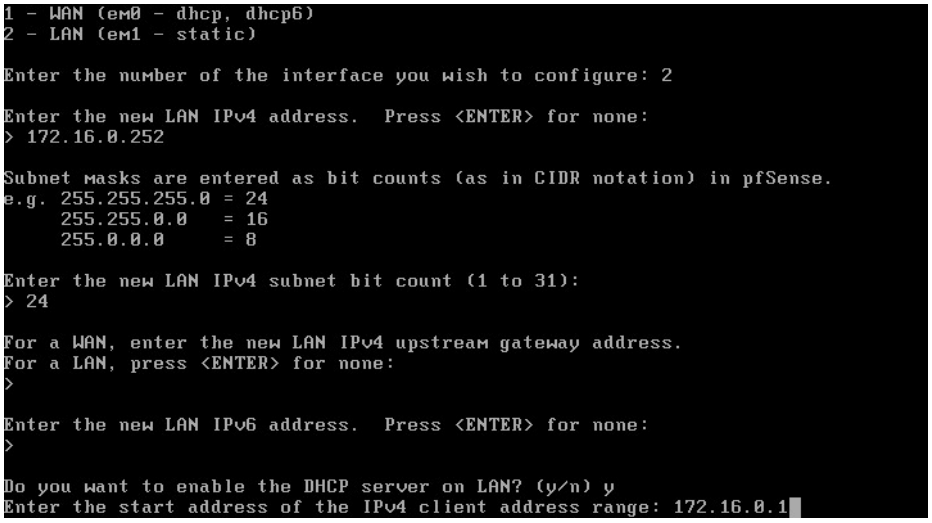
On ignore la question demander, en appuyant sur « Entrer »



On fait de même, car nous avons un réseau en IPv4



Nous pouvons ou non utiliser un serveur DHCP, pour mon cas j'en ai utiliser un pour faciliter la distribution d'IP



Si l'on utilise un DHCP, nous devons saisir le début de la plage d'adresse

```
2 - LAN (em1 - static)

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

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 172.16.0.252

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 31):
> 24

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

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

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 172.16.0.1
Enter the end address of the IPv4 client address range: 172.16.0.200
```

Et pour finir avec le DHCP, on saisit la fin de la plage d'adresse

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

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 172.16.0.252

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 31):
> 24

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

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

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 172.16.0.1
Enter the end address of the IPv4 client address range: 172.16.0.200
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y
```

Il nous ai demander si l'on veut utiliser l'interface web pour configurer pfsense

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

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

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 172.16.0.1
Enter the end address of the IPv4 client address range: 172.16.0.200
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

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

The IPv4 LAN address has been set to 172.16.0.252/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://172.16.0.252/

Press <ENTER> to continue.
```

Il nous affiche l'adresse de configuration

```
               http://172.16.0.252/

Press <ENTER> to continue.
Message from syslogd@pfSense at Nov  9 19:15:15 ...
pfSense php-fpm[339]: /index.php: Successful login for user 'admin' from: 172.16
.0.1

VMware Virtual Machine - Netgate Device ID: 20bee1522d68a1935aeb

*** Welcome to pfSense 2.4.1-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.1.85/24
 LAN (lan)       -> em1        -> v4: 172.16.0.252/24

 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
```

On fait de même avec l'interface « Wan »

```
VMware Virtual Machine - Netgate Device ID: 20bee1522d68a1935aeb

*** Welcome to pfSense 2.4.1-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.1.85/24
 LAN (lan)       -> em1        -> v4: 172.16.0.252/24

 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: 1
```

On sélectionne donc l'interface « 1 »

```
*** Welcome to pfSense 2.4.1-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.1.85/24
 LAN (lan)       -> em1        -> v4: 172.16.0.252/24

 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: 1

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

On saisit une adresse IP fixe, on refuse donc la configuration par DHCP

```
LAN (lan)       -> em1        -> v4: 172.16.0.252/24

 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: 1

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

Enter the new WAN IPv4 address.  Press <ENTER> for none:
> 192.168.1.201
```

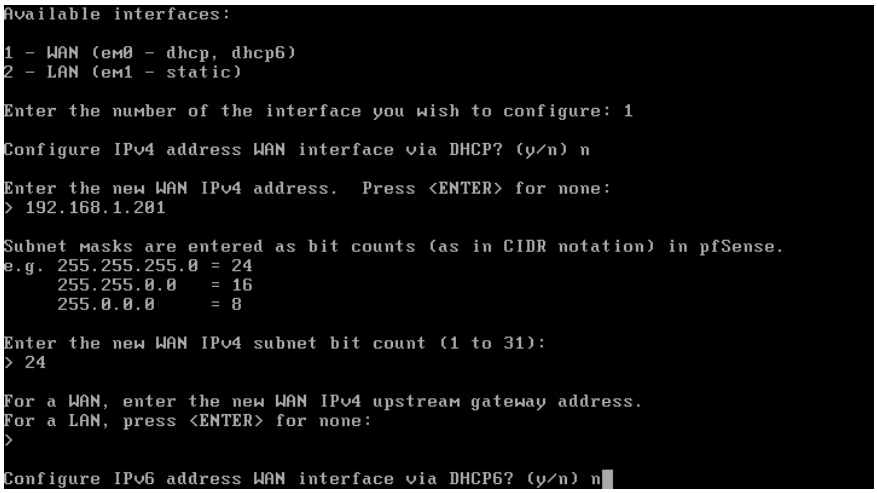
On indique donc l'adresse IP de l'interface

```
 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: 1

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

Enter the new WAN IPv4 address.  Press <ENTER> for none:
> 192.168.1.201

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 WAN IPv4 subnet bit count (1 to 31):
> 24
```

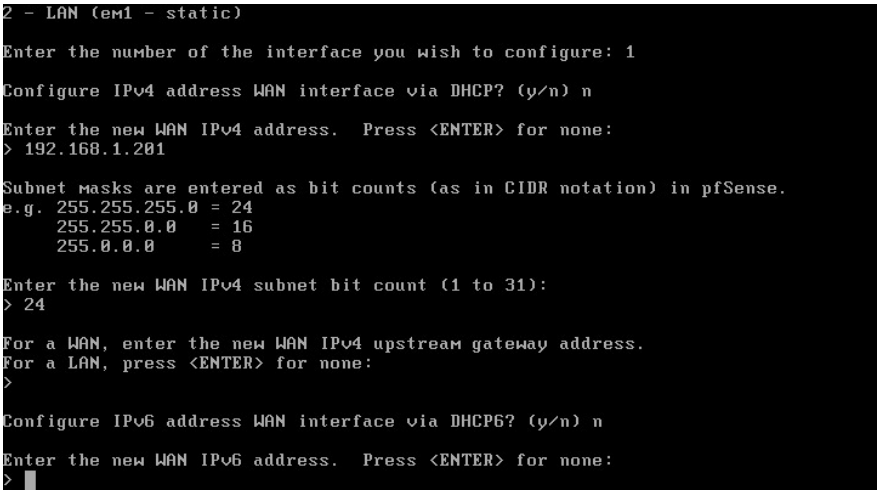
Le masque de sous réseau en « CIDR »

```
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: 1

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

Enter the new WAN IPv4 address.  Press <ENTER> for none:
> 192.168.1.201

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 WAN IPv4 subnet bit count (1 to 31):
> 24

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

On ignore la question, en appuyant sur « entrer »



Notre réseau « Wan », étant aussi en IPv4, on répond « non »



On fait de même pour cette question, en appuyant sur « entrer »

5. Configuration du serveur PFSENSE B

On fait de meme avec le serveur pfsenseB, avec cette configuration :

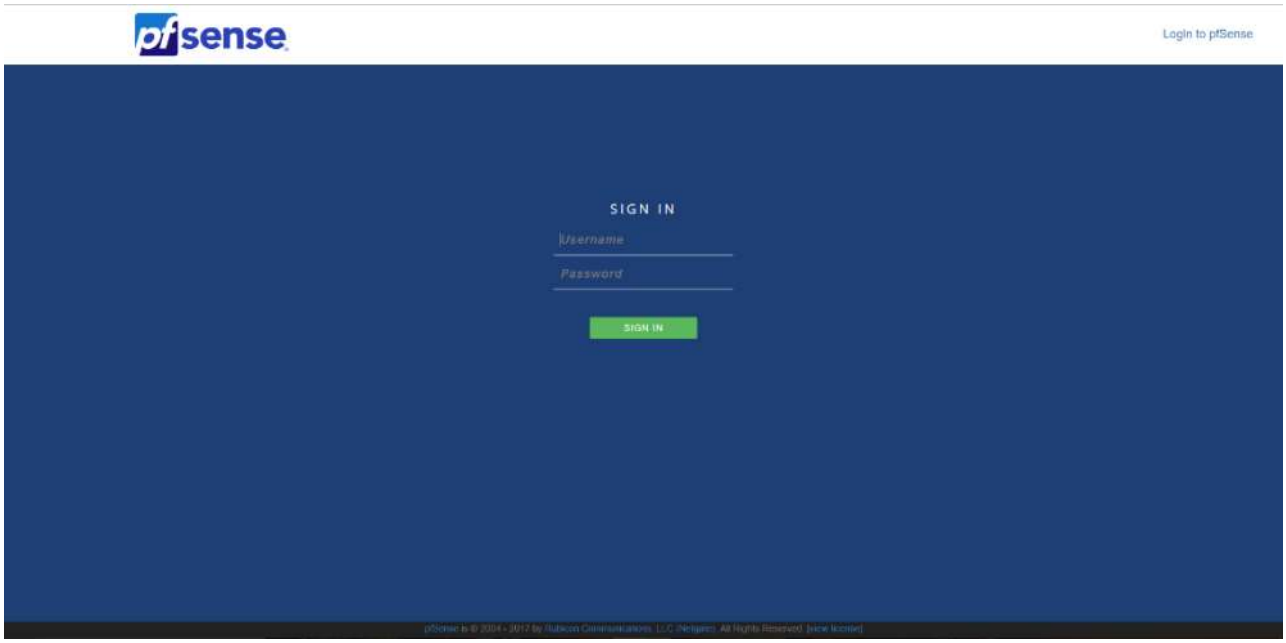
Lan : 192.168.1.202/24, Activation de la configuration web

Wan : 172.16.0.253/24

La configuration du 2^{émè} PFSENSE est identique, seul les IP des cartes réseaux change.

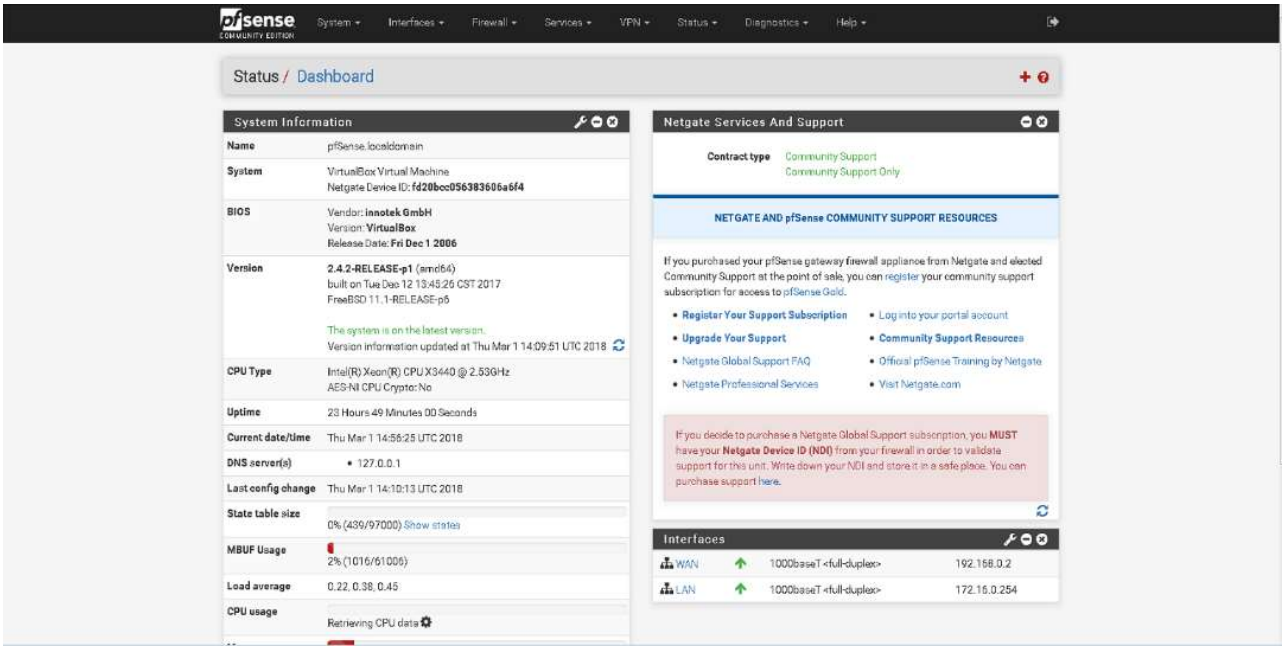
6. Interface Web PFSENSE

Pour cela, se connecter sur le panel PFSENSE



Login : admin **Password :** pfsense

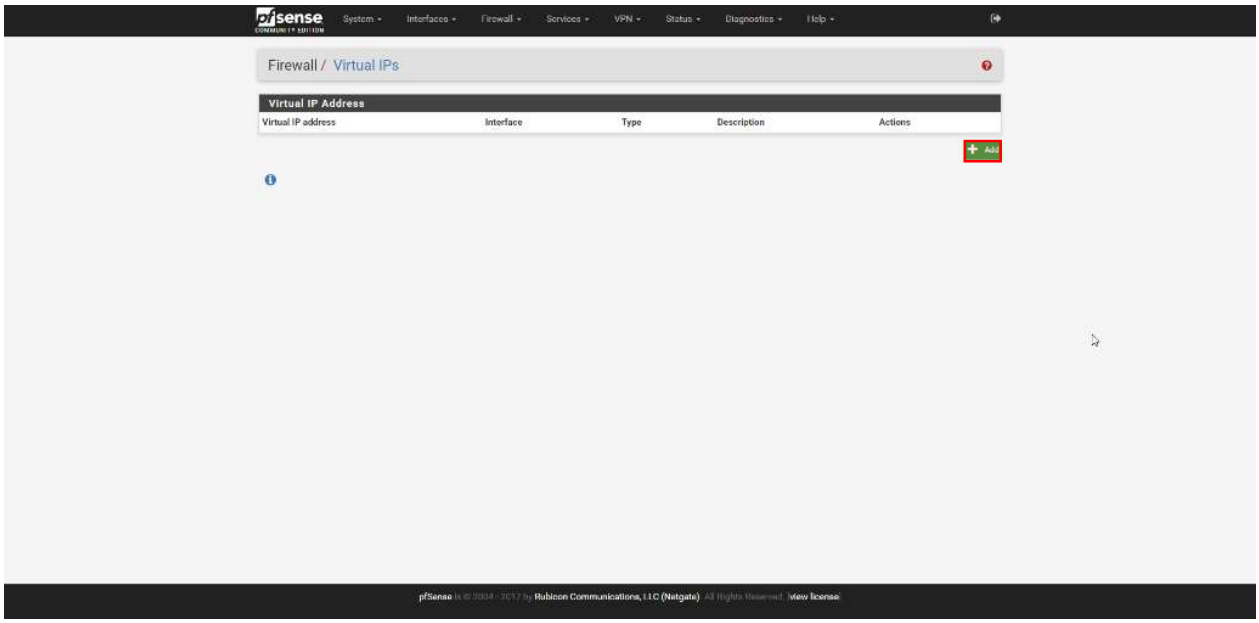
Nous avons le dashboard de PFSENSE, avec les informations principale et les informations système.



Nous avons le tableau de board avec pleins d'informations a propos du routeur/Firewall.

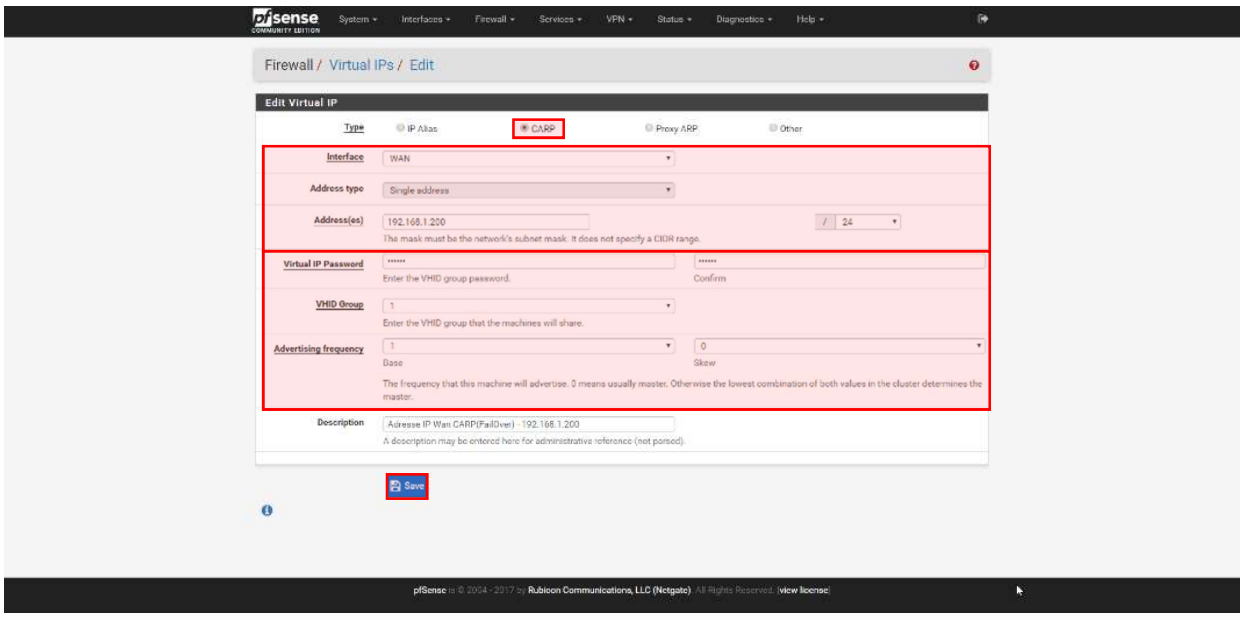
7. Configuration des adresses IP virtuelle (Haut Dispo)

La configuration des adresses IP, permet un basculement entre deux adresses IP. Cela permet de faire une redirection d'adresse IP. Si l'adresse 172.16.0.252 est down, il n'est pas possible de passer instantanément en adresse 172.16.0.253. Alors que si l'on créer une adresse IP en 172.16.0.254, qui permet de faire une redondance sur des adresses IP. Cela est utiliser pour les routeurs et les serveurs. Cela permet de rediriger le flux vers le serveur et en cas de chute de celui-ci le basculement est invisible pour l'utilisateur. Nous allons mettre en place une IP virtuelle entre deux PFSENSE coté Wan et Lan. La mise en place et identique sauf la carte réseau qui diffère.



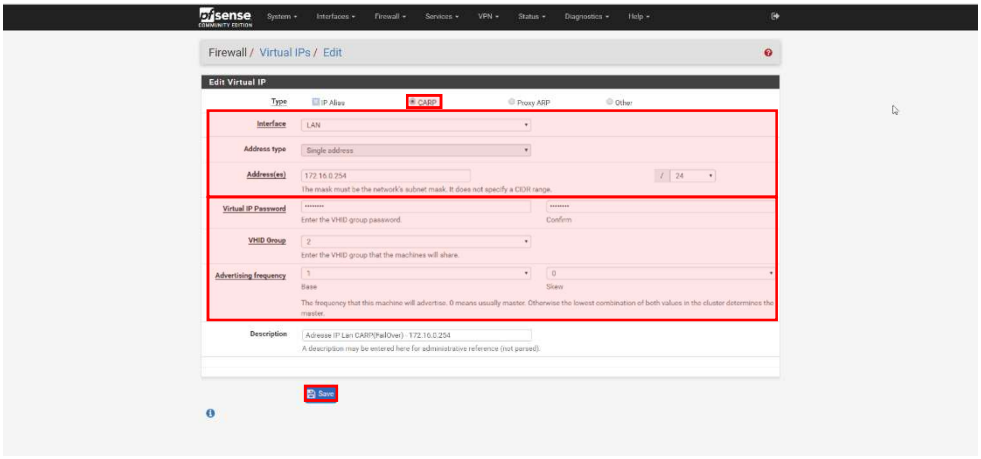
*Dans « **Firewall / Virtual IPs** », nous pouvons mettre en place les deux IP virtuelle coté Wan et Lan*

Nous allons créer l'IP virtuelle se trouvant, coté WAN



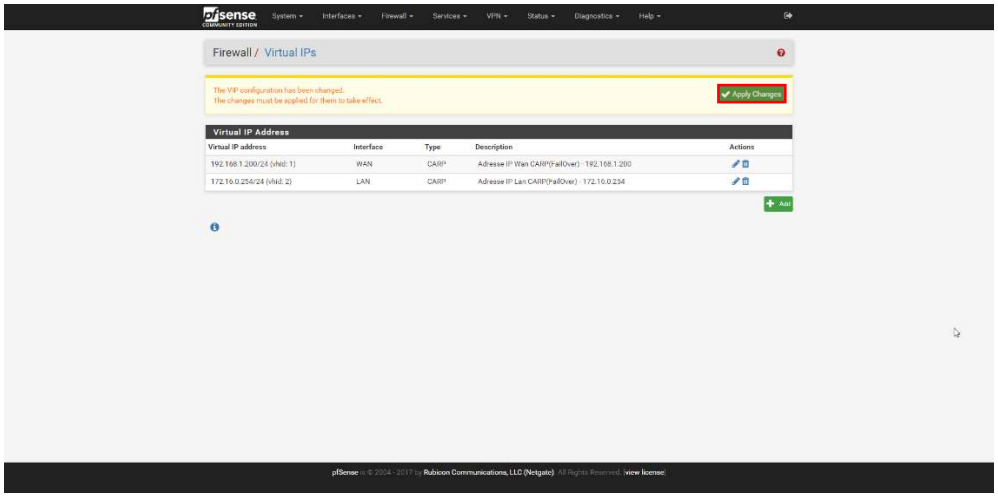
On créer notre IP virtuel WAN, comme ceci

Nous allons créer l'IP virtuelle se trouvant, coté WAN.



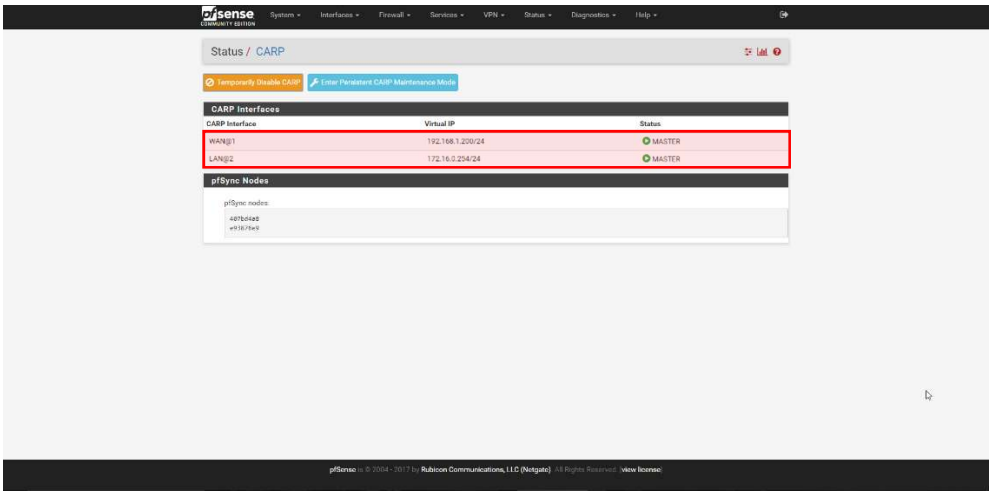
On fait de même pour l'interface Lan.

Nous allons pouvoir appliquer les paramètres



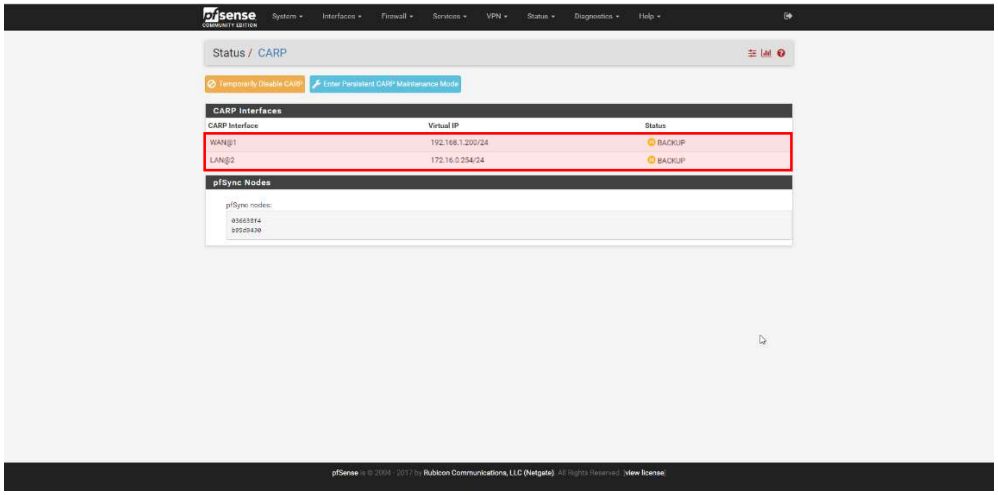
On à un récapitulatif de nos IP virtuelle. Il faut appliquer les parametres pour activer l'IP virtuelle

On peut voir dans le staus CARP, et savoir si l'interface est en "Master" ou bien en "Backup"



On peut voir le status des IP virtuelle, on voit que le PfsenseA est bien en master

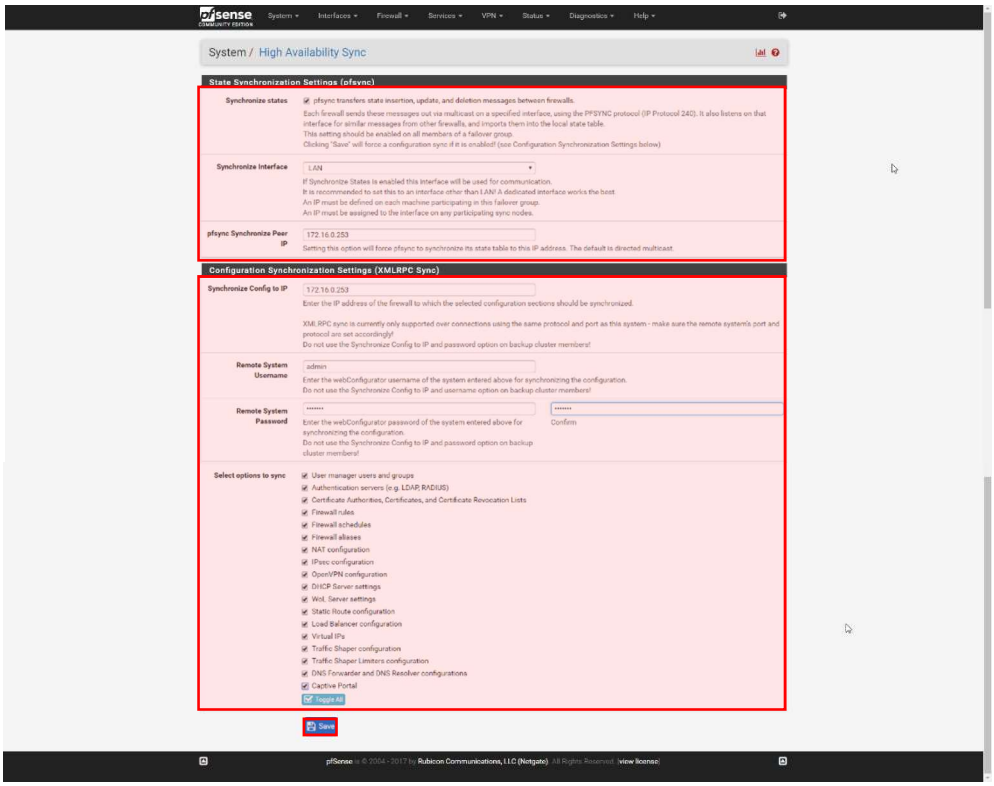
Le statut des IP virtuelle sur le second PFSENSE, il sont donc bien en backup



On peut voir le status des IP virtuelle, on voit que le PfsenseB est lui en backup

8. Configuration de la redondance

La mise en place de la redondance, nous permet une réplications des régles de filtrage, NAT, VPN, etc…. Ce permet de devoir effectuer la création d'une régle ou autre, uniquement d'un seul coté. La réplication s'effectue automatiquement.

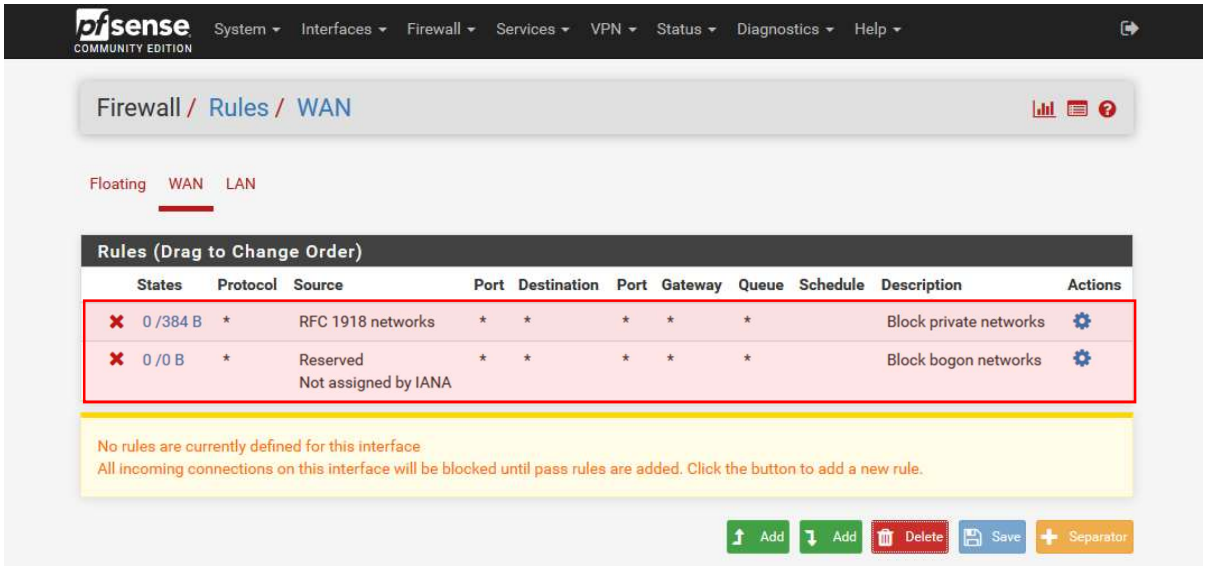


Nous allons mettre en place la redondance de Pfsense, afin d'avoir les memes paramétrages coté PfsenseA et PfsenseB. La configuration doit être actif des deux cotés

9. Mise en place de règles de filtrage

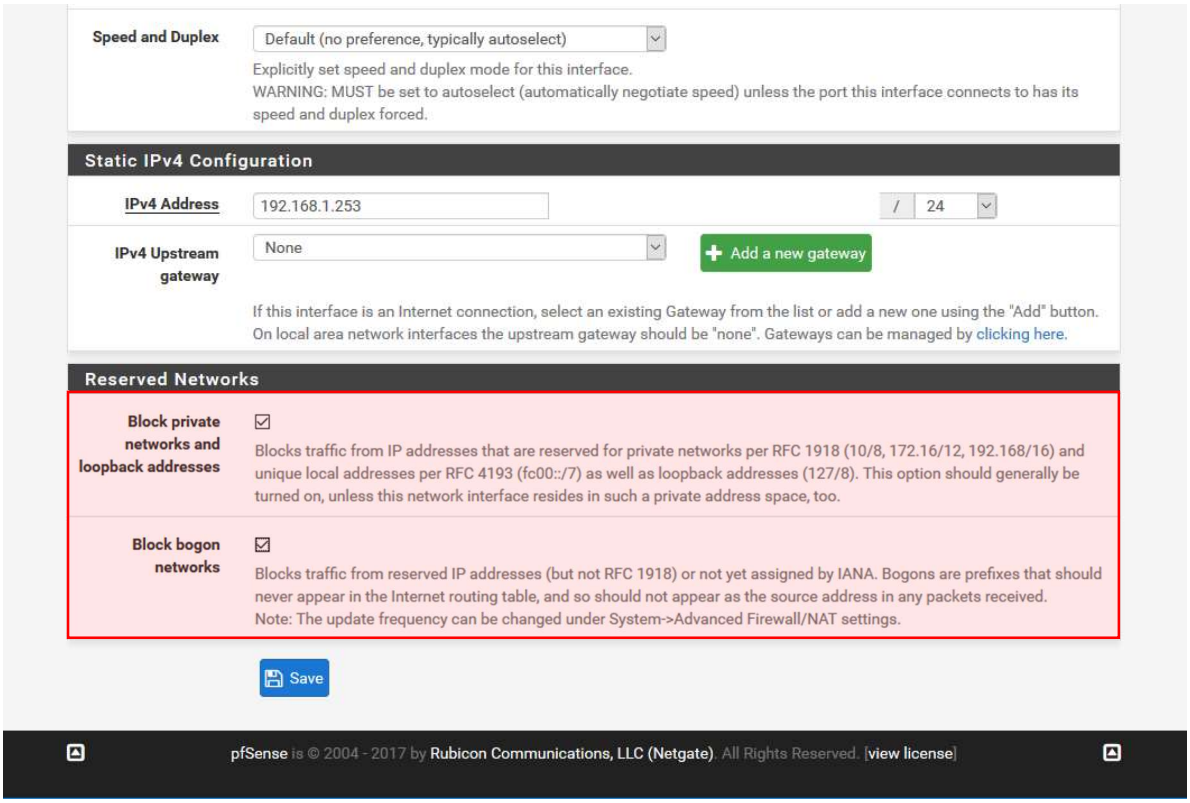
Les règles de filtrages permettent de mettre des restrictions sur des protocoles, Port, adresse IP.

Pour mettre en place des règles de filtrage coté WAN, nous devons désactiver une règle, car elle nous empêche d'ajouter des règles.



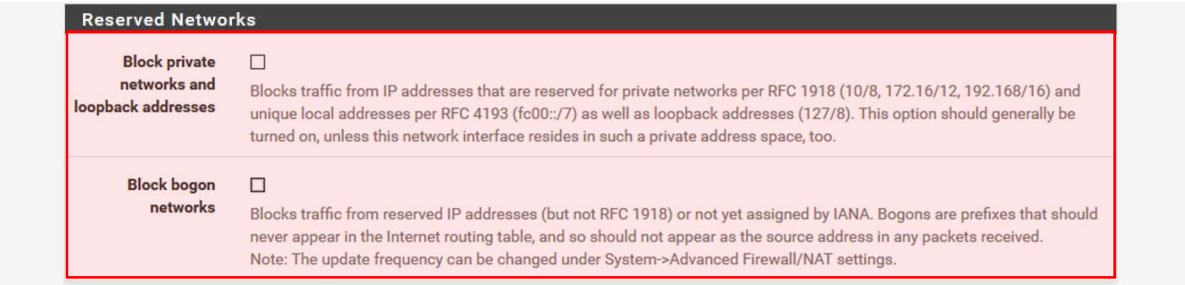
Nous devons enlever ces deux règles

Pour cela, nous devons aller dans les paramètres de l'interface WAN(**Interfaces / WAN**), ou bien cliquer sur l'engrenage à coté de nos deux règles de refus.



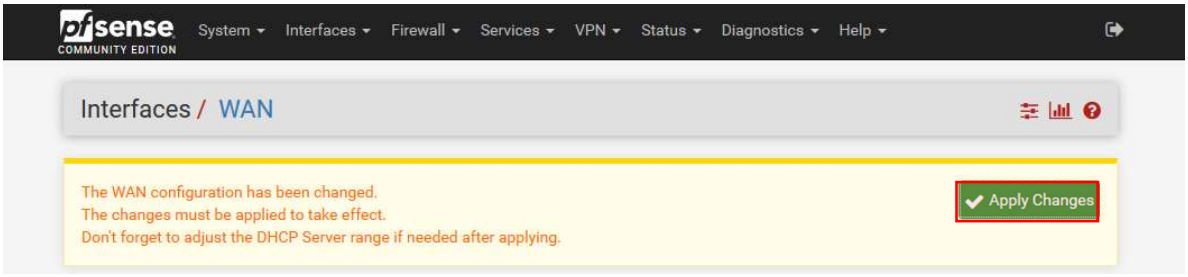
*Nous devons décocher les deux règles dans "**Reserved Networks**", elle empêche de créer des règles ce sont des sécurités actives de base.*

On doit se retrouver donc sans nos deux cases cocher



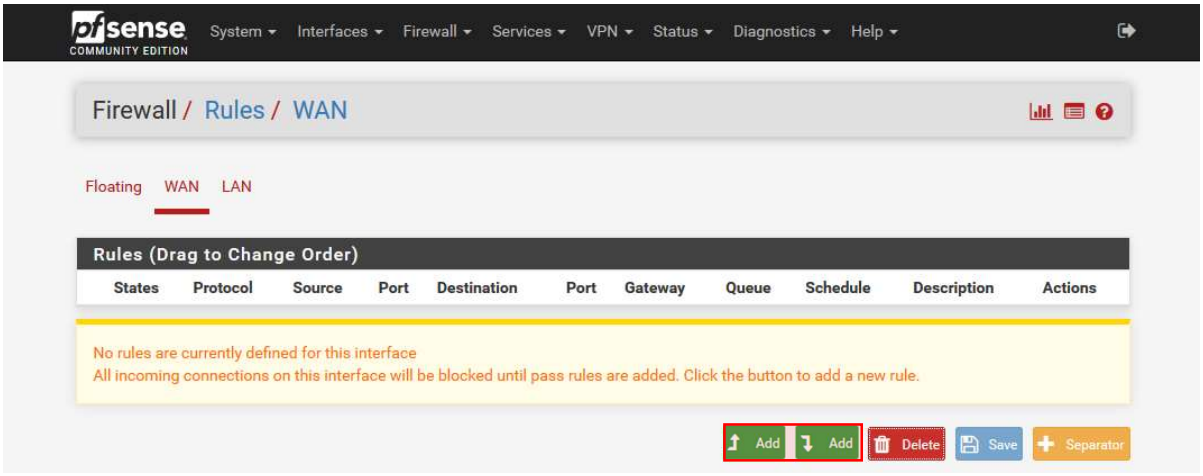
Aucune ne doit être cocher

Une fois enlever, nous devons appliquer les modifications



*Pour appliquer nous devons juste cliquer sur "**Apply Changes**"*

Comme on peut le voir maintenant, les deux règles ne sont plus présentes et nous pouvons donc en créer de nouvelles.



Pour ajouter une règle, nous devons cliquer sur "Add"

Il y'a plusieurs actions qui peuvent être appliquer sur la régles :

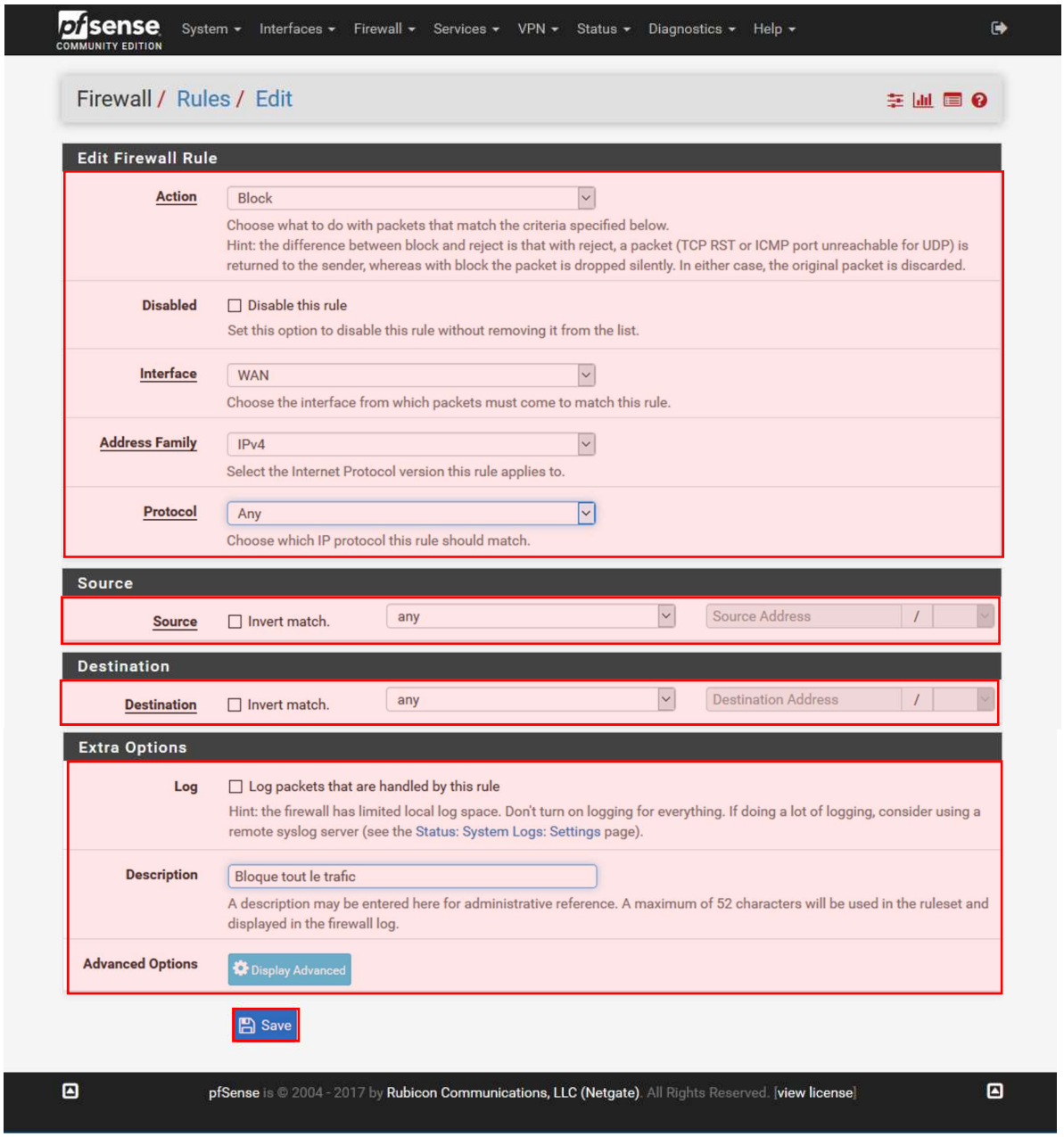
- Block : Détruit le paquet sans retour vers la source
- Reject : Un retour est effectué vers la source disant qu'il est refusé
- Pass : Accepte le paquet

Nous devons sélectioner notre interface (WAN ou LAN), sur la quelle la regle sera actif

On sélectionne si cela concerne IPv4 ou IPv6, ou bien les deux

Et pour finir on parametre notre régle, c'est-à-dire le protocole, la source et la destination et la source et on peut aussi mettre une description afin de savoir rapidement son action.

Dans ce cas-là c'est une régle de blockage, mais le principle est le meme pour toutes régles.



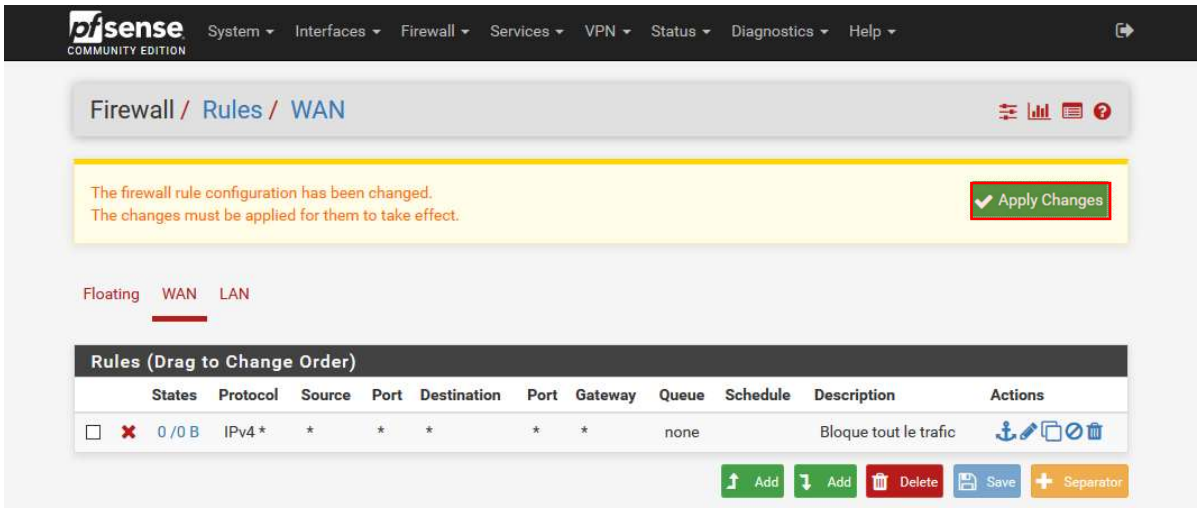
*Cliquer sur "**Save**", afin de créer notre règle.*

Attention la règles de blocage doit être effectuer en dernière coté LAN, elle risque de bloquer l'accès à l'interface web. Pour le coté LAN et WAN, le principe est le même. Il est possible de désactiver l'utilisations de certains protocoles ou bien bloquer une partie du réseau au certaines machines. Cet outil et pratique et puissant. Une liste de protocole et de port est pré-enregistrer, mais il est possible d'utiliser d'autres ports garce à la ligne "**Other**".

Il faut faire attention aux protocoles à bloquer, le plus simple est de désactiver tous les protocoles/Ports et créer une autorisation pour chaque protocoles/Ports ce qui augmente la sécurité du réseau.

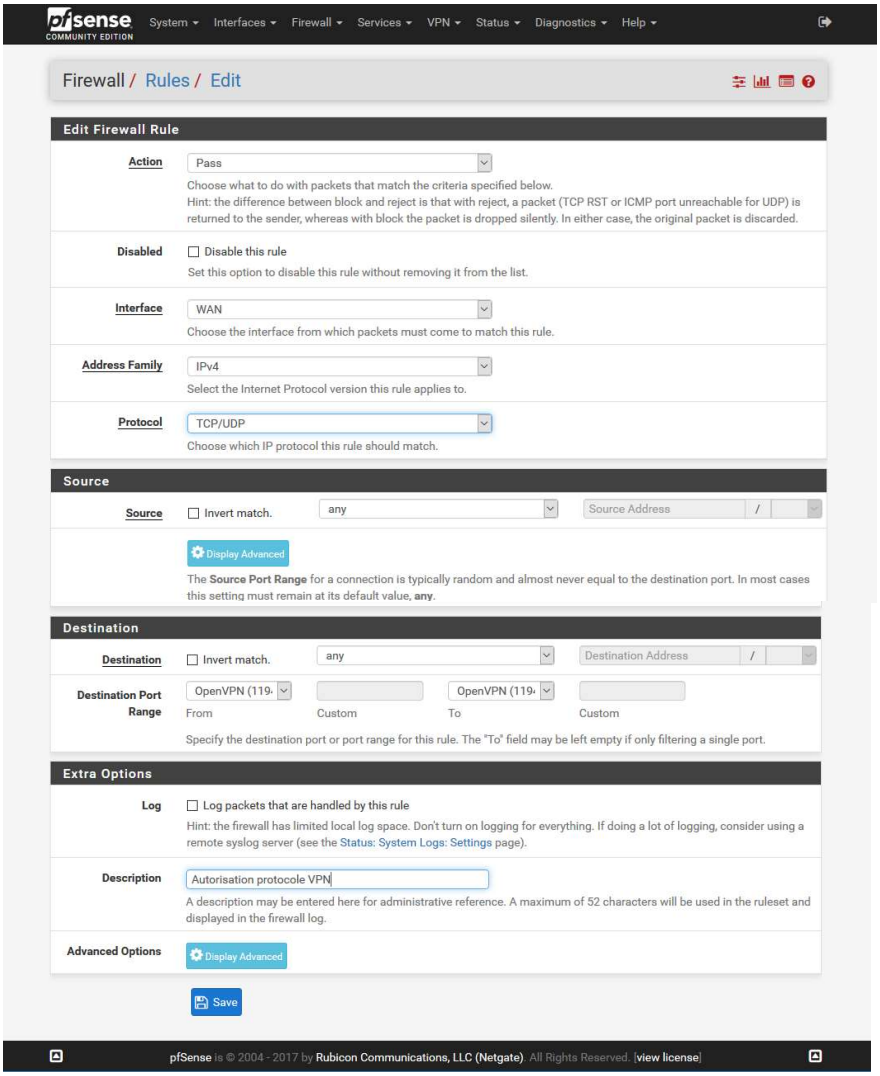
Faire attention à l'interface web coté Wan, ne pas oublier de vérifier la règle de l'interface web. Il y a une règle déjà créer normalement et ne doit pas être supprimer.

Une fois notre règle créer, nous devons l'appliquer



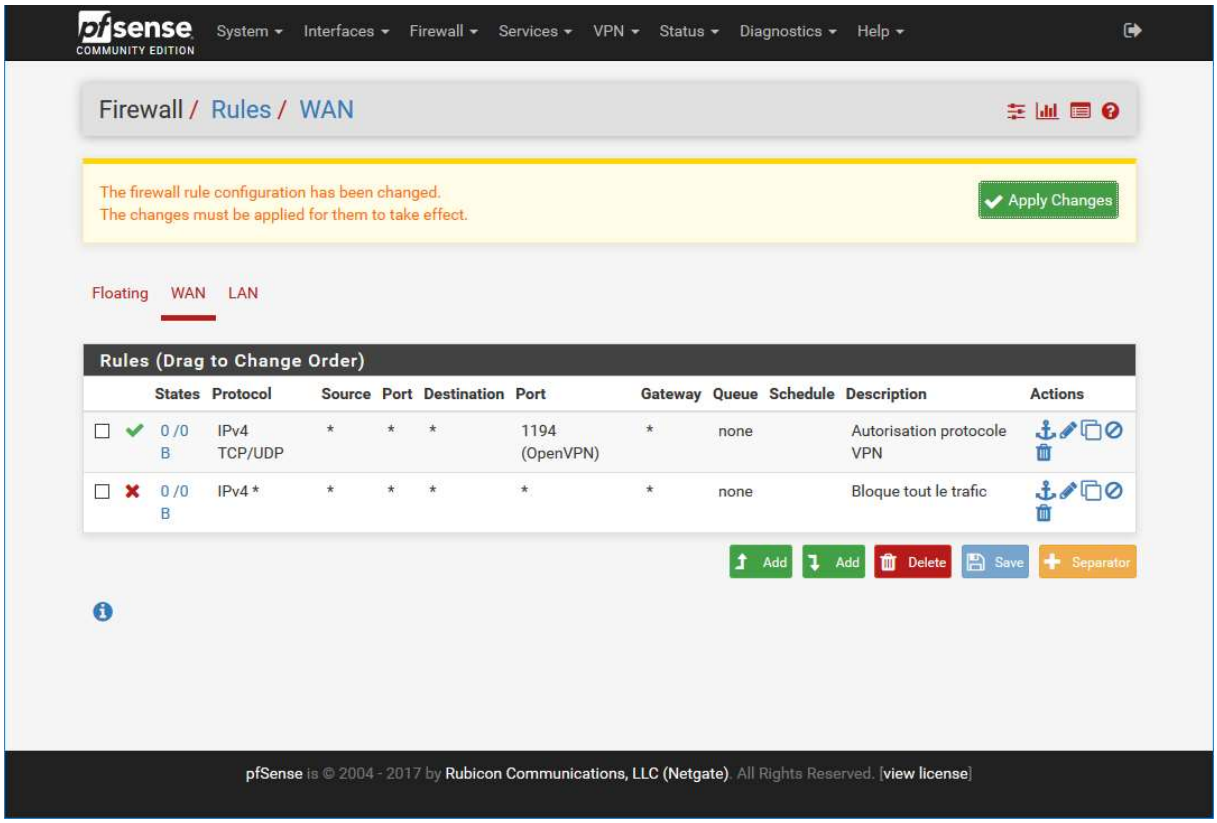
*Cliquer sur "**Apply Changes**", afin d'activer notre règle.*

Nous allons voir comment ajouter une règle coté WAN à destination du PFSENSE, comme le fait d'utiliser le serveur VPN(OpenVPN) de PFSENSE.



Exemple de règle de filtrage autorisent le protocole OpenVPN, elle reste semblable à toute autres protocoles

Une fois nos règles créer, nous devons les appliquer. Nous avons une rapide vision sur les règles et leurs actions. Attentions leurs ordres et important. Si la règle de blocage est en première aucune des règles après sera fonctionne.

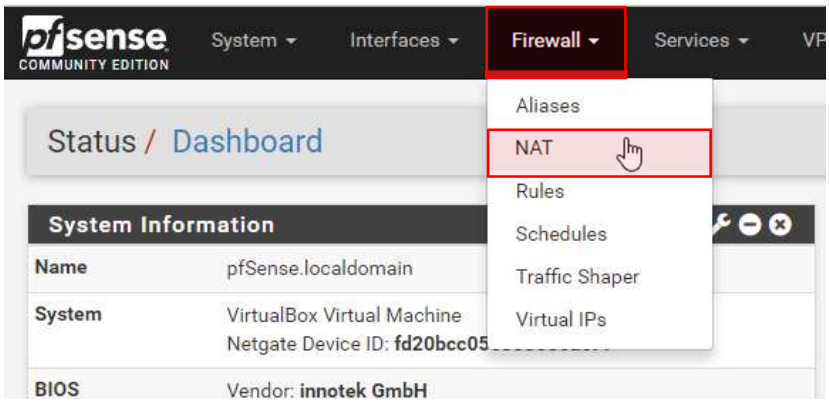


10. Mise en place redirection de port(NAT/PAT)

La redirection de port permet de transferer un port exemple :

Routeur 192.168.1.200 Machine 172.16.0.102

Port d'entrer 192.168.1.200 :8080 Port de sortie 172.16.0.102:80



*Pour cela, nous devons aller dans « **Firewall / Nat** »*

Voila un exemple de régles qui sont translaté

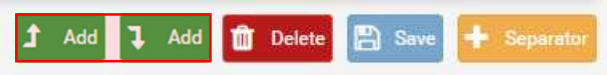
Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
Machine Hopper - 172.16.0.101										
	WAN	TCP	*	*	WAN address	8081	172.16.0.101	80 (HTTP)	Serveur Web - Hopper	
	WAN	TCP	*	*	WAN address	2121	172.16.0.101	21 (FTP)	Serveur FTP - Hopper	
	WAN	TCP	*	*	WAN address	2201	172.16.0.101	22 (SSH)	Serveur Web - Hopper	
	WAN	TCP/UDP	*	*	WAN address	8001	172.16.0.101	8000	Serveur Ajenti - Hopper	
	WAN	TCP	*	*	WAN address	49152 - 50000	172.16.0.101	49152 - 50000	Serveur FTP Port Passif - Hopper	
Machine Physique - 172.16.0.102										
	WAN	TCP	*	*	WAN address	8080	172.16.0.102	80 (HTTP)	Serveur Web - Physique	
	WAN	TCP/UDP	*	*	WAN address	33890	172.16.0.102	3389 (MS RDP)	RDP - Physique	
	WAN	TCP/UDP	*	*	WAN address	33891	172.16.0.102	33891	RDP - Hopper	
	WAN	TCP/UDP	*	*	WAN address	33892	172.16.0.102	33892	RDP - Intratec	
	WAN	TCP/UDP	*	*	WAN address	33893	172.16.0.102	33893	RDP - Centreon	
	WAN	TCP/UDP	*	*	WAN address	33894	172.16.0.102	33894	RDP - PFSENSE	
Machine Intratec - 172.16.0.103										
	WAN	TCP	*	*	WAN address	2203	172.16.0.103	22 (SSH)	Serveur SSH - Intratec	
	WAN	TCP	*	*	WAN address	1138	172.16.0.103	1138	Serveur Web - Intratec	
	WAN	TCP	*	*	WAN address	8003	172.16.0.103	8000	Serveur Ajenti - Intratec	
Machine Centreon - 172.16.0.104										
	WAN	TCP	*	*	WAN address	8084	172.16.0.104	80 (HTTP)	Serveur Web - Centreon	
	WAN	TCP	*	*	WAN address	2204	172.16.0.104	22 (SSH)	Serveur SSH - Centreon	
Machine PFSENSE - 172.16.0.254										
	WAN	TCP	*	*	WAN address	8888	172.16.0.254	80 (HTTP)	Serveur Web - PFSENSE	
	WAN	TCP	*	*	WAN address	22254	172.16.0.254	22 (SSH)	Serveur SSH - PFSENSE	

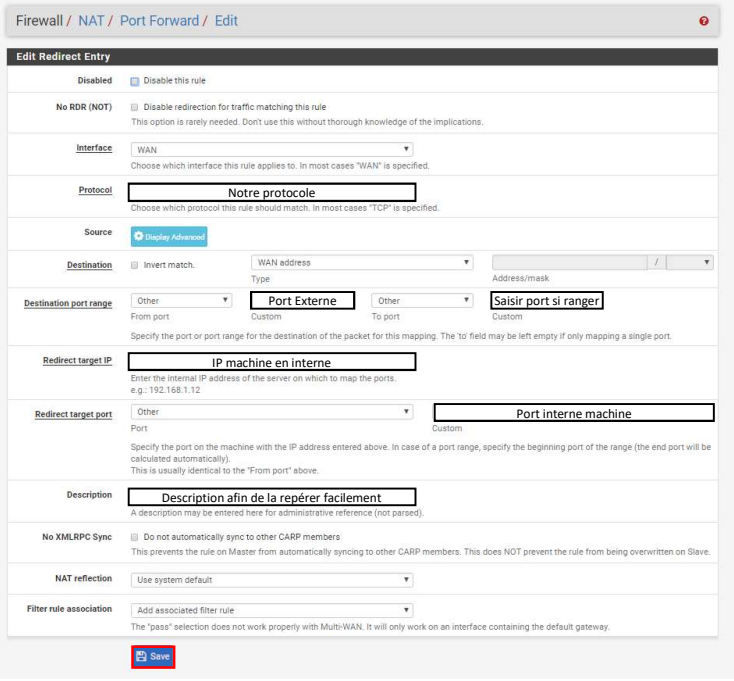
Add Add Delete Save Separator

Exemple de régles qui peuvent être crées

Pour créer une régle NAT, cliquer sur "**ADD**"



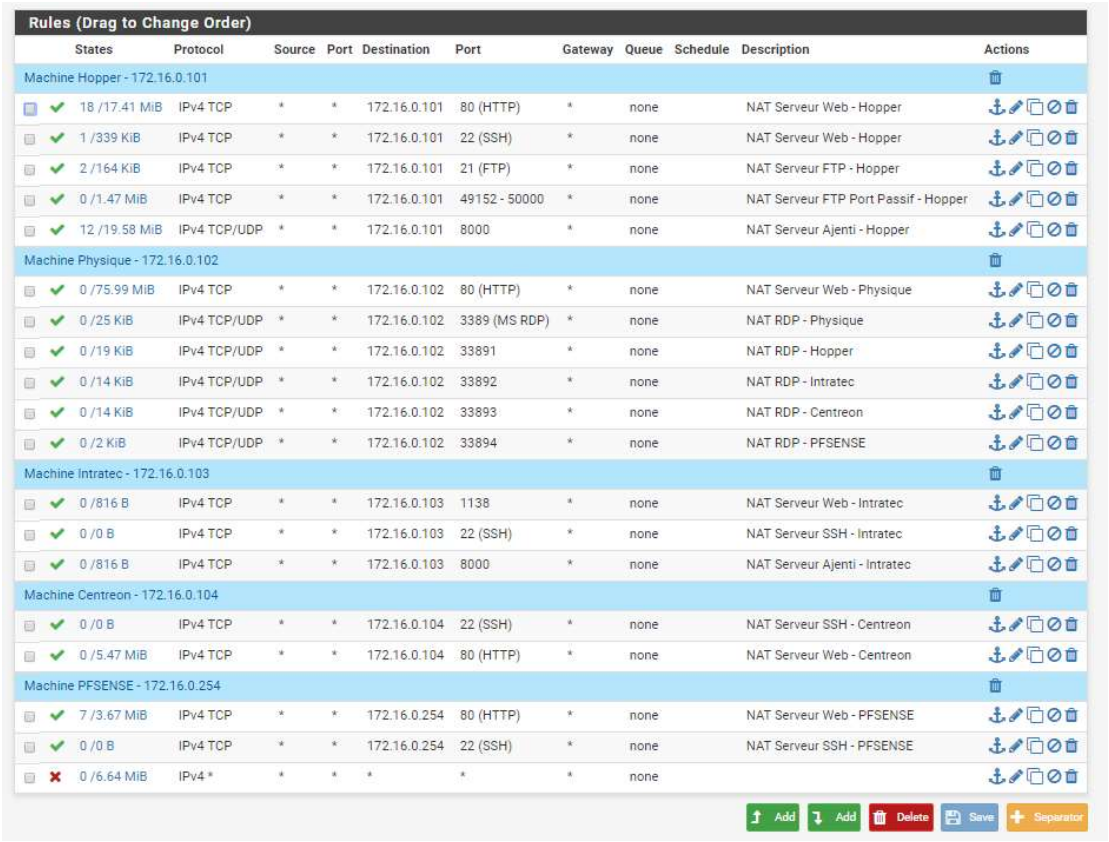
*Pour cela, nous devons cliquer sur « **ADD** »*



Créer notre régle, puis la sauvegarder

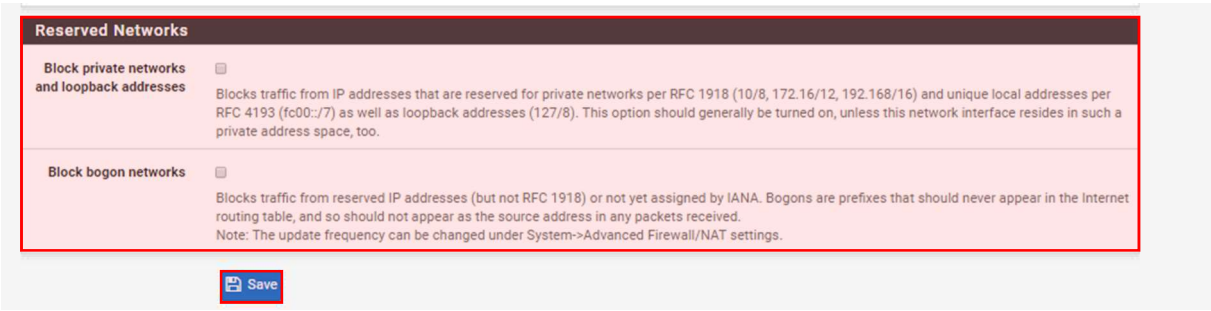
Une fois créer, nous devons la mettre dans le bon séparateur pour mieux se repérer.

Puis, nous devons aller dans « **Firewall / Rules** ». Toutes régles dans rules sont crées grâce au NAT créer précédament, il faut juste effectuer plusieurs manipulations si elle ne sont pas dans le bon ordre.



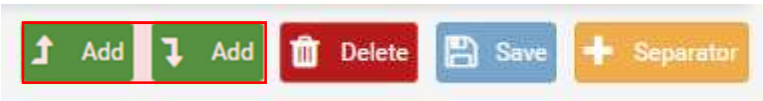
Exemple de liste de régles NAT/PAT

Nous devons elever les 2 régles qui bloque toutes entrées « **Interface / WAN** »

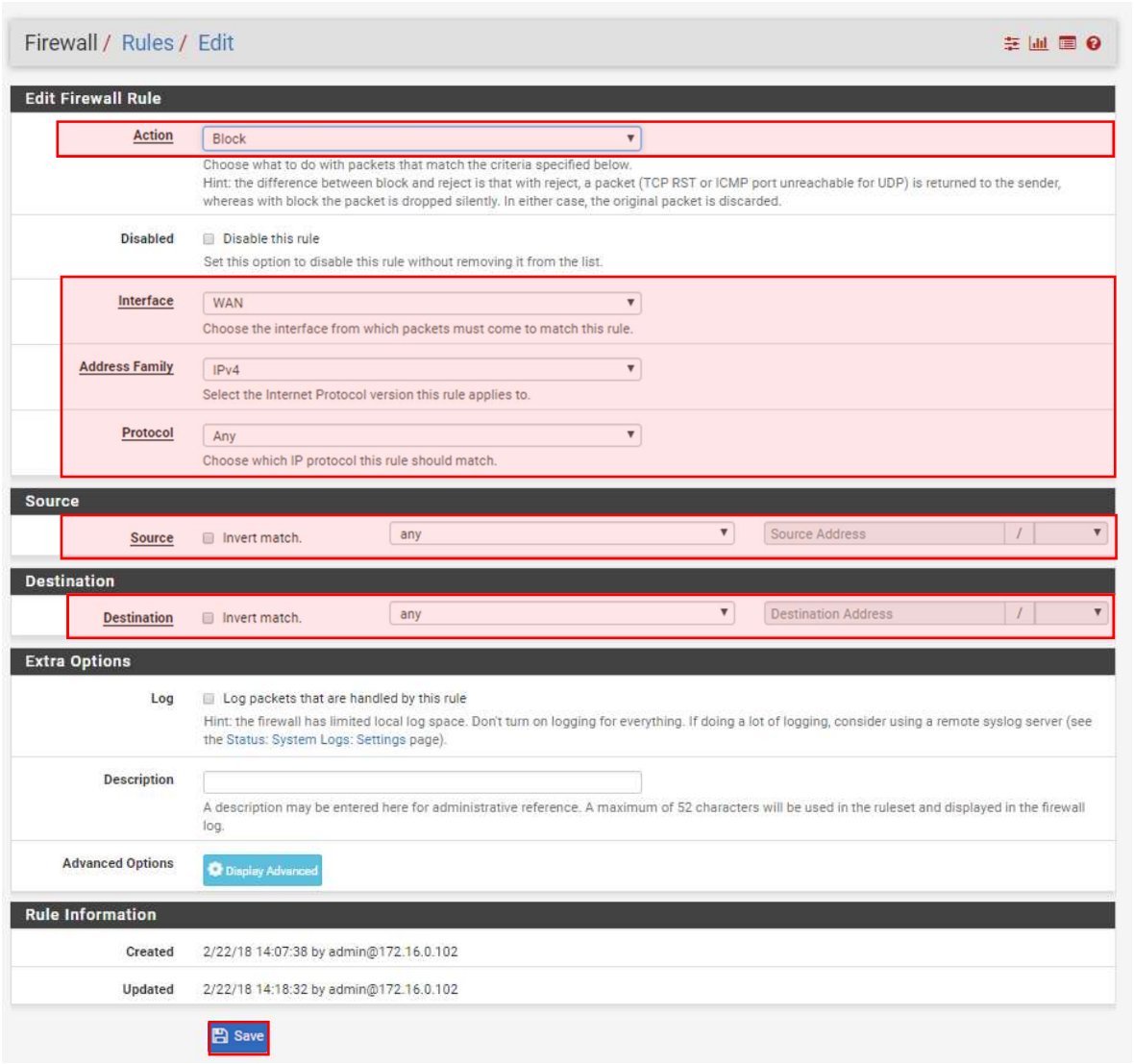


Les deux cases doivent être décochées, car elles empechent de faire du filtrage et bloquent toutes les entrées.

Afin de sécuriser notre réseau, nous allons bloquer tout les autres trafiques qui veulent entrer(Si elle n'existe pas). Nous allons donc créer une rule dans « **Firewall / Rules** », qui doit être en dernier. Pour cela, nous devons cliquer sur "**ADD**"



La régle doit être identique



Cette régle bloque tout le trafic et donc doit être mis tout à la fin, elle permet que tous les autres protocoles/réquetes soit abandoneronner

11. Mise en plage de Liste de blockage

Nous allons voir comment mettre en place un liste de blockage, qui permet de refuser l'accés à certains site web, en fonction des catégories(Téléchargement illégale, Site d'achats, Sites adules, etc…).

Pour cela, nous pouvons la créer ou bien en utiliser une déjà prete créer par d'autres personnes qui on ressencer ces sites.

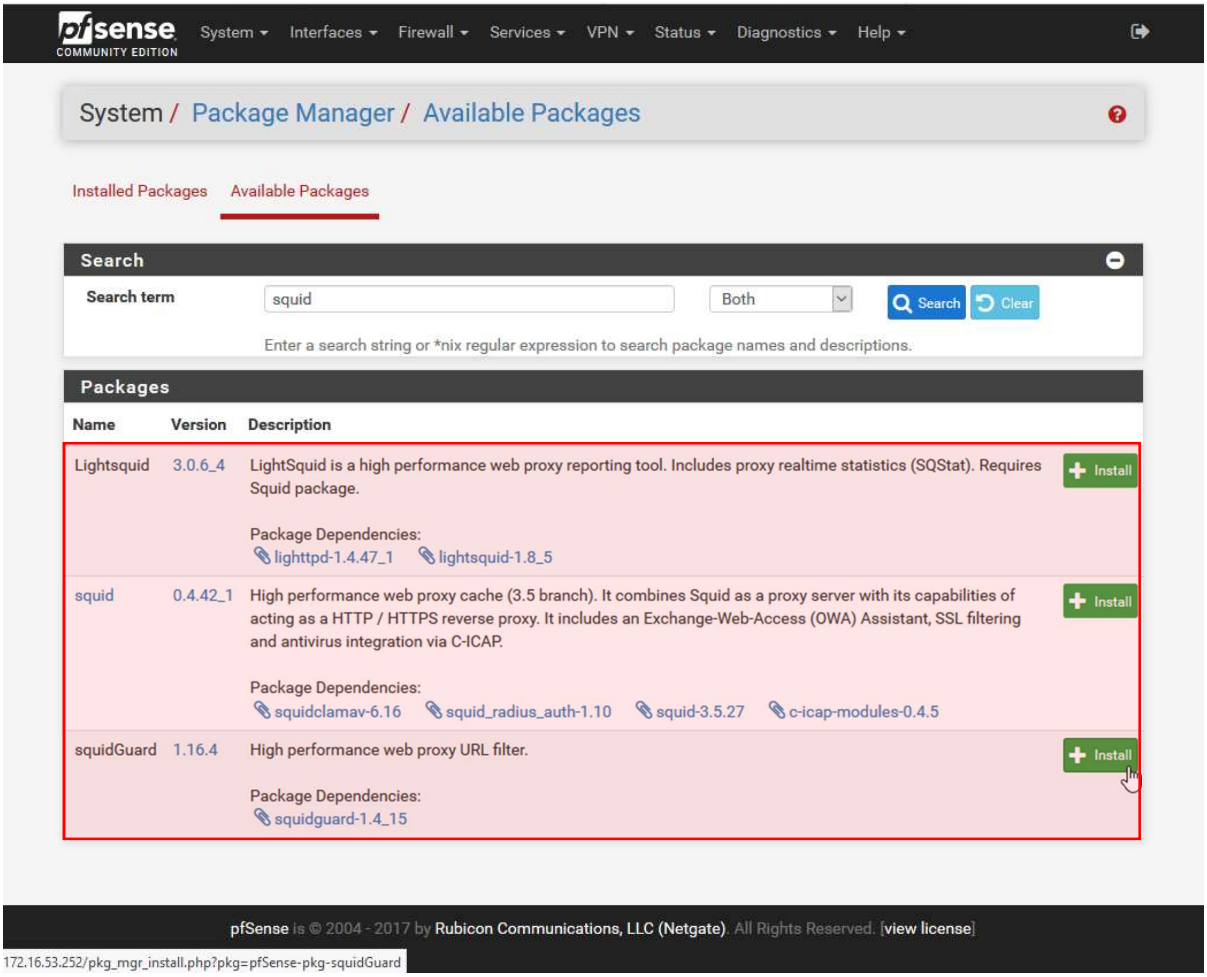
Pour pouvoir mettre en place des listes de blockage, nous devons installer plusieurs packages qui doivent être installer sans ces paquets il nous sera impossible de mettre en place des restriction grace aux listes.

Dans mon cas, je vais mettre en place la blackliste de Toulouse.

Pour cela, nous devons installer les paquets nous devons aller dans "**Système / Packages Manager**"

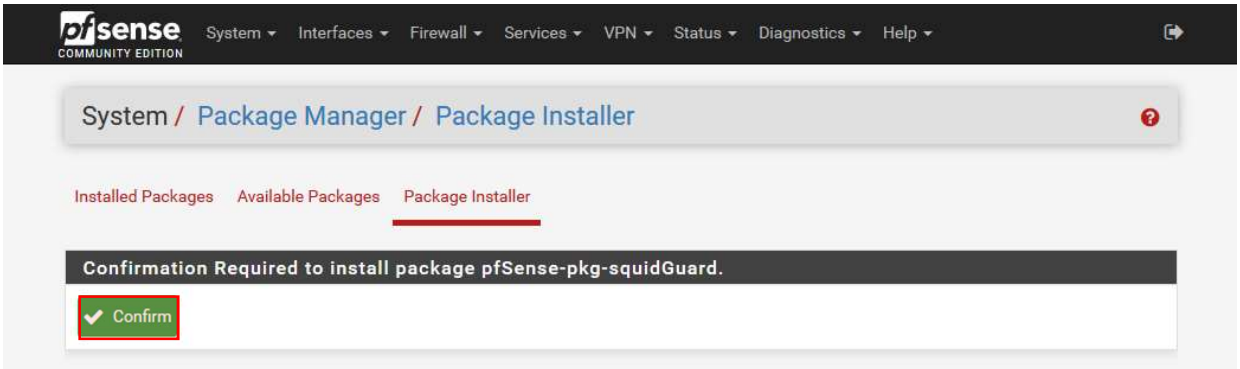
Une fois dans le manageur, nous devons aller dans "**Available Packages**" et installer les paquets Squid, SquidGuard et Lightsquid. Nous pouvons rechercher les paquets avec le terme "squid"

Si il nous manque des paquets, il nous sera impossible de mettre en place notre filtrage par rapport a nos sites web.



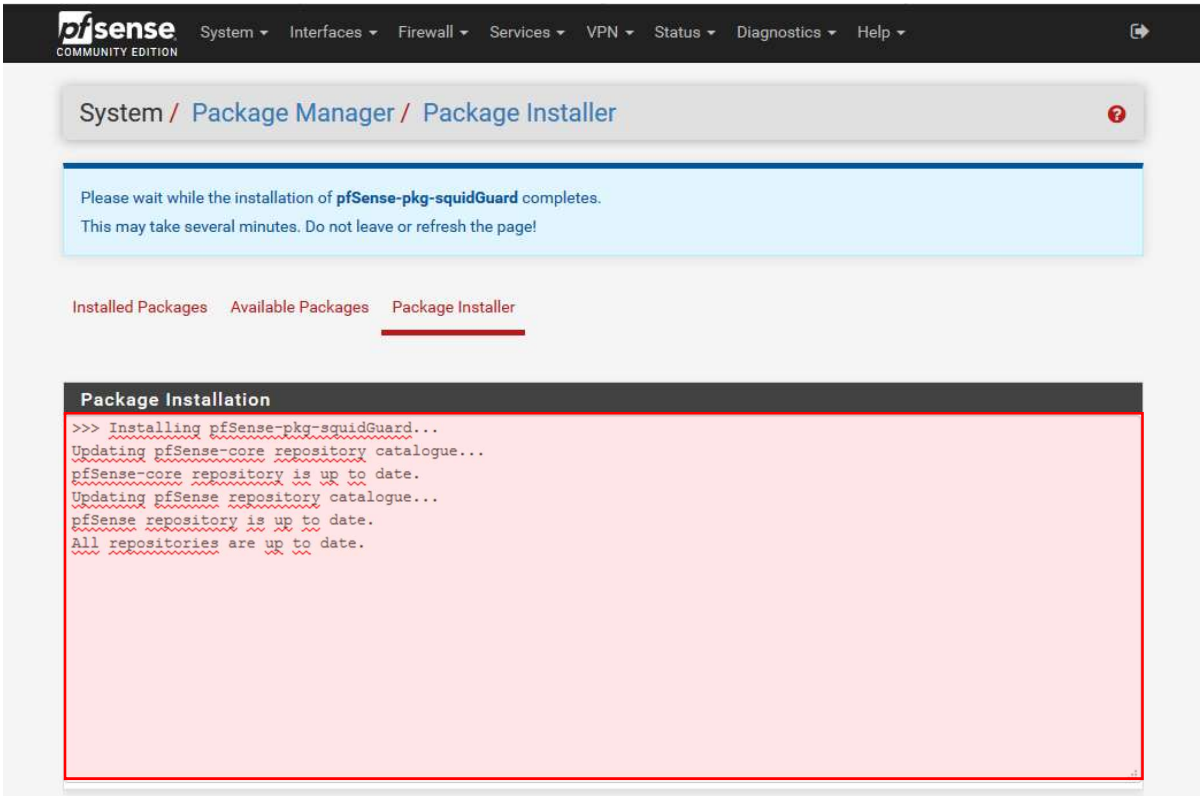
Chaque paquets doivent être installer séparement

Pour chaque installation une demande de confirmation d'installation nous ai demander



Nous devons confirmer, afin qu'il soit installer

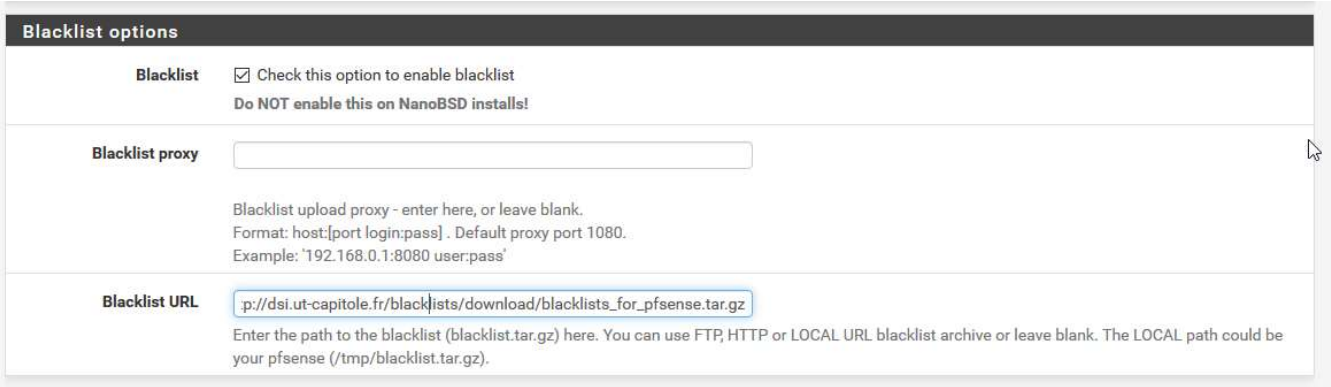
Pour chaque installation, nous avons l'avancement, il est important de ne pas fermer la page, si non l'installation échou.



Nous avons l'avancement et le détail des actions effectuer lors de l'installation

Une fois les paquets installer, nous allons pouvoir installer notre blacklist, pour cela, nous devons aller dans "**Services / SquidGuard Proxy Filter**".

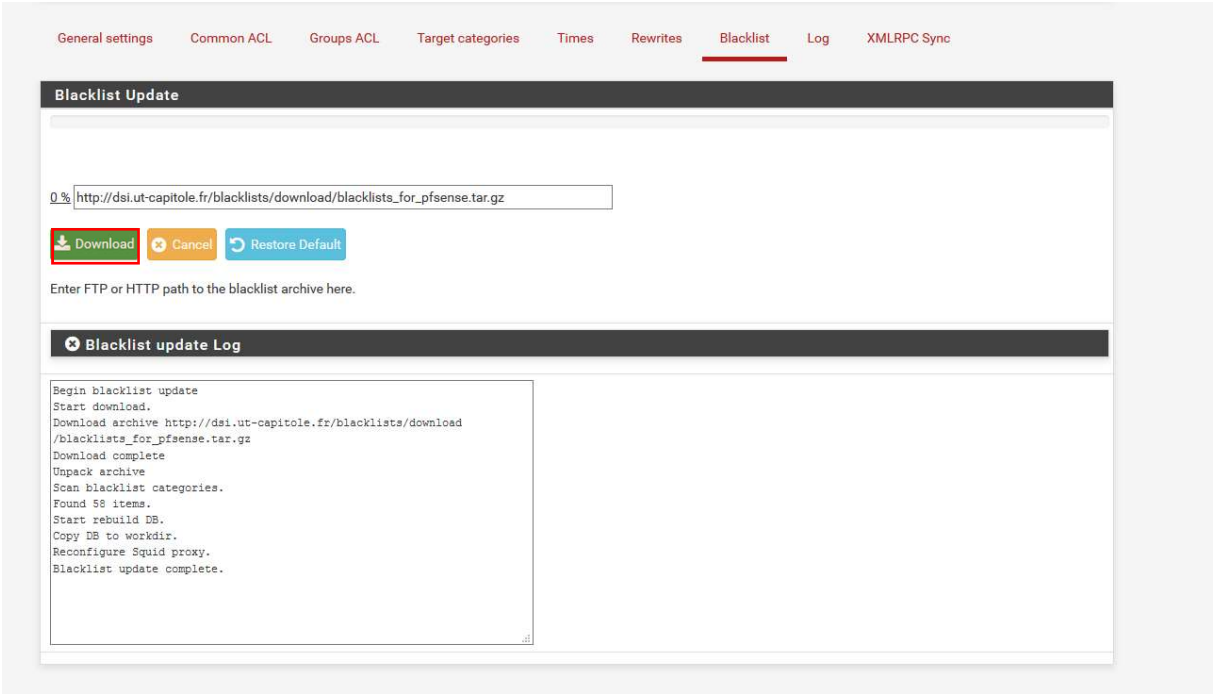
Nous devons activer la blacklist et nous devons mettre le lien de notre blackliste, ce qui nous permet de la mettre à jour facilement en cas de mise à jour de celle-ci



Lien de la blacklist : http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz

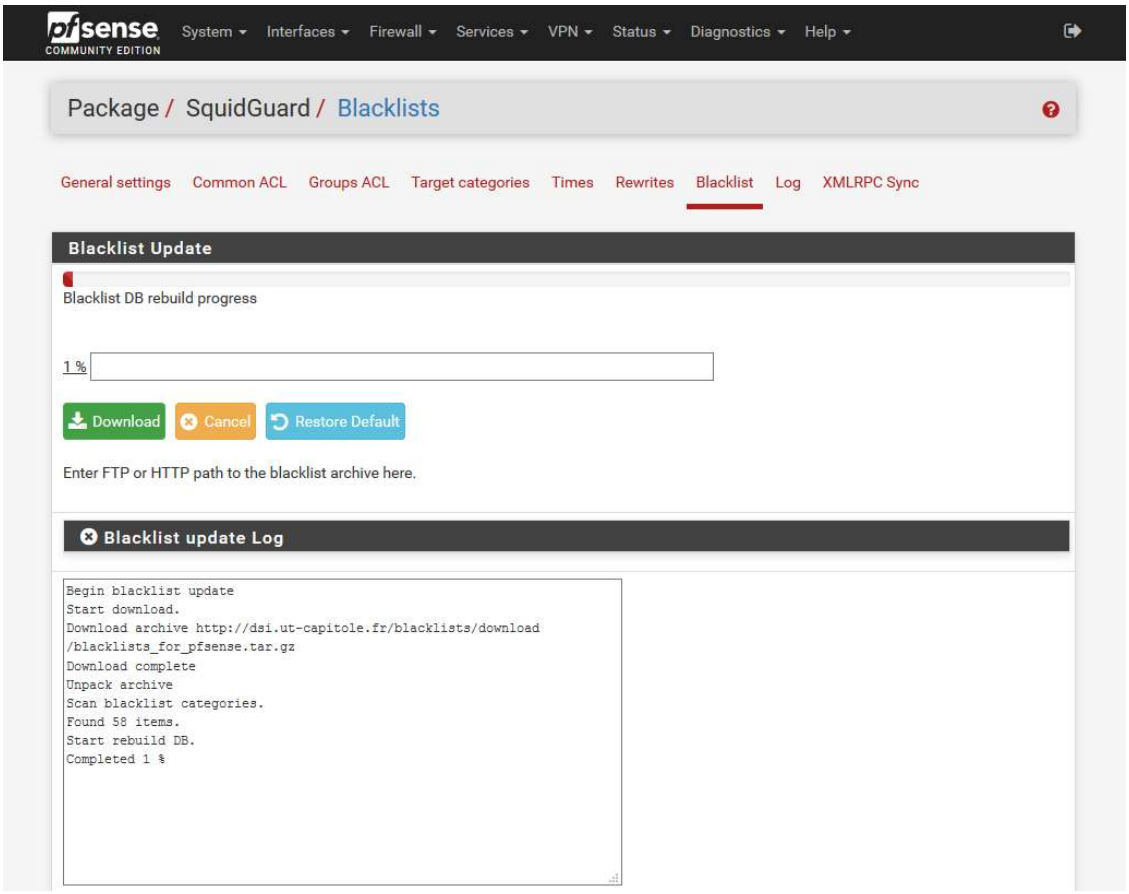
Ce n'est pas la seul blackliste existante, mais elle comprend beaucoup de site.

Maintenant, nous devons nous rendre dans "**Système / Géneral / Blacklist**", puis la télécharger



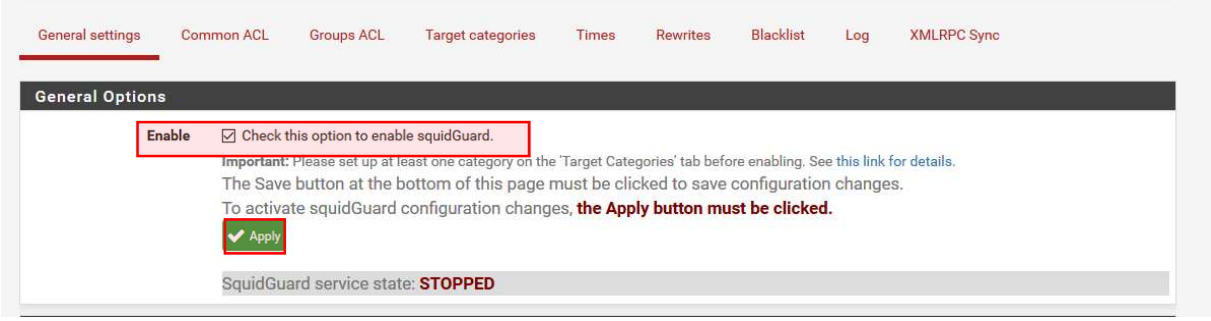
*Pour mettre à jour ou installer notre liste de blockage, nous devons la télécharger avec le bouton "**Download**"*

Un avancement du téléchargement est fait et la base de données ajoute les éléments de la liste



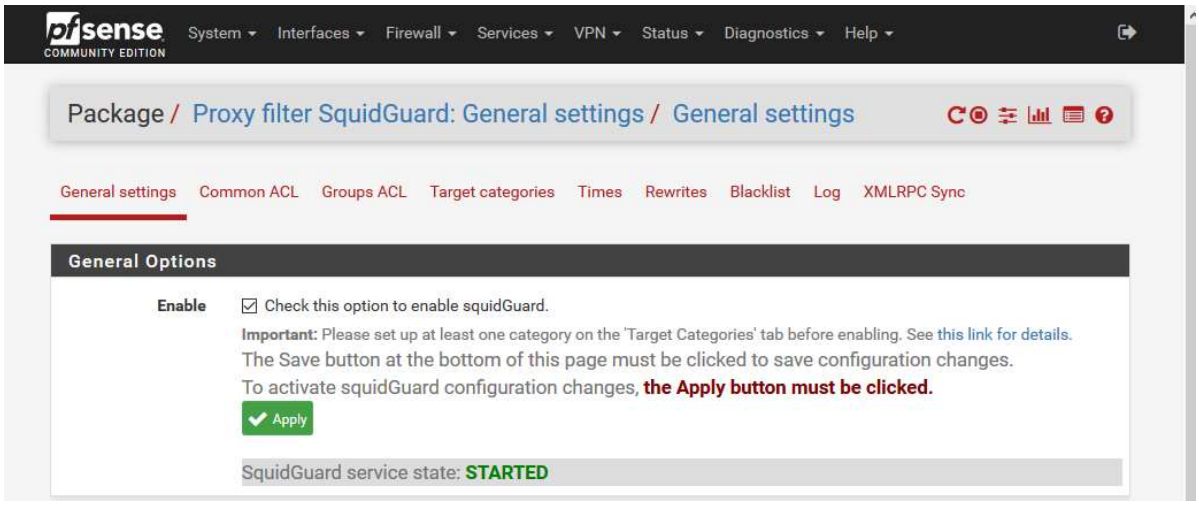
Nous avons un status d'avancement du téléchargement de notre blacklist, cela peut prendre un moment

Une fois notre blackliste télécharger et ajouter, nous devons nous rendre dans "**Services / SquidGuard Proxy Filter**" et activer le service SquidGuard si il ne l'est pas



*Pour l'activer, cocher la chase "**Enable**" et cliquer sur "**Apply**"*

On verifie que notre paquet squidGuard soit bien actif

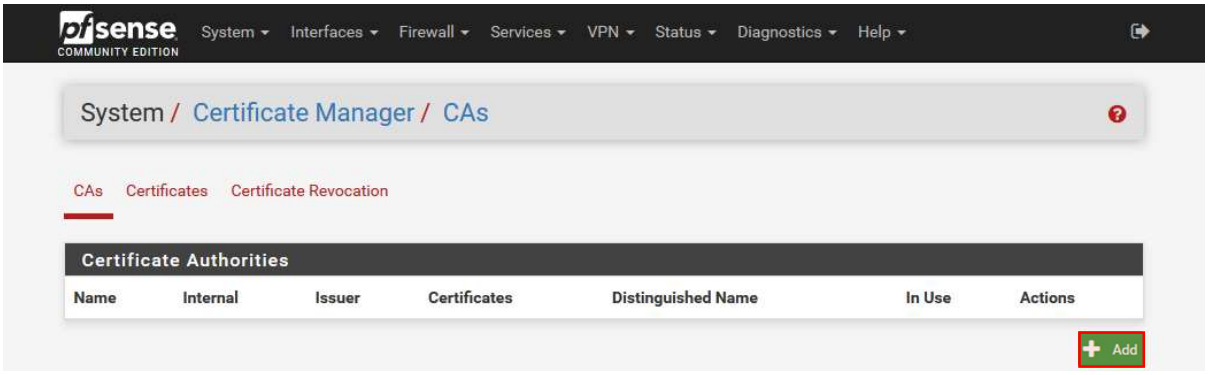


Si il ne démarre pas, il est possible qu'il ne soit pas bien installer ou bien la configuration incorrecte

12. Mise en place d'un VPN (OpenVPN)

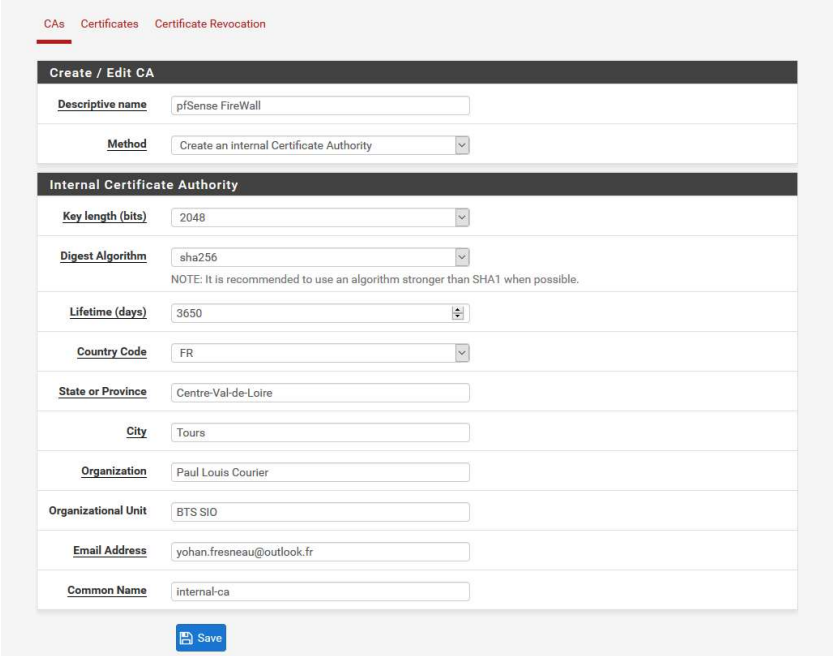
Il est possible avec PFSENSE de mettre en place directement le VPN sur le routeur, ce qui nous evite d'avoir un serveur dédié à cette tache.

Pour cela, nous devons nous rendre dans "**Système / Certificate Manager / CAs**"



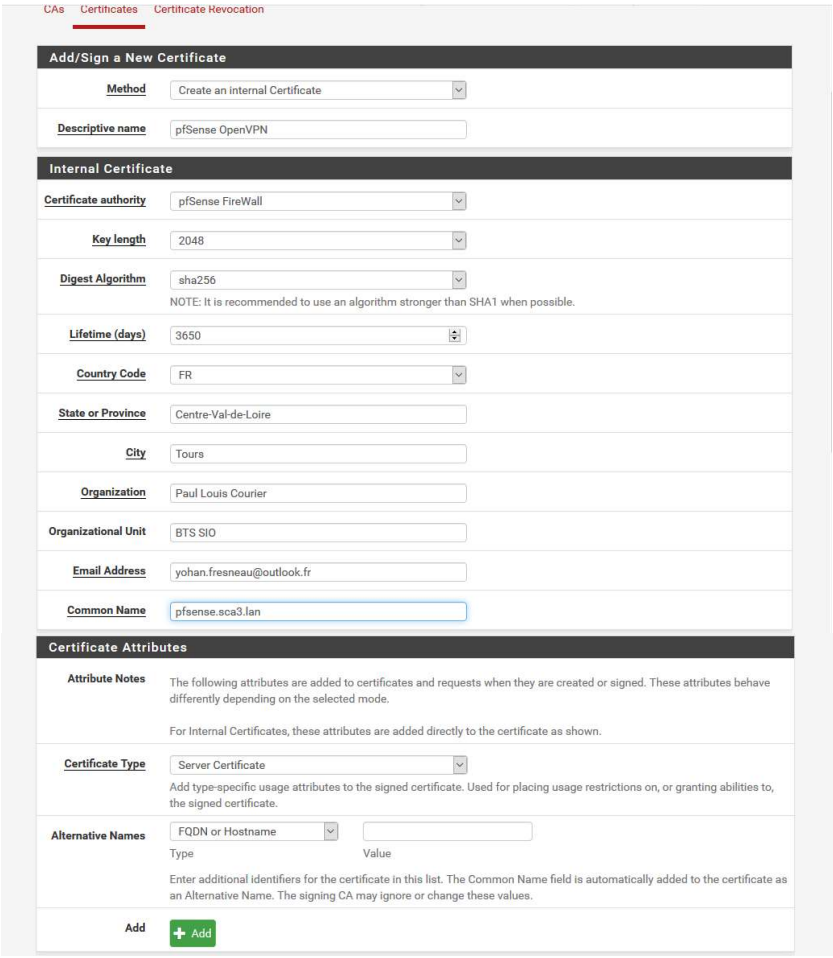
*Nous devons créer notre autorité de certification, pour cela nous devons l'ajouter grace au bouton "**ADD**"*

Nous allons créer notre autorité de certification.



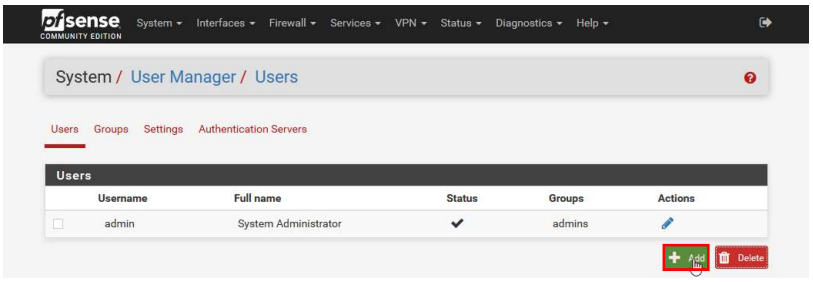
Les informations peuvent être modifier et doivent être adapter

Nous allons créer le certification de notre serveur OpenVPN



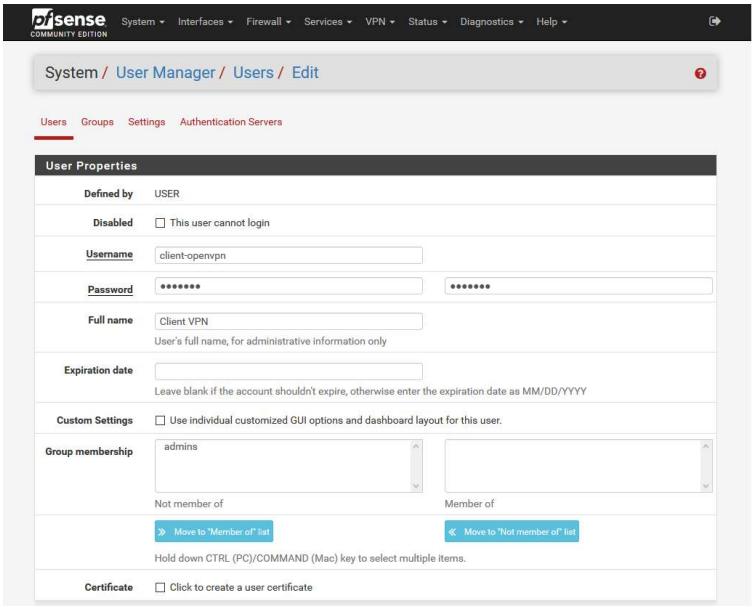
Les informations du certification du serveur VPN doivent être identique ou bien adapter

Nous créer un utilisateur qui pourra par la suite se connecter directement au VPN.



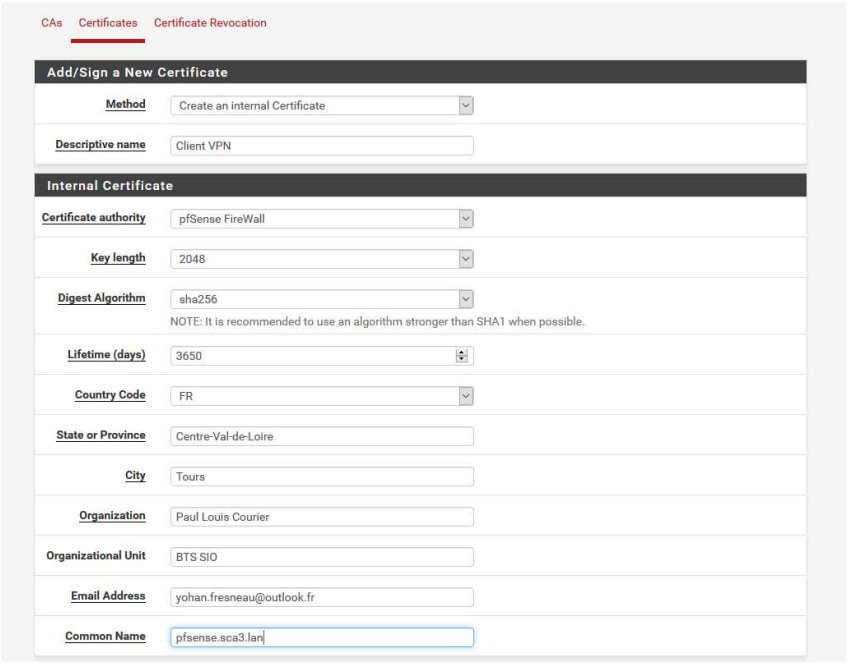
*Pour ajouter un utilisateur, nous devons cliquer sur "**ADD**"*

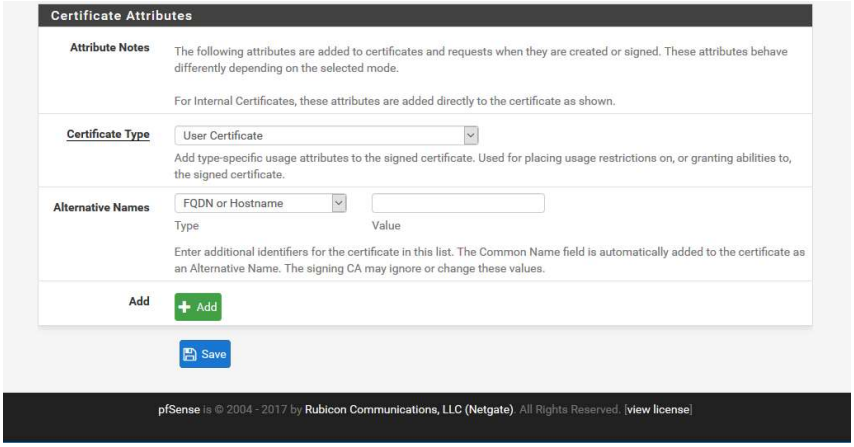
La création de notre utilisateur se fait comme ceci



Cela est identique pour tous autres utilisateurs si l'on souhaite en ajouter d'autres

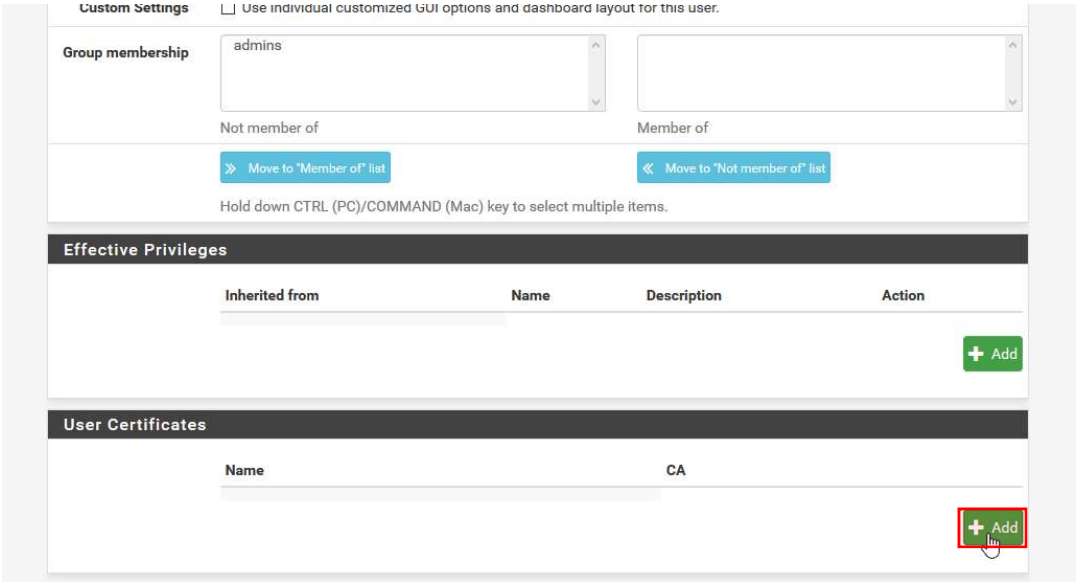
Nous allons créer le ceritificat pour les client, afin qu'il puissent se connecter au VPN





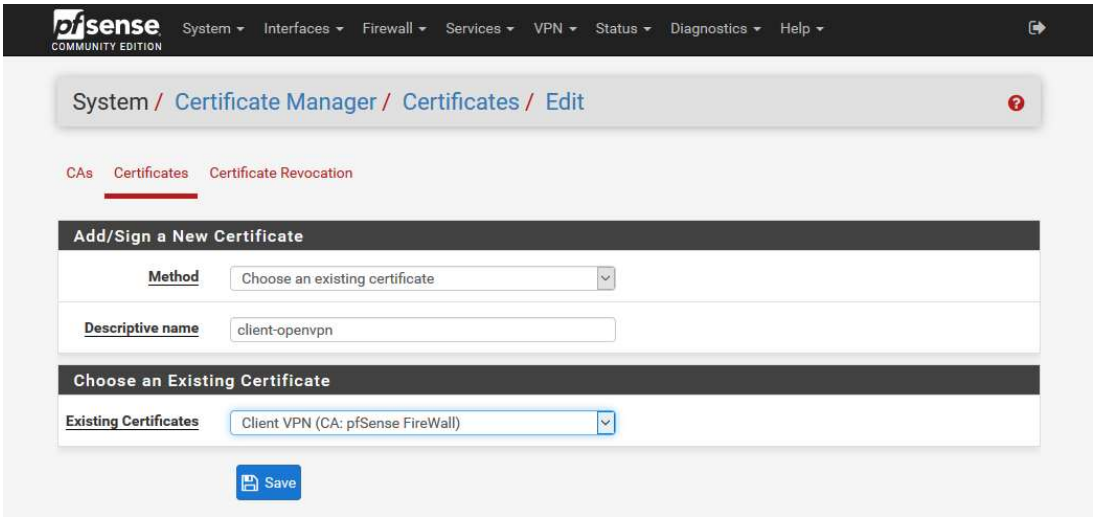
Notre certificat est universelle pour tous les clients voulent se connecter, car il se connecte grace à des mot de passe et des nom utilisateur

Nous devons lié ce certificat à notre utilisateur, pour cela nous devons retourner sur notre utilisateur



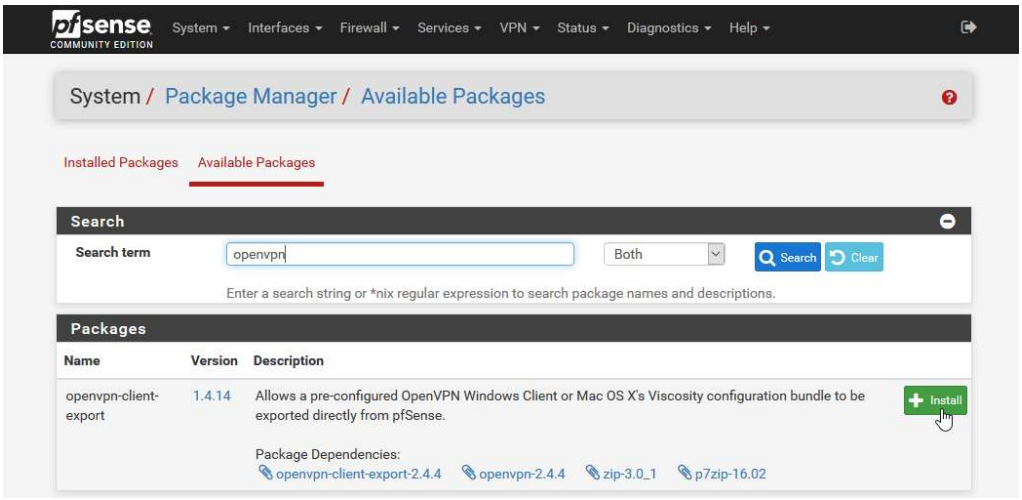
*Nous devons cliquer sur "**ADD**", dans "**User Certificates**"*

Nous devons séléctionner le certificat au quelle on le lie



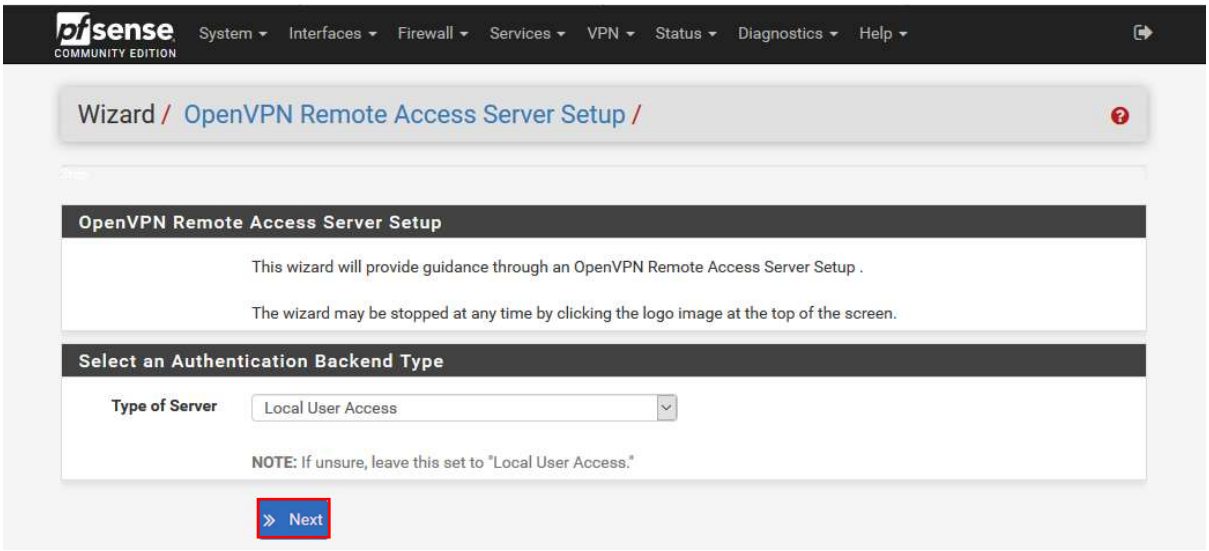
On séléctionne notre certificat créer précédament pour nos utilisateurs

Nous allons maintenant, mettre en place notre serveur VPN, nous allons intaller le paquet openVPN-client-export qui va nous permettre de créer nos fichiers pour OpenVPN client.

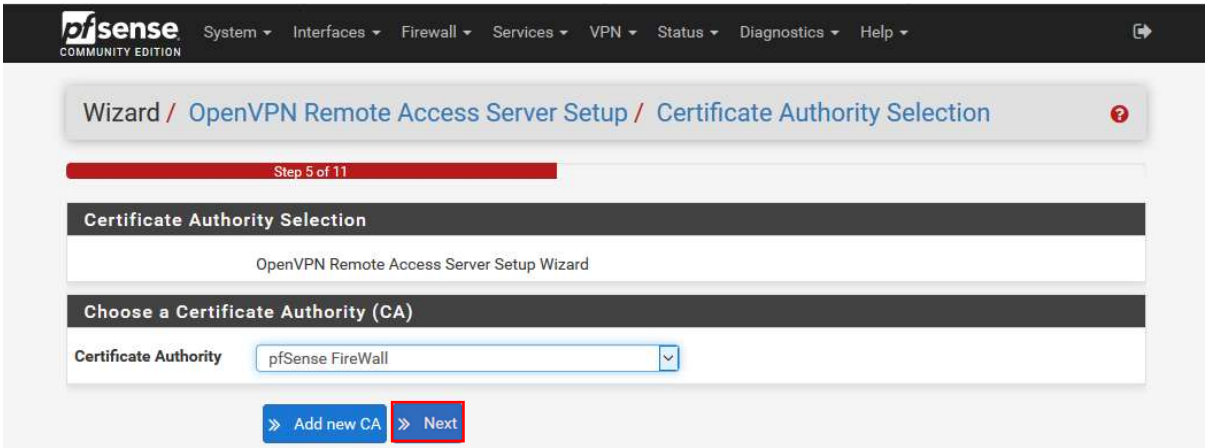


On cliquer sur intaller afin d'ajouter le paquet

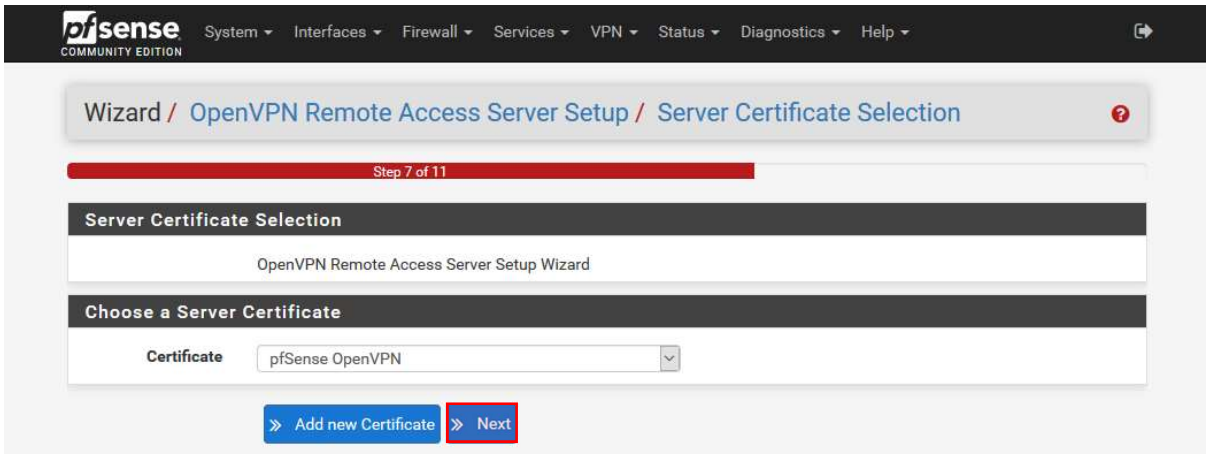
Nous allons installer le serveur VPN et le configurer



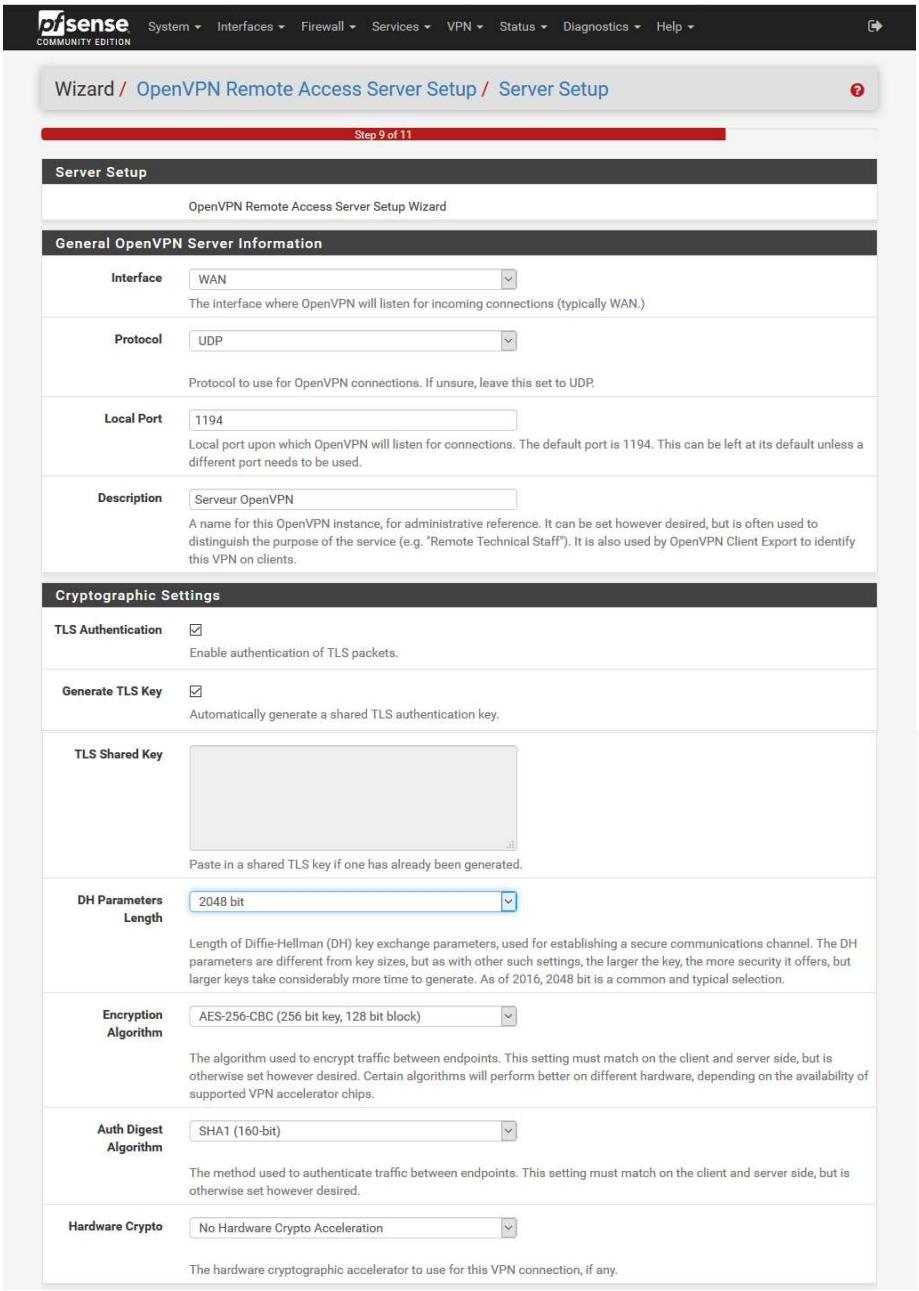
*Choisir "**Local User Access**", puis faire "**Next**"*

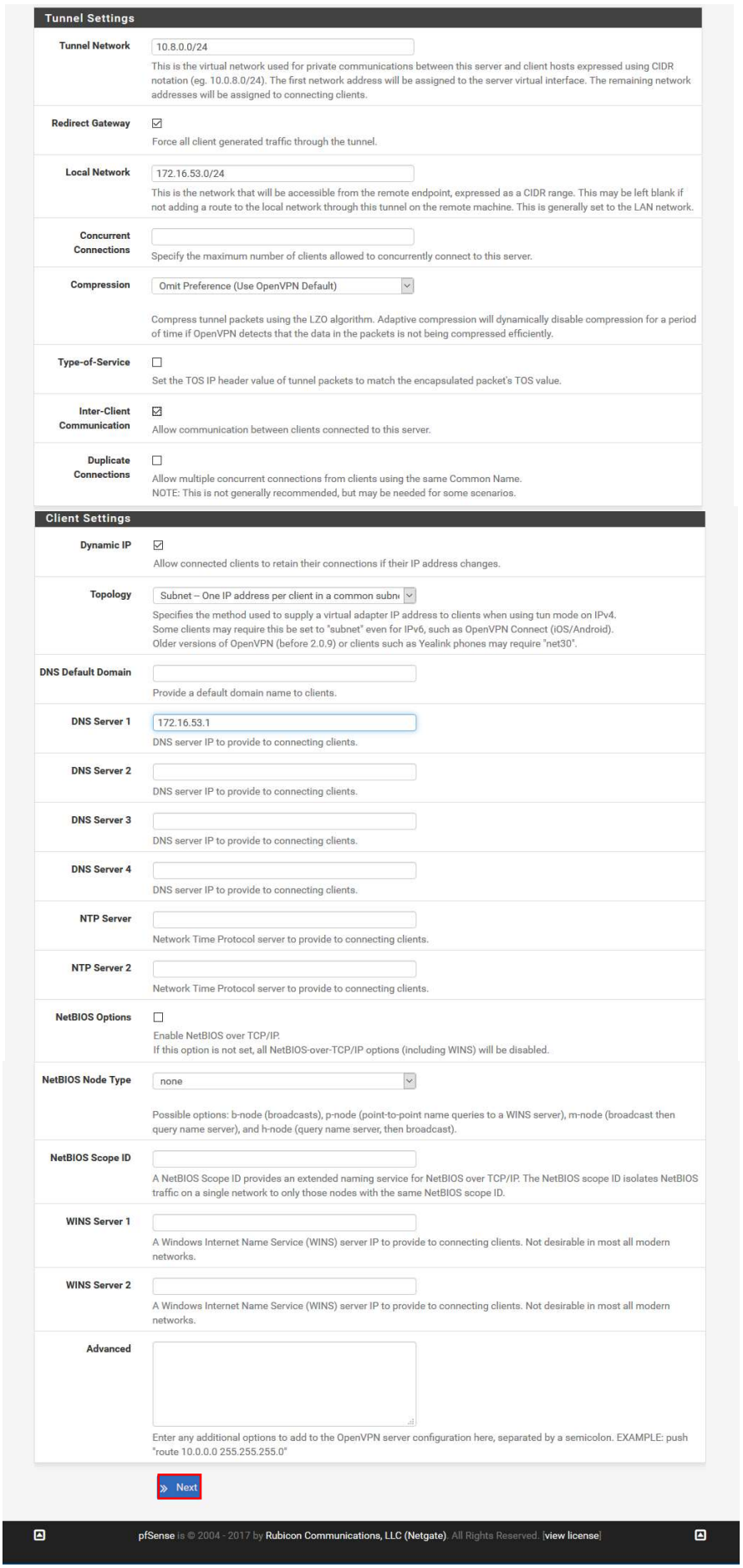


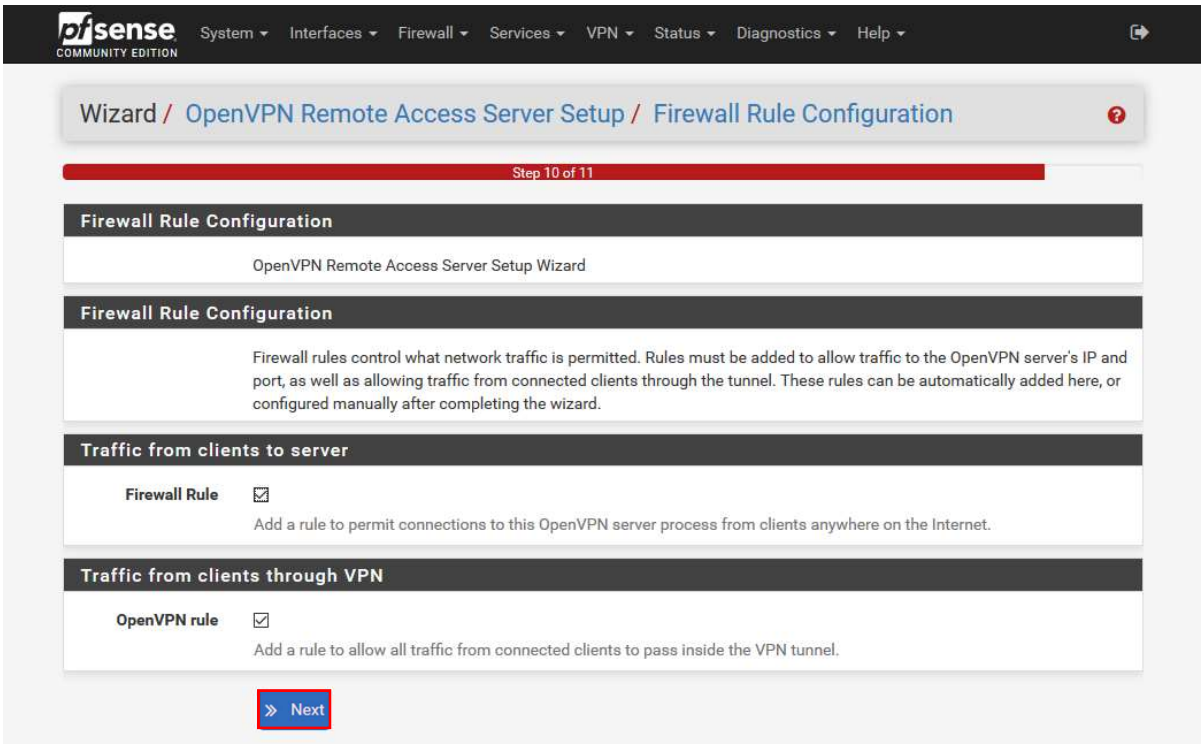
*On séléctionne notre autorité de certification, puis on clique sur "**Next**"*



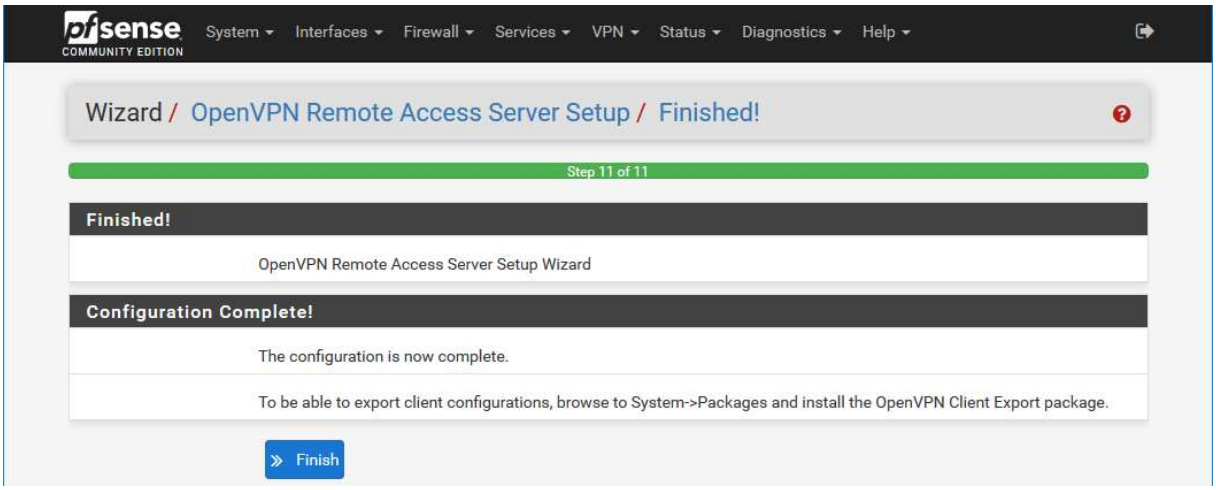
*On séléctionne le certificat que l'on à créer pour notre serveur, puis "**Next**"*




Tunnel Settings
Tunnel Network
10.8.0.0/24
This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.
Redirect Gateway
Force all client generated traffic through the tunnel.
Local Network
172.16.53.0/24
This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
Concurrent Connections
Specify the maximum number of clients allowed to concurrently connect to this server.
Compression
Omit Preference (Use OpenVPN Default)
Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.
Type-of-Service
Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
Inter-Client Communication
Allow communication between clients connected to this server.
Duplicate Connections
Allow multiple concurrent connections from clients using the same Common Name.
NOTE: This is not generally recommended, but may be needed for some scenarios.
Client Settings
Dynamic IP
Allow connected clients to retain their connections if their IP address changes.
Topology
Subnet -- One IP address per client in a common subn
Specifies the method used to supply a virtual adapter IP address to clients when using tun mode on IPv4.
Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android).
Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".
DNS Default Domain
Provide a default domain name to clients.
DNS Server 1
172.16.53.1
DNS server IP to provide to connecting clients.
DNS Server 2
DNS server IP to provide to connecting clients.
DNS Server 3
DNS server IP to provide to connecting clients.
DNS Server 4
DNS server IP to provide to connecting clients.
NTP Server
Network Time Protocol server to provide to connecting clients.
NTP Server 2
Network Time Protocol server to provide to connecting clients.
NetBIOS Options
Enable NetBIOS over TCP/IP.
If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.
NetBIOS Node Type
none
Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast).
NetBIOS Scope ID
A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID.
WINS Server 1
A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.
WINS Server 2
A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.
Advanced
Enter any additional options to add to the OpenVPN server configuration here, separated by a semicolon. EXAMPLE: push "route 10.0.0.0 255.255.255.0"
Next
pfSense is © 2004 - 2017 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license]



*On peut laisser par défaut et faire "**Next**"*

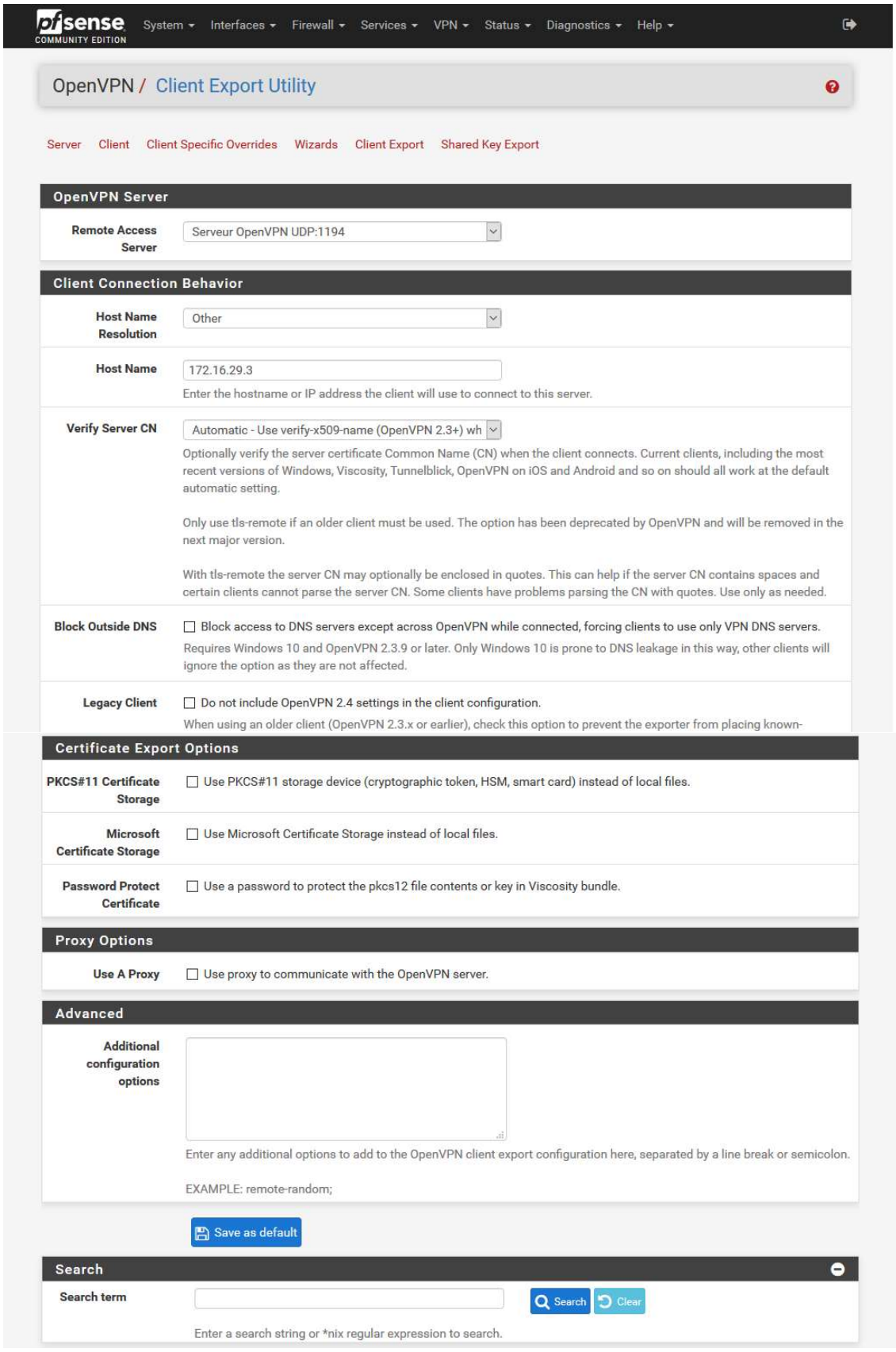


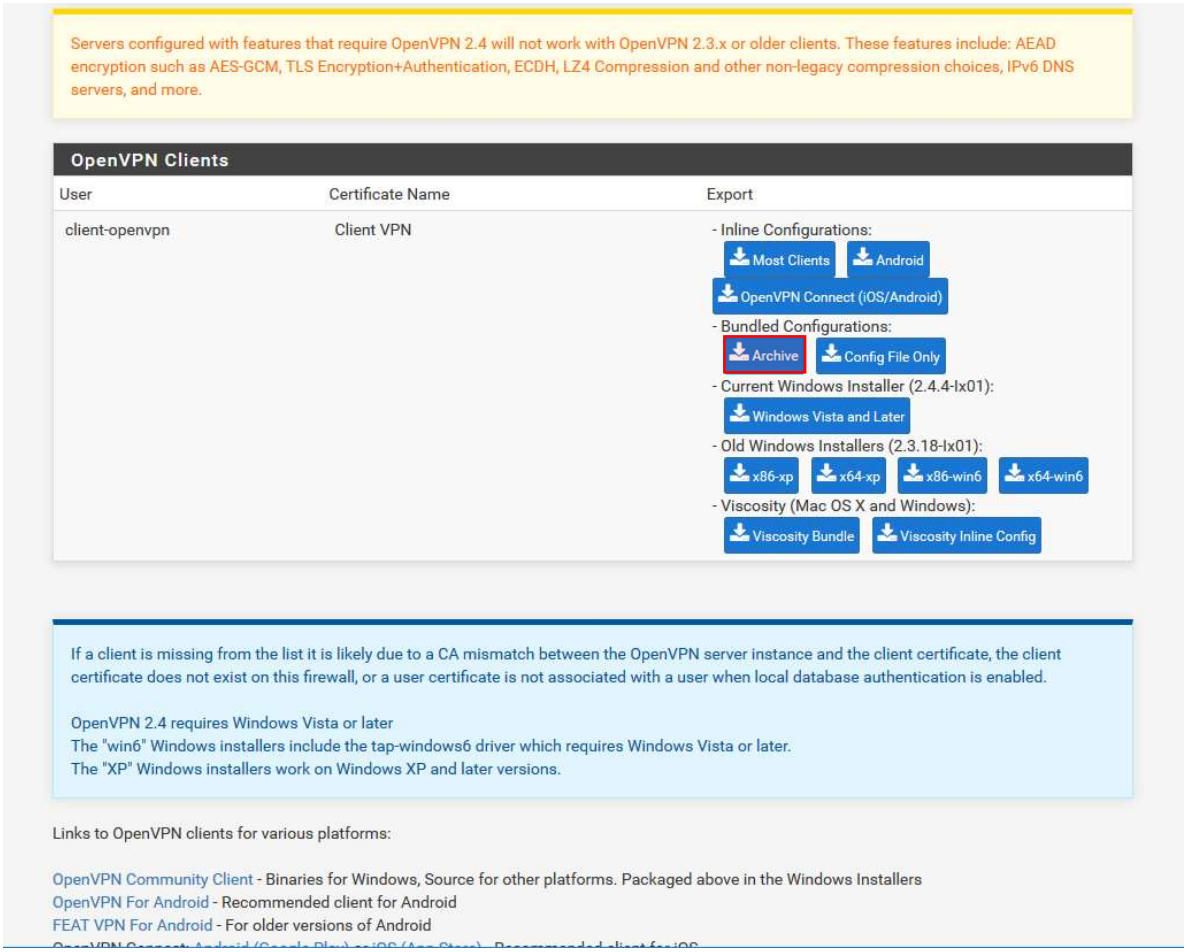
*Notre serveur VPN est installer, nous pouvons donc cliquer sur "**Finish**"*

Notre VPN est donc configurer, il nous reste plus qu'a installer un client VPN sur un poste et ce connecter à distance.

Précedament, nous avons installer un paquets OpenVPN, qui nous permet de prégénere des fichiers de configuration pour les clients VPN.

Il est possible de télécharger le client depuis cette interface.


pfsense COMMUNITY EDITION
System Interfaces Firewall Services VPN Status Diagnostics Help
OpenVPN / Client Export Utility
Server Client Client Specific Overrides Wizards Client Export Shared Key Export
OpenVPN Server
Remote Access Server
Serveur OpenVPN UDP:1194
Client Connection Behavior
Host Name Resolution
Other
Host Name
172.16.29.3
Enter the hostname or IP address the client will use to connect to this server.
Verify Server CN
Automatic - Use verify-x509-name (OpenVPN 2.3+) wh
Optionally verify the server certificate Common Name (CN) when the client connects. Current clients, including the most recent versions of Windows, Viscosity, Tunnelblick, OpenVPN on iOS and Android and so on should all work at the default automatic setting.
Only use tls-remote if an older client must be used. The option has been deprecated by OpenVPN and will be removed in the next major version.
With tls-remote the server CN may optionally be enclosed in quotes. This can help if the server CN contains spaces and certain clients cannot parse the server CN. Some clients have problems parsing the CN with quotes. Use only as needed.
Block Outside DNS
Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers.
Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.
Legacy Client
Do not include OpenVPN 2.4 settings in the client configuration.
When using an older client (OpenVPN 2.3.x or earlier), check this option to prevent the exporter from placing known-
Certificate Export Options
PKCS#11 Certificate Storage
Use PKCS#11 storage device (cryptographic token, HSM, smart card) instead of local files.
Microsoft Certificate Storage
Use Microsoft Certificate Storage instead of local files.
Password Protect Certificate
Use a password to protect the pkcs12 file contents or key in Viscosity bundle.
Proxy Options
Use A Proxy
Use proxy to communicate with the OpenVPN server.
Advanced
Additional configuration options
Enter any additional options to add to the OpenVPN client export configuration here, separated by a line break or semicolon.
EXAMPLE: remote-random;
Save as default
Search
Search term
Search
Clear
Enter a search string or *nix regular expression to search.

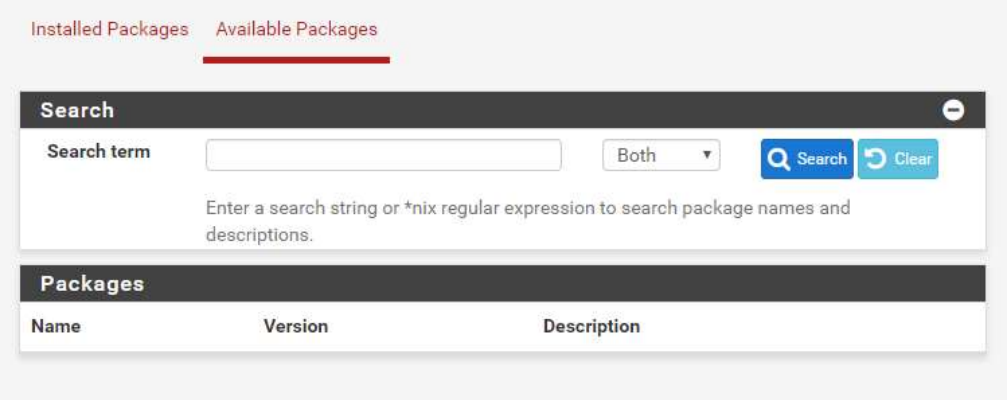


Nous avons les fichiers de config et l'on peut aussi télécharger directement l'installation de OpenVPN

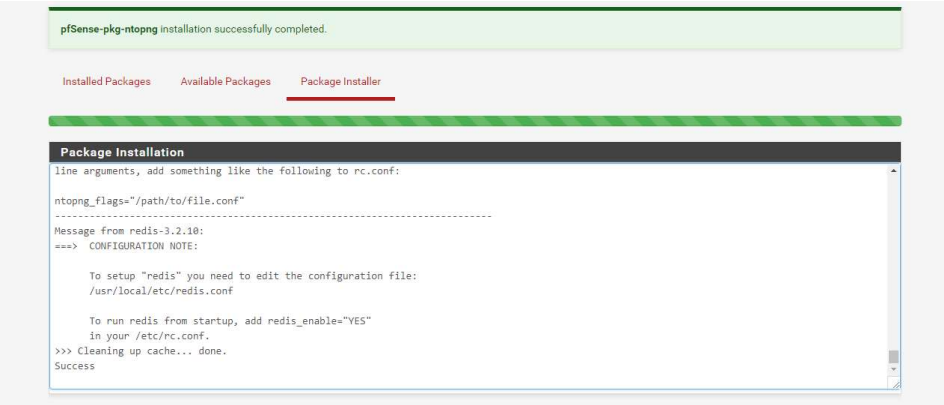
13. Mise en place d'une journalisation du trafic réseau

Nous allons utiliser ntopng qui nous permet d'avoir des information détailler des connexion actuelle(Tout ceci se configure dans les paramétres de ntopng dans l'interface graphique). On à aussi un historique de qui à éffectuer des demandes et savoir ce qui rentre et sort du réseau.

Pour installer ntopng, il faut aller dans « **System\Package Manager** »

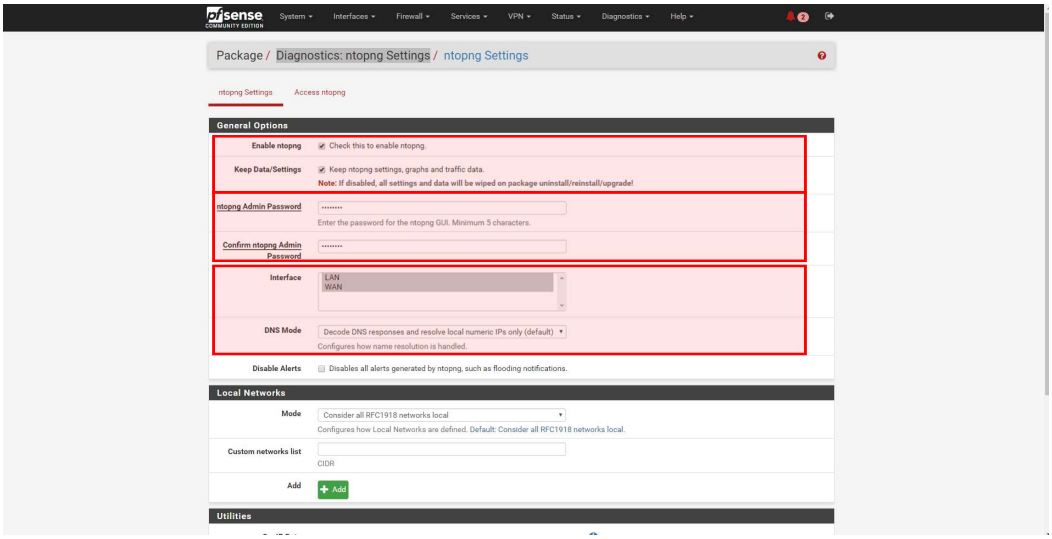


*Nous recherchons « **ntopng** », puis nous l'installons*



Nous devons attendre que Success soit affichier, car si on quitte la page ntopng ne sera pas completement installer

Nous allons donc configurer ntopng, pour cela aller dans « **Diagnostics / ntopng Settings** »



*Il faut « **Enable ntopng** », puis saisir le mot de passe de l'interface web de ntopng et on séléctionne les deux interfaces Lan et Wan. D'autres parametres peut etre modifier.*

Pour la mise en place, nous alons utiliser un serveur Mysql. Le serveur MySQL va nous permettre de sauvegarder les informations qui passe sur le réseau. Pour cela, nous devons créer une table « ntopng » sur le serveur MySQL.

IP: 172.16.0.200 ***Utilisateur:*** root ***Mot de passe:*** Toor01

Un petit bug existe dans l'interface, il est possible de modifier le temps de rétention des infomation mais si on modifier le temps et que l'on redemarre l'informations n'est pas sauvegarder. Pour mon cas, j'ai trouver une solution qui conciste à enelver les droit de « Delete et Update », afin qu'il ne supprime pas les information au dela de 7 Jours par défaut.

Une fois ceci fait, nous pouvons tester si on à bien accés à la base de données depuis Pfsense avec comme commande

```
mysql -h 172.16.0.200 -uroot -p
```

Cette commande doit être fait sur Pfsense(En SSH)

Si la connexion s'effectue bien cela veut dire qu'il est donc possible d'atteindre la base de données.

Si ce n'est pas le cas voici les solutions possibles :

- Configurer le serveur MySQL

nano /etc/mysql/my.cnf

```
[mysqld]
user = mysql
port=3306
bind-address=0.0.0.0
```

*Contenue du fichier « **/etc/mysql/my.cnf** »*

- Verifier les permission de l'utilisateurs
- Verifier le nom d'utilisateur et le mot de passe et l'IP du serveur

Nous allons dire à Pfsense, qu'il doit enregistrer les informations dans la base de données. Nous allons modifier un fichier de config.

nano /usr/local/pkg/ntopng.inc -l

```
/usr/local/bin/ntopng -d /var/db/ntopng -S all -D none -q -e -F
"mysql;172.16.0.200;ntopng;flows;root;Toor01"  -G /var/run/ntopng.pid -s -e {$http_args}
{$disable_alerts} {$dump_flows} {$ifaces} {$dns_mode}  {$aggregations} {$local_networks} &
```

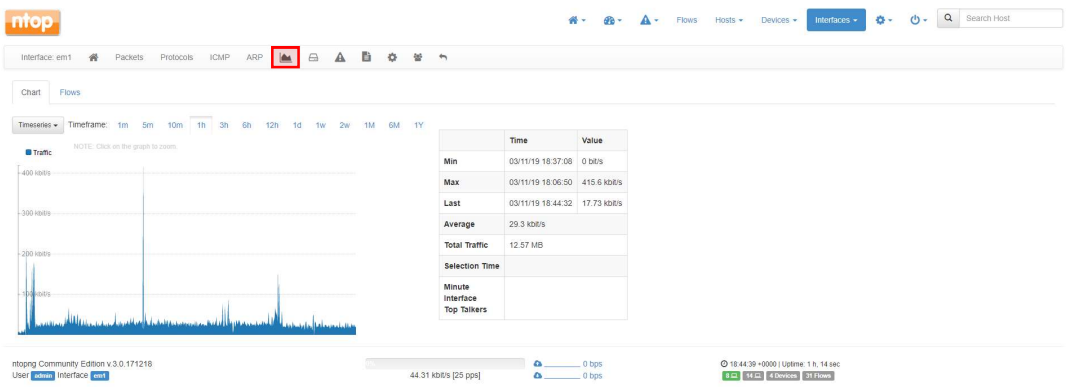
*Contenue du fichier « **/usr/local/pkg/ntopng.inc** ». Ligne **168***

Une fois fait, nous allons pouvoir redémarrer et nous connecter.

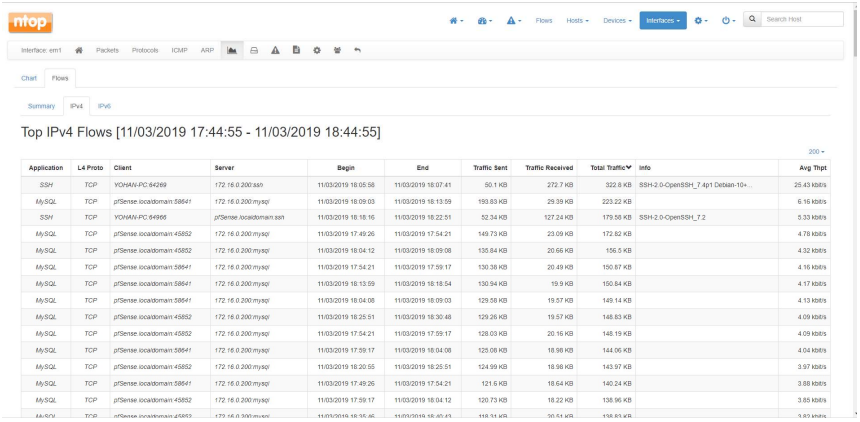
Utilisateur: admin ***Mot de passe:*** *<définie précédement>* ***URL:*** *http://<ip_pfsense>:3000/*

Puis, nous allons choisir l'interface que l'on veut voir ou espionner

Puis, nous allons choisir le graphique et nous avons une vue du trafic et des informations rapide



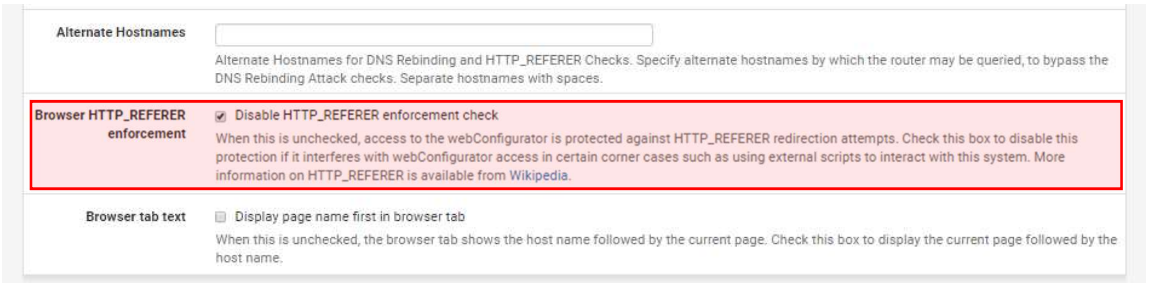
Et pour voir en détaille les connexions effectuer, nous utilisons dans « **Flows** », puis « **IPv4** »



On peut sélectionner le temps voulu grâce au graphique précédent. Nous avons les informations disponibles dans la base de données également.

14. Autorisation interfaces web (Sous réseau)

Afin de pouvoir controler notre PFSENSE, depuis un autre réseau, nous avons besoin de désactiver une régle http. Nous devons aller dans « **System / Advanced**», puis cocher cette case.

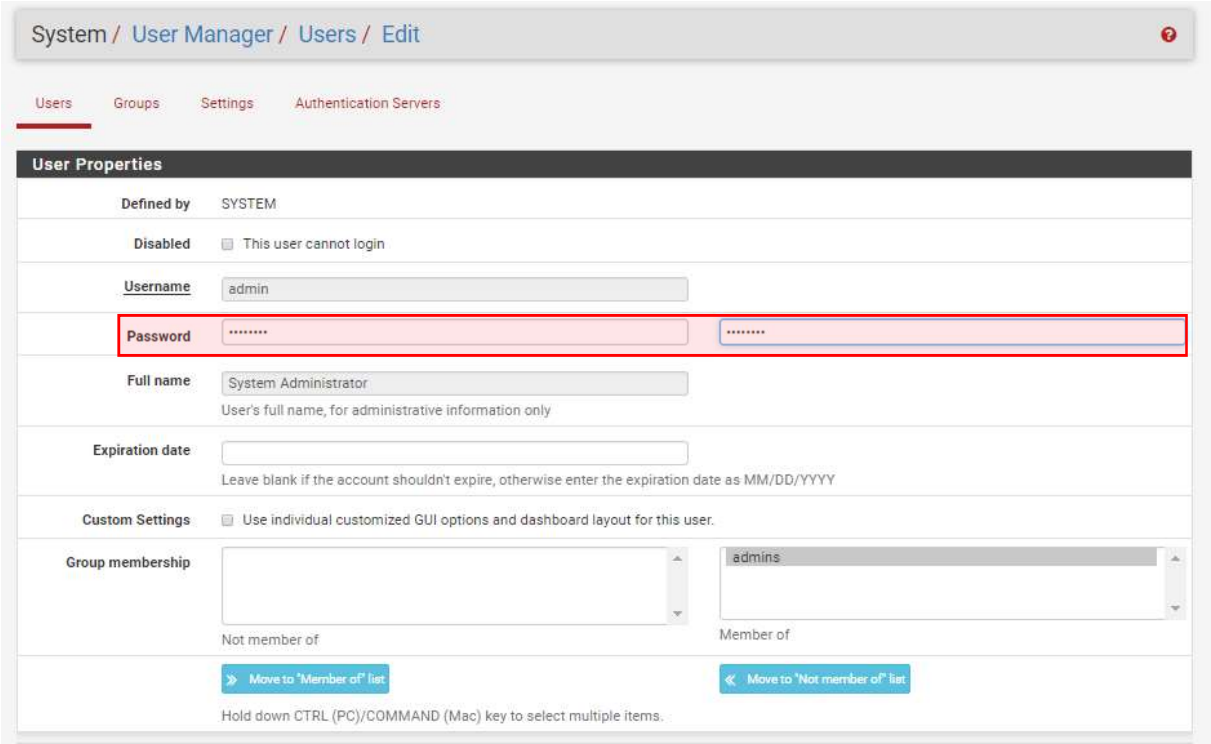


Le routeur est maintenant administrable depuis d'autres réseaux LAN(Sans régles ACL).

15. Changement du mot de passe de l'interface web

Pour modifier le mot de passe pour plus de sécurité, pour cela on va dans « **System / User Manager** » et l'on modifie le compte « **admin** »

On clique sur le petit crayon, pour modifier notre compte

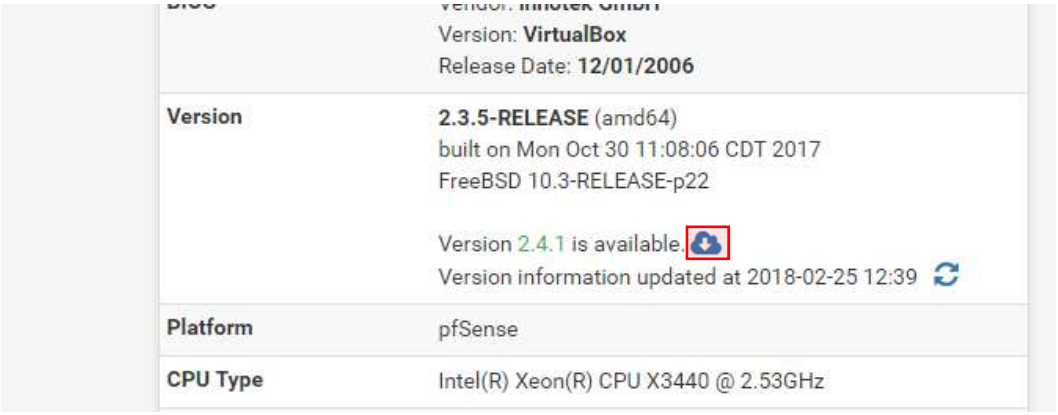


*Nous saisissons notre nouveau mot de passe, puis on clique sur « **Save** » et notre mot de passe est changé.*

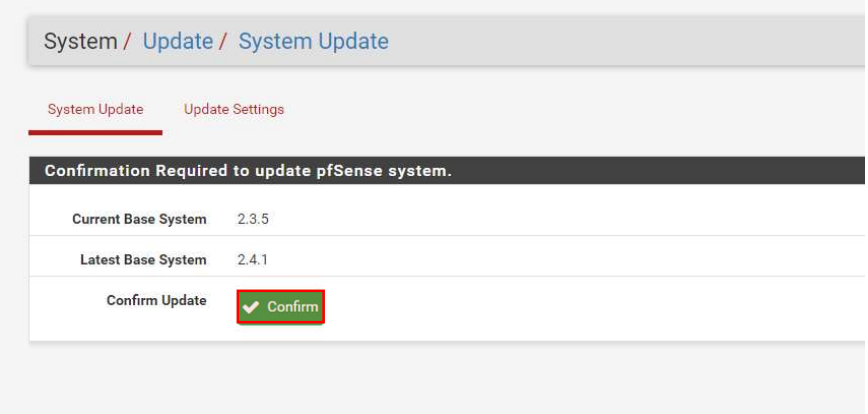
16. Mise à jour PFSENSE(Update Système)

Les mises à jour sont importantes, niveau fonctionnalité et surtout niveau sécurité

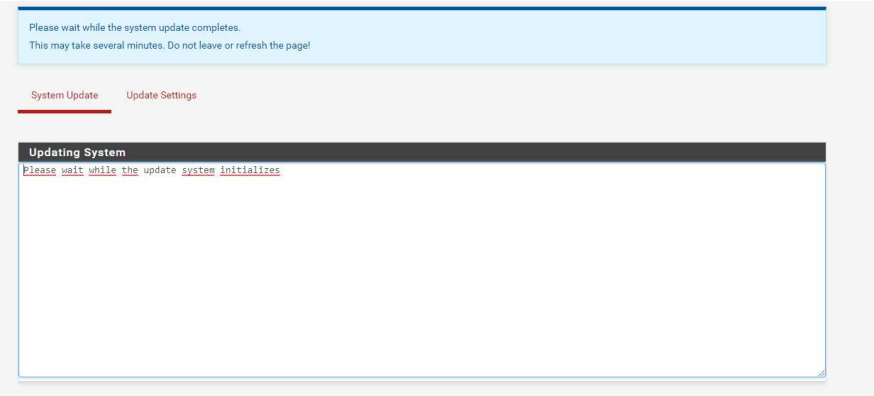
Une mise à jour PFSENSE est facile à faire, pour cela nous devons nous connecter sur le Panel, et sur le Dashboard nous avons la version et comme on peut le voir la version 2.4.1 est disponible, nous pouvons donc la mettre à jour grâce au petit nuage download.



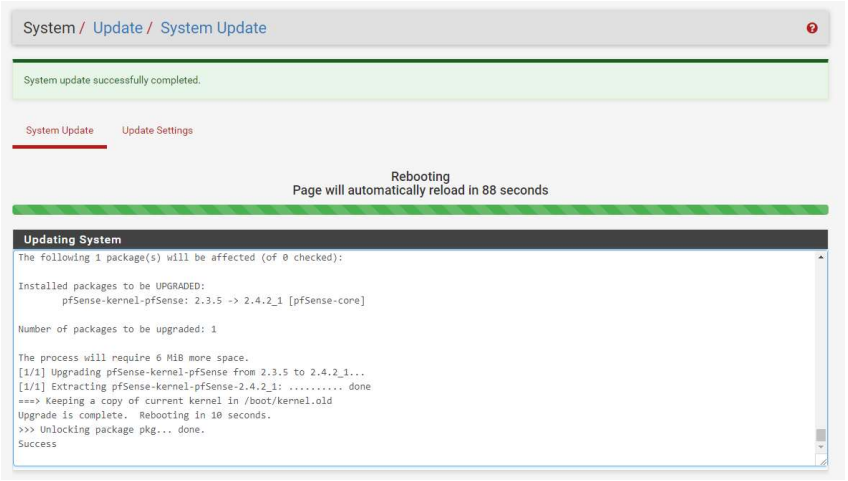
Une demande de confirmation nous ai demandé si l'on veut bien mettre à jour notre version, pour cela cliquer sur « **Confirm** »



Puis l'installation se fait, mais on ne doit ni quitter ni fermer cette page car la mise à jour va s'arrêter et risque de planter PFSENSE.



Nous avons un message qui nous informe que la mise à jour est fini et que PFSENSE doit redémarrer



Puis une fois redémarrer, sur le Dashboard nous avons bien l'information qui nous dit que c'est bien la dernière version que nous avons