

1. Pourquoi mettre en place PFSENSE

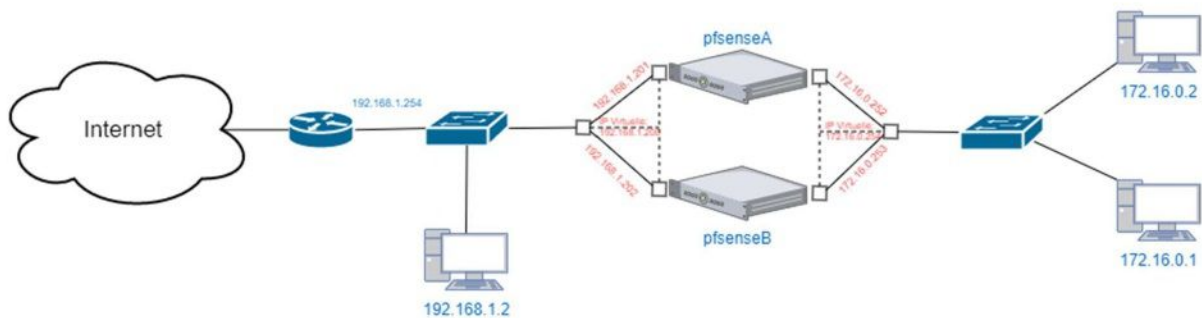
Pfsense est un routeur/pare-feu qui est libre de droit. Il est entièrement configurable par interface web et il a de nombreux service supporter comme :

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

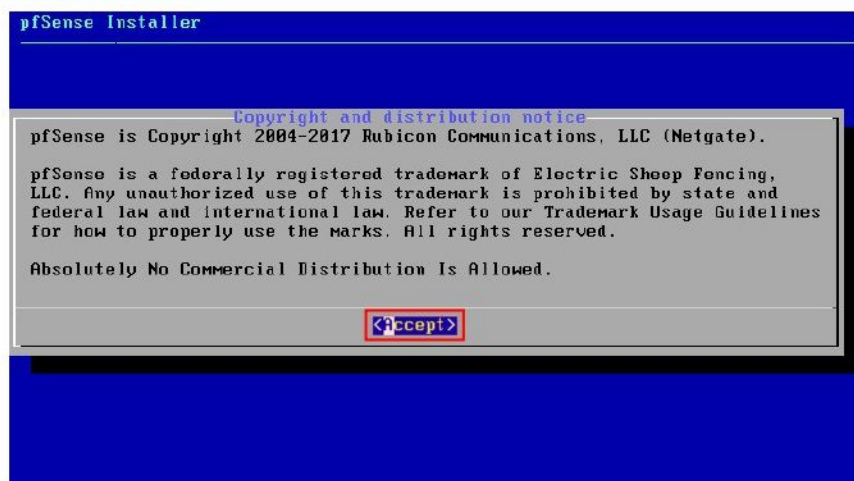
Il y'a aussi la possibilité de faire de la redondance et de la haute disponibilité, et de mettre en place des adresses IP virtuelle.

2. Configuration réseau

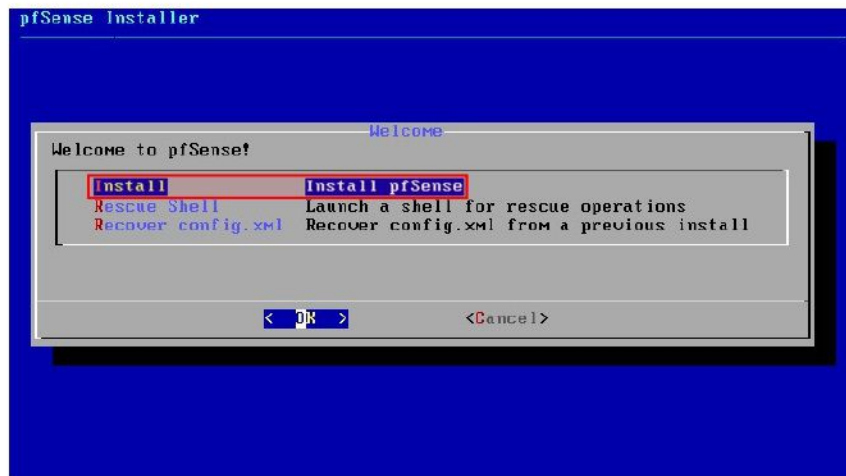
Pour cette installation, nous allons mettre en place 2 serveurs en redondance et avec une haute disponibilité comme sur le schéma suivant :



3. Installation Pfsense

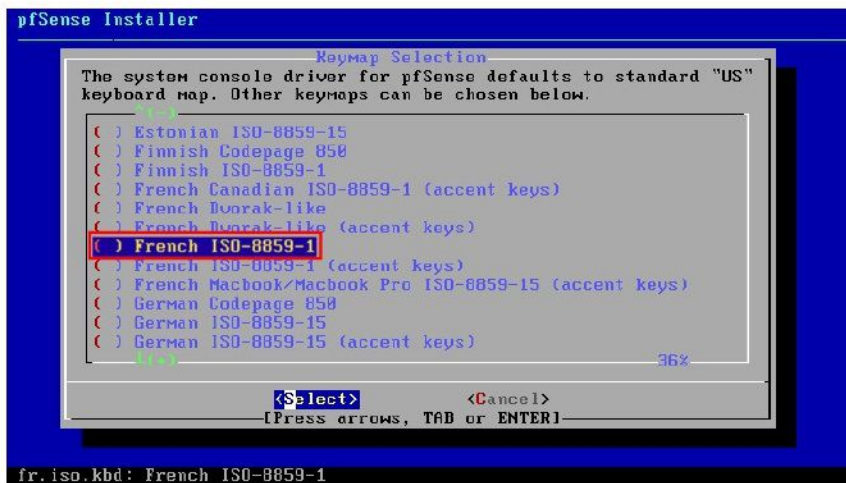


Accepter les termes afin d'installer pfsense

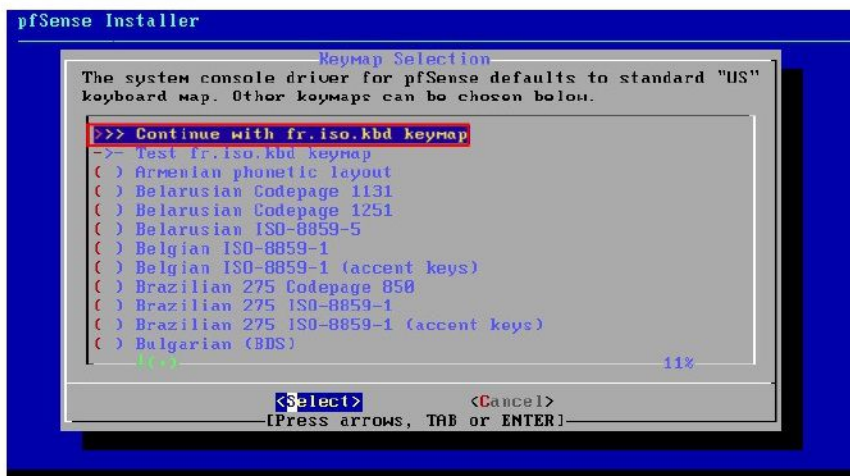


Sélectionner « Installer pfsense »

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

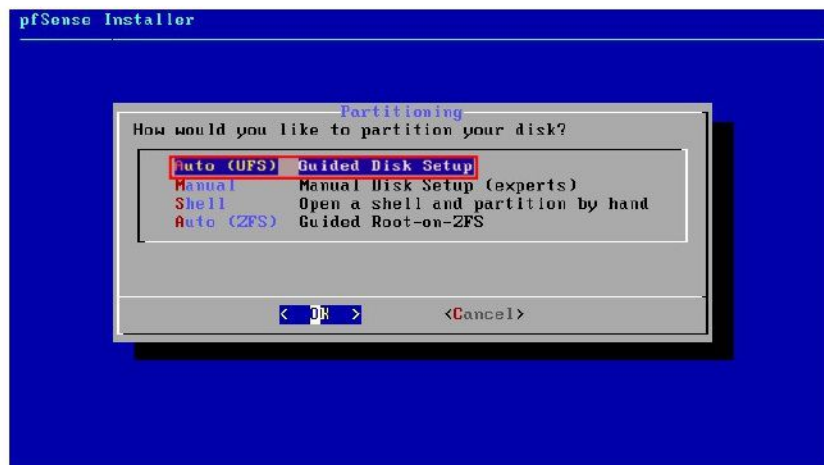


Sélectionner « French ISO-8859-1 »



On confirme bien notre choix, choisir Continuer

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



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



La progression d'installation nous indique son état

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



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



Confirmation du choix "Reboot", pour redémarrer

4. Configuration du serveur PFSENSE A

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

```
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[339]: /index.php: Successful login for user 'admin' from: 172.16
.0.1

VMware Virtual Machine - Netgate Device ID: 20bee1522d68a1935aeb

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

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

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 2

```

On fait de même avec l'interface « Wan »

```

VMware Virtual Machine - Netgate Device ID: 20bee1522d68a1935aeb

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

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

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

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

Enter the number of the interface you wish to configure: 1

```

On sélectionne donc l'interface « 1 »

```

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

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

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

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

Enter the number of the interface you wish to configure: 1

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

```

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


```

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

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

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

Enter the number of the interface you wish to configure: 1

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

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

```

On indique donc l'adresse IP de l'interface

```

6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

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

Enter the number of the interface you wish to configure: 1

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

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

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

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

```

Le masque de sous réseau en « CIDR »

```

Enter an option: 2

Available interfaces:

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

Enter the number of the interface you wish to configure: 1

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

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

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

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

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

```

On ignore la question, en appuyant sur « entrer »

```
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 :

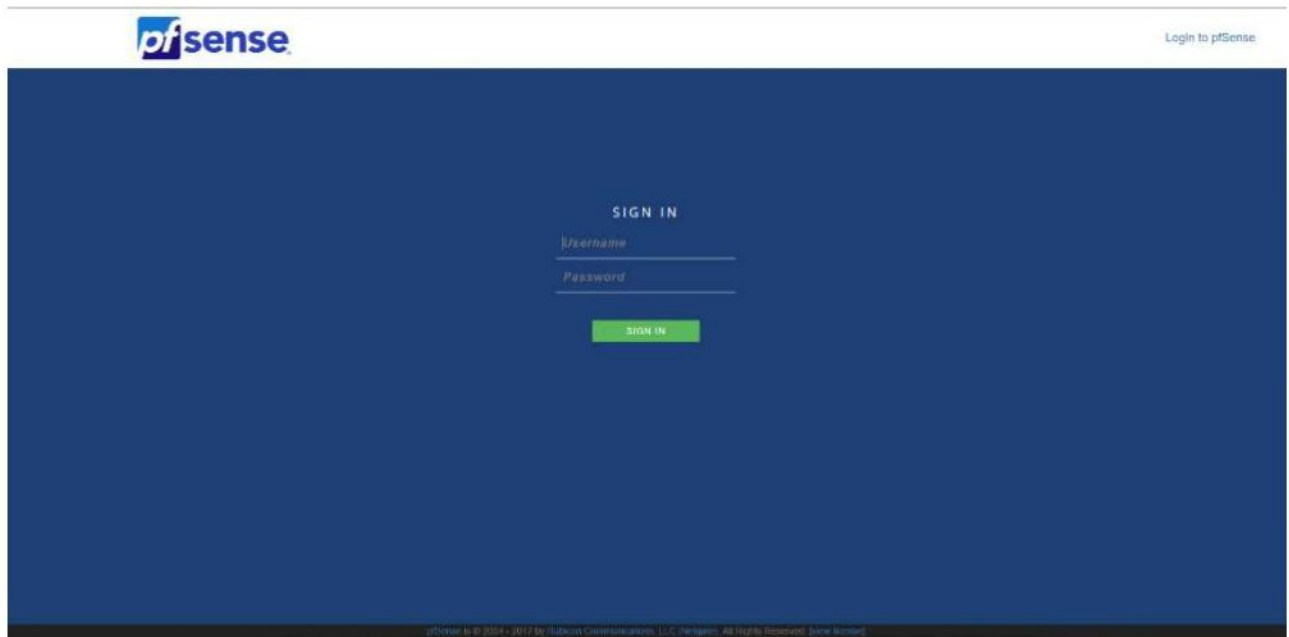
Lan : 192.168.1.202/24, Activation de la configuration web

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.

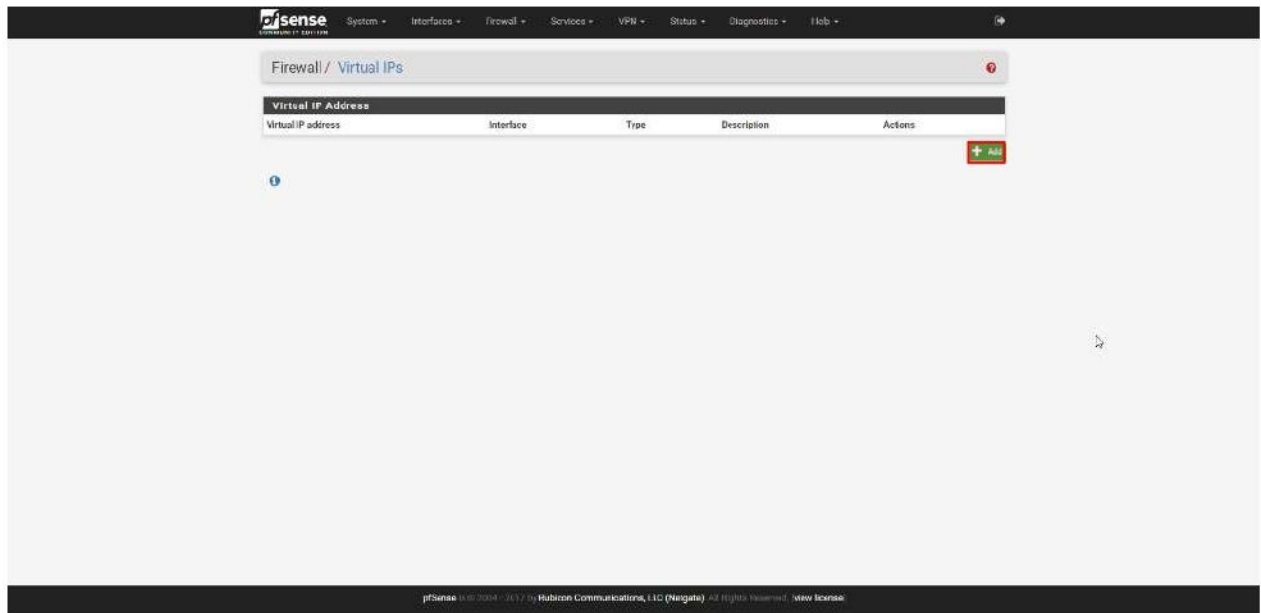
System Information	
Name	pfSense.localdomain
System	VirtuBox Virtual Machine Netgate Device ID: fd20bec056383616a6f4
BIOS	Vendor: Insanetek GmbH Version: VirtuBox Release Date: Fri Dec 1 2006
Version	2.4.3-RELEASE-p1 (amd64) built on Tue Dec 12 13:45:26 CST 2017 FreeBSD 11.1-RELEASE-p5 The system is on the latest version. Version information updated at Thu Mar 1 14:09:51 UTC 2018
CPU Type	Intel(R) Xeon(R) CPU X3440 @ 2.83GHz AES-NI CPU Crypto: No
Uptime	23 Hours 49 Minutes 00 Seconds
Current date/time	Thu Mar 1 14:20:23 UTC 2018
DNS server(s)	127.0.0.1
Last config change	Thu Mar 1 14:10:13 UTC 2018
State table size	0% (436/97000) Show status
MBUF Usage	2% (1016/61000)
Load average	0.22 0.38 0.45
CPU usage	Retrieving CPU data

Netgate Services And Support	
Contract type	Community Support Community Support Only
NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES If you purchased your pfSense gateway firewall appliance from Netgate and elected Community Support at the point of sale, you can register your community support subscription for access to pfSense Gold. <ul style="list-style-type: none">Register Your Support SubscriptionUpgrade Your SupportNetgate Global Support FAQNetgate Professional ServicesLogin to your portal accountCommunity Support ResourcesOfficial pfSense Training by NetgateVisit Netgate.com If you decide to purchase a Netgate Global Support subscription, you MUST have your Netgate Device ID (NDI) from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase support here .	
Interfaces	
WAN	100%baseT- full-duplex 192.168.0.2
LAN	100%baseT- full-duplex 172.16.0.254

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

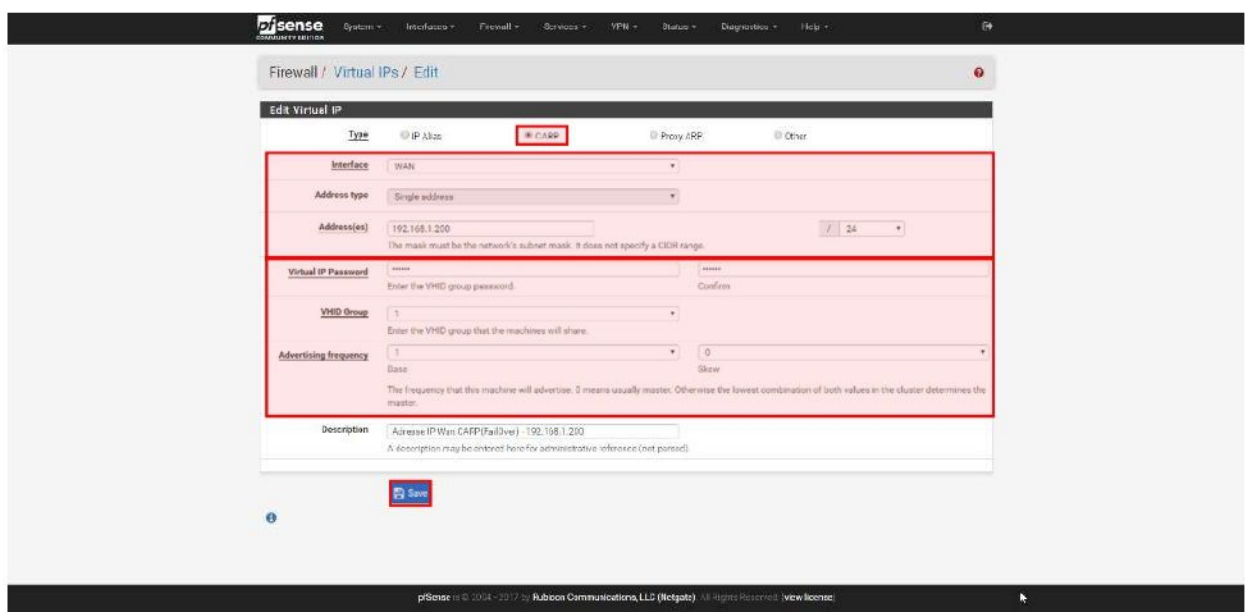
7. Configuration des adresses IP virtuelle (Haut Dispo)

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 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 virtuel WAN, comme ceci

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

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type: ☒ IP Address ☐ Floating Address ☐ Other

Interface: LAN

Address type: Single address

Address: 172.16.0.254

Virtual IP Password: Pfsense

VMS Group: 2

Advertising frequency: 1

Description: Address (IP:LAN:CARP:Virtual IP) - 172.16.0.254

On fait de même pour l'interface Lan.

Nous allons pouvoir appliquer les paramètres

Firewall / Virtual IPs

Virtual IP configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Virtual IP address	Interface	Type	Description	Actions
192.168.1.200/24 (WAN: 1)	WAN	CARP	Address (IP:WAN:CARP:Virtual IP) - 192.168.1.200	Edit Delete
172.16.0.254/24 (LAN: 2)	LAN	CARP	Address (IP:LAN:CARP:Virtual IP) - 172.16.0.254	Edit Delete

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"

Status / CARP

Refresh CARP Status

Enter PfSense CARP Maintenance Mode

CARP Interface	Virtual IP	Status
WAN01	192.168.1.200/24	MASTER
LAN02	172.16.0.254/24	MASTER

pfSense Nodes

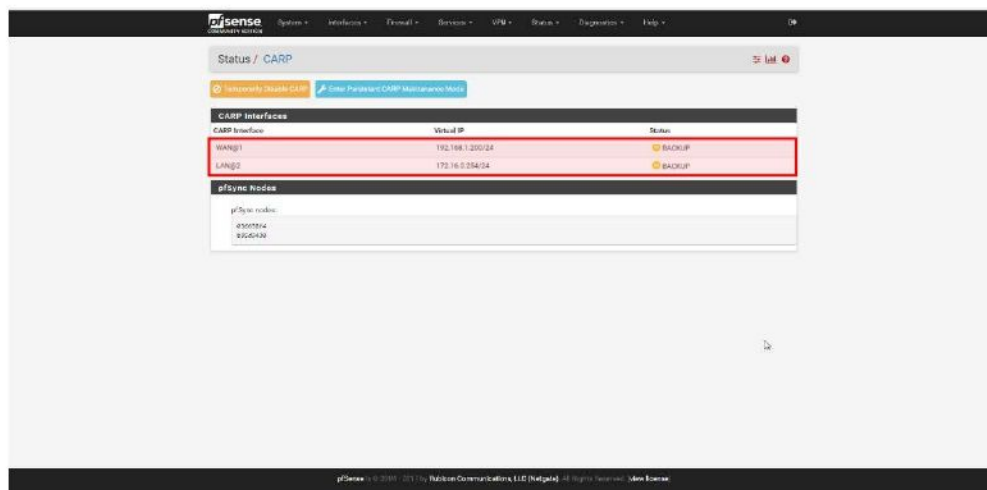
pfSense nodes

WAN01

LAN02

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

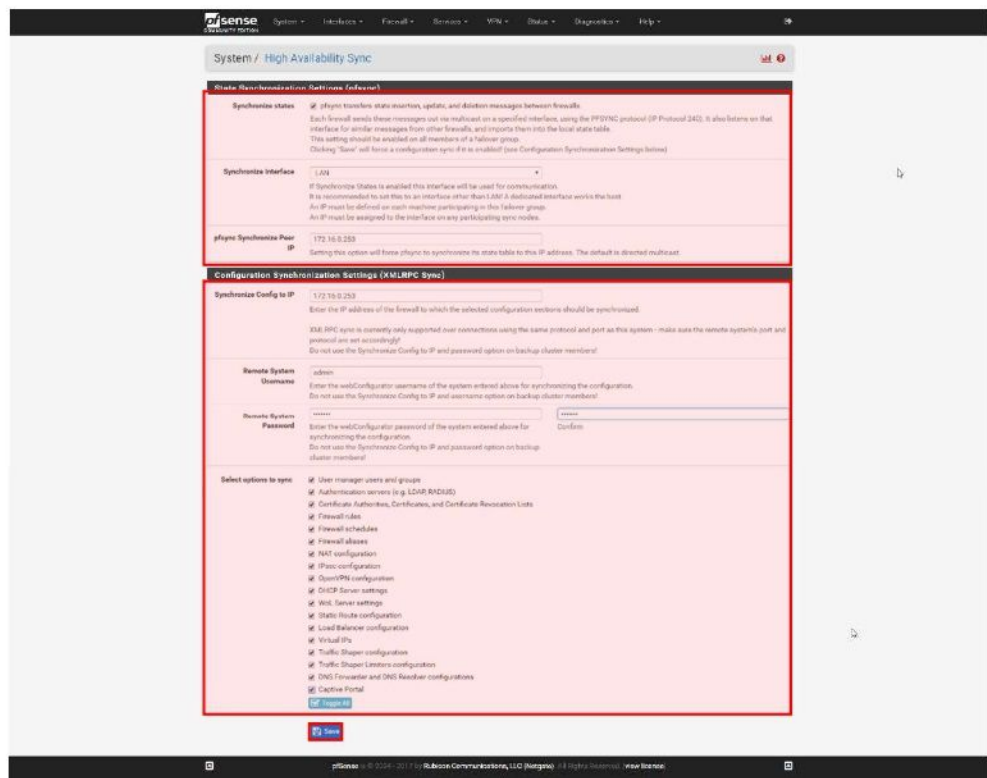
Le statut des IP virtuelle sur le second PFSENSE, il sont donc bien en backup



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

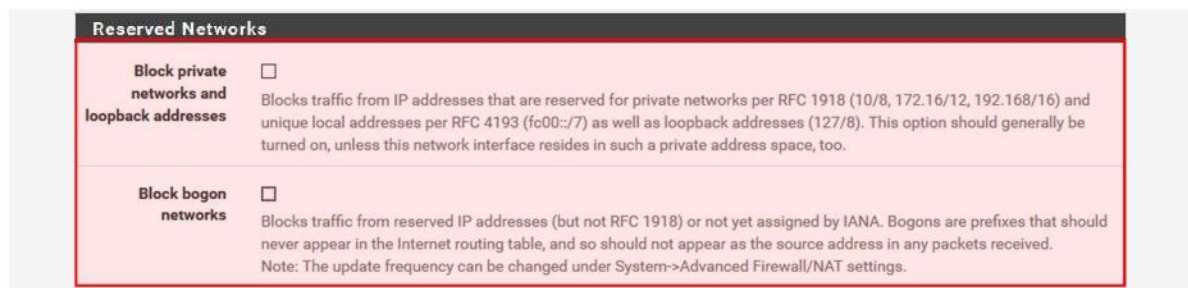
Reserved Networks

- ☒ 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 cochées



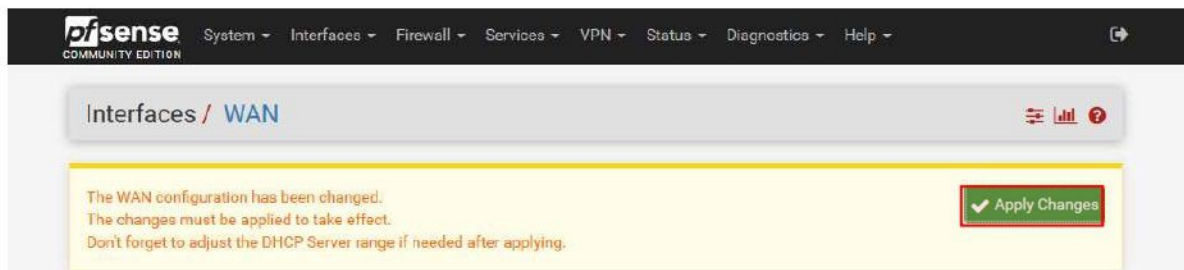
Reserved Networks

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.

Aucune ne doit être cochée

Une fois enlever, nous devons appliquer les modifications



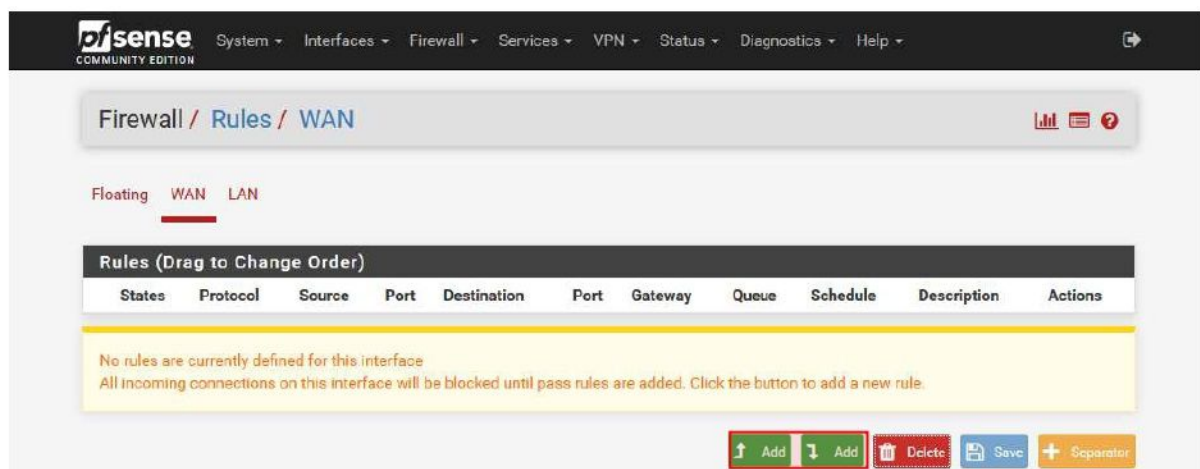
Interfaces / WAN

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.



Firewall / Rules / WAN

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 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 même pour toutes règles.

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 Bloque tout le trafic
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](#)

[Save](#)

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

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

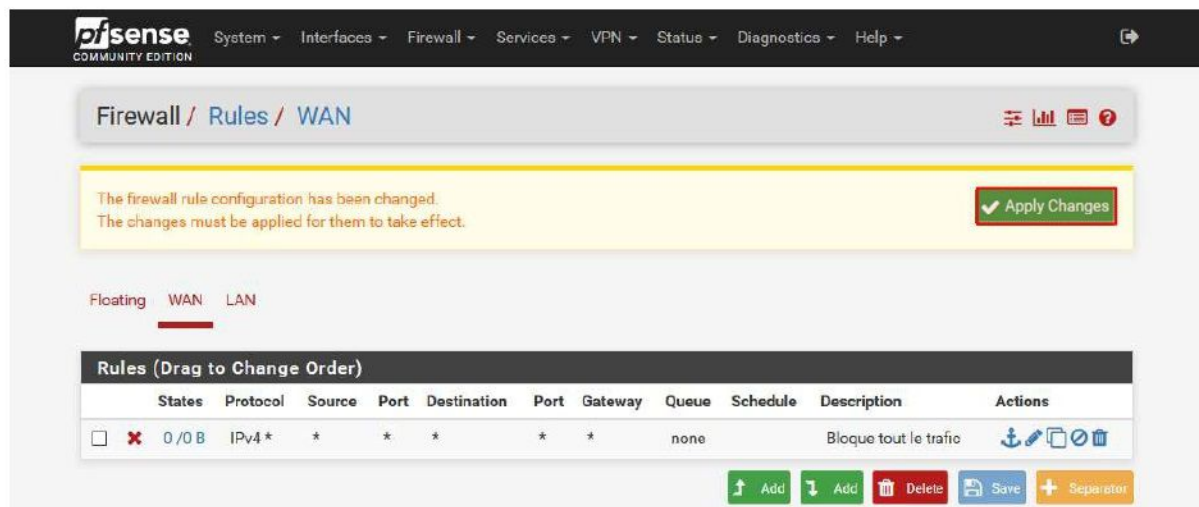
Attention la règle de blocage doit être effectuée en dernière côté LAN, elle risque de bloquer l'accès à l'interface web. Pour le côté LAN et WAN, le principe est le même. Il est possible de désactiver l'utilisation de certains protocoles ou bien bloquer une partie du réseau au certaines machines. Cet outil est pratique et puissant. Une liste de protocole et de port est pré-enregistrée, 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 côté 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 supprimée.

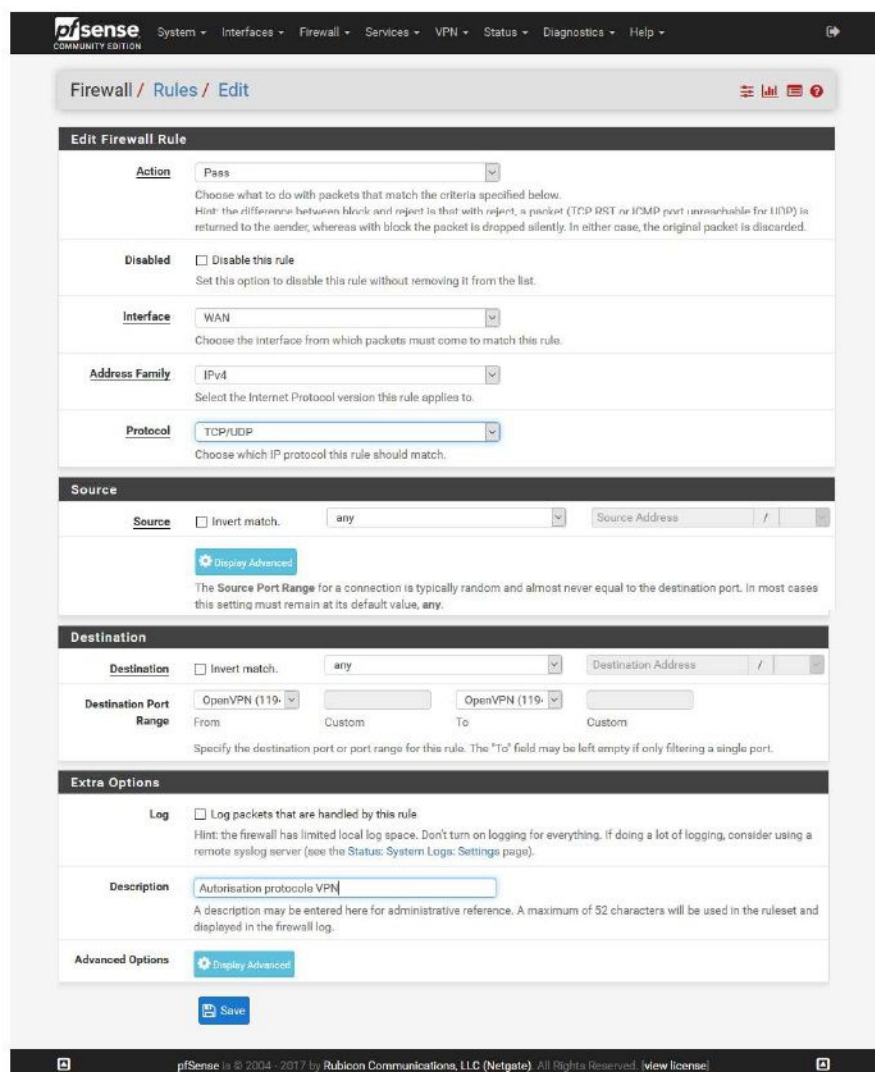
✓	1 / 1.58	*	*	*	LAN	80	*	*	Anti-Lockout Rule	⚙
	MIB				Address					

Une fois notre règle créer, nous devons l'appliquer



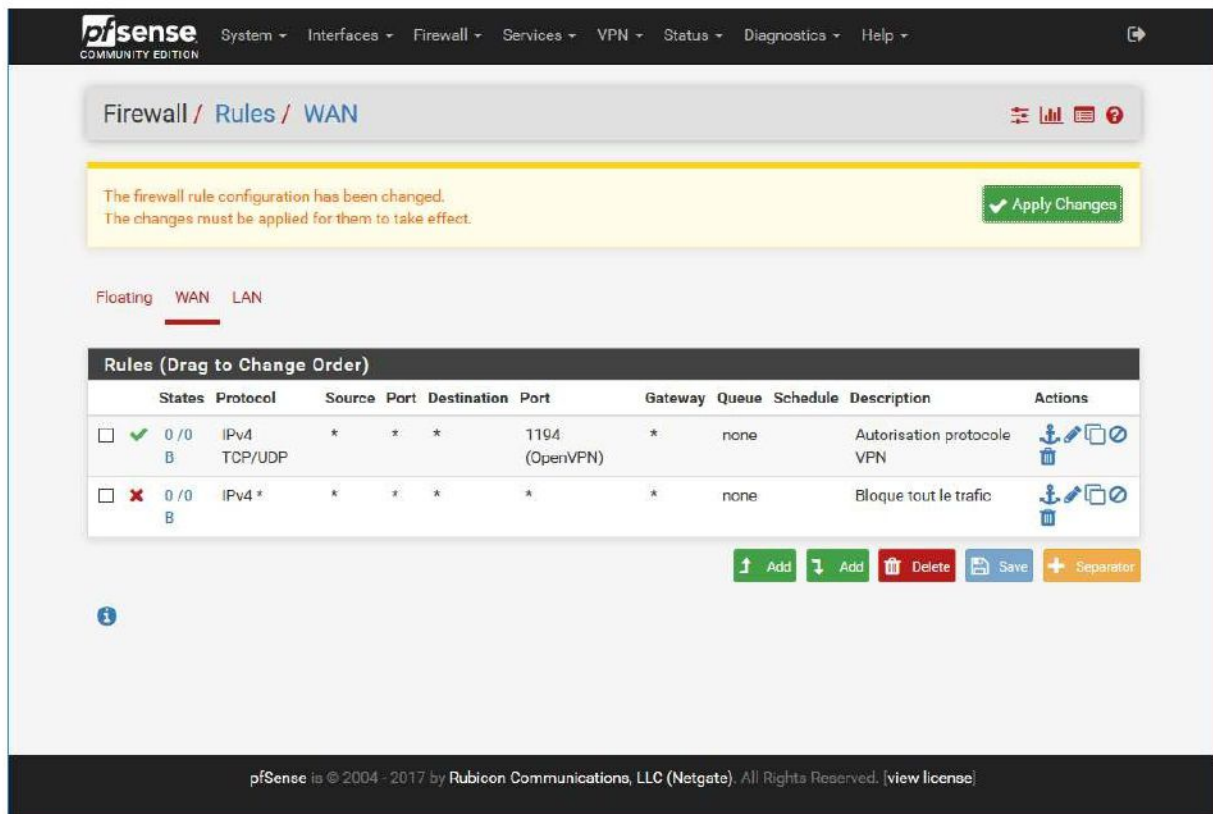
Cliquer sur "Apply Changes", afin d'activer notre règle.

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 à leurs ordres et à leur importance. Si la règle de blocage est en première, aucune des règles après ne fonctionnera.



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

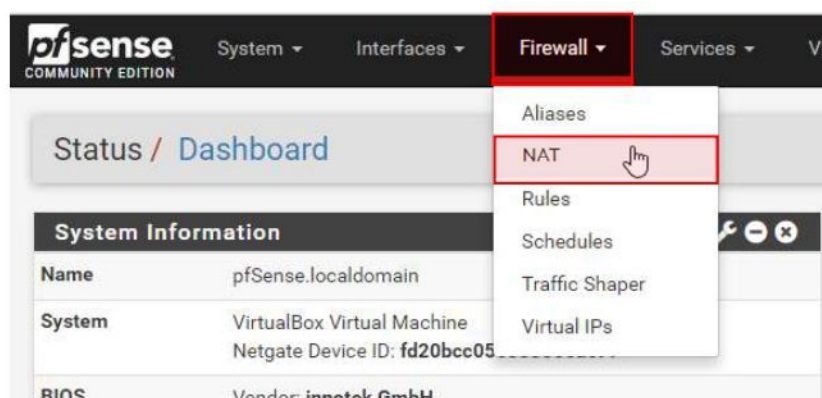
La redirection de port permet de transférer un port exemple :

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



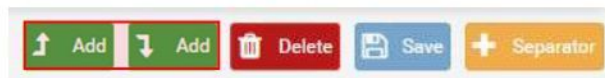
Pour cela, nous devons aller dans « Firewall / Nat »

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										
<input type="checkbox"/>	<input checked="" 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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<input checked="" type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	33690	172.16.0.102 3369 (MS RDP)	RDP - Physique
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	33691	172.16.0.102 33691	RDP - Hopper
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	33692	172.16.0.102 33692	RDP - Intratec
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	33693	172.16.0.102 33693	RDP - Centreon
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	33694	172.16.0.102 33694	RDP - PFSENSE
Machine Intratec - 172.16.0.103										
<input type="checkbox"/>	<input checked="" 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"/>	<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	1136	172.16.0.103 1136	Serveur Web - Intratec
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	8000	172.16.0.103 8000	Serveur Ajenti - Intratec
Machine Centreon - 172.16.0.104										
<input type="checkbox"/>	<input checked="" 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"/>	<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"/>	<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"/>	<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

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

WAN

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

Protocol

Notre protocole

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

Source

Display Advanced

Destination

Invert match.

WAN address

Type

Address/mask

Destination port range

Other

Port Externe

Other

Saisir port si ranger

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

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 interne machine

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

Description afin de la repérer facilement

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

Use system default

Filter rule association

Add associated filter rule

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

Save

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 précédament, 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 / 154 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 / 19.53 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 empechent de faire du filtrage et bloquent toutes les entrées.

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

