



Installation PFSENSE (Redondance, Filtrage, NAT, VPN)



Sommaire

1.	Pourquoi mettre en place pfsense	3
2.	Configuration réseau	3
3.	Installation Pfsense	3
1.	Configuration du serveur pfsenseA.....	6
2.	Configuration du serveur pfsenseB.....	12
3.	Configuration des adresses IP virtuelle	14
4.	Mise en place de règles de filtrage.....	17
5.	Mise en place de Liste de blockage.....	24
6.	Mise en place d'une journalisation du trafic réseau.....	37

1. Pourquoi mettre en place PFSENSE

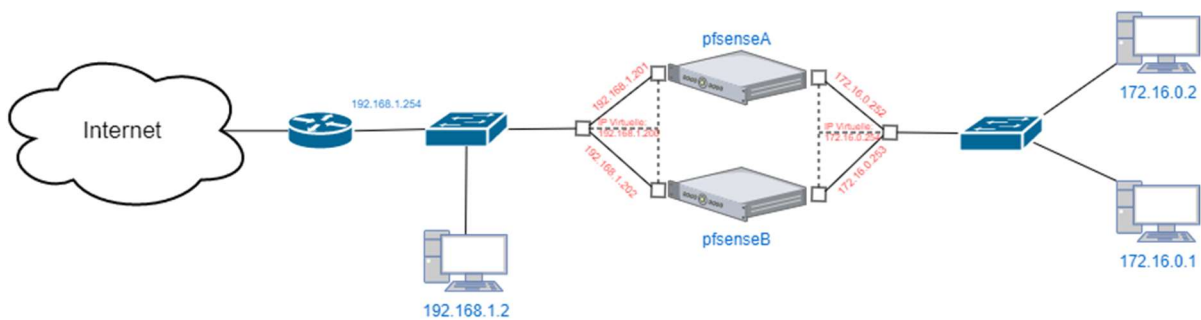
Pfsense est un routeur/pare-feu qui est libre de droit. Il est entièrement configurable par interface web et il a de nombreux services supportés comme :

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

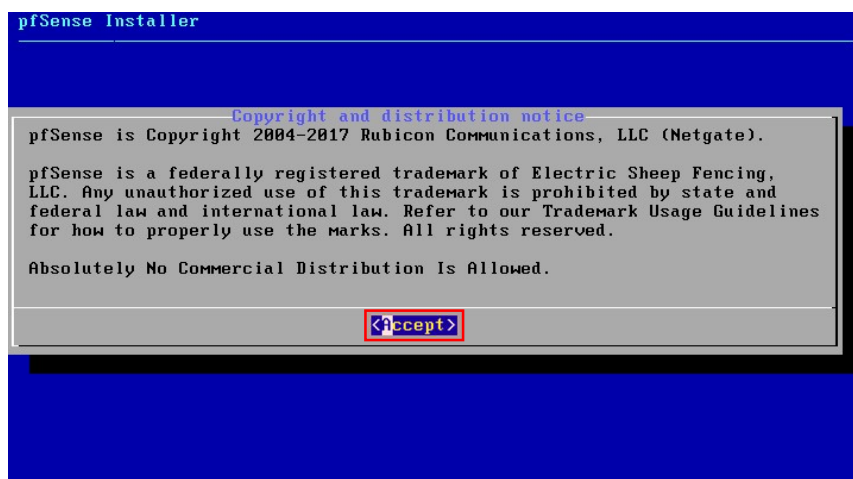
Il y'a aussi la possibilité de faire de la redondance et de la haute disponibilité, et de mettre en place des adresses IP virtuelles.

2. Configuration réseau

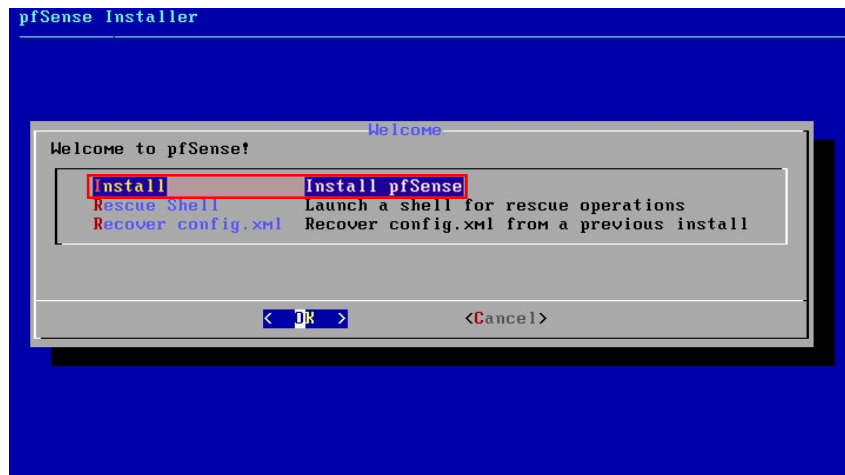
Pour cette installation, nous allons mettre en place 2 serveurs en redondance et avec une haute disponibilité comme sur le schéma suivant :



3. Installation Pfsense

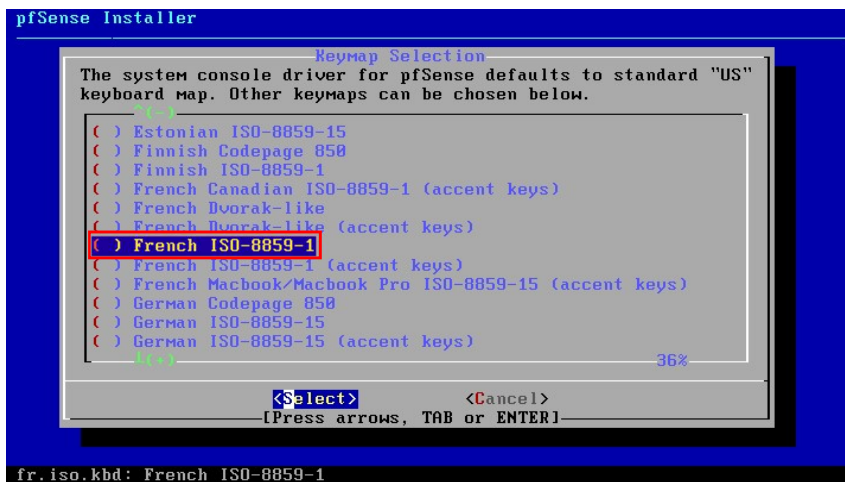


Accepter les termes afin d'installer pfsense

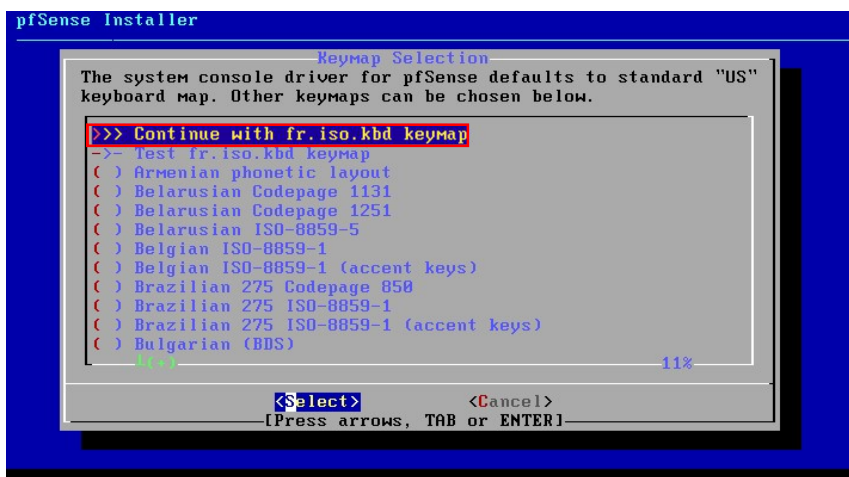


Sélectionner « Installer pfsense »

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

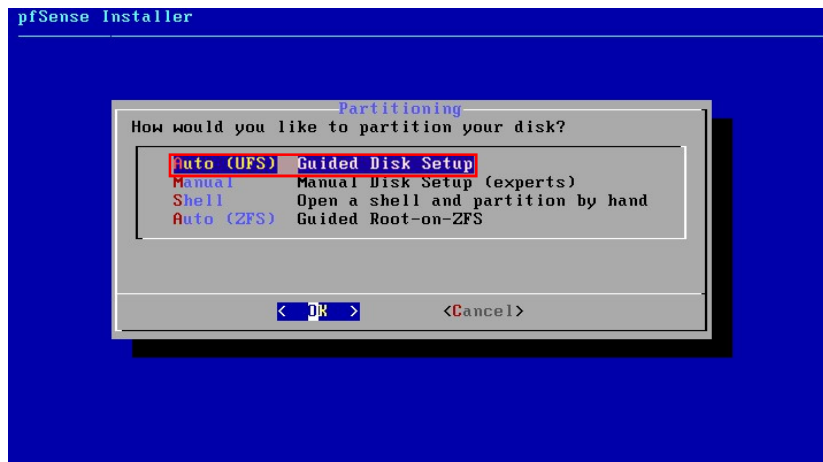


Sélectionner « French ISO-8859-1 »



On confirme bien notre choix, choisir Continuer

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

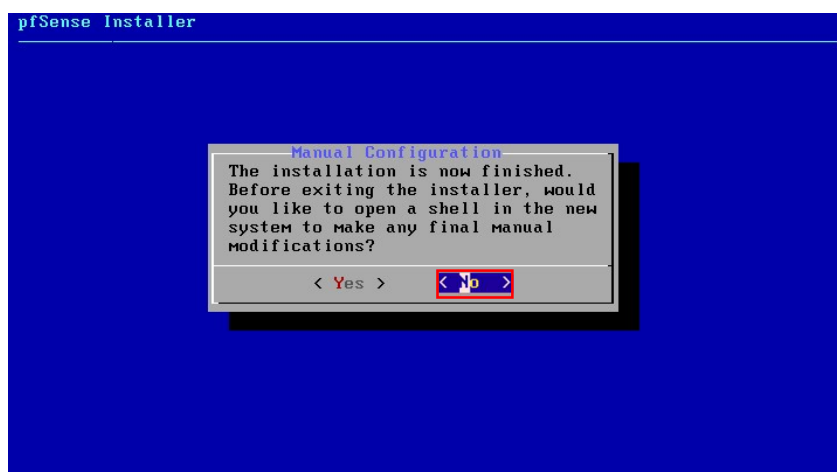


J'ai utilisé le partitionnement automatique, mais cela n'est pas obligé

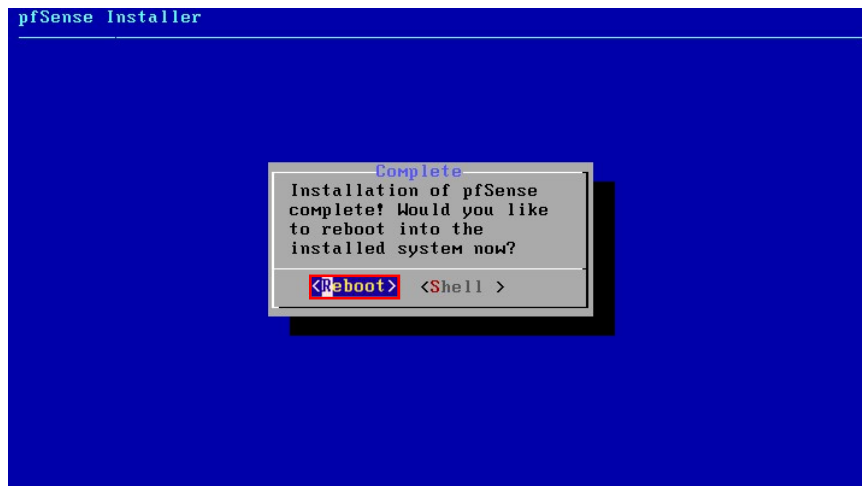


La progression d'installation nous indique son état

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.

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.4.1-RELEASE amd64 Sun Oct 22 17:26:33 CDT 2017
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

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: 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
```

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

```
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: 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
```

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 »

```

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:
>

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

```

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

```

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:
>

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

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

```

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

```

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:
>

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

```

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[3391]: /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 »

```
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:
>

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

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

```
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:
>

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

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

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

5. Configuration du serveur PFSENSE B

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

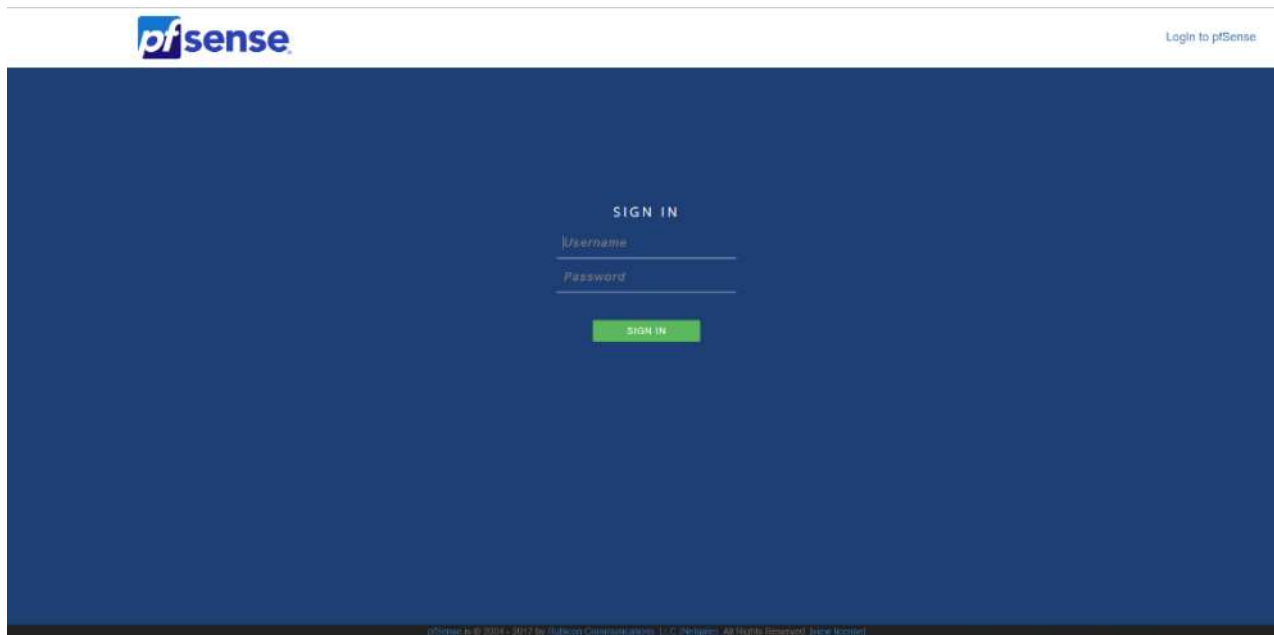
Lan : 192.168.1.202/24, Activation de la configuration web

Wan : 172.16.0.253/24

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

6. Interface Web PFSENSE

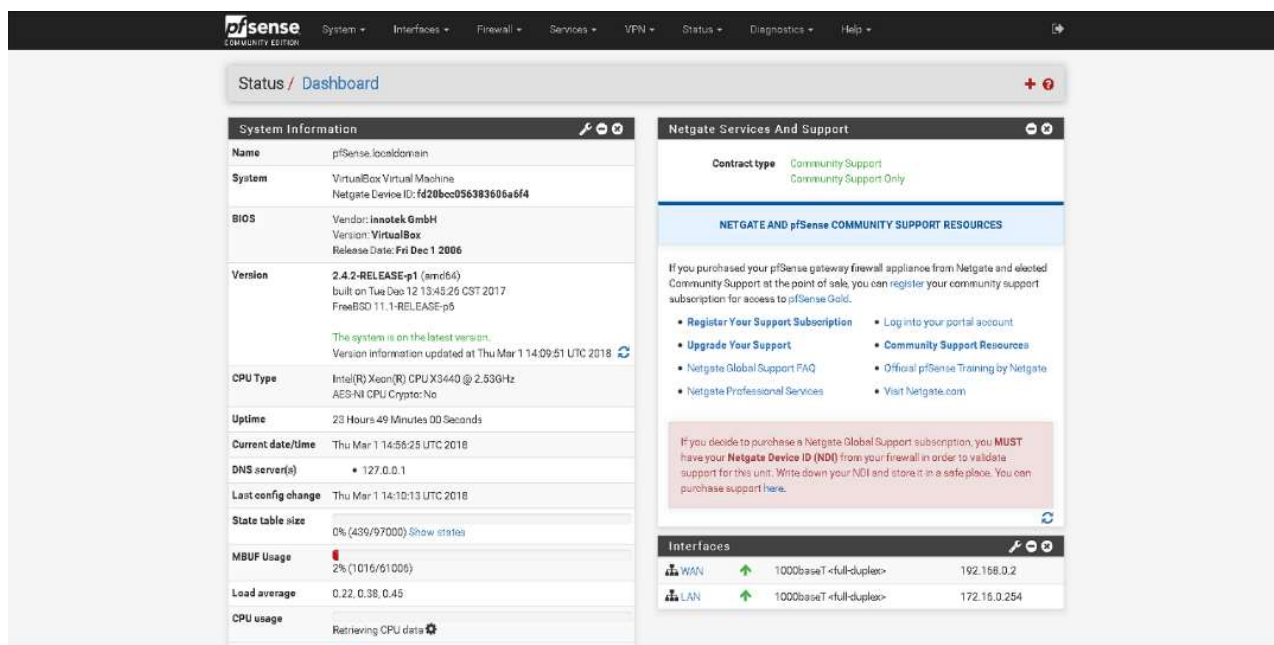
Pour cela, se connecter sur le panel PFSENSE



Login : admin

Password : pfsense

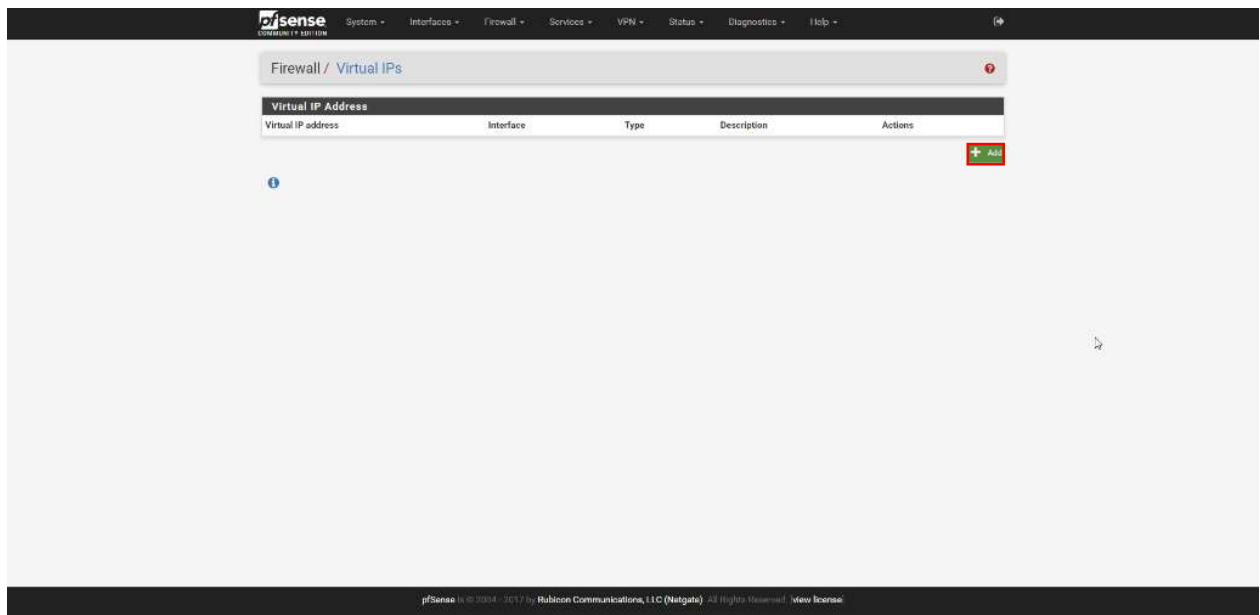
Nous avons le dashboard de PFSENSE, avec les informations principale et les informations système.



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

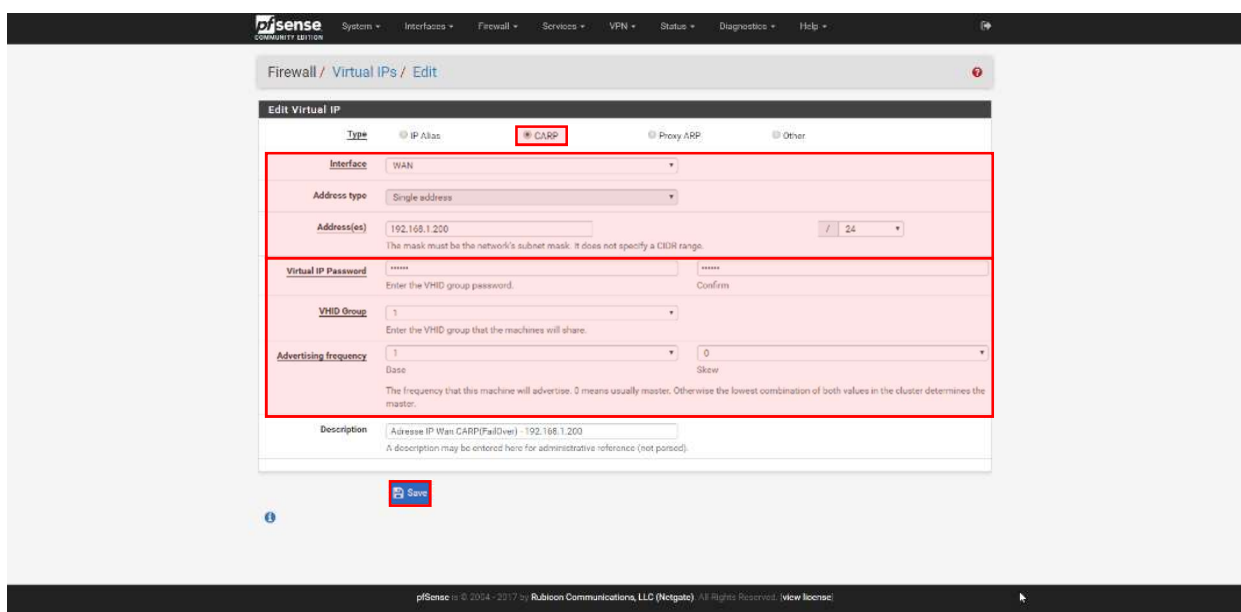
7. Configuration des adresses IP virtuelle (Haut Dispo)

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 crée une adresse IP en 172.16.0.254, qui permet de faire une redondance sur des adresses IP. Cela est utilisé 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 est 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 crée notre IP virtuelle WAN, comme ceci

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

The screenshot shows the 'Edit Virtual IP' configuration page in pfSense. The 'Type' is set to 'CARP'. The 'Interface' is 'LAN'. The 'Address type' is 'Single address'. The 'Address' is '172.16.0.254' with a subnet mask of '24'. The 'Virtual IP Password' is set to '2'. The 'Advertising frequency' is '1'. The 'Description' is 'Address IP Lan CARP(PaOver) - 172.16.0.254'.

On fait de même pour l'interface Lan.

Nous allons pouvoir appliquer les paramètres

The screenshot shows the 'Virtual IP Address' configuration page in pfSense. It displays a table with two entries:

Virtual IP address	Interface	Type	Description	Actions
192.168.1.200/24 (vif0.1)	WAN	CARP	Adresse IP Wan CARP(PaOver) - 192.168.1.200	Edit Delete
172.16.0.254/24 (vif0.2)	LAN	CARP	Adresse IP Lan CARP(PaOver) - 172.16.0.254	Edit Delete

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

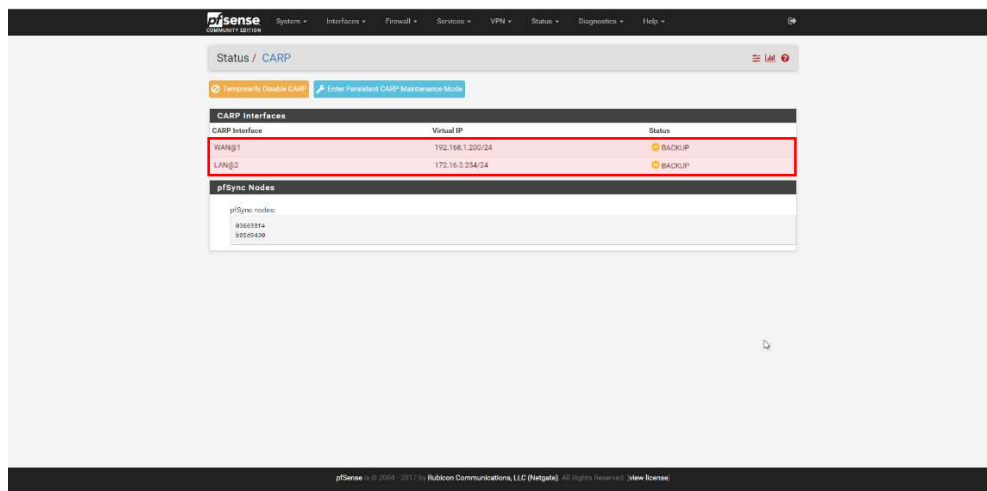
On peut voir dans le staus CARP, et savoir si l'interface est en "Master" ou bien en "Backup"

The screenshot shows the 'Status / CARP' page in pfSense. It displays a table with two entries:

CARP Interface	Virtual IP	Status
WAN@1	192.168.1.200/24	MASTER
LAN@2	172.16.0.254/24	MASTER

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

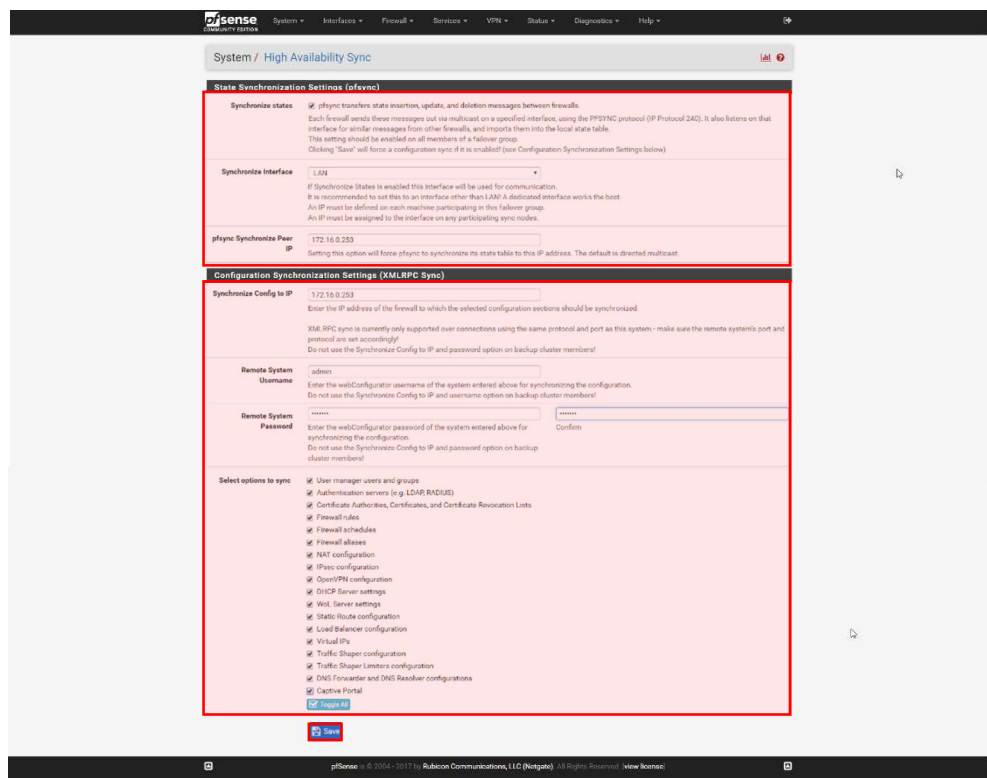
Le statut des IP virtuelle sur le second PFSense, il sont donc bien en backup



On peut voir le statut 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 répliquions des règles de filtrage, NAT, VPN, etc.... Ce permet de devoir effectuer la création d'une règle ou autre, uniquement d'un seul coté. La répliquion s'effectue automatiquement.

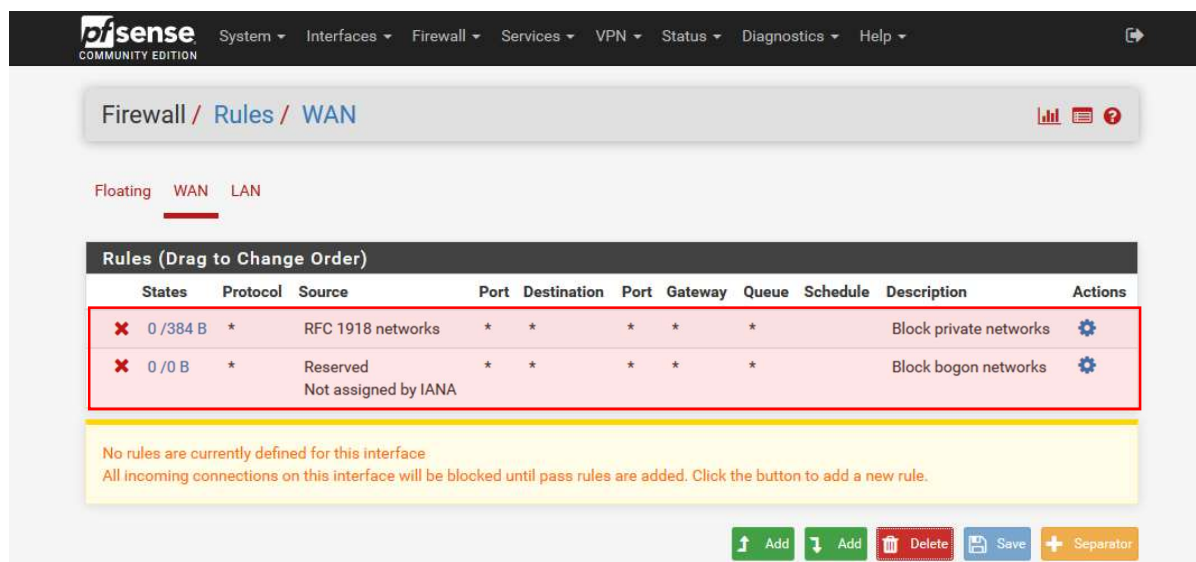


Nous allons mettre en place la redondance de Pfsense, afin d'avoir les memes paramétrages coté PfsenseA et PfsenseB. La configuration doit être actif des deux cotés

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.



Firewall / Rules / WAN

Floating WAN LAN

Rules (Drag to Change Order)

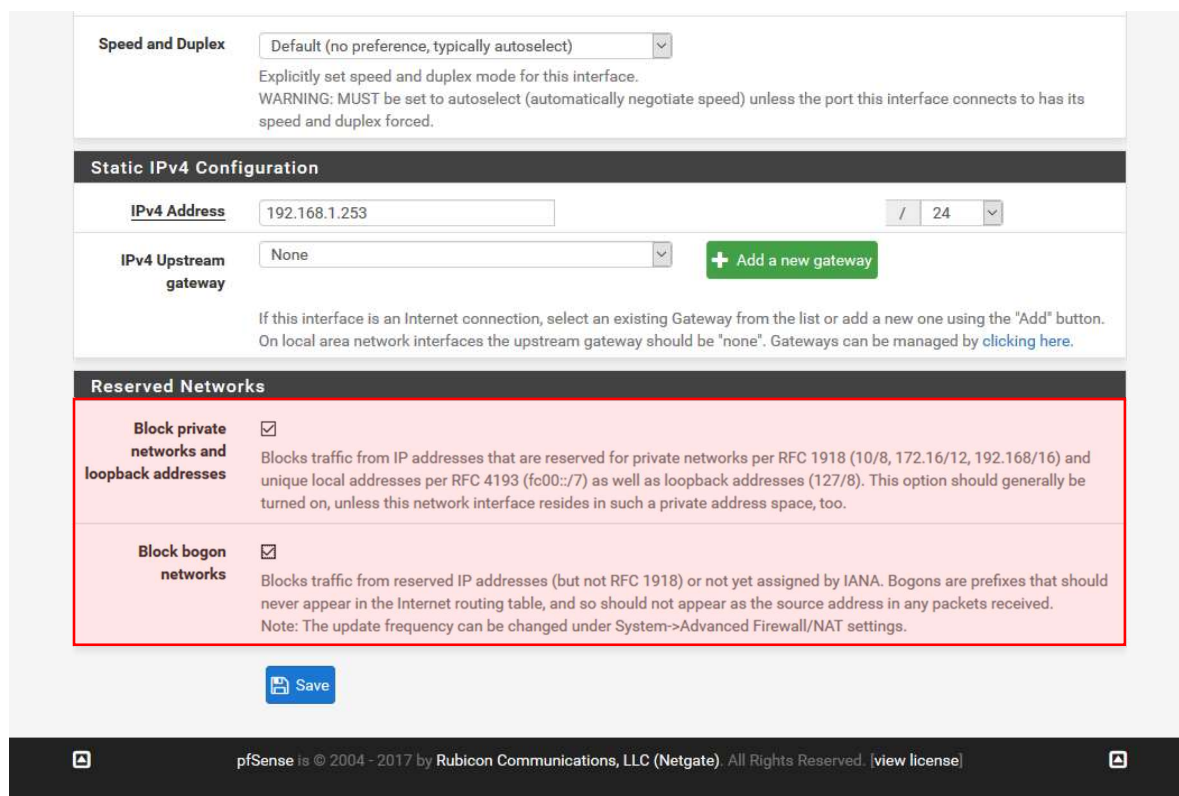
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗ 0 / 384 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙
✗ 0 / 0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙

No rules are currently defined for this interface.
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

↑ Add ↓ Add Delete Save + Separator

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.



Speed and Duplex: Default (no preference, typically autoselect)

Static IPv4 Configuration

IPv4 Address: 192.168.1.253 / 24

IPv4 Upstream gateway: None + Add a new gateway

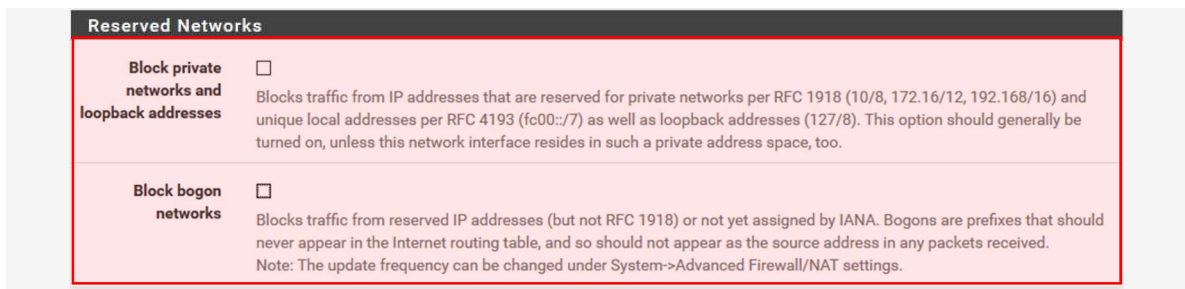
Reserved Networks

- ☒ Block private networks and loopback addresses
- ☒ Block bogon networks

Save

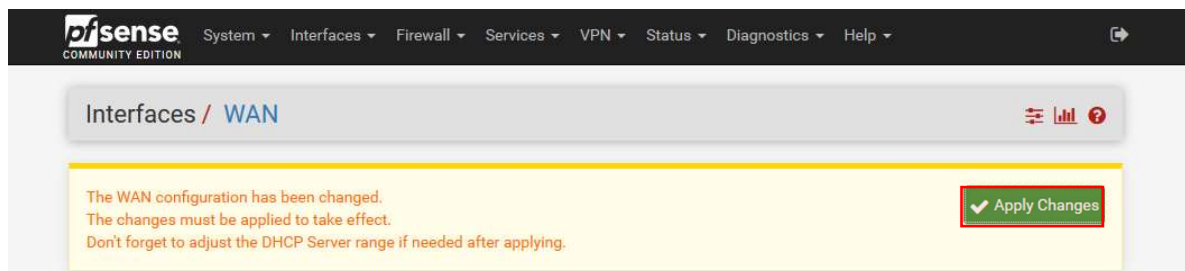
Nous devons décocher les deux règles dans "**Reserved Networks**", elle empêche de créer des règles ce sont des sécurités actives de base.

On doit se retrouver donc sans nos deux cases cocher



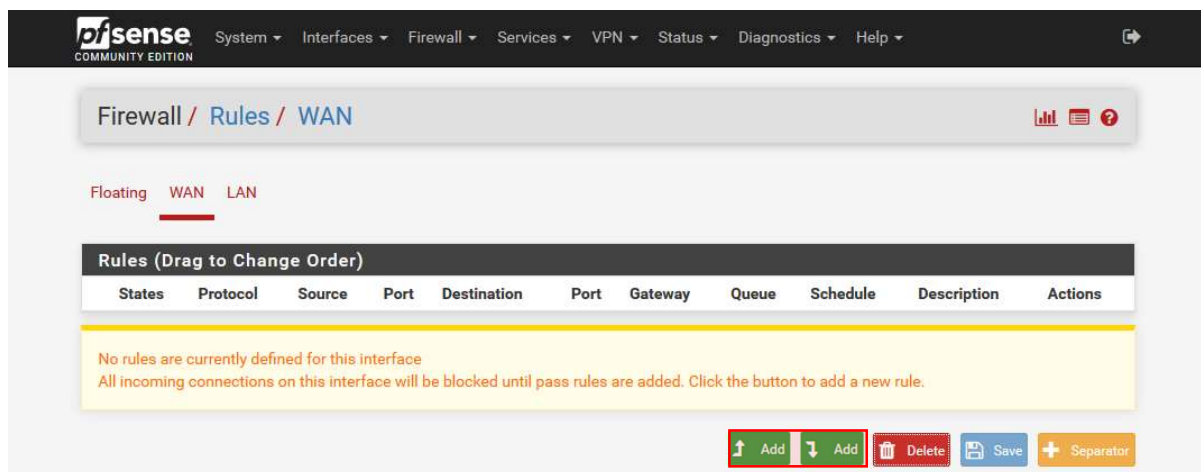
Aucune ne doit être cocher

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 appliquées sur les règles :

- 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 sélectionner notre interface (WAN ou LAN), sur laquelle la règle sera activée

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

Et pour finir on paramètre notre règle, 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 règle de blockage, mais le principe est le meme pour toutes règles.

The screenshot shows the 'Edit Firewall Rule' interface in pfSense. The form is divided into several sections: 'Action' (Block), 'Disabled' (checkbox), 'Interface' (WAN), 'Address Family' (IPv4), 'Protocol' (Any), 'Source' (any), 'Destination' (any), 'Extra Options' (Log checkbox, Description: 'Bloque tout le trafic'), and 'Advanced Options' (Display Advanced button). A 'Save' button is at the bottom. The interface is in French.

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

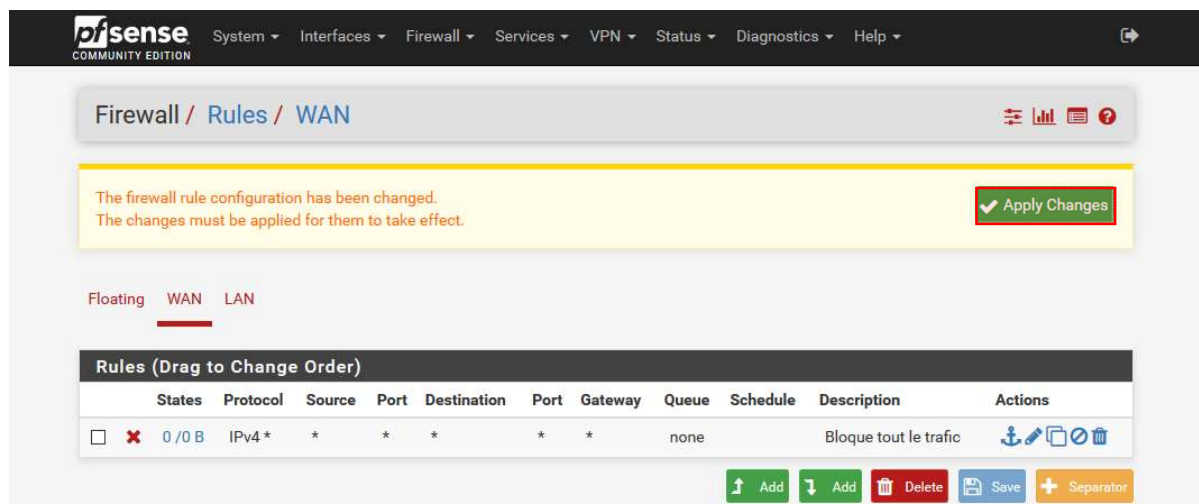
Attention la règles de blocage doit être effectuer en dernière coté LAN, elle risque de bloquer l'accès à l'interface web. Pour le coté LAN et WAN, le principe est le même. Il est possible de désactiver l'utilisations de certains protocoles ou bien bloquer une partie du réseau au certaines machines. Cet outil est 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.

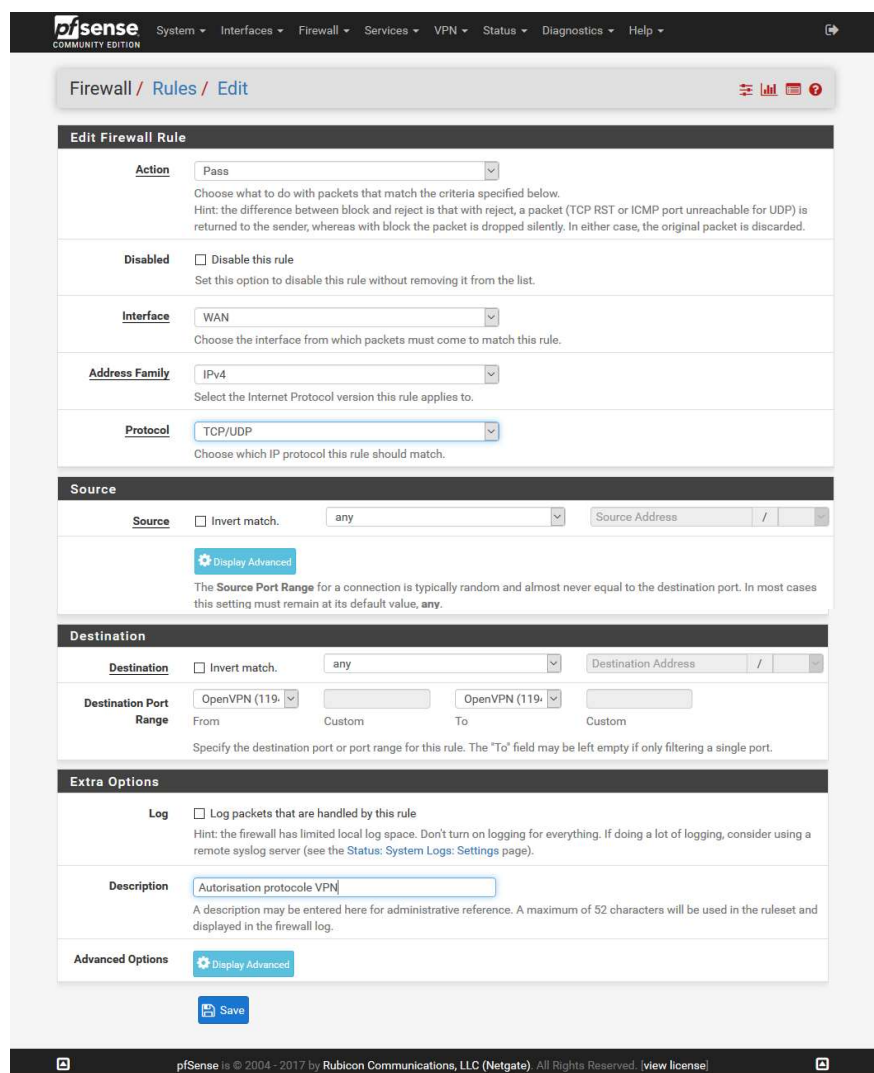
✓	1/1.58	*	*	*	LAN	80	*	*	Anti-Logout Rule	⚙
	MIB				Address					

Une fois notre règle créer, nous devons l'appliquer



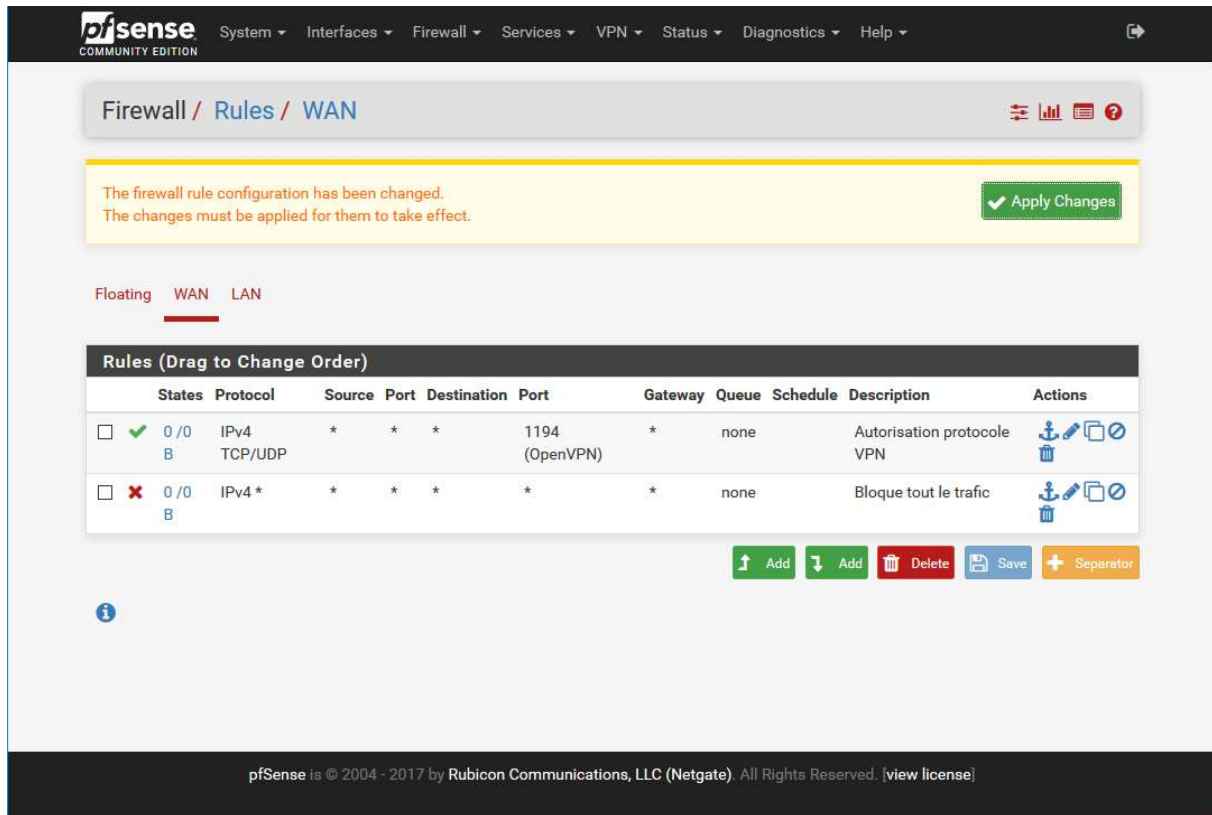
Cliquer sur "Apply Changes", afin d'activer notre règle.

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 créées, nous devons les appliquer. Nous avons une rapide vision sur les règles et leurs actions. Attention leurs ordres et importance. Si la règle de blocage est en première aucune des règles après ne fonctionnera.



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

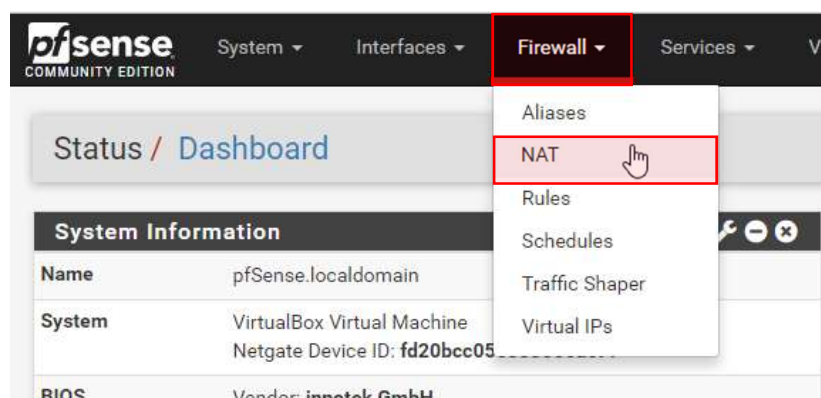
La redirection de port permet de transférer un port exemple :

Routeur 192.168.1.200

Machine 172.16.0.102

Port d'entrée 192.168.1.200 :8080

Port de sortie 172.16.0.102:80



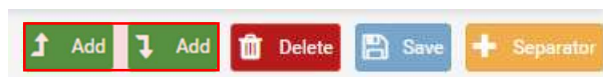
Pour cela, nous devons aller dans « Firewall / Nat »

Voila un exemple de règles qui sont traduité

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

Exemple de règles qui peuvent être créés

Pour créer une règle NAT, cliquer sur "ADD"



Pour cela, nous devons cliquer sur « ADD »

Firewall / NAT / Port Forward / Edit

Edit Redirect Entry

☐ Disabled ☐ Disable this rule

No RDR (NOT) ☐ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface
Choose which interface this rule applies to. In most cases "WAN" is specified.

Protocol
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

Destination ☐ Invert match.

Destination port range
From port Custom To port Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP
Enter the internal IP address of the server to which to map the ports.
e.g.: 192.168.1.12

Redirect target port
Port Custom

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

Description
A description may be entered here for administrative reference (not parsed).

No XMLRPC Sync ☐ Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection

Filter rule association
The "pass" selection does not work properly with Multi-WAN. It will only work on an interface containing the default gateway.

Créer notre règle, 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 règles dans rules sont créés grâce au NAT créer précédemment, il faut juste effectuer plusieurs manipulations si elle ne sont pas dans le bon ordre.

Rules (Drag to Change Order)										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
Machine Hopper - 172.16.0.101										
☒	18 /17.41 MiB	IPv4 TCP	*	*	172.16.0.101	80 (HTTP)	*	none	NAT Serveur Web - Hopper	
☒	1 /339 KiB	IPv4 TCP	*	*	172.16.0.101	22 (SSH)	*	none	NAT Serveur Web - Hopper	
☒	2 /164 KiB	IPv4 TCP	*	*	172.16.0.101	21 (FTP)	*	none	NAT Serveur FTP - Hopper	
☒	0 /1.47 MiB	IPv4 TCP	*	*	172.16.0.101	49152 - 50000	*	none	NAT Serveur FTP Port Passif - Hopper	
☒	12 /19.58 MiB	IPv4 TCP/UDP	*	*	172.16.0.101	8000	*	none	NAT Serveur Ajenti - Hopper	
Machine Physique - 172.16.0.102										
☒	0 /75.99 MiB	IPv4 TCP	*	*	172.16.0.102	80 (HTTP)	*	none	NAT Serveur Web - Physique	
☒	0 /25 KiB	IPv4 TCP/UDP	*	*	172.16.0.102	3389 (MS RDP)	*	none	NAT RDP - Physique	
☒	0 /19 KiB	IPv4 TCP/UDP	*	*	172.16.0.102	33891	*	none	NAT RDP - Hopper	
☒	0 /14 KiB	IPv4 TCP/UDP	*	*	172.16.0.102	33892	*	none	NAT RDP - Intratec	
☒	0 /14 KiB	IPv4 TCP/UDP	*	*	172.16.0.102	33893	*	none	NAT RDP - Centreon	
☒	0 /2 KiB	IPv4 TCP/UDP	*	*	172.16.0.102	33894	*	none	NAT RDP - PFSENSE	
Machine Intratec - 172.16.0.103										
☒	0 /816 B	IPv4 TCP	*	*	172.16.0.103	1138	*	none	NAT Serveur Web - Intratec	
☒	0 /0 B	IPv4 TCP	*	*	172.16.0.103	22 (SSH)	*	none	NAT Serveur SSH - Intratec	
☒	0 /816 B	IPv4 TCP	*	*	172.16.0.103	8000	*	none	NAT Serveur Ajenti - Intratec	
Machine Centreon - 172.16.0.104										
☒	0 /0 B	IPv4 TCP	*	*	172.16.0.104	22 (SSH)	*	none	NAT Serveur SSH - Centreon	
☒	0 /5.47 MiB	IPv4 TCP	*	*	172.16.0.104	80 (HTTP)	*	none	NAT Serveur Web - Centreon	
Machine PFSENSE - 172.16.0.254										
☒	7 /3.67 MiB	IPv4 TCP	*	*	172.16.0.254	80 (HTTP)	*	none	NAT Serveur Web - PFSENSE	
☒	0 /0 B	IPv4 TCP	*	*	172.16.0.254	22 (SSH)	*	none	NAT Serveur SSH - PFSENSE	
☒	0 /6.64 MiB	IPv4 *	*	*	*	*	*	none		

Exemple de liste de règles NAT/PAT

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

Reserved Networks

Block private networks and loopback addresses

Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

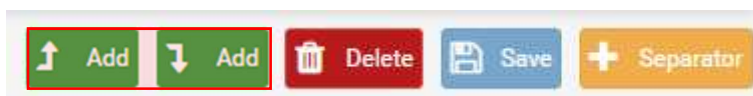
Block bogon networks

Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
Note: The update frequency can be changed under System->Advanced Firewall/NAT settings.

Save

Les deux cases doivent être décochées, car elles empêchent 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 règle doit être identique

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 WAN
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 ☐ Invert match. any Source Address /

Destination ☐ Invert match. any Destination Address /

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
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

Created	2/22/18 14:07:38 by admin@172.16.0.102
Updated	2/22/18 14:18:32 by admin@172.16.0.102

[Save](#)

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

11. Mise en place de Liste de blockage

Nous allons voir comment mettre en place un liste de blockage, qui permet de refuser l'accès à certains site web, en fonction des catégories(Téléchargement illégale, Site d'achats, Sites adultes, 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 blacklist de Toulouse.

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

Une fois dans le manager, 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.

The screenshot shows the pfSense Package Manager interface. The top navigation bar includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The breadcrumb trail is System / Package Manager / Available Packages. The 'Available Packages' tab is selected. A search bar contains the term 'squid'. Below the search bar, a table lists available packages:

Name	Version	Description	Action
Lightsquid	3.0.6_4	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package. Package Dependencies: lighttpd-1.4.47_1 lightsquid-1.8_5	+ Install
squid	0.4.42_1	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP. Package Dependencies: squidclamav-6.16 squid_radius_auth-1.10 squid-3.5.27 c-icap-modules-0.4.5	+ Install
squidGuard	1.16.4	High performance web proxy URL filter. Package Dependencies: squidguard-1.4_15	+ Install

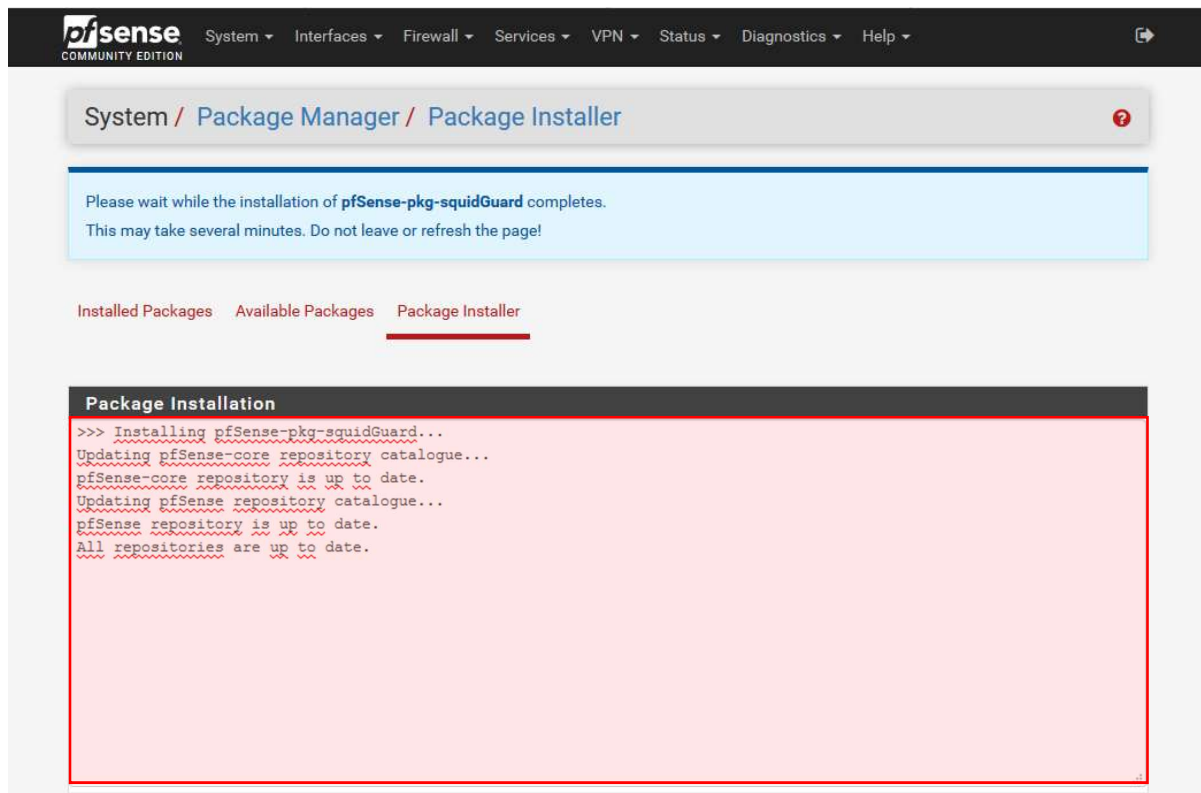
Chaque paquets doivent être installer séparément

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

The screenshot shows the pfSense Package Manager interface. The breadcrumb trail is System / Package Manager / Package Installer. The 'Package Installer' tab is selected. A confirmation message is displayed: "Confirmation Required to install package pfSense-pkg-squidGuard." Below the message is a green button with a checkmark and the text "Confirm".

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 échoue.



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

Une fois les paquets installés, 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 blacklist, ce qui nous permet de la mettre à jour facilement en cas de mise à jour de celle-ci

Blacklist options

Blacklist ☒ Check this option to enable blacklist
Do NOT enable this on NanoBSD installs!

Blacklist proxy

Blacklist upload proxy - enter here, or leave blank.
Format: host:[port login:pass] . Default proxy port 1080.
Example: '192.168.0.1:8080 user:pass'

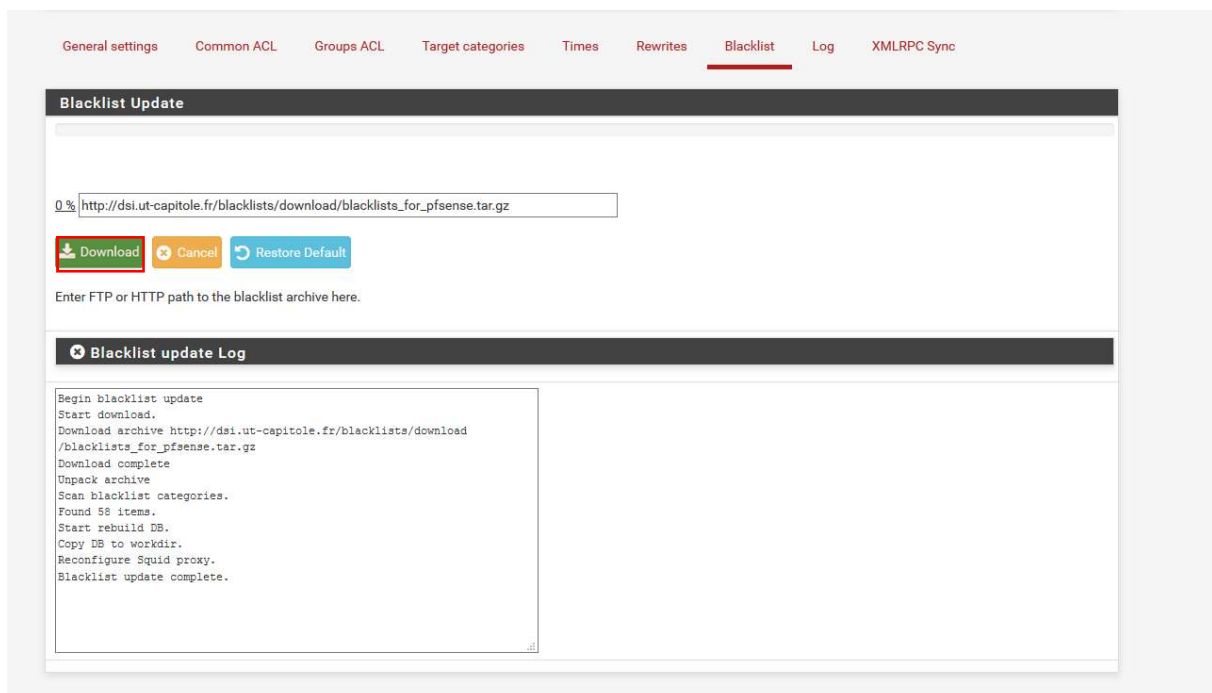
Blacklist URL

Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL blacklist archive or leave blank. The LOCAL path could be your pfSense (/tmp/blacklist.tar.gz).

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

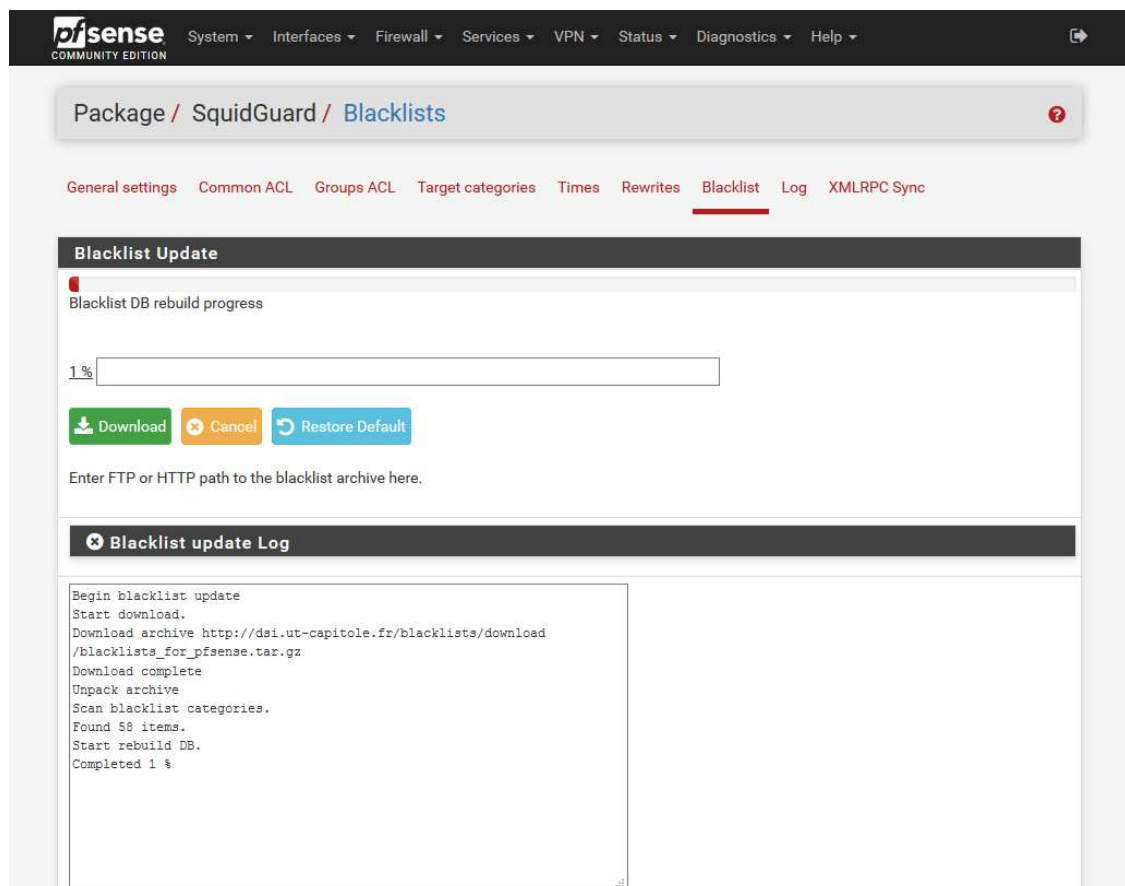
Ce n'est pas la seule blacklist existante, mais elle comprend beaucoup de sites.

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



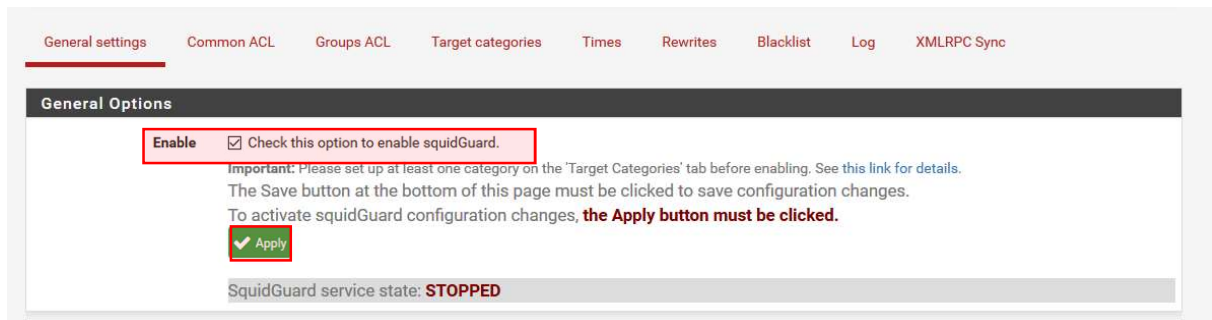
Pour mettre à jour ou installer notre liste de blockage, nous devons la télécharger avec le bouton "**Download**"

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



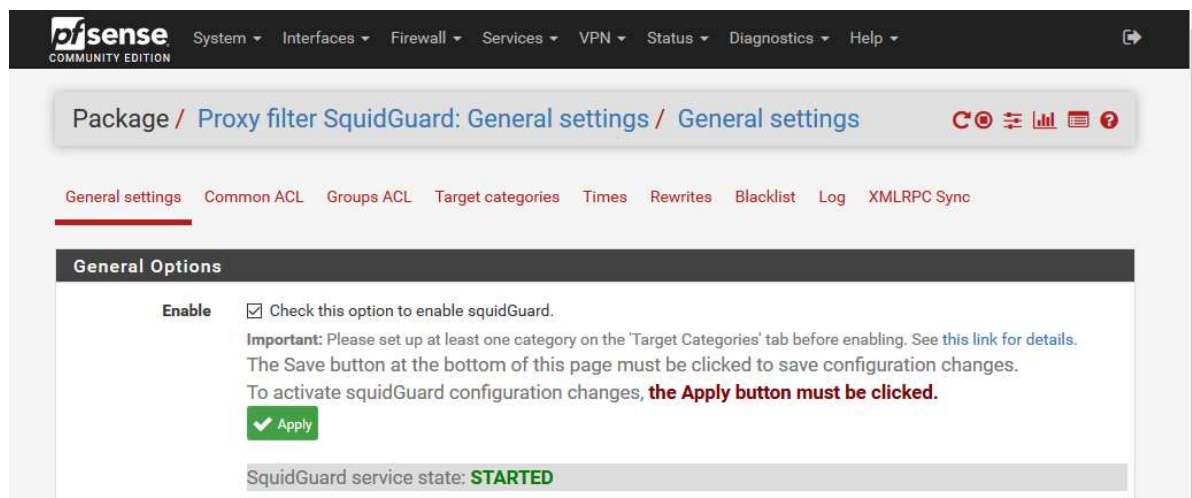
Nous avons un status d'avancement du téléchargement de notre blacklist, cela peut prendre un moment

Une fois notre blacklist 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 case "**Enable**" et cliquer sur "**Apply**"

On vérifie que notre paquet squidGuard soit bien actif

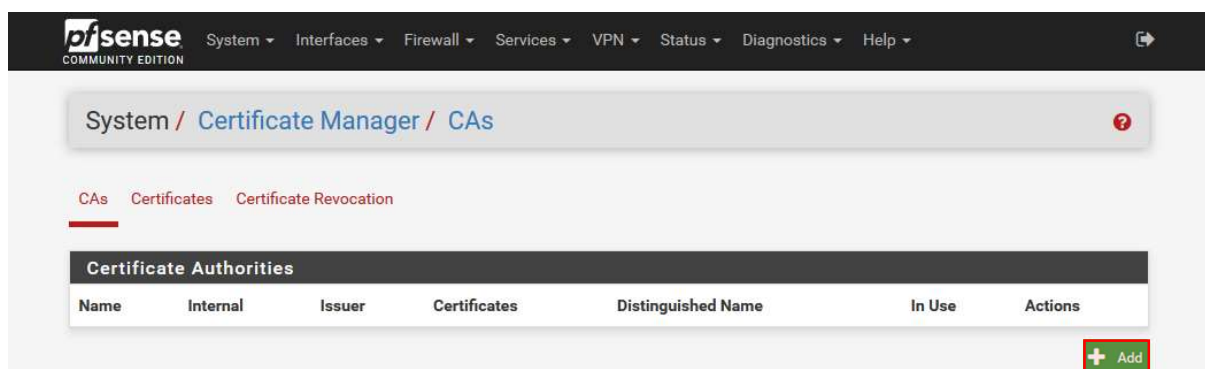


Si il ne démarre pas, il est possible qu'il ne soit pas bien installé ou bien la configuration incorrecte

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 évite d'avoir un serveur dédié à cette tâche.

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



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

Nous allons créer notre autorité de certification.

CA's Certificates Certificate Revocation

Create / Edit CA

Descriptive name pfSense FireWall

Method Create an internal Certificate Authority

Internal Certificate Authority

Key length (bits) 2048

Digest Algorithm sha256
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

Lifetime (days) 3650

Country Code FR

State or Province Centre-Val-de-Loire

City Tours

Organization Paul Louis Courier

Organizational Unit BTS SIO

Email Address yohan.fresneau@outlook.fr

Common Name internal-ca

Save

Les informations peuvent être modifier et doivent être adapter

Nous allons créer le certification de notre serveur OpenVPN

CA's Certificates Certificate Revocation

Add/Sign a New Certificate

Method Create an internal Certificate

Descriptive name pfSense OpenVPN

Internal Certificate

Certificate authority pfSense FireWall

Key length 2048

Digest Algorithm sha256
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

Lifetime (days) 3650

Country Code FR

State or Province Centre-Val-de-Loire

City Tours

Organization Paul Louis Courier

Organizational Unit BTS SIO

Email Address yohan.fresneau@outlook.fr

Common Name pfsense.sca3.lan

Certificate Attributes

Attribute Notes The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.
For Internal Certificates, these attributes are added directly to the certificate as shown.

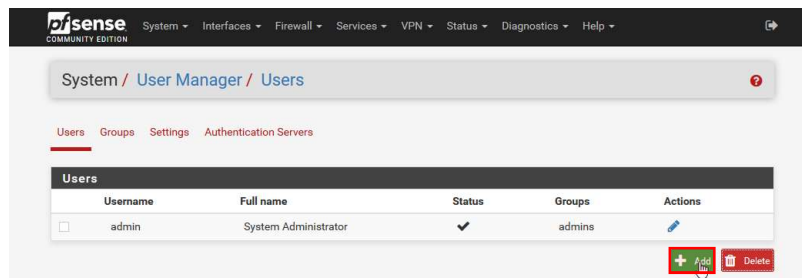
Certificate Type Server Certificate
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names FQDN or Hostname
Type Value
Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Add + Add

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 certificat pour les client, afin qu'il puissent se connecter au VPN

Certificate Attributes

Attribute Notes The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type User Certificate

Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names FQDN or Hostname

Type Value

Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Add **+ Add**

Save

pfSense is © 2004 - 2017 by Rubicon Communications, LLC (Netgate) All Rights Reserved. [view license](#)

Notre certificat est universelle pour tous les clients veulent 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

Custom Settings ☐ Use individual customized GUI options and dashboard layout for this user.

Group membership admins

Not member of Member of

Move to "Member of" list **Move to "Not member of" list**

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Effective Privileges

Inherited from	Name	Description	Action
			+ Add

User Certificates

Name	CA

+ Add

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

Nous devons sélectionner le certificat au quelle on le lie

System / Certificate Manager / Certificates / Edit

CA's Certificates Certificate Revocation

Add/Sign a New Certificate

Method Choose an existing certificate

Descriptive name client-openvpn

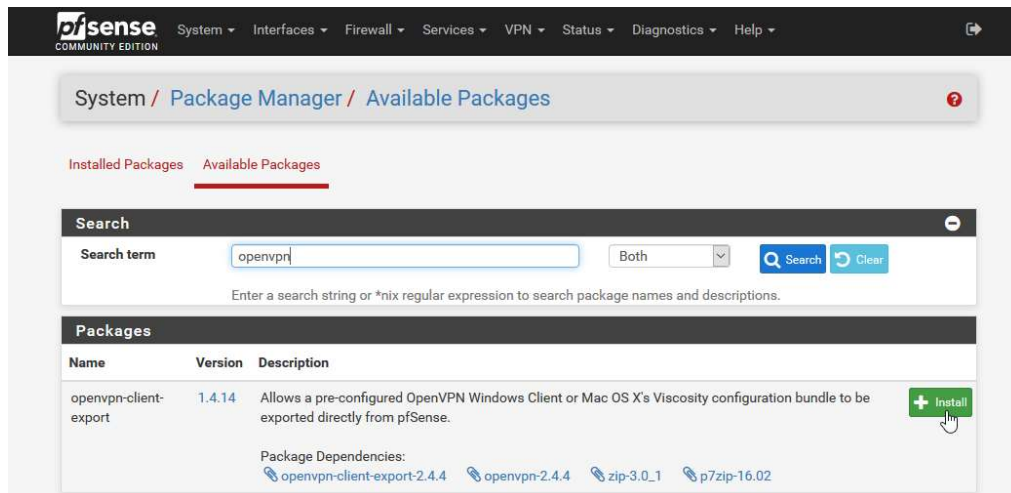
Choose an Existing Certificate

Existing Certificates Client VPN (CA: pfSense FireWall)

Save

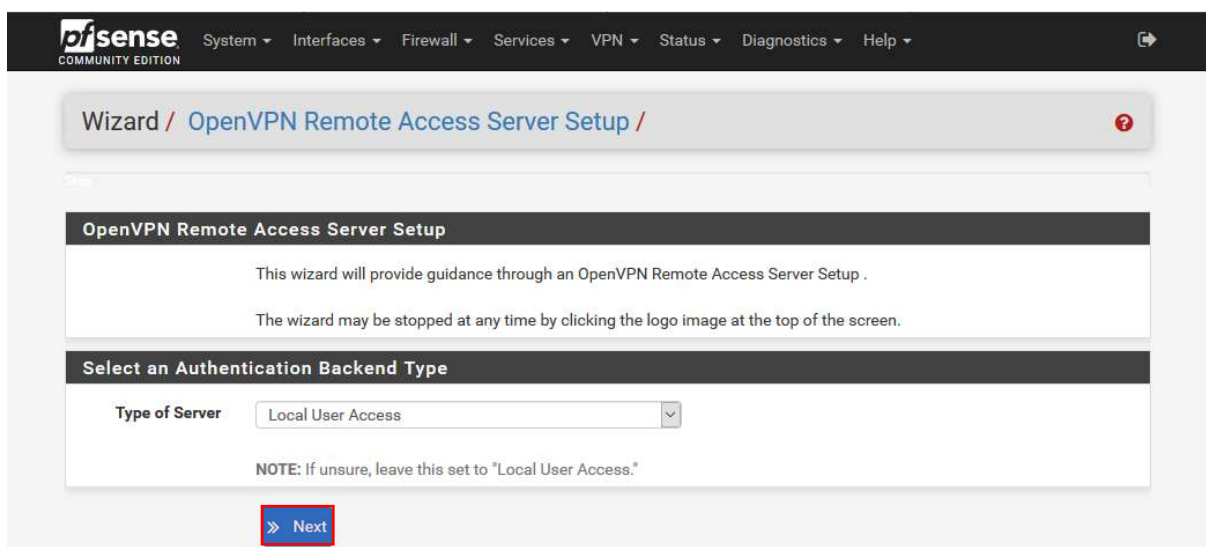
On sélectionne notre certificat créer précédament pour nos utilisateurs

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

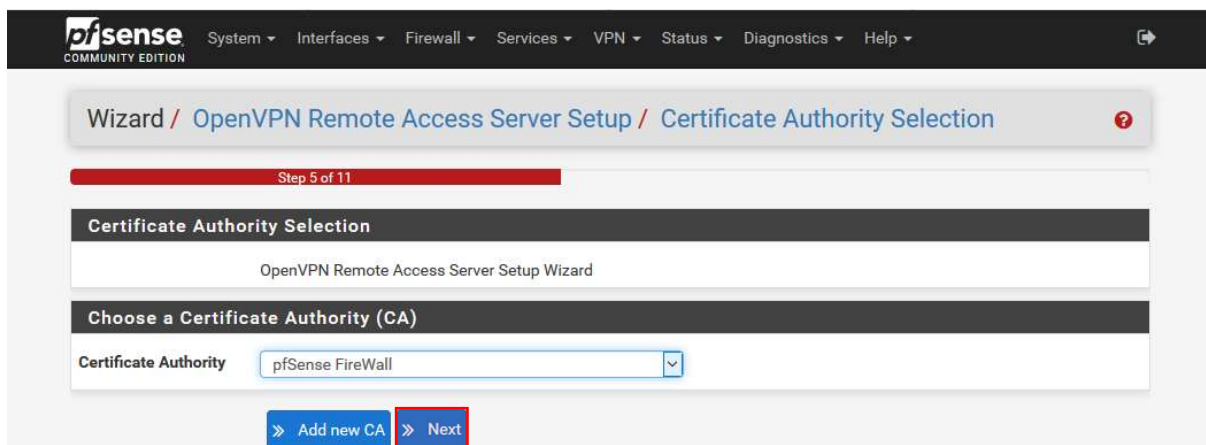


On clique sur installer afin d'ajouter le paquet

Nous allons installer le serveur VPN et le configurer



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



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

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Wizard / OpenVPN Remote Access Server Setup / Server Certificate Selection

Step 7 of 11

Server Certificate Selection

OpenVPN Remote Access Server Setup Wizard

Choose a Server Certificate

Certificate: pfSense OpenVPN ▾

» Add new Certificate » Next

On sélectionne le certificat que l'on a créé pour notre serveur, puis "Next"

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Wizard / OpenVPN Remote Access Server Setup / Server Setup

Step 9 of 11

Server Setup

OpenVPN Remote Access Server Setup Wizard

General OpenVPN Server Information

Interface: WAN ▾
The interface where OpenVPN will listen for incoming connections (typically WAN.)

Protocol: UDP ▾
Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.

Local Port: 1194
Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.

Description: Serveur OpenVPN
A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.

Cryptographic Settings

TLS Authentication ☒
Enable authentication of TLS packets.

Generate TLS Key ☒
Automatically generate a shared TLS authentication key.

TLS Shared Key
Paste in a shared TLS key if one has already been generated.

DH Parameters Length: 2048 bit ▾
Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.

Encryption Algorithm: AES-256-CBC (256 bit key, 128 bit block) ▾
The algorithm used to encrypt traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips.

Auth Digest Algorithm: SHA1 (160-bit) ▾
The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.

Hardware Crypto: No Hardware Crypto Acceleration ▾
The hardware cryptographic accelerator to use for this VPN connection, if any.

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 subnet

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

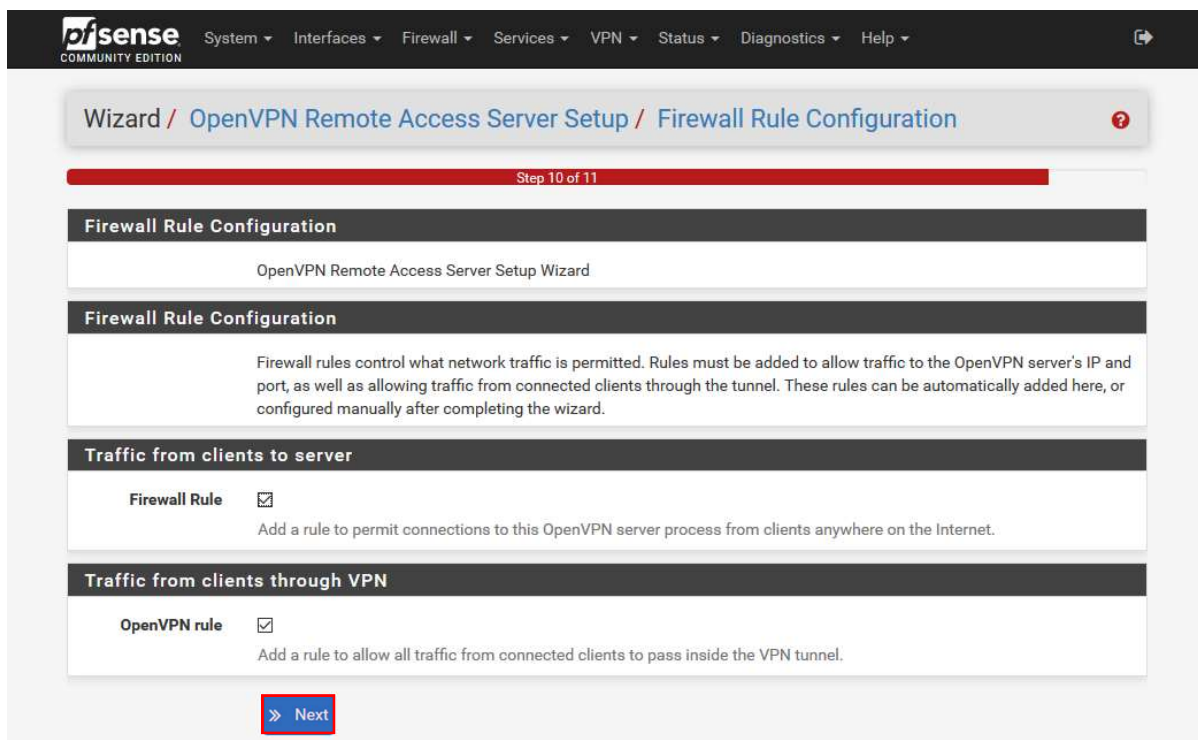
A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.

Advanced

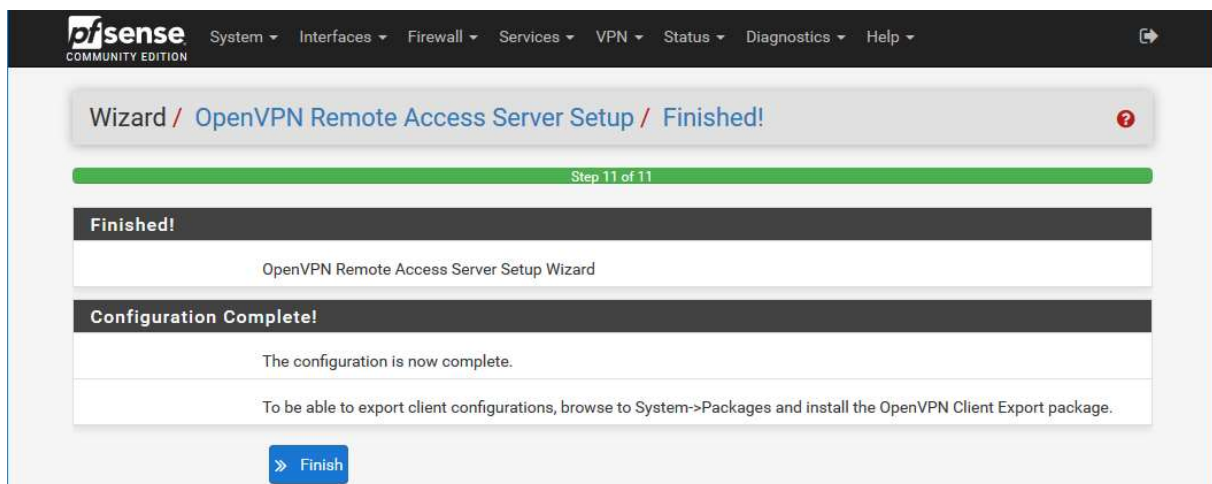
Enter any additional options to add to the OpenVPN server configuration here, separated by a semicolon. EXAMPLE: push "route 10.0.0.0 255.255.255.0"

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 configuré, il nous reste plus qu'à installer un client VPN sur un poste et ce connecter à distance.

Précédemment, nous avons installé un paquet OpenVPN, qui nous permet de pré-générer 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.

Servers configured with features that require OpenVPN 2.4 will not work with OpenVPN 2.3.x or older clients. These features include: AEAD encryption such as AES-GCM, TLS Encryption+Authentication, ECDH, LZ4 Compression and other non-legacy compression choices, IPv6 DNS servers, and more.

OpenVPN Clients

User	Certificate Name	Export
client-openvpn	Client VPN	- Inline Configurations: Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: Archive Config File Only - Current Windows Installer (2.4.4-1x01): Windows Vista and Later - Old Windows Installers (2.3.18-1x01): x86-xp x64-xp x86-win6 x64-win6 - Viscosity (Mac OS X and Windows): Viscosity Bundle Viscosity Inline Config

If a client is missing from the list it is likely due to a CA mismatch between the OpenVPN server instance and the client certificate, the client certificate does not exist on this firewall, or a user certificate is not associated with a user when local database authentication is enabled.

OpenVPN 2.4 requires Windows Vista or later

The "win6" Windows installers include the tap-windows6 driver which requires Windows Vista or later.

The "XP" Windows installers work on Windows XP and later versions.

Links to OpenVPN clients for various platforms:

OpenVPN Community Client - Binaries for Windows, Source for other platforms. Packaged above in the Windows Installers

OpenVPN For Android - Recommended client for Android

FEAT VPN For Android - For older versions of Android

OpenVPN Connect (iOS/Android) - Recommended client for iOS

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

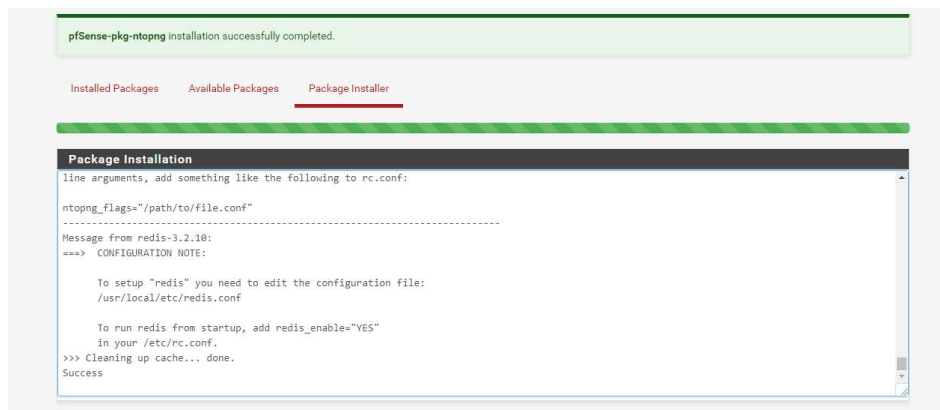
13. Mise en place d'une journalisation du trafic réseau

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

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

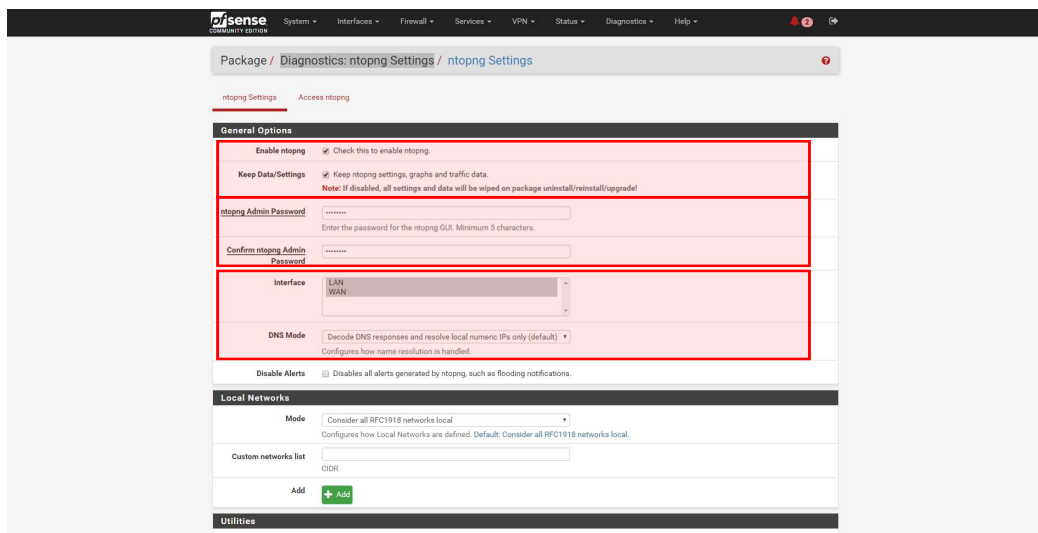
The screenshot shows the 'System Package Manager' window. At the top, there are two tabs: 'Installed Packages' and 'Available Packages', with 'Available Packages' being the active tab. Below the tabs is a search bar with the label 'Search'. Inside the search bar, there is a text input field for 'Search term', a dropdown menu set to 'Both', and two buttons: 'Search' and 'Clear'. Below the search bar, there is a text prompt: 'Enter a search string or *nix regular expression to search package names and descriptions.' Below this is a table titled 'Packages' with three columns: 'Name', 'Version', and 'Description'. The table is currently empty.

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



Nous devons attendre que Success soit affiché, car si on quitte la page ntopng ne sera pas complètement installée

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 sélectionne les deux interfaces Lan et Wan. D'autres paramètres peuvent être modifiés.

Pour la mise en place, nous allons utiliser un serveur MySQL. Le serveur MySQL va nous permettre de sauvegarder les informations qui passent 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 informations mais si on modifie le temps et que l'on redémarre l'information n'est pas sauvegardée. Pour mon cas, j'ai trouvé une solution qui consiste à enlever les droits de « Delete et Update », afin qu'il ne supprime pas les informations au-delà de 7 jours par défaut.

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

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

Cette commande doit être faite 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

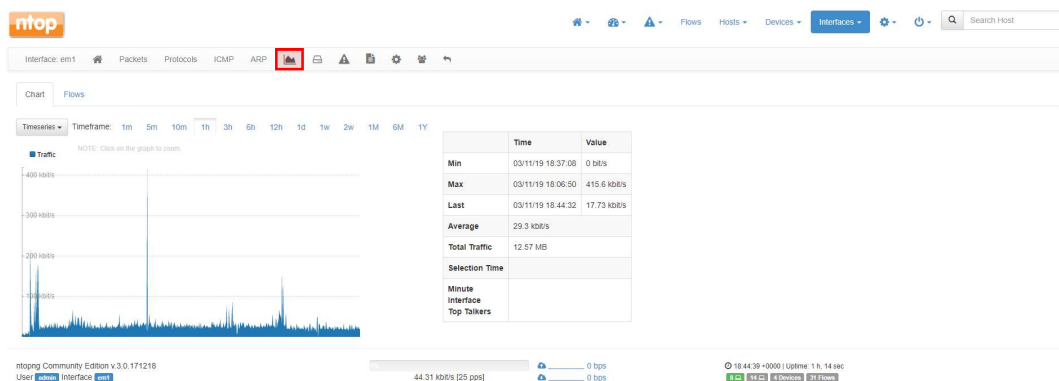
Une fois fait, nous allons pouvoir redémarrer et nous connecter.

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 détail les connexions effectuées, nous utilisons dans « **Flows** », puis « **IPv4** »

Application	L4 Proto	Client	Server	Begin	End	Traffic Sent	Traffic Received	Total Traffic	Info	Avg Thpt
SSH	TCP	172.16.0.200	172.16.0.200:22	11/03/2019 18:05:58	11/03/2019 18:07:41	50.1 KB	272.7 KB	322.8 KB	SSH 2.0-OpenSSH_7.4p1 Debian-10...	25.43 MB/s
MySQL	TCP	172.16.0.200	172.16.0.200:3306	11/03/2019 18:09:03	11/03/2019 18:13:59	193.83 KB	29.39 KB	223.22 KB		6.16 MB/s
SSH	TCP	172.16.0.200	172.16.0.200:22	11/03/2019 18:16:16	11/03/2019 18:22:51	52.34 KB	127.24 KB	179.58 KB	SSH 2.0-OpenSSH_7.2	5.33 MB/s
MySQL	TCP	172.16.0.200	172.16.0.200:3306	11/03/2019 17:45:26	11/03/2019 17:54:21	149.73 KB	23.09 KB	172.82 KB		4.78 MB/s
MySQL	TCP	172.16.0.200	172.16.0.200:3306	11/03/2019 18:04:12	11/03/2019 18:09:08	130.54 KB	20.66 KB	151.2 KB		4.32 MB/s
MySQL	TCP	172.16.0.200	172.16.0.200:3306	11/03/2019 17:54:21	11/03/2019 17:59:17	130.58 KB	20.66 KB	151.24 KB		4.16 MB/s
MySQL	TCP	172.16.0.200	172.16.0.200:3306	11/03/2019 18:13:59	11/03/2019 18:18:54	130.54 KB	19.9 KB	150.44 KB		4.17 MB/s
MySQL	TCP	172.16.0.200	172.16.0.200:3306	11/03/2019 18:04:08	11/03/2019 18:09:03	129.58 KB	19.57 KB	149.14 KB		4.09 MB/s
MySQL	TCP	172.16.0.200	172.16.0.200:3306	11/03/2019 18:25:51	11/03/2019 18:30:48	129.26 KB	19.57 KB	148.83 KB		4.09 MB/s
MySQL	TCP	172.16.0.200	172.16.0.200:3306	11/03/2019 17:54:21	11/03/2019 17:59:17	128.03 KB	20.16 KB	148.19 KB		4.09 MB/s
MySQL	TCP	172.16.0.200	172.16.0.200:3306	11/03/2019 17:59:17	11/03/2019 18:04:08	128.03 KB	19.96 KB	148.00 KB		4.04 MB/s
MySQL	TCP	172.16.0.200	172.16.0.200:3306	11/03/2019 18:20:55	11/03/2019 18:25:51	124.99 KB	18.96 KB	143.95 KB		3.97 MB/s
MySQL	TCP	172.16.0.200	172.16.0.200:3306	11/03/2019 17:45:26	11/03/2019 17:54:21	121.6 KB	18.64 KB	140.24 KB		3.88 MB/s
MySQL	TCP	172.16.0.200	172.16.0.200:3306	11/03/2019 17:59:17	11/03/2019 18:04:12	120.73 KB	18.22 KB	138.95 KB		3.85 MB/s
MySQL	TCP	172.16.0.200	172.16.0.200:3306	11/03/2019 18:18:54	11/03/2019 18:23:51	119.11 KB	18.11 KB	137.22 KB		3.83 MB/s

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

Alternate Hostnames

Alternate Hostnames for DNS Rebinding and HTTP_REFERER Checks. Specify alternate hostnames by which the router may be queried, to bypass the DNS Rebinding Attack checks. Separate hostnames with spaces.

Browser HTTP_REFERER enforcement ☒ **Disable HTTP_REFERER enforcement check**

When this is unchecked, access to the webConfigurator is protected against HTTP_REFERER redirection attempts. Check this box to disable this protection if it interferes with webConfigurator access in certain corner cases such as using external scripts to interact with this system. More information on HTTP_REFERER is available from Wikipedia.

Browser tab text ☐ **Display page name first in browser tab**

When this is unchecked, the browser tab shows the host name followed by the current page. Check this box to display the current page followed by the host name.

Le routeur est maintenant administrable depuis d'autres réseaux LAN (Sans règles 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** »

Username	Full name	Status	Groups	Actions
admin	System Administrator	✓	admins	

On clique sur le petit crayon, pour modifier notre compte

System / User Manager / Users / Edit

Users Groups Settings Authentication Servers

User Properties

Defined by	SYSTEM		
Disabled	☐ This user cannot login		
Username	admin		
Password	*****	*****	
Full name	System Administrator User's full name, for administrative information only		
Expiration date	 Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY		
Custom Settings	☐ Use individual customized GUI options and dashboard layout for this user.		
Group membership	admins Not member of Member of Move to 'Member of' list Move to 'Not member of' list Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.		

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

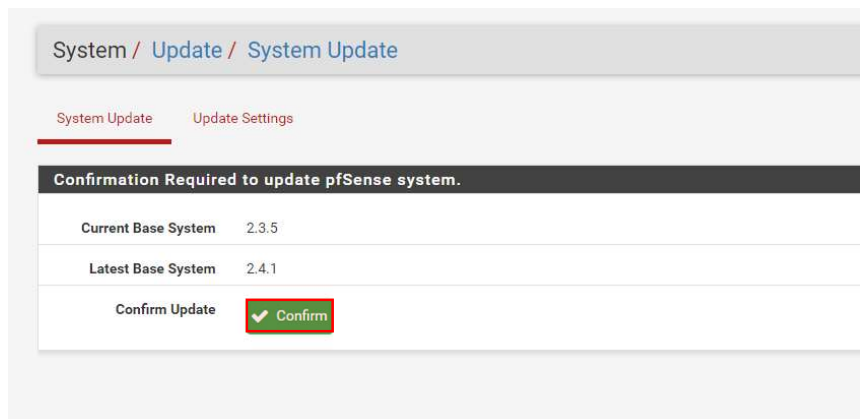
16. Mise à jour PFSENSE(Update Système)

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

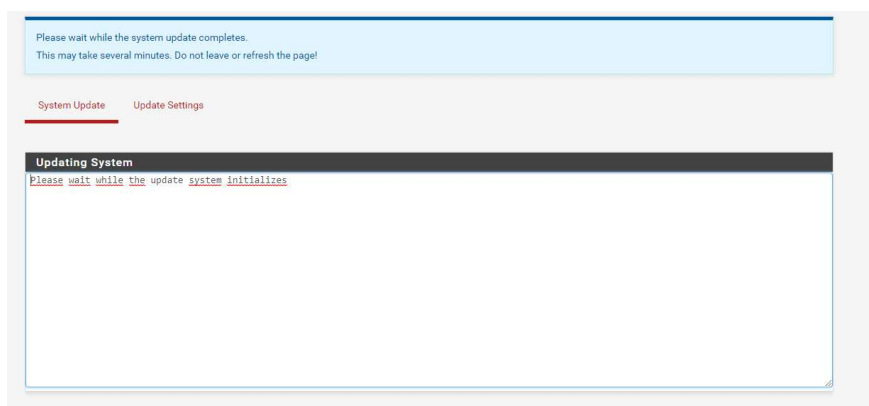
Une mise à jour PFSENSE est facile à faire, pour cela nous devons nous connecter sur le Panel, et sur le Dashboard nous avons la version et comme on peut le voir la version 2.4.1 est disponible, nous pouvons donc la mettre à jour grâce au petit nuage download.

Version	2.3.5-RELEASE (amd64) built on Mon Oct 30 11:08:06 CDT 2017 FreeBSD 10.3-RELEASE-p22
Platform	pfSense
CPU Type	Intel(R) Xeon(R) CPU X3440 @ 2.53GHz
Version 2.3.5-RELEASE Release Date: 12/01/2006 Version 2.4.1 is available.  Version information updated at 2018-02-25 12:39 	

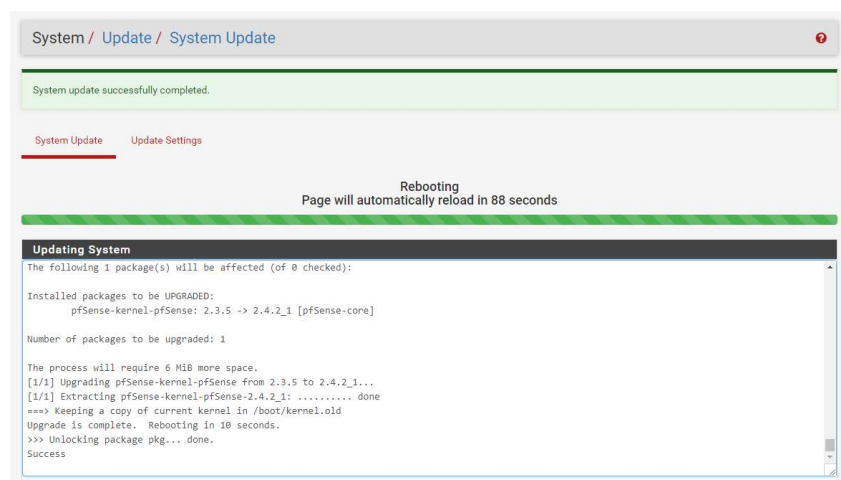
Une demande de confirmation nous a demandé si l'on veut bien mettre à jour notre version, pour cela cliquer sur « Confirm »



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

