



Installation PFSENSE (Redondance, Filtrage, NAT, VPN)



The word "PROXY" in a large, bold, red sans-serif font, with each letter having a 3D perspective effect that makes them appear to be floating or receding.

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 plage de Liste de blockage.....	24
6.	Mise en place d'une journalisation du trafic réseau.....	37

1. Pourquoi mettre en place PFSENSE

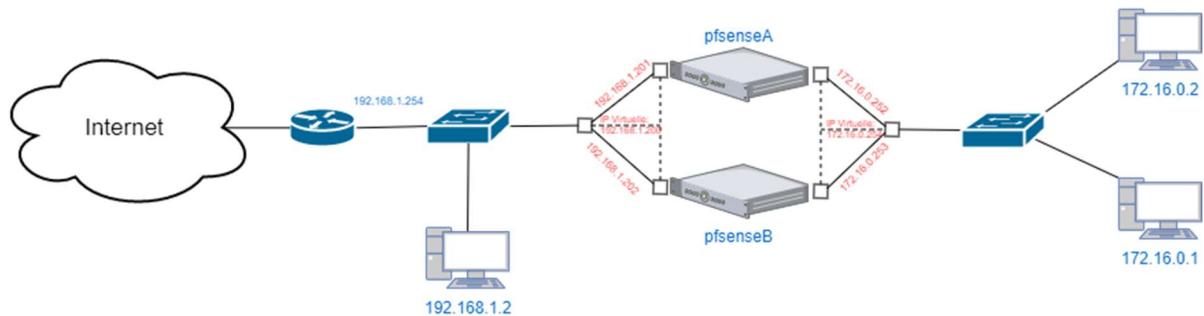
Pfsense est un routeur/pare-feu qui est libre de droit. Il est entièrement configurable par interface web et il a de nombreux services à proposer comme :

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

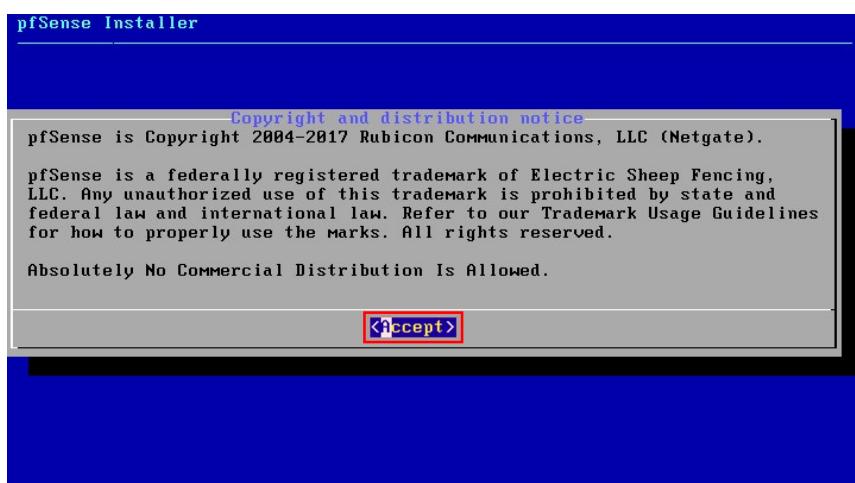
Il y'a aussi la possibilité de faire de la redondance et de la haute disponibilité, et de mettre en place des adresses IP virtuelle.

2. Configuration réseau

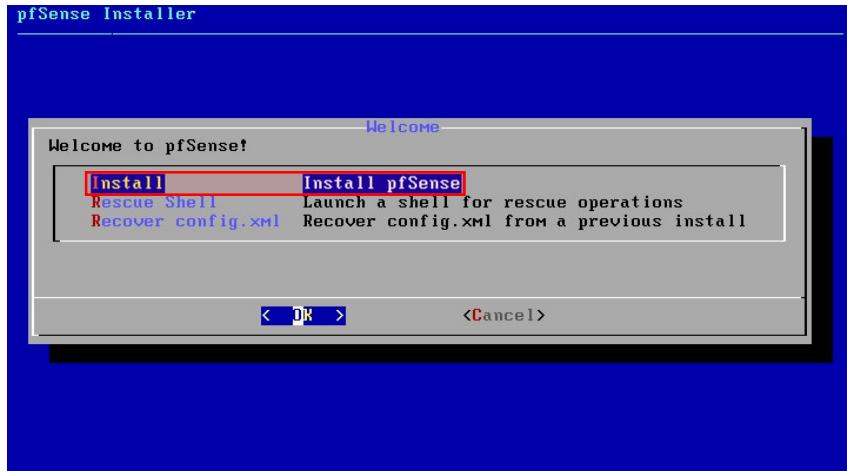
Pour cette installation, nous allons mettre en place 2 serveurs en redondance et avec une haute disponibilité comme sur le schéma suivant :



3. Installation Pfsense

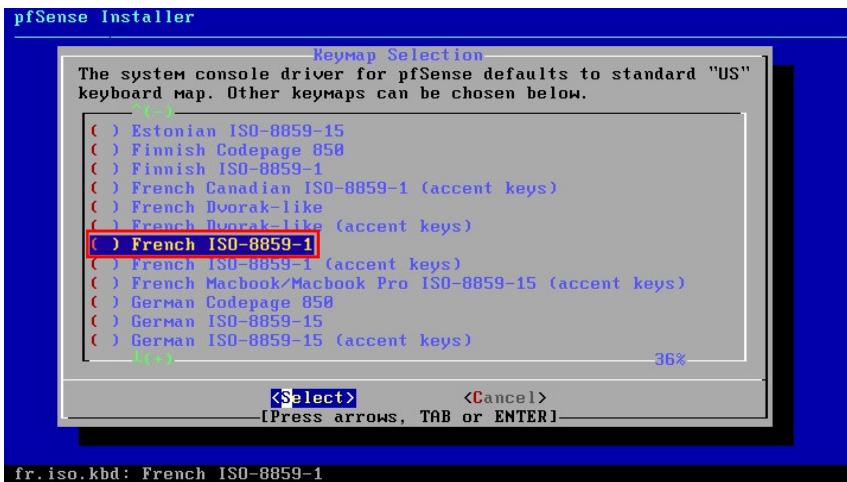


Accepter les termes afin d'installer pfsense

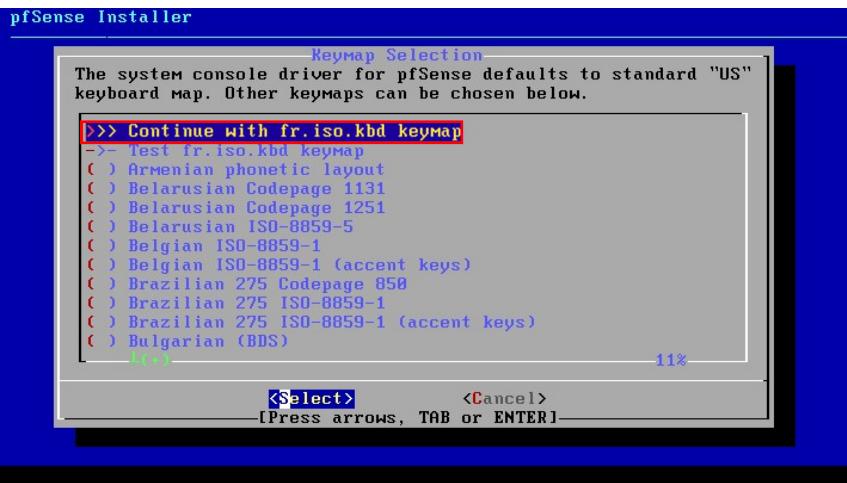


Sélectionner « *Installer pfSense* »

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

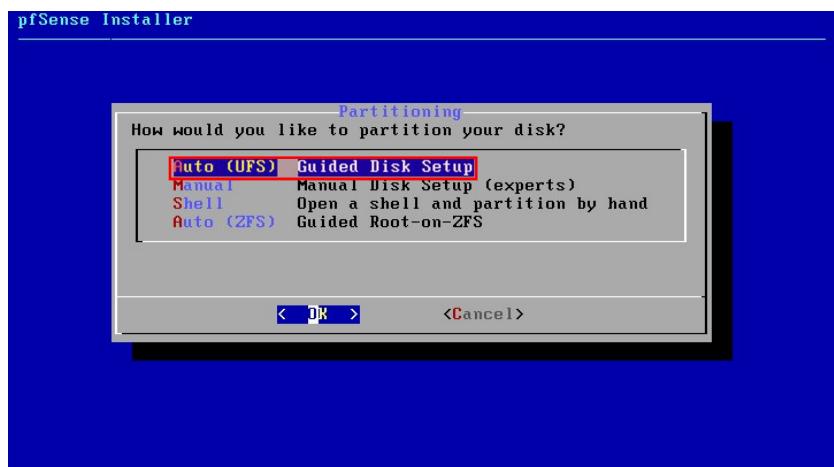


Sélectionner « *French ISO-8859-1* »



On confirme bien notre choix, choisir Continuer

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

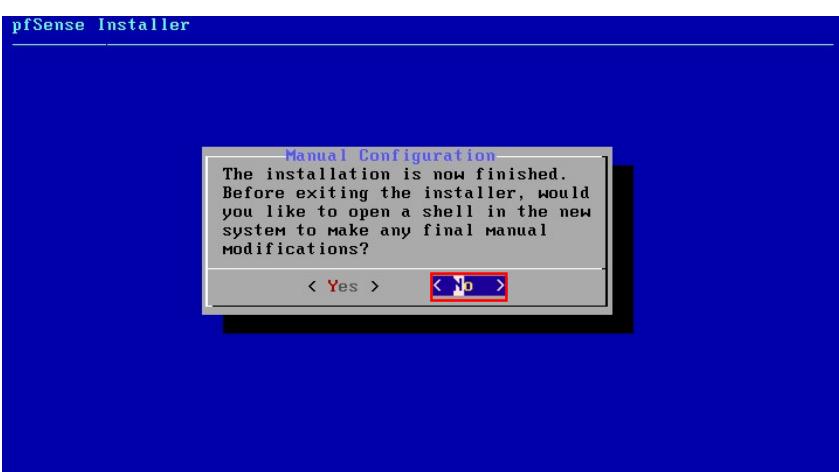


J'ai utilisé le partitionnement automatique, mais cela n'est pas obligé

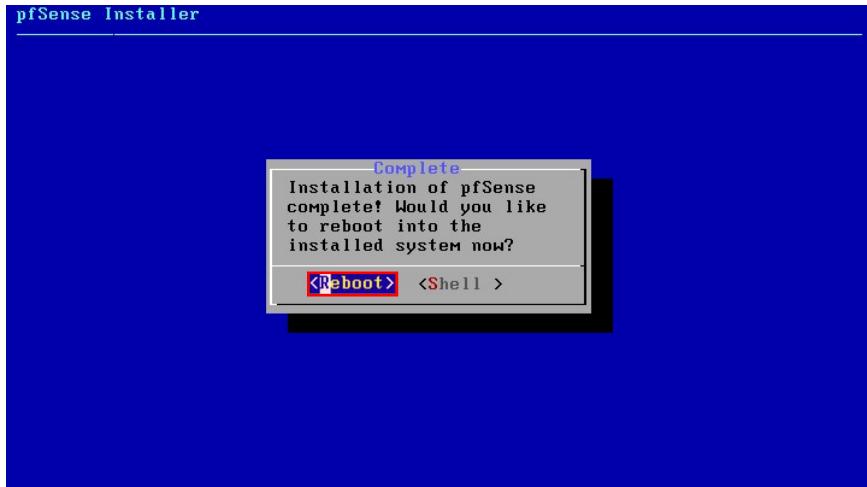


La progression d'installation nous indique son état

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.

```

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[1339]: /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 :

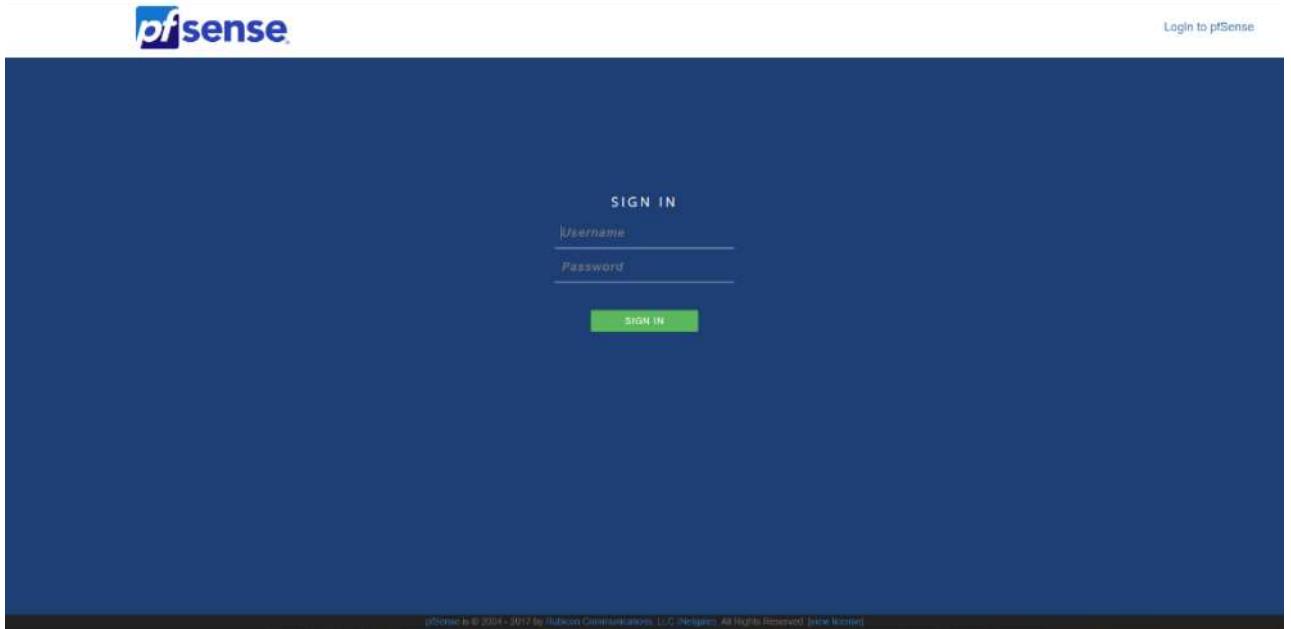
Lan : 192.168.1.202/24, Activation de la configuration web

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 board avec pleins d'informations a propos du routeur/Firewall.

7. Configuration des adresses IP virtuelle (Haut Dispo)

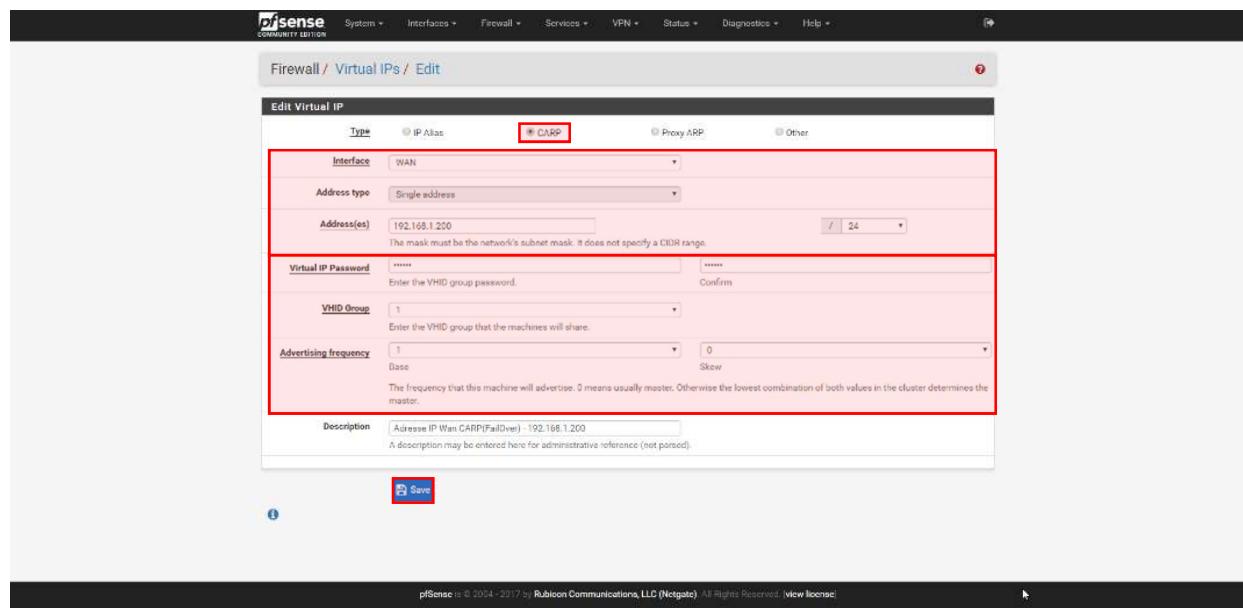
La configuration des adresses IP, permet un basculement entre deux adresses IP. Cela permet de faire une redirection d'adresse IP. Si l'adresse 172.16.0.252 est down, il n'est pas possible de passer instantanément en adresse 172.16.0.253. Alors que si l'on créer une adresse IP en 172.16.0.254, qui permet 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.



The screenshot shows the pfSense web interface under the 'Firewall / Virtual IPs' section. A table titled 'Virtual IP Address' is displayed with the following columns: 'Virtual IP address', 'Interface', 'Type', 'Description', and 'Actions'. There is one row in the table with a status icon. A red '+' button labeled 'Add' is located at the bottom right of the table area. The pfSense logo and navigation menu are visible at the top.

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



The screenshot shows the 'Edit Virtual IP' dialog box. The 'CARP' tab is selected. The 'Interface' dropdown is set to 'WAN'. The 'Address(es)' field contains '192.168.1.200'. The 'Save' button is highlighted with a red box. The pfSense logo and navigation menu are visible at the top.

On créer notre IP virtuel WAN, comme ceci

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

The screenshot shows the 'Edit Virtual IP' configuration for a CARP virtual IP. The 'Interface' is set to 'LAN' and the 'Type' is 'CARP'. The 'Address type' is 'Single address' with the value '172.16.0.254'. The 'Address(es)' field contains '172.16.0.254' with a subnet mask of '24'. The 'Virtual IP Password' and 'VHD Group' fields are filled. The 'Advertising frequency' is set to 'Base'. A note at the bottom states: 'The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.' The 'Save' button is highlighted in red.

On fait de même pour l'interface Lan.

Nous allons pouvoir appliquer les paramètres

The screenshot shows the 'Virtual IP Address' table. It lists two entries: '192.168.1.200/24 (vhd: 1)' on the 'WAN' interface and '172.16.0.254/24 (vhd: 2)' on the 'LAN' interface. Both are of type 'CARP'. The 'Description' column for the WAN entry is 'Adresse IP Wan CARP(PalOver) 192.168.1.200'. The 'Actions' column for the LAN entry has a green 'Edit' icon. A yellow banner at the top right says 'The VR configuration has been changed. The changes must be applied for them to take effect.' with a 'Apply Changes' button.

On à un récapitulatif de nos IP virtuelle. Il faut appliquer les paramètres 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' screen. It displays the 'CARP Interfaces' table with two entries: 'WAN[1]' and 'LAN[2]'. Both interfaces have a 'Virtual IP' of '192.168.1.200/24' and are in 'MASTER' status. The 'pSync Nodes' section below shows '401b1a2d' and '401b1a2e'. A note at the bottom states: 'pfSense is © 2004 - 2017 by Rubicon Communications, LLC (Netgate). All Rights Reserved. View license.'

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

The screenshot shows the pfSense web interface under the 'Status / CARP' tab. It displays two CARP interfaces: WAN#1 and LAN#0. Both interfaces have a virtual IP of 192.168.1.200/24 and are in a 'BACKUP' status, indicated by yellow icons. Below the interfaces, there is a section for 'pfSync Nodes' which lists two nodes: 03663814 and 09529429.

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 règles de filtrage, NAT, VPN, etc.... Ce permet de devoir effectuer la création d'une règle ou autre, uniquement d'un seul coté. La réPLICATION s'effectue automatiquement.

The screenshot shows the pfSense web interface under the 'System / High Availability Sync' tab. It displays the 'State Synchronization Settings (ofwsync)' and 'Configuration Synchronization Settings (XMLRPC Sync)'. In the 'State Synchronization Settings (ofwsync)', the 'Synchronize Interface' is set to 'LAN'. In the 'Configuration Synchronization Settings (XMLRPC Sync)', the 'Synchronize Config to IP' is set to '172.16.0.253'. Both sections are highlighted with a red border.

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.

The screenshot shows the pfSense Firewall configuration under the Rules section for the WAN interface. There are two rules listed:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
X 0/384 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
X 0/0 B	*	Reserved	*	*	*	*	*		Block bogon networks	

A message below the table states: "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." At the bottom are buttons for Add, Delete, Save, and 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 côté de nos deux règles de refus.

The screenshot shows the pfSense Interfaces configuration for the WAN interface. It includes sections for Speed and Duplex (set to Default) and Static IPv4 Configuration (IP 192.168.1.253, Subnet mask 24). Below these, the Reserved Networks section is highlighted with a red border, containing two options:

- Block private networks and loopback addresses**: A checked checkbox with a note explaining it blocks traffic from RFC 1918 and loopback addresses.
- Block bogon networks**: A checked checkbox with a note explaining it blocks reserved IP addresses not assigned by IANA.

At the bottom is a Save button.

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

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

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.

Aucune ne doit être cocher

Une fois enlever, nous devons appliquer les modifications

The WAN configuration has been changed.
The changes must be applied to take effect.
Don't forget to adjust the DHCP Server range if needed after applying.

Apply Changes

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.

Floating WAN LAN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
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

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

Il y'a plusieurs actions qui peuvent être appliquer sur la 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 la quelle la regle sera actif

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

Et pour finir on paramettrre 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 blocage, mais le principe est le même pour toutes les règles.

The screenshot shows the pfSense Firewall Rules Edit interface. A new rule is being created with the following settings:

- Action:** Block
- Disabled:** Disable this rule
- Interface:** WAN
- Address Family:** IPv4
- Protocol:** Any

Source: Invert match. any / Source Address

Destination: Invert match. any / Destination Address

Extra Options:

- Log:** Log packets that are handled by this rule
- Description:** Bloque tout le trafic
- Advanced Options:** Display Advanced

A blue "Save" button is located at the bottom left.

Cliquez 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 grâce 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 créée normalement et ne doit pas être supprimer.

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

Une fois notre règle créer, nous devons l'appliquer

The screenshot shows the pfSense Firewall / Rules / WAN interface. A message at the top states: "The firewall rule configuration has been changed. The changes must be applied for them to take effect." A red box highlights the "Apply Changes" button. Below the message, there are tabs for Floating, WAN, and LAN, with WAN selected. A table titled "Rules (Drag to Change Order)" lists one rule: "Bloque tout le trafic". The rule details are: State: 0 / 0 B, Protocol: IPv4, Source: *, Port: *, Destination: *, Port: *, Gateway: *, Queue: none, Schedule: none, Description: Bloque tout le trafic. Action buttons include Add, Add, Delete, Save, and Separator.

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.

The screenshot shows the pfSense Firewall / Rules / Edit interface for creating a new rule. The "Edit Firewall Rule" section includes fields for Action (Pass), Disabled (unchecked), Interface (WAN), Address Family (IPv4), and Protocol (TCP/UDP). The "Source" section shows a source of "any" and a note about the source port range being typically random. The "Destination" section shows a destination of "OpenVPN (119-)" and a note about specifying destination ports. The "Extra Options" section includes Log (unchecked) and a Description field containing "Autorisation protocole VPN". A "Save" button is at the bottom.

Exemple de règle de filtrage autorisant 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 à leurs ordres et importants. Si la règle de blocage est en première, aucune des règles après sera fonctionnelle.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> ✓	0 / 0 B	IPv4 TCP/UDP	*	*	*	1194 (OpenVPN)	*	none	Autorisation protocole VPN	
<input type="checkbox"/> ✗	0 / 0 B	IPv4 B	*	*	*	*	*	none	Bloque tout le trafic	

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

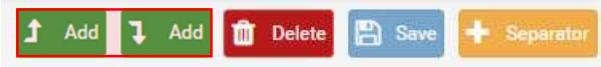
Pour cela, nous devons aller dans « Firewall / Nat »

Voilà un exemple de règles qui sont traduites

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

Exemple de règles qui peuvent être créées

Pour créer une règle NAT, cliquer sur "ADD"



Pour cela, nous devons cliquer sur « ADD »

Firewall / NAT / Port Forward / Edit

Edit Redirect Entry

Disabled	<input type="checkbox"/> Disable this rule			
No RDR (NOT)	<input type="checkbox"/> Disable redirection for traffic matching this rule This option is rarely needed. Don't use this without thorough knowledge of the implications.			
Interface	WAN			
Protocol	Notre protocole			
Source	<input type="checkbox"/> Display Advanced			
Destination	<input type="checkbox"/> Invert match.	WAN address	Type	Address/mask
Destination port range	Other	Port Externe	Other	Saisir port si ranger
Redirect target IP	IP machine en interne	Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12		
Redirect target port	Other	Port	From port	To port
Description	Description afin de la repérer facilement			
No XMLRPC Sync	<input type="checkbox"/> 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	Use system default			
Filter rule association	Add associated filter rule			

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 crées 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										
<input checked="" type="checkbox"/>	✓ 18 /17.41 MiB	IPv4 TCP	*	*	172.16.0.101	80 (HTTP)	*	none	NAT Serveur Web - Hopper	
<input checked="" type="checkbox"/>	✓ 1 /339 KiB	IPv4 TCP	*	*	172.16.0.101	22 (SSH)	*	none	NAT Serveur Web - Hopper	
<input checked="" type="checkbox"/>	✓ 2 /164 KiB	IPv4 TCP	*	*	172.16.0.101	21 (FTP)	*	none	NAT Serveur FTP - Hopper	
<input checked="" type="checkbox"/>	✓ 0 /1.47 MiB	IPv4 TCP	*	*	172.16.0.101	49152 - 50000	*	none	NAT Serveur FTP Port Passif - Hopper	
<input checked="" type="checkbox"/>	✓ 12 /19.58 MiB	IPv4 TCP/UDP	*	*	172.16.0.101	8000	*	none	NAT Serveur Ajenti - Hopper	
Machine Physique - 172.16.0.102										
<input checked="" type="checkbox"/>	✓ 0 /75.99 MiB	IPv4 TCP	*	*	172.16.0.102	80 (HTTP)	*	none	NAT Serveur Web - Physique	
<input checked="" type="checkbox"/>	✓ 0 /25 KiB	IPv4 TCP/UDP	*	*	172.16.0.102	3389 (MS RDP)	*	none	NAT RDP - Physique	
<input checked="" type="checkbox"/>	✓ 0 /19 KiB	IPv4 TCP/UDP	*	*	172.16.0.102	33891	*	none	NAT RDP - Hopper	
<input checked="" type="checkbox"/>	✓ 0 /14 KiB	IPv4 TCP/UDP	*	*	172.16.0.102	33892	*	none	NAT RDP - Intratec	
<input checked="" type="checkbox"/>	✓ 0 /14 KiB	IPv4 TCP/UDP	*	*	172.16.0.102	33893	*	none	NAT RDP - Centreon	
<input checked="" type="checkbox"/>	✓ 0 /2 KiB	IPv4 TCP/UDP	*	*	172.16.0.102	33894	*	none	NAT RDP - PFSense	
Machine Intratec - 172.16.0.103										
<input checked="" type="checkbox"/>	✓ 0 /816 B	IPv4 TCP	*	*	172.16.0.103	1138	*	none	NAT Serveur Web - Intratec	
<input checked="" type="checkbox"/>	✓ 0 /0 B	IPv4 TCP	*	*	172.16.0.103	22 (SSH)	*	none	NAT Serveur SSH - Intratec	
<input checked="" type="checkbox"/>	✓ 0 /816 B	IPv4 TCP	*	*	172.16.0.103	8000	*	none	NAT Serveur Ajenti - Intratec	
Machine Centreon - 172.16.0.104										
<input checked="" type="checkbox"/>	✓ 0 /0 B	IPv4 TCP	*	*	172.16.0.104	22 (SSH)	*	none	NAT Serveur SSH - Centreon	
<input checked="" type="checkbox"/>	✓ 0 /5.47 MiB	IPv4 TCP	*	*	172.16.0.104	80 (HTTP)	*	none	NAT Serveur Web - Centreon	
Machine PFSense - 172.16.0.254										
<input checked="" type="checkbox"/>	✓ 7 /3.67 MiB	IPv4 TCP	*	*	172.16.0.254	80 (HTTP)	*	none	NAT Serveur Web - PFSense	
<input checked="" type="checkbox"/>	✓ 0 /0 B	IPv4 TCP	*	*	172.16.0.254	22 (SSH)	*	none	NAT Serveur SSH - PFSense	
<input checked="" type="checkbox"/>	✗ 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

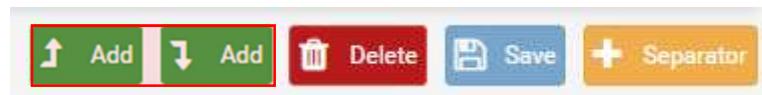
Block private networks and loopback addresses
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless 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: Source: Invert match. any Source Address /

Destination: 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 abandonneronner

11. Mise en plage 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 adules, etc...).

Pour cela, nous pouvons la créer ou bien en utiliser une déjà prete créée 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 gestionnaire, 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 à nos sites web.

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term: squid Both Search Clear

Enter a search string or *nix regular expression to search package names and descriptions.

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.	+ 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.	+ Install
squidGuard	1.16.4	High performance web proxy URL filter.	+ Install

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

172.16.53.252/pkg_mngr_install.php?pkg=pfSense-pkg-squidGuard

Chaque paquet doit être installé séparément

Pour chaque installation une demande de confirmation d'installation nous a demandé

System / Package Manager / Package Installer

Installed Packages Available Packages Package Installer

Confirmation Required to install package pfSense-pkg-squidGuard.

Confirm

Nous devons confirmer, afin qu'il soit installé

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

The screenshot shows the pfSense Package Manager interface. At the top, there's a navigation bar with links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation bar, the title "System / Package Manager / Package Installer" is displayed. A message box in the center says: "Please wait while the installation of **pfSense-pkg-squidGuard** completes. This may take several minutes. Do not leave or refresh the page!" Below the message box, there are three tabs: "Installed Packages", "Available Packages", and "Package Installer". The "Package Installer" tab is selected and highlighted with a red border. In the main content area, under the heading "Package Installation", there is a terminal-like window showing the command output: >>> Installing pfSense-pkg-squidGuard... Updating pfSense-core repository catalogue... pfSense-core repository is up to date. Updating pfSense repository catalogue... pfSense repository is up to date. All repositories are up to date.

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

The screenshot shows the pfSense Services / SquidGuard Proxy Filter configuration page. At the top, there's a header "Blacklist options". Below it, there's a section for "Blacklist" with a checked checkbox labeled "Check this option to enable blacklist" and a note "Do NOT enable this on NanoBSD installs!". There's also a "Blacklist proxy" input field with a help text: "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'". Below that, there's a "Blacklist URL" input field containing "p://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz" and a note: "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 seul blackliste existante, mais elle comprend beaucoup de site.

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

The screenshot shows the "Blacklist Update" page. At the top, there is a navigation bar with tabs: General settings, Common ACL, Groups ACL, Target categories, Times, Rewrites, Blacklist (which is highlighted in red), Log, and XMLRPC Sync. Below the navigation bar, there is a progress bar showing "0 %". A text input field contains the URL "http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfSense.tar.gz". Below the input field are three buttons: "Download" (red), "Cancel" (orange), and "Restore Default" (blue). A note below the input field says "Enter FTP or HTTP path to the blacklist archive here." At the bottom of the page is a "Blacklist update Log" section with a title "Blacklist update Log". The log content is as follows:

```
Begin blacklist update
Start download.
Download archive http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfSense.tar.gz
Download complete
Unpack archive
Scan blacklist categories.
Found 58 items.
Start rebuild DB.
Copy DB to workdir.
Reconfigure Squid proxy.
Blacklist update complete.
```

*Pour mettre à jour ou installer notre liste de blocage, 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

The screenshot shows the "Package / SquidGuard / Blacklists" page. At the top, there is a navigation bar with tabs: General settings, Common ACL, Groups ACL, Target categories, Times, Rewrites, Blacklist (which is highlighted in red), Log, and XMLRPC Sync. Below the navigation bar, there is a progress bar showing "1 %". A text input field contains the URL "http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfSense.tar.gz". Below the input field are three buttons: "Download" (red), "Cancel" (orange), and "Restore Default" (blue). A note below the input field says "Enter FTP or HTTP path to the blacklist archive here." At the bottom of the page is a "Blacklist update Log" section with a title "Blacklist update Log". The log content is as follows:

```
Begin blacklist update
Start download.
Download archive http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfSense.tar.gz
Download complete
Unpack archive
Scan blacklist categories.
Found 58 items.
Start rebuild DB.
Completed 1 $
```

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

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

The screenshot shows the "General settings" tab selected in the top navigation bar. Under the "General Options" section, there is a checkbox labeled "Enable" with the text "Check this option to enable squidGuard." Below it is an "Important" note: "Please set up at least one category on the 'Target Categories' tab before enabling. See this link for details." A red box highlights the "Apply" button. At the bottom, a message says "SquidGuard service state: STOPPED".

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

On vérifie que notre paquet squidGuard soit bien actif

The screenshot shows the "General settings" tab selected in the top navigation bar. Under the "General Options" section, there is a checkbox labeled "Enable" with the text "Check this option to enable squidGuard." Below it is an "Important" note: "Please set up at least one category on the 'Target Categories' tab before enabling. See this link for details." A red box highlights the "Apply" button. At the bottom, a message says "SquidGuard service state: STARTED".

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 évite d'avoir un serveur dédié à cette tâche.

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

The screenshot shows the "System / Certificate Manager / CAs" page. The "CAs" tab is selected in the top navigation bar. The main area displays a table of "Certificate Authorities" with columns: Name, Internal, Issuer, Certificates, Distinguished Name, In Use, and Actions. A red box highlights the "Add" button in the bottom right corner.

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

Nous allons créer notre autorité de certification.

CAs 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

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

CAs 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

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

Alternative Names FQDN or Hostname

Type Value

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.

The screenshot shows the pfSense User Manager interface. At the top, there's a navigation bar with links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below that is a breadcrumb trail: System / User Manager / Users. Under the title 'Users', there's a table with columns: Username, Full name, Status, Groups, and Actions. A single row is listed for 'admin' with 'System Administrator' as the full name and 'admins' in the Groups column. At the bottom right of the table are three buttons: '+ Add' (highlighted with a red box), 'Edit', and 'Delete'.

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

La création de notre utilisateur se fait comme ceci

This screenshot shows the 'Edit' screen for a user. The title bar says 'System / User Manager / Users / Edit'. The main area is titled 'User Properties'. It includes fields for 'Defined by' (set to 'USER'), 'Disabled' (unchecked), 'Username' ('client-openvpn'), 'Password' (redacted), 'Full name' ('Client VPN'), 'Expiration date' (empty), 'Custom Settings' (unchecked), 'Group membership' ('admins'), and 'Certificate' (unchecked). There are also buttons for moving items between 'Member of' and 'Not member of' lists.

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

This screenshot shows the 'Add/Sign a New Certificate' screen. The title bar has tabs for 'CA's', 'Certificates' (selected), and 'Certificate Revocation'. The 'Certificates' tab has a sub-tab 'Internal Certificate'. The form fields include: 'Method' (set to 'Create an internal Certificate'), 'Descriptive name' ('Client VPN'), 'Internal Certificate' section with 'Certificate authority' ('pfSense FireWall'), 'Key length' ('2048'), 'Digest Algorithm' ('sha256'), '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'), and '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 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 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

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

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Certificate Manager / Certificates / Edit

CA 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.

The screenshot shows the pfSense Package Manager interface. The search term 'openvpn' has been entered into the search bar. The results table shows one package: 'openvpn-client-export' version 1.4.14. The 'Install' button for this package is highlighted with a mouse cursor.

On cliquer sur installer afin d'ajouter le paquet

Nous allons installer le serveur VPN et le configurer

The screenshot shows the 'OpenVPN Remote Access Server Setup' wizard. The current step is 'Select an Authentication Backend Type'. The 'Type of Server' dropdown is set to 'Local User Access'. The 'Next' button is highlighted with a mouse cursor.

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

The screenshot shows the 'OpenVPN Remote Access Server Setup' wizard. The current step is 'Certificate Authority Selection'. The 'Choose a Certificate Authority (CA)' dropdown is set to 'pfSense FireWall'. The 'Next' button is highlighted with a mouse cursor.

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 à créer 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.

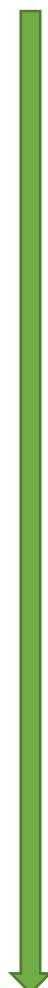
TLS Shared Key:
Paste in a shared TLS key if one has already been generated.

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	<input type="text" value="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	<input checked="" type="checkbox"/>	Force all client generated traffic through the tunnel.
Local Network	<input type="text" value="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	<input type="text"/>	Specify the maximum number of clients allowed to concurrently connect to this server.
Compression	<input type="text" value="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	<input type="checkbox"/>	Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
Inter-Client Communication	<input checked="" type="checkbox"/>	Allow communication between clients connected to this server.
Duplicate Connections	<input type="checkbox"/>	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	<input checked="" type="checkbox"/>	Allow connected clients to retain their connections if their IP address changes.
Topology	<input type="text" value="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	<input type="text"/>	Provide a default domain name to clients.
DNS Server 1	<input type="text" value="172.16.53.1"/>	DNS server IP to provide to connecting clients.
DNS Server 2	<input type="text"/>	DNS server IP to provide to connecting clients.
DNS Server 3	<input type="text"/>	DNS server IP to provide to connecting clients.
DNS Server 4	<input type="text"/>	DNS server IP to provide to connecting clients.
NTP Server	<input type="text"/>	Network Time Protocol server to provide to connecting clients.
NTP Server 2	<input type="text"/>	Network Time Protocol server to provide to connecting clients.
NetBIOS Options	<input type="checkbox"/>	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	<input type="text" value="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	<input type="text"/>	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	<input type="text"/>	A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.
WINS Server 2	<input type="text"/>	A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.
Advanced	<input type="text"/> 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



The screenshot shows the PFSense OpenVPN Remote Access Server Setup Wizard at Step 10 of 11. The title bar reads "Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration". A red question mark icon is in the top right corner. Below the title, a progress bar shows "Step 10 of 11". The main content area has a dark header "Firewall Rule Configuration". Underneath it, a sub-header says "OpenVPN Remote Access Server Setup Wizard". Another dark header "Firewall Rule Configuration" is followed by a descriptive text: "Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard." Below this, there are two sections: "Traffic from clients to server" and "Traffic from clients through VPN". Each section contains a checkbox labeled "Firewall Rule" or "OpenVPN rule" with a checked box. To the right of each checkbox is a text input field. At the bottom of the page is a blue "Next" button.

On peut laisser par défaut et faire "Next"

The screenshot shows the PFSense OpenVPN Remote Access Server Setup Wizard at Step 11 of 11. The title bar reads "Wizard / OpenVPN Remote Access Server Setup / Finished!". A red question mark icon is in the top right corner. Below the title, a green progress bar shows "Step 11 of 11". The main content area has a dark header "Finished!". Underneath it, a sub-header says "OpenVPN Remote Access Server Setup Wizard". Another dark header "Configuration Complete!" is followed by a message: "The configuration is now complete." Below this, another message says: "To be able to export client configurations, browse to System->Packages and install the OpenVPN Client Export package." At the bottom of the page is a blue "Finish" button.

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 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

Optional 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:

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	<ul style="list-style-type: none"> - Inline Configurations: <ul style="list-style-type: none"> Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: <ul style="list-style-type: none"> Archive Config File Only - Current Windows Installer (2.4.4-1x01): <ul style="list-style-type: none"> Windows Vista and Later - Old Windows Installers (2.3.18-1x01): <ul style="list-style-type: none"> x86-xp x64-xp x86-win6 x64-win6 - Viscosity (Mac OS X and Windows): <ul style="list-style-type: none"> 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](#)

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

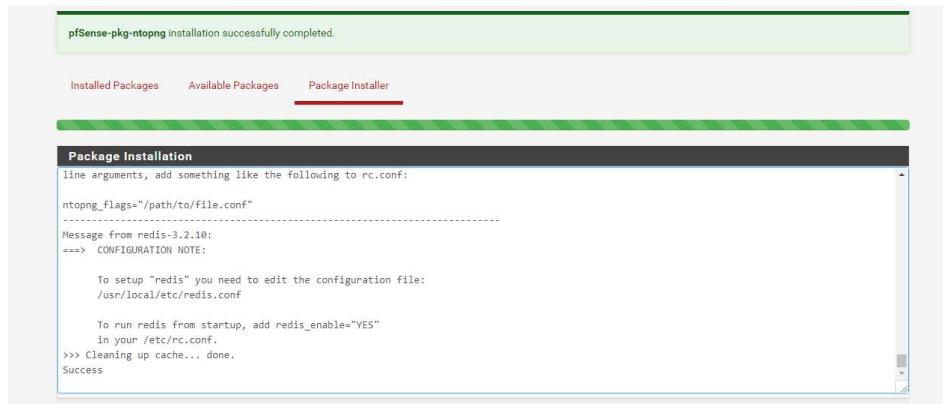
13. Mise en place d'une journalisation du trafic réseau

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 pfSense Package Manager interface. 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 a placeholder "Search term" and a "Search" button. A note below the search bar says "Enter a search string or *nix regular expression to search package names and descriptions." The main area is titled "Packages" and contains a table with columns "Name", "Version", and "Description".

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



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

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

The screenshot shows the pfSense Diagnostics / ntopng Settings page. The "ntopng Settings" tab is selected. The "General Options" section is highlighted with a red box and contains the following fields:

- Enable ntopng:** Check this to enable ntopng.
- Keep Data/Settings:** Keep ntopng settings, graphs and traffic data. Note: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade!
- ntopng Admin Password:** (password field)
- Confirm ntopng Admin Password:** (password field)
- Interface:** LAN, WAN (dropdown menu)
- DNS Mode:** Decode DNS responses and resolve local numeric IPs only (default) (dropdown menu)

*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 cela fait, nous pouvons tester si on a bien accès à la base de données depuis Pfsense avec la 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
```

Contenu du fichier « /etc/mysql/my.cnf »

- Vérifier les permission de l'utilisateurs
- Vérifier 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} &
```

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

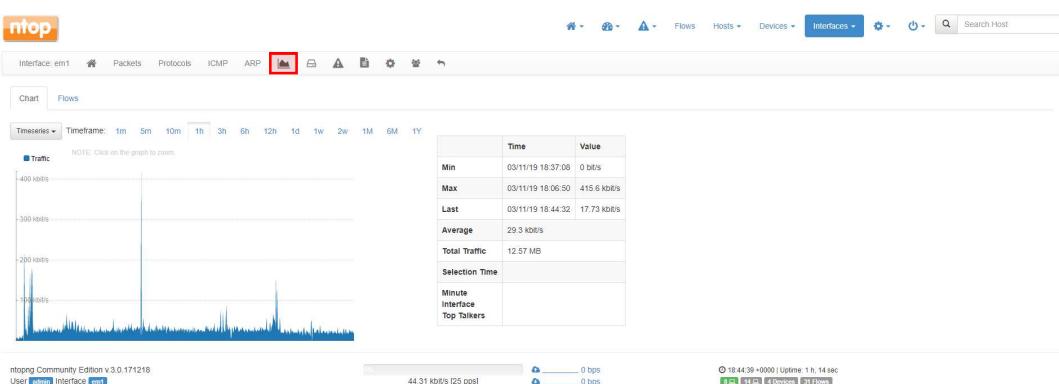
Une fois fait, nous allons pouvoir redémarrer et nous connecter.

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

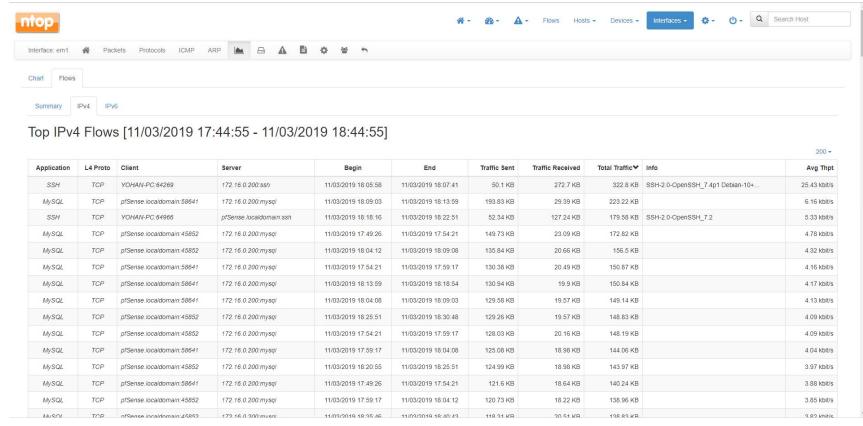
Puis, nous allons choisir l'interface que l'on veut voir ou espionner



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



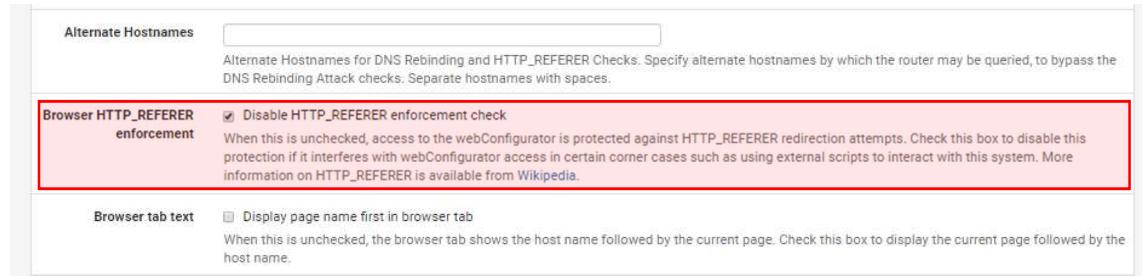
Et pour voir en détaille les connexions effectuer, nous utilisons dans « **Flows** », puis « **IPv4** »



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 règle http. Nous devons aller dans « **System / Advanced**», puis cocher cette case.



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** »

Users					
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	<input type="checkbox"/> This user cannot login						
Username	admin						
Password						
Full name	System Administrator User's full name, for administrative information only						
Expiration date							
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.						
Group membership	<table border="1"> <tr> <td>Not member of</td> <td>admins</td> </tr> <tr> <td>>> Move to "Member of" list</td> <td><< Move to "Not member of" list</td> </tr> <tr> <td colspan="2">Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.</td> </tr> </table>	Not member of	admins	>> Move to "Member of" list	<< Move to "Not member of" list	Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.	
Not member of	admins						
>> 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.

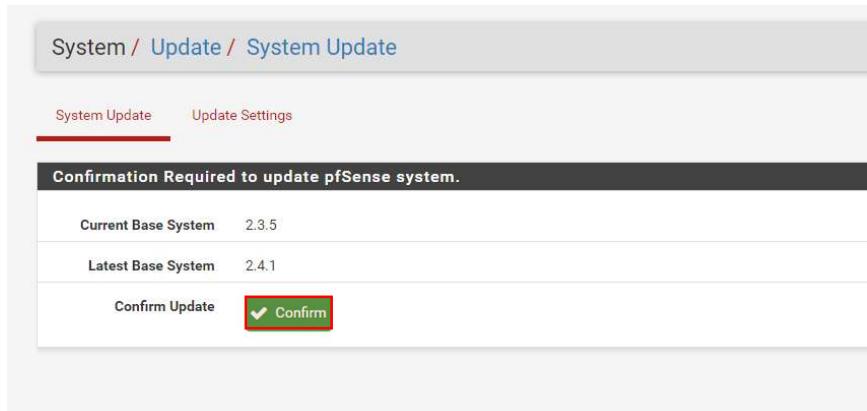
16. Mise à jour PFSENSE(Update Système)

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

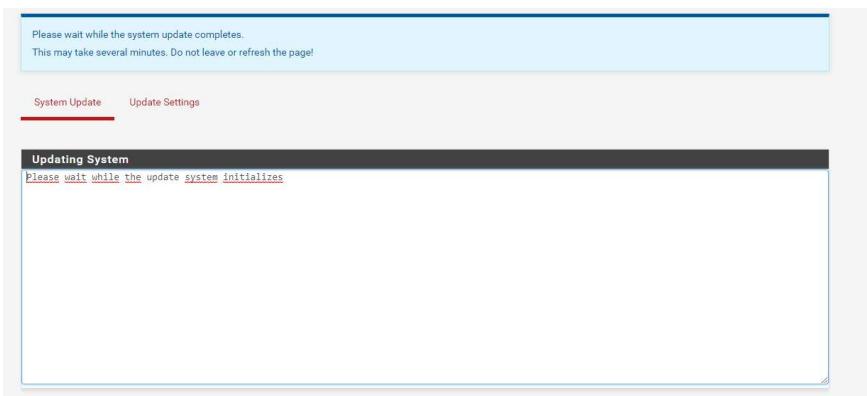
Une mise à jour PFSENSE est facile à faire, pour cela nous devons nous connecter sur le Panel, et sur le Dashboard nous avons la version et comme on peut le voir la version 2.4.1 est disponible, nous pouvons donc la mettre à jour grâce au petit nuage download.

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

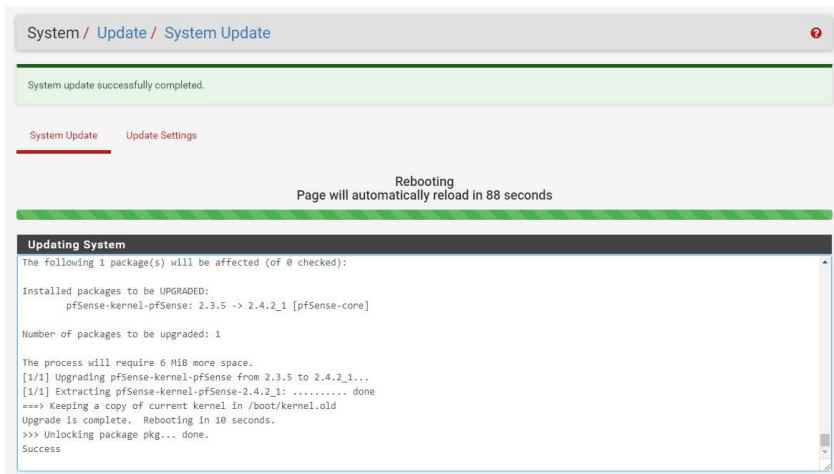
Une demande de confirmation nous a demandé si l'on veut bien mettre à jour notre version, pour cela cliquer sur « **Confirm** »



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

