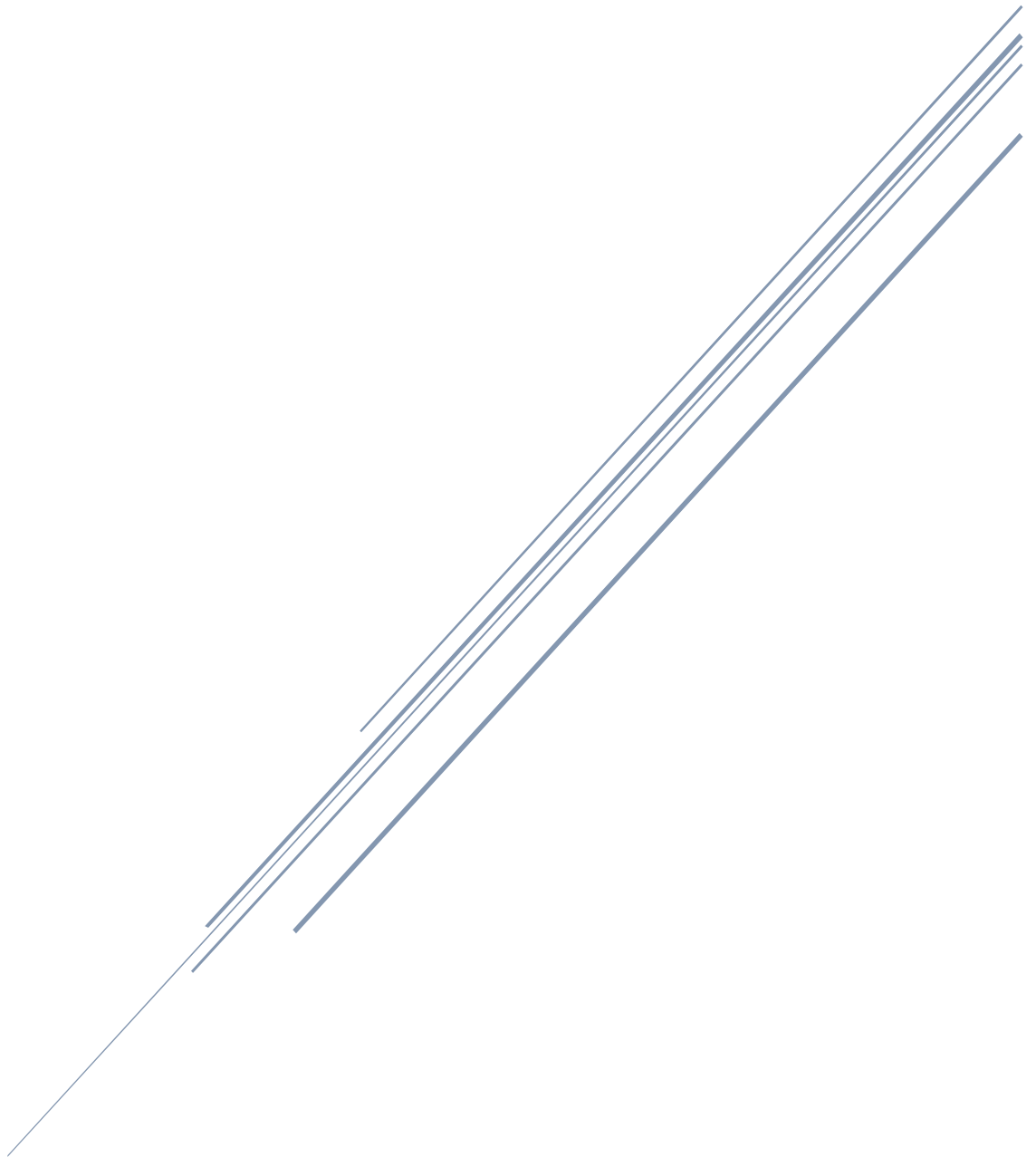


# MISE EN PLACE DE 2 PARE-FEU PFSENSE

Avec redondance



Open-IT  
Kevin THOMAS – BTS SIO SISR

## Sommaire

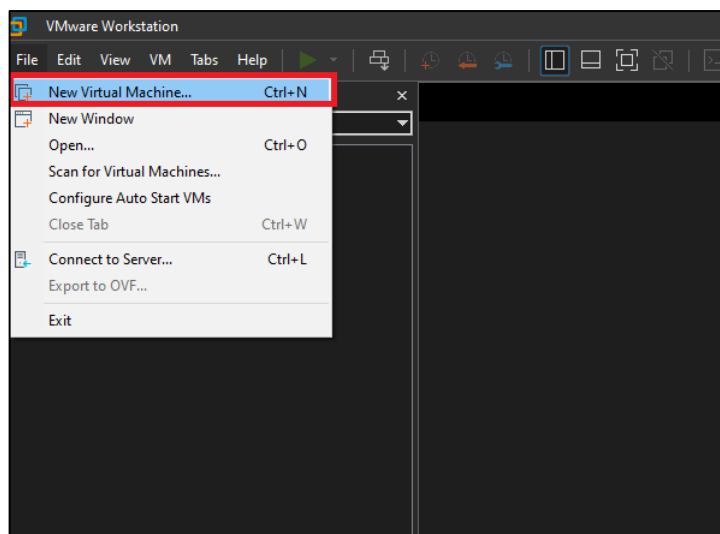
Installation PfSense .....	2
Qu'est-ce que PfSense ? .....	2
Installation de PfSense sous VmWare Workstation Pro .....	2
Configuration de PfSense .....	8
Configuration du serveur PfSense principale .....	10
Paramétrage des interfaces .....	10
Paramétrage de l'interface LAN .....	10
Paramétrage de l'interface WAN .....	12
Création du serveur PfSense secondaire.....	13
Clonage de la VM du PfSense principale .....	13
Paramétrage des interfaces .....	16
Paramétrage de l'interface LAN .....	16
Paramétrage de l'interface WAN .....	17
Configuration de PfSense .....	18
Connexion à l'interface de PfSense .....	18
Configuration des adresses IP virtuelle .....	19
Configuration de la redondance.....	24
Configuration sur le Pfsense principale.....	24
Configuration sur le Pfsense secondaire .....	25
Autoriser la redondance .....	26
Configuration du DHCP.....	30
Configuration de l'adresse IP virtuelle pour le trafic sortant .....	32
Vérification de la configuration de la redondance.....	34
Règles de filtrage .....	35

## Installation PfSense

### Qu'est-ce que PfSense ?

PfSense est un système d'exploitation open source basé sur FreeBSD, qui sert de pare-feu et de routeur pour les réseaux informatiques. Il assure la protection des réseaux contre les menaces en appliquant des politiques de sécurité et de filtrage sur les connexions entrantes et sortantes. PfSense propose une interface web intuitive pour configurer et gérer le système, ainsi que de nombreuses fonctionnalités avancées telles que la surveillance de la bande passante, la prise en charge de VPN, la gestion de la qualité de service, et bien plus encore. C'est une solution de sécurité réseau performante, flexible et accessible pour les entreprises, les organisations et les particuliers.

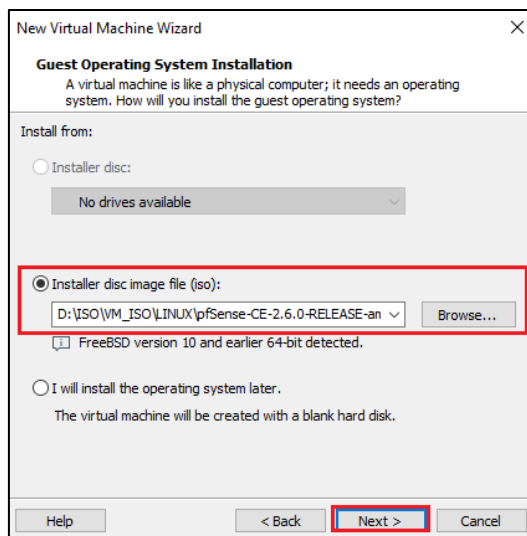
### Installation de PfSense sous VmWare Workstation Pro



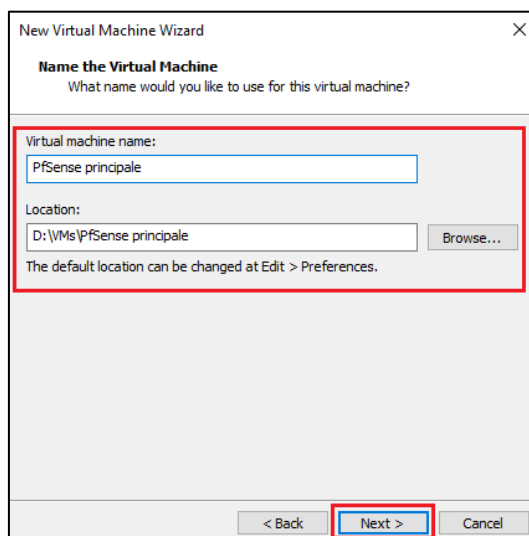
*Cliquer sur « File » et sélectionner « New Virtual Machine »*



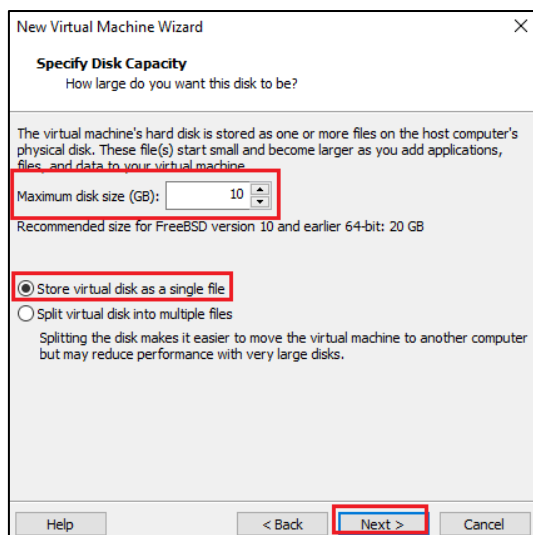
*Sélectionner « Typical » car nous utiliserons le paramétrage recommandé et cliquer sur « Next »*



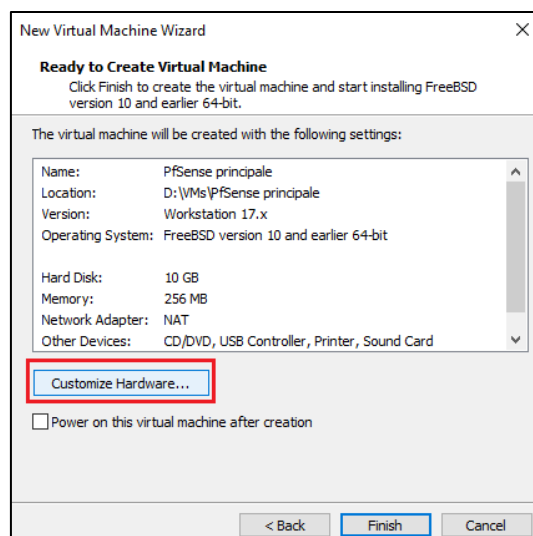
*Cliquer sur « **Browse** » puis sélectionner votre fichier .iso  
Enfin appuyer sur « **Next** »*



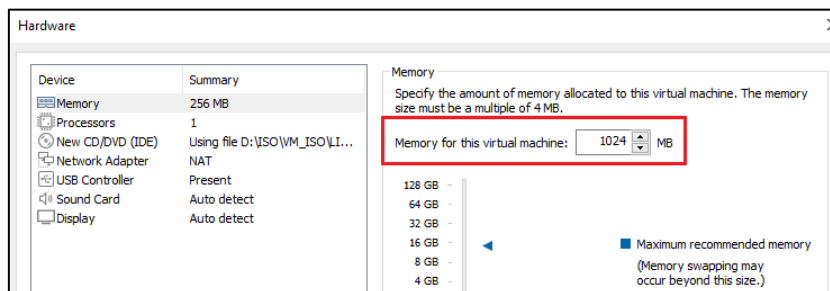
*Choisir le nom de la machine virtuelle et son endroit de stockage  
Puis cliquer sur « **Next** »*



*Indiquer la taille du disque de stockage (10GB est suffisant, mais plus peut être ajouté à tout moment)  
Cliquer sur « **Store virtual disk as a single file** »  
Cliquer ensuite sur « **Next** »*

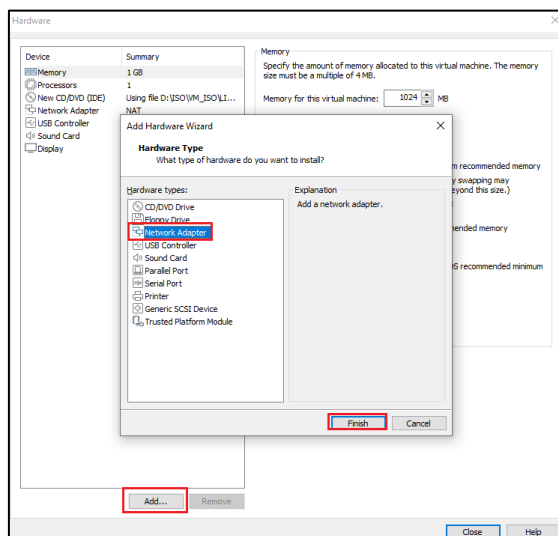


*Cliquer sur « **Customize Hardware** » car il est important qu'on configure notre machine virtuelle correctement avant le démarrage*

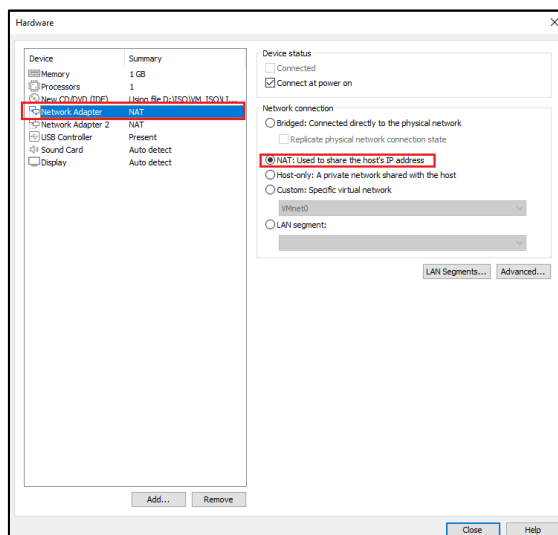


*1024MB est suffisant*

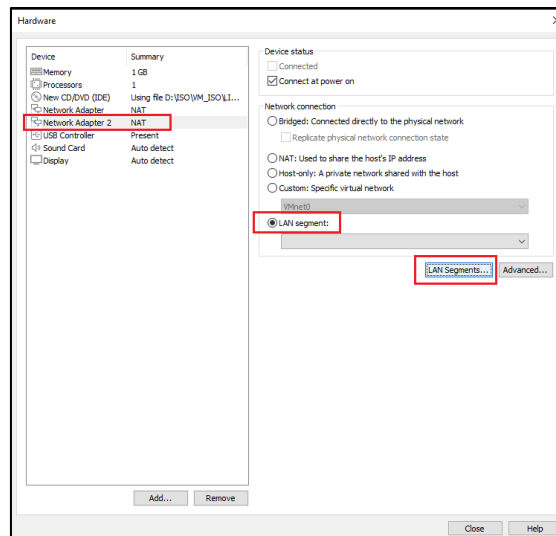
Pour respecter l'architecture demandé dans la réalisation professionnelle il faut ajouter impérativement une carte réseau supplémentaire



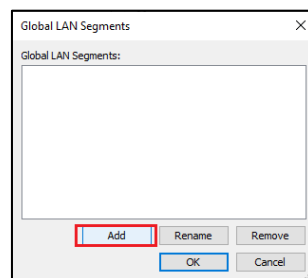
*Cliquer sur « Add » puis sélectionner « Network Adapter » et terminer par « Finish »*



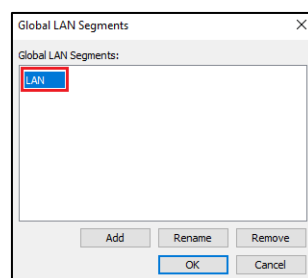
*La carte réseau nous donnant accès à l'accès internet doit être configuré en NAT*



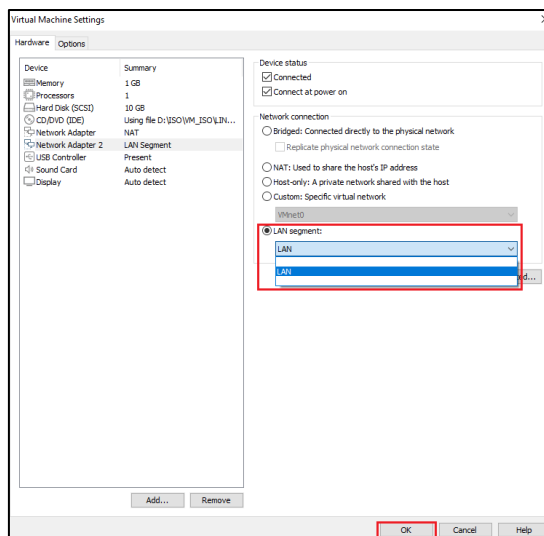
*La seconde cependant, doit être configuré avec un « **LAN Segment** »  
Pour en configurer un, cliquer sur « **LAN Segments** »*



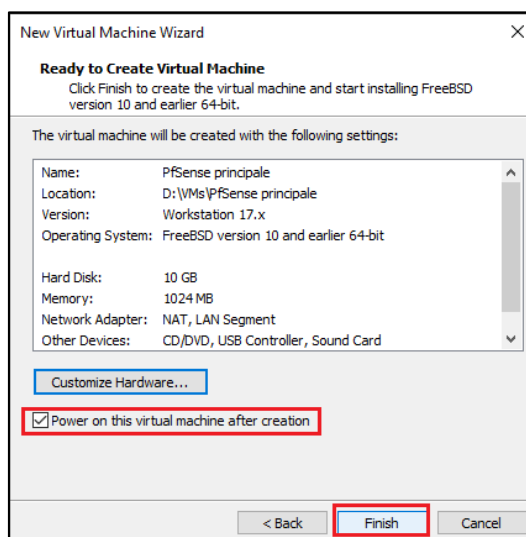
*Cliquer sur « **Add** »*



*Ecrire le nom voulu puis cliquer sur « **OK** »*



Sélectionner votre **LAN Segment** puis cliquer sur « **Close** »



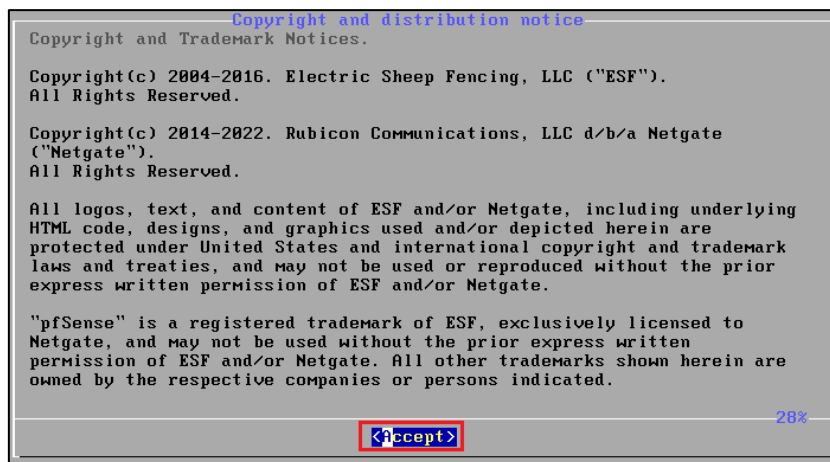
Cocher « **Power on..** »  
Puis cliquer sur « **Finish** »  
La machine virtuelle va démarrer automatiquement



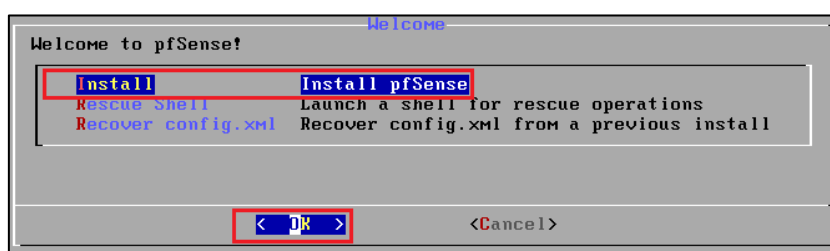
## Configuration de PfSense

### Installation du système d'exploitation

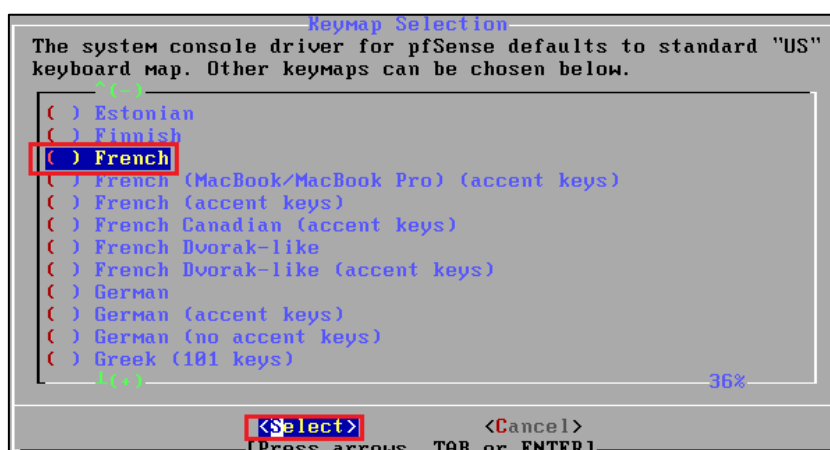
On utilisera uniquement les flèches du clavier et la touche « **Entrée** » pour naviguer dans les menus d'installation



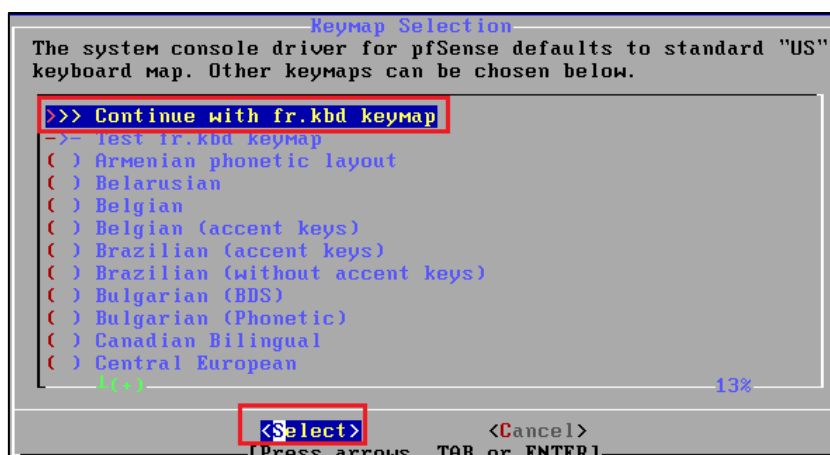
Appuyer sur « **Entrée** » pour procéder à l'installation



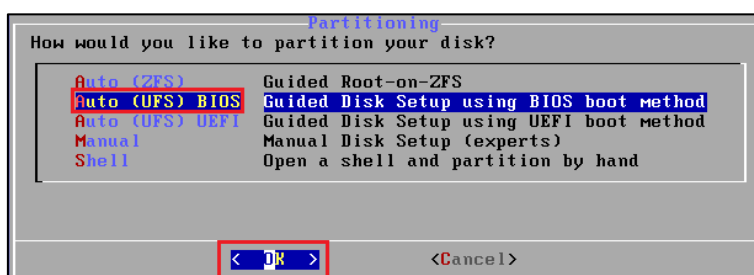
Se positionner sur « **Install** » puis appuyer sur « **Entrée** »



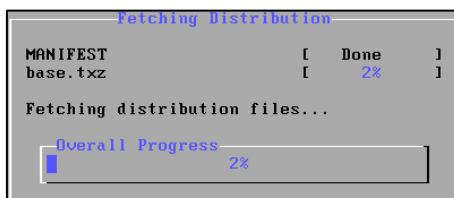
Se positionner sur « **French** » puis appuyer sur « **Entrée** »  
Cela installera le clavier français



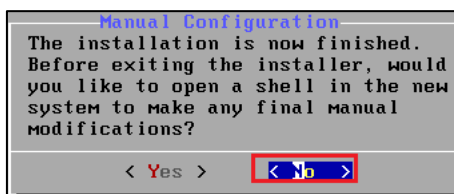
Appuyer sur « Entrée » à nouveau



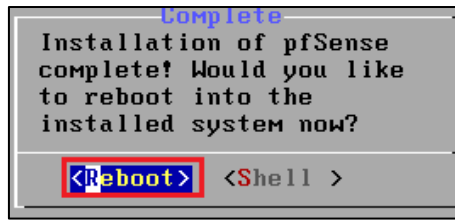
Sélectionner « Auto (UFS) BIOS » puis appuyer sur « Entrée »



Une progression est en cours  
Il suffit de patienter



Sélectionner « No » puis faire « Entrée »



Sélectionner « Reboot » et faire « Entrée »

## Configuration du serveur PfSense principale

### Paramétrage des interfaces

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 63ec90b62c1056f79c95

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      ->
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: █
```

Après redémarrage le serveur atteint cette interface

### Paramétrage de l'interface LAN

Commençons par paramétrer l'interface « LAN », c'est-à-dire le LAN SEGMENT que nous avons configuré précédemment.

```
VMware Virtual Machine - Netgate Device ID: 63ec90b62c1056f79c95

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      ->
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 █
```

Sélectionner l'option « 2 » pour configurer les interfaces puis sélectionner « 2 » pour paramétrer l'interface LAN

```
Enter the new LAN IPv4 address. Press <ENTER> for none:  
> 172.16.0.101
```

*Indiquer l'adresse IP de l'interface LAN puis faire « Entrée »*

```
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.  
e.g. 255.255.255.0 = 24  
     255.255.0.0   = 16  
     255.0.0.0     = 8  
  
Enter the new LAN IPv4 subnet bit count (1 to 32):  
> 16
```

*Entrée le CIDR pour le masque de sous réseau puis faire « Entrée »*

```
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:  
>
```

*Ne pas remplir pour les 2 cas et faire « Entrée »  
Car dans le 1<sup>er</sup> cas c'est utile pour l'interface WAN  
Dans le 2eme cas nous travaillons en IPv4*

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

*PfSense va gérer le service DHCP de l'interface LAN, pour cela appuyer sur « y » puis « Entrée »*

```
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: 172.16.0.100  
Disabling IPv6 DHCPD...
```

*Indiquer la plage de début, faire « Entrée » puis indiquer la plage de fin et appuyer sur « Entrée »  
Cela peut être modifié par la suite*

```
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 172.16.0.101/16  
You can now access the webConfigurator by opening the following URL in your web  
browser:  
http://172.16.0.101/
```

*Appuyer sur « y » puis « Entrée » pour configurer l'accès à l'interface WEB de PfSense via l'interface LAN*

```
Press <ENTER> to continue.
```

*Terminer la configuration en appuyant sur « Entrée »*

## Paramétrage de l'interface WAN

```
VMware Virtual Machine - Netgate Device ID: 63ec90b62c1056f79c95

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      ->
LAN (lan)      -> em1      -> v4: 172.16.0.101/16

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
```

Sélectionner l'option « 2 » pour configurer les interfaces puis sélectionner « 1 » pour paramétrer l'interface WAN

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

Appuyer sur « n » pour ne pas prendre la configuration du DHCP

```
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.75.201
```

Indiquer l'adresse IP de l'interface WAN et appuyer sur « Entrée »

```
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 32):
> 24
```

Indiquer le CIDR de l'interface puis faire « Entrée »

```
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.75.2
```

Indiquer l'adresse IP de la passerelle puis « Entrée »

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

Nous utilisons uniquement de l'IPv4, appuyer sur « n » puis faire « Entrée »

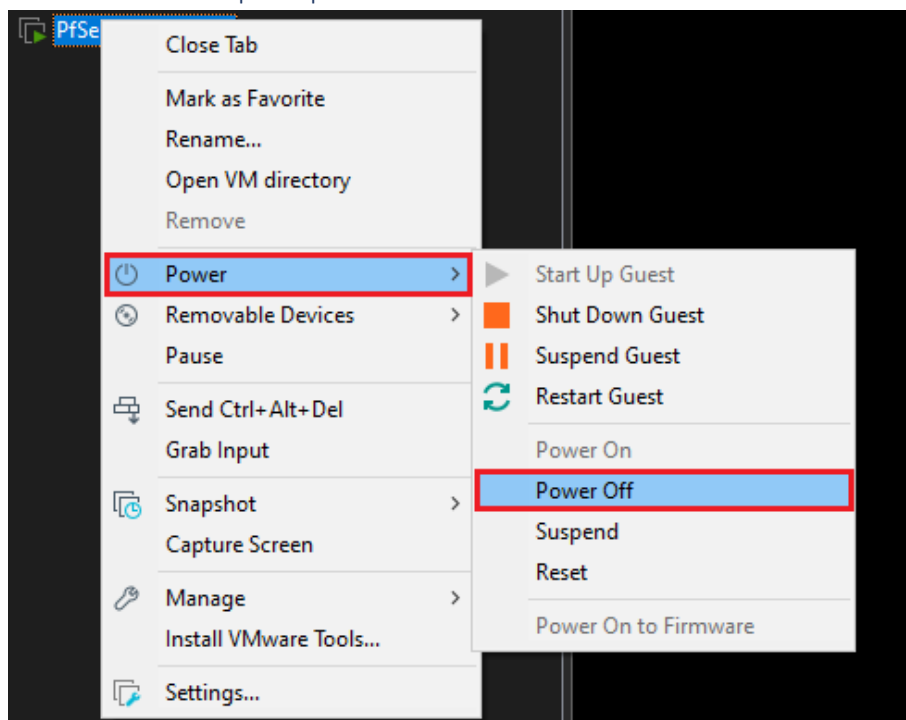
```
The IPv4 WAN address has been set to 192.168.75.201/24
Press <ENTER> to continue.
```

Appuyer sur « Entrée » pour terminer

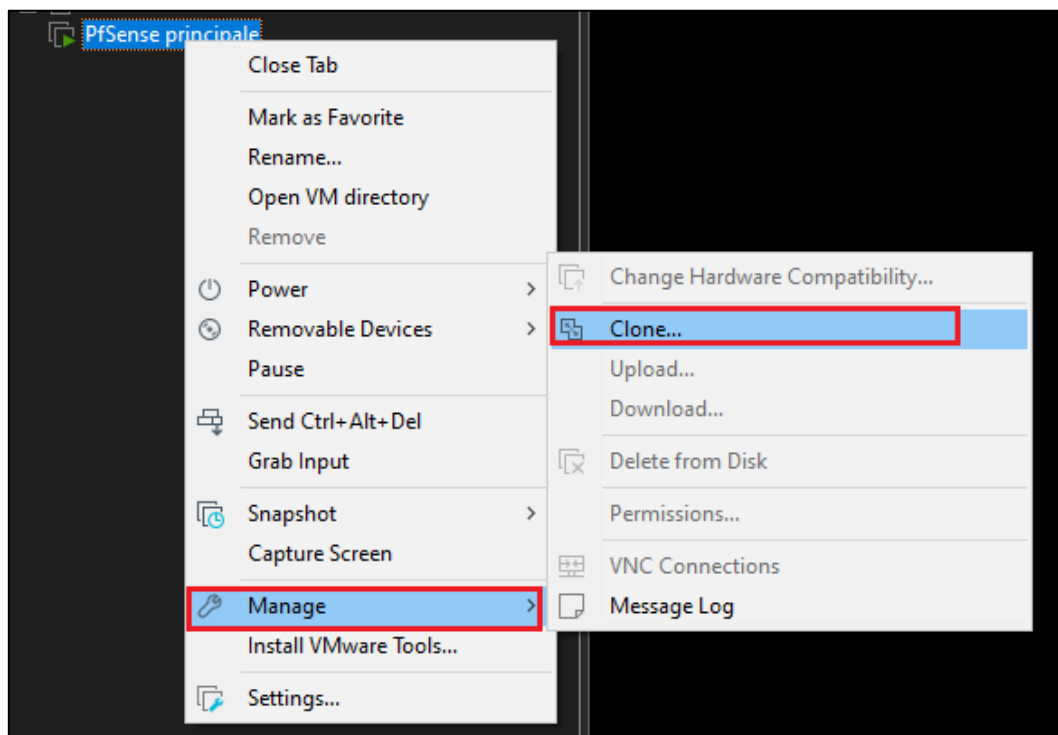
## Création du serveur PfSense secondaire

Pour le second serveur nous utiliserons le modèle de la machine virtuelle du Pfsense principale. Nous allons créer un clone de la VM puis modifier l'adressage IP.

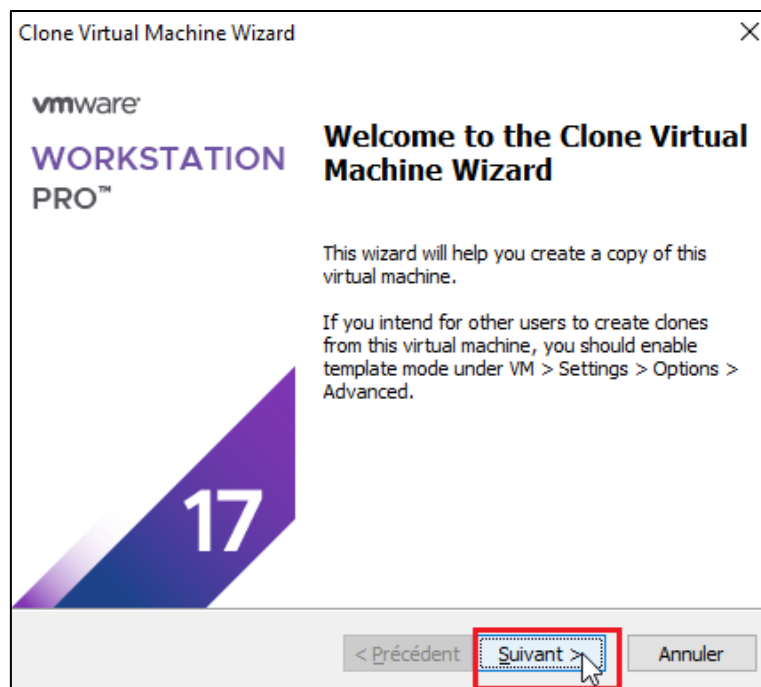
Clonage de la VM du PfSense principale



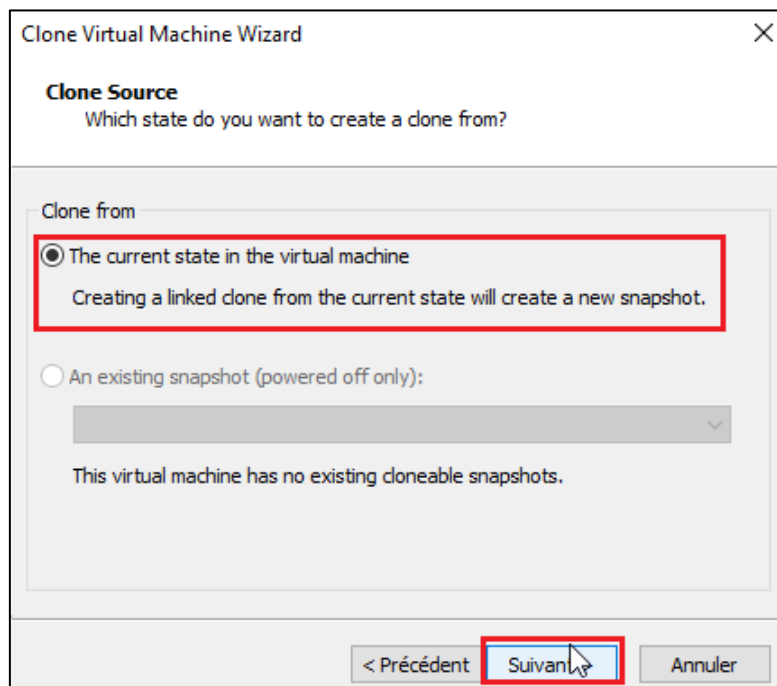
*Il faut d'abord éteindre la machine virtuelle*



*Faire un clic droit sur la VM puis sélectionner « Manage » et enfin « Clone »*



*Cliquer sur « Suivant »*



*Bien sélectionner « The current state in the virtual machine » et cliquer sur « Suivant »*

Clone Virtual Machine Wizard

**Clone Type**  
How do you want to clone this virtual machine?

Clone method

☐ Create a linked clone  
A linked clone is a reference to the original virtual machine and requires less disk space to store. However, it cannot run without access to the original virtual machine.

☒ Create a full clone  
A full clone is a complete copy of the original virtual machine at its current state. This virtual machine is fully independent, but requires more disk space to store.

< Précédent Suivant > Annuler

Sélectionner « **Create a full clone** » puis « **Suivant** »

Clone Virtual Machine Wizard

**Name of the New Virtual Machine**  
What name would you like to use for this virtual machine?

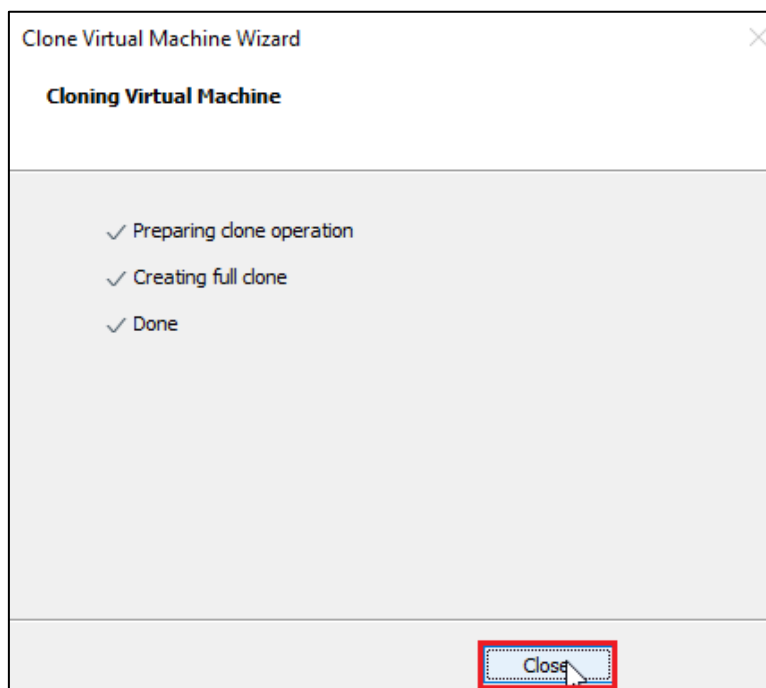
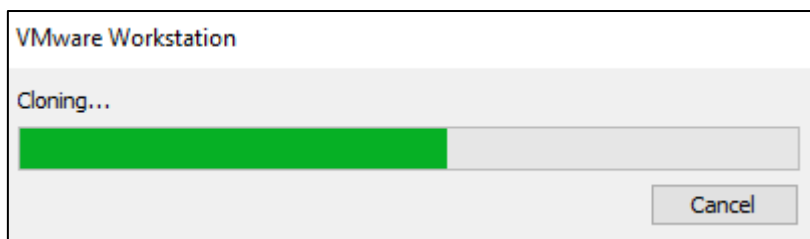
Virtual machine name  
PfSense secondaire

Location  
D:\VMs\PfSense secondaire Browse...

< Précédent Terminer Annuler

Sélectionner le nom de la machine virtuel et son lieu de stockage puis cliquer sur « **Terminer** »





Cliquer enfin sur « Close »

## Paramétrage des interfaces

### Paramétrage de l'interface LAN

```
VMware Virtual Machine - Netgate Device ID: 3fdbb50ec46c4127f045
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 192.168.75.201/24
LAN (lan)      -> em1      -> v4: 172.16.0.101/16

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 - static)
2 - LAN (em1 - static)

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

Sélectionner l'option « 2 » pour configurer les interfaces puis sélectionner « 2 » pour paramétrer l'interface LAN

```
Enter the new LAN IPv4 address. Press <ENTER> for none:  
> 172.16.0.102
```

*Indiquer l'adresse IP du PfSense secondaire*

```
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.  
e.g. 255.255.255.0 = 24  
     255.255.0.0   = 16  
     255.0.0.0     = 8  
  
Enter the new LAN IPv4 subnet bit count (1 to 32):  
> 16
```

*Indiquer le CIDR de l'interface*

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

*Désactiver le DHCP en appuyant sur « n » puis faire « Entrée »*

```
The IPv4 LAN address has been set to 172.16.0.102/16  
You can now access the webConfigurator by opening the following URL in your web  
browser:  
      http://172.16.0.102/  
  
Press <ENTER> to continue.
```

*Faire « Entrée » pour terminer*

## Paramétrage de l'interface WAN

```
VMware Virtual Machine - Netgate Device ID: 3fdbb50ec46c4127f045  
  
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***  
  
WAN (wan)      -> em0      -> v4: 192.168.75.201/24  
LAN (lan)      -> em1      -> v4: 172.16.0.102/16  
  
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 - static)  
2 - LAN (em1 - static)  
  
Enter the number of the interface you wish to configure: 1
```

*Sélectionner l'option « 2 » pour configurer les interfaces puis sélectionner « 1 » pour paramétrer l'interface WAN*

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

*Appuyer sur « n » pour ne pas prendre la configuration du DHCP*

```
Enter the new WAN IPv4 address. Press <ENTER> for none:  
> 192.168.75.202
```

*Indiquer l'adresse IP de l'interface WAN et appuyer sur « Entrée »*

```
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 32):  
> 24
```

*Indiquer le CIDR de l'interface puis faire « Entrée »*

```
For a WAN, enter the new WAN IPv4 upstream gateway address.  
For a LAN, press <ENTER> for none:  
> 192.168.75.2
```

*Indiquer l'adresse IP de la passerelle puis « Entrée »*

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

*Nous utilisons uniquement de l'IPv4, appuyer sur « n » puis faire « Entrée »*

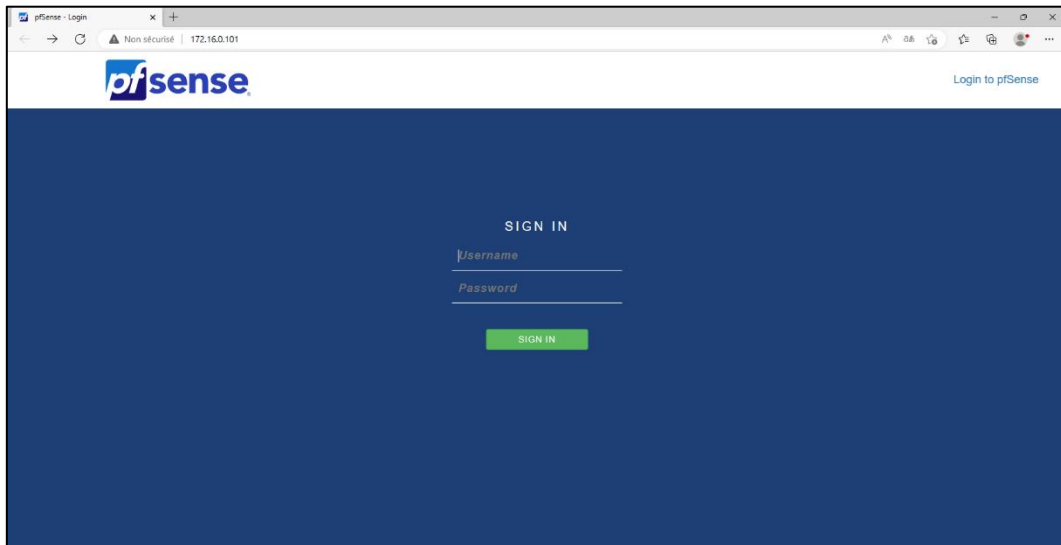
```
Press <ENTER> to continue.
```

*Appuyer sur « Entrée » pour terminer*

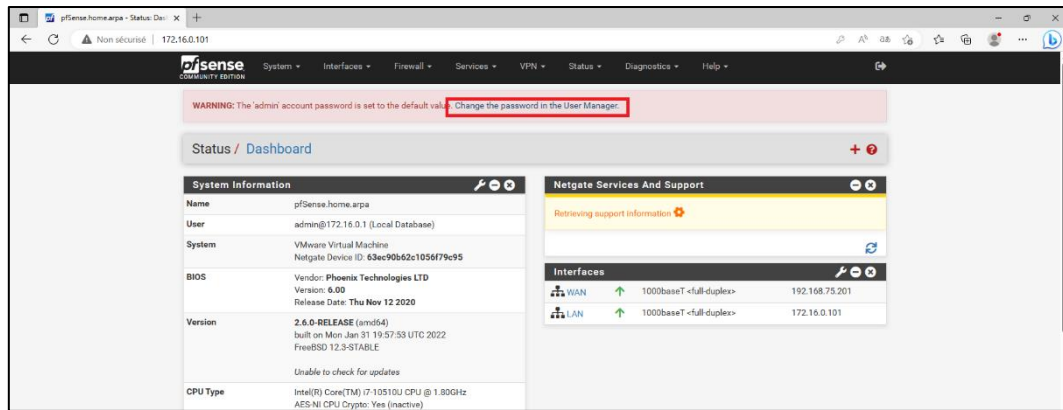
## Configuration de PfSense

### Connexion à l'interface de PfSense

Pour se connecter à l'interface WEB du PfSense je connecte une machine sur l'interface lan



*Entrer l'adresse IP du Pfsense principale ou secondaire puis utiliser le compte générique  
admin  
pfsense*



Changer le mot de passe en cliquant sur « **Change the password in the User Manager** »

## Configuration des adresses IP virtuelle

pfSense établit des connexions sur les réseaux LAN et WAN en utilisant des adresses IP virtuelles, évitant ainsi d'utiliser l'adresse IP assignée à son interface.

En cas de défaillance du pfSense primaire, le pfSense secondaire prend le relais de manière transparente, sans aucune interruption de service. La transition de pfSenseA vers pfSenseB s'opère en toute transparence.

Pour garantir la réplication, trois éléments doivent être configurés : CARP, pfsync et XML-RPC.

### CARP

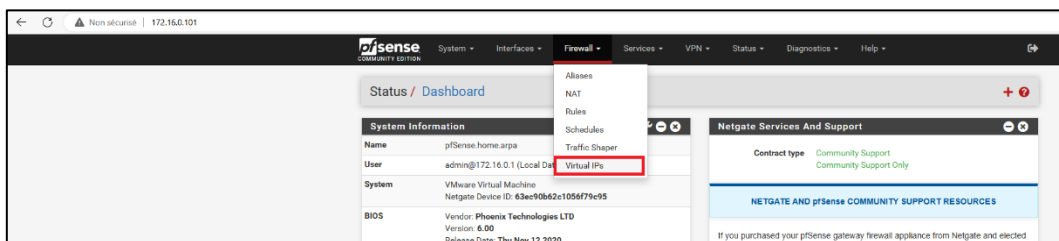
Le protocole CARP (Common Address Redundancy Protocol) permet à plusieurs hôtes présents sur un même réseau de partager une adresse IP commune.

### pfsync

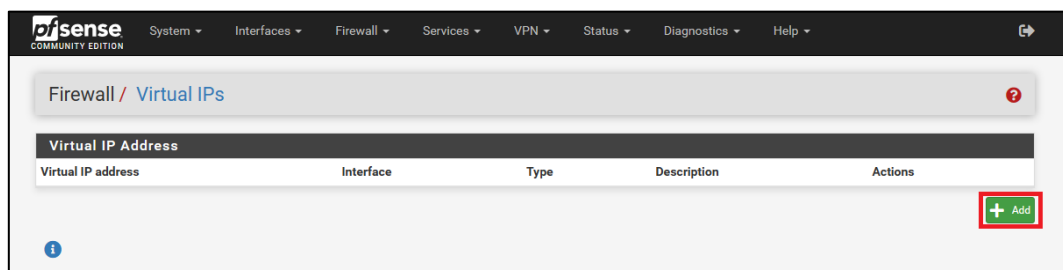
Le protocole pfsync permet la synchronisation de l'état des connexions en cours entre deux serveurs pfSense (ou plus généralement entre deux serveurs exécutant le pare-feu Packet Filter).

### XML-RPC

XML-RPC est un protocole utilisé dans pfSense pour répliquer la configuration du serveur primaire vers le serveur secondaire. Il permet la transmission de données entre les serveurs.



Se rendre dans « **Firewall** » puis « **Virtual IPs** »



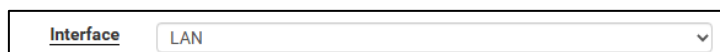
Cliquer sur « **Add** »

## Configuration IP virtuelle pour le LAN

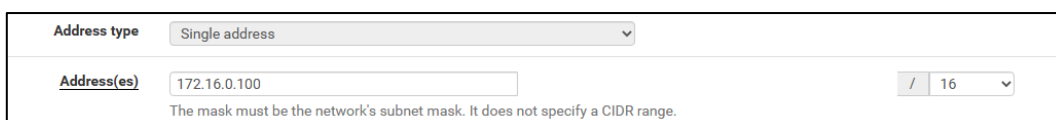
### Configuration sur le Pfsense principale



Sélectionner « **CARP** »



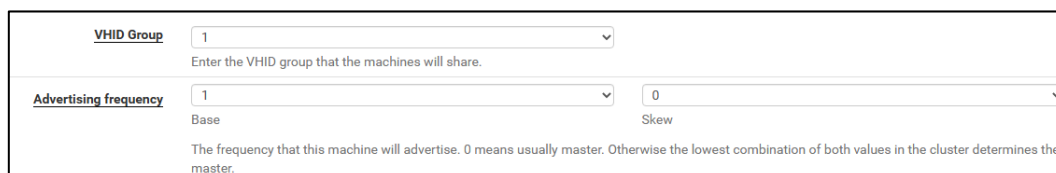
Sélectionner l'interface « **LAN** »



Renseigner l'adresse IP virtuelle à utiliser, dans notre cas « **172.16.0.100/16** »

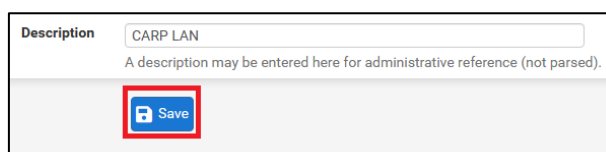


Renseigner le mot de passe à utiliser pour ce réseau virtuel

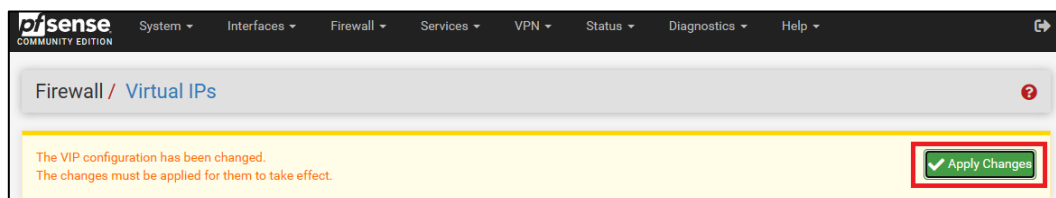


Sélectionner « **1** » pour « **VHID Group** »

Laisser « **Advertising frequency Base** » en « **1** » et mettre le « **Skew** » à « **0** »  
Cela permet de signaler que ce Pfsense a le rôle de « **master** »



Renseigner la description souhaité puis cliquer sur « **Save** »



Finaliser enfin en cliquant sur « **Apply Changes** »

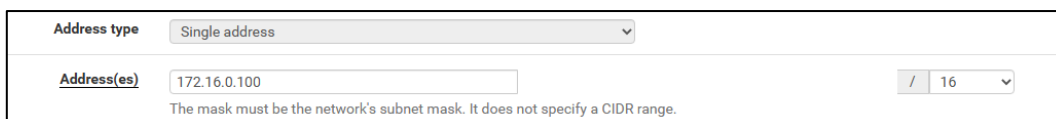
## Configuration sur le PfSense secondaire



Sélectionner « **CARP** »



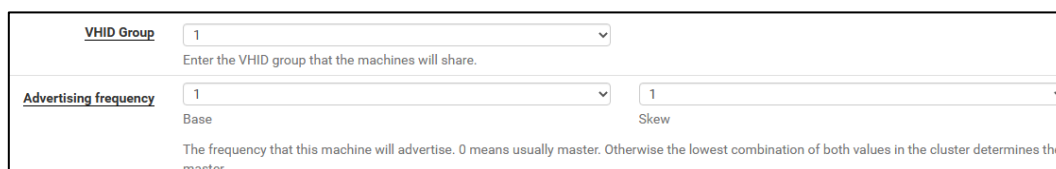
Sélectionner l'interface « **LAN** »



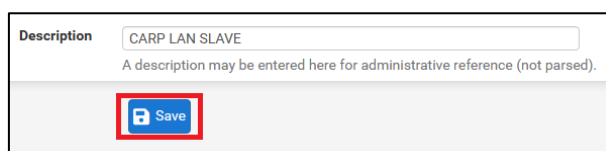
Renseigner l'adresse IP virtuelle à utiliser, dans notre cas « **172.16.0.100/16** »



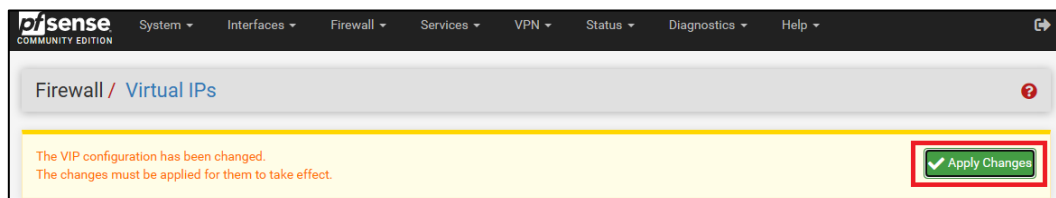
Renseigner le mot de passe à utiliser pour ce réseau virtuel



Sélectionner « **1** » pour « **VHID Group** »  
Laisser « **Advertising frequency Base** » en « **1** » et mettre le « **Skew** » à « **1** »  
Cela permet de signaler que ce PfSense a le rôle de « **Slave** »



Renseigner la description souhaité puis cliquer sur « **Save** »



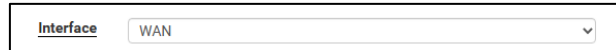
Finaliser enfin en cliquant sur « **Apply Changes** »

## Configuration IP virtuelle pour le WAN

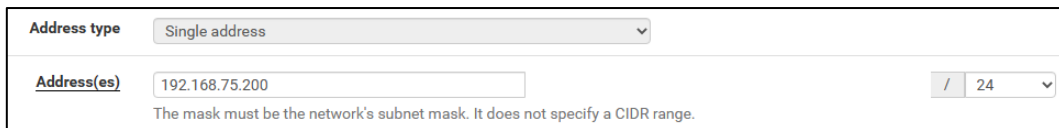
### Configuration sur le Pfsense principale



Sélectionner « **CARP** »



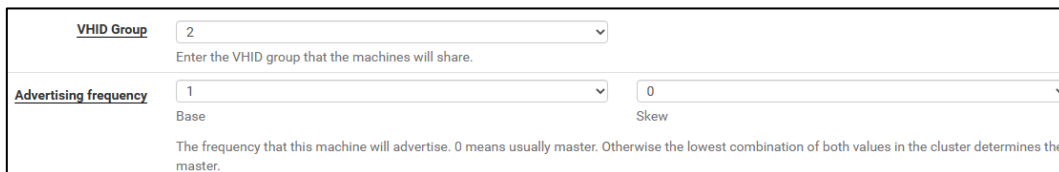
Sélectionner l'interface « **WAN** »



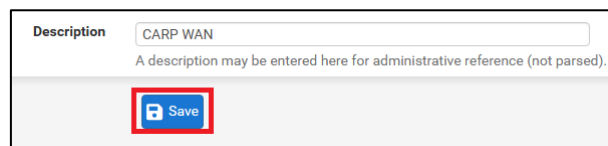
Renseigner l'adresse IP virtuelle à utiliser, dans notre cas « **192.168.75.200/24** »



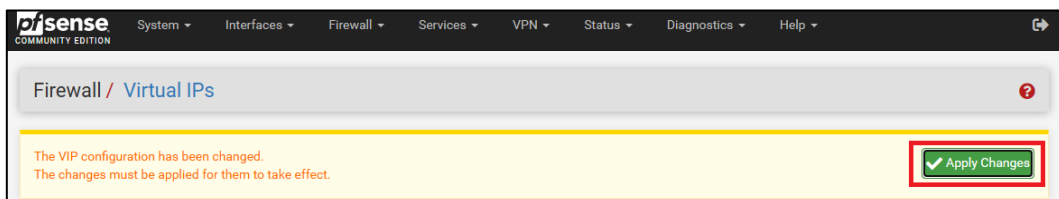
Renseigner le mot de passe à utiliser pour ce réseau virtuel



Sélectionner « **2** » pour « **VHID Group** » pour ne pas créer un conflit de groupe avec le **CARP LAN**  
Laisser « **Advertising frequency Base** » en « **1** » et mettre le « **Skew** » à « **0** »  
Cela permet de signaler que ce Pfsense a le rôle de « **master** »



Renseigner la description souhaité puis cliquer sur « **Save** »




Finaliser enfin en cliquant sur « **Apply Changes** »

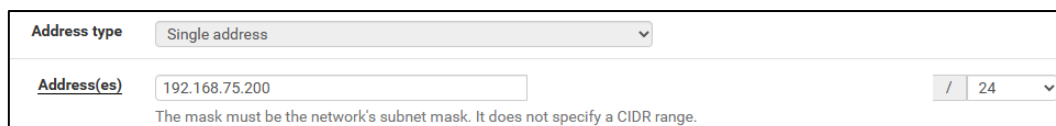
## Configuration sur le Pfsense secondaire



Sélectionner « **CARP** »



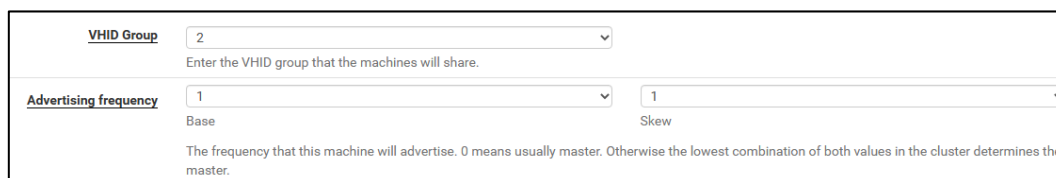
Sélectionner l'interface « **WAN** »



Renseigner l'adresse IP virtuelle à utiliser, dans notre cas « **192.168.75.200/24** »



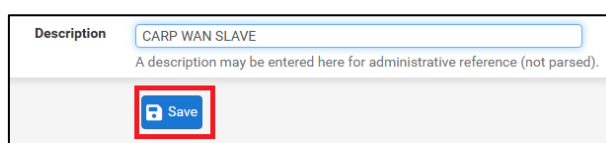
Renseigner le mot de passe à utiliser pour ce réseau virtuel



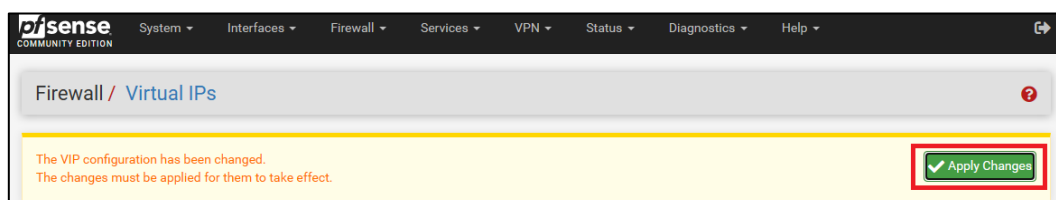
Sélectionner « **2** » pour « **VHID Group** » pour ne pas créer un conflit de groupe avec le **CARP LAN**

Laisser « **Advertising frequency Base** » en « **1** » et mettre le « **Skew** » à « **1** »

Cela permet de signaler que ce Pfsense a le rôle de « **slave** »



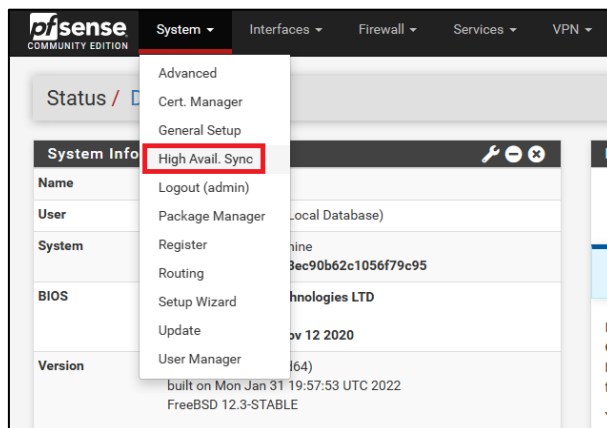
Renseigner la description souhaité puis cliquer sur « **Save** »



Finaliser enfin en cliquant sur « **Apply Changes** »



## Configuration de la redondance



Se rendre dans « **System** » puis dans « **High Avail. Sync** »

## Configuration sur le PfSense principale

State Synchronization Settings (pfsync)	
Synchronize states	<input checked="" type="checkbox"/> pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table. This setting should be enabled on all members of a failover group. Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Cocher la première case pour activer le protocole pfsync

Synchronize Interface	LAN
If Synchronize States is enabled this interface will be used for communication. It is recommended to set this to an interface other than LAN! A dedicated interface works the best. An IP must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes.	

Sélectionner l'interface « **LAN** »

pfsync Synchronize Peer IP	172.16.0.102
Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.	

Indiquer l'adresse IP de l'interface LAN du PfSense secondaire, dans notre cas : « **172.16.0.102** »

Configuration Synchronization Settings (XMLRPC Sync)	
Synchronize Config to IP	172.16.0.102
Enter the IP address of the firewall to which the selected configuration sections should be synchronized.	

Indiquer l'adresse IP de l'interface LAN du PfSense secondaire, dans notre cas : « **172.16.0.102** »

Remote System Username	admin	Enter the webConfigurator username of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and username option on backup cluster members!	
Remote System Password	*****	*****	Confirm
Enter the webConfigurator password of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and password option on backup cluster members!			

Renseigner le compte administrateur utilisé pour se connecter sur l'interface Web du PfSense secondaire

Select options to sync

☒ User manager users and groups

☒ Authentication servers (e.g. LDAP, RADIUS)

☒ Certificate Authorities, Certificates, and Certificate Revocation Lists

☒ Firewall rules

☒ Firewall schedules

☒ Firewall aliases

☒ NAT configuration

☒ IPsec configuration

☒ OpenVPN configuration (Implies CA/Cert/CRL Sync)

☒ DHCP Server settings

☒ DHCP Relay settings

☒ DHCPv6 Relay settings

☒ WoL Server settings

☒ Static Route configuration

☒ Virtual IPs

☒ Traffic Shaper configuration

☒ Traffic Shaper Limiters configuration

☒ DNS Forwarder and DNS Resolver configurations

☒ Captive Portal

☒ Toggle All

Save

Sélectionner les options à synchroniser sur le Pfsense puis terminer en cliquant sur « **Save** »

## Configuration sur le Pfsense secondaire

State Synchronization Settings (pfsync)

Synchronize states

☒ pfsync transfers state insertion, update, and deletion messages between firewalls.

Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.

This setting should be enabled on all members of a failover group.

Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Cocher la première case pour activer le protocole pfsync

Synchronize Interface

LAN

If Synchronize States is enabled this interface will be used for communication.  
It is recommended to set this to an interface other than LAN! A dedicated interface works the best.  
An IP must be defined on each machine participating in this failover group.  
An IP must be assigned to the interface on any participating sync nodes.

Sélectionner l'interface « **LAN** »

pfsync Synchronize Peer IP

172.16.0.101

Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Indiquer l'adresse IP de l'interface LAN du Pfsense secondaire, dans notre cas : « **172.16.0.101** »

**Configuration Synchronization Settings (XMLRPC Sync)**

**Synchronize Config to IP**   
Enter the IP Address of the firewall to which the selected configuration sections should be synchronized.  
XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!  
Do not use the Synchronize Config to IP and password option on backup cluster members!

**Remote System Username**   
Enter the webConfigurator username of the system entered above for synchronizing the configuration.  
Do not use the Synchronize Config to IP and username option on backup cluster members!

**Remote System Password**    
Enter the webConfigurator password of the system entered above for synchronizing the configuration.  
Do not use the Synchronize Config to IP and password option on backup cluster members!

**Synchronize admin** ☒ synchronize admin accounts and autoupdate sync password.  
By default, the admin account does not synchronize, and each node may have a different admin password.  
This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

**Select options to sync**

- ☒ User manager users and groups
- ☒ Authentication servers (e.g. LDAP, RADIUS)
- ☒ Certificate Authorities, Certificates, and Certificate Revocation Lists
- ☒ Firewall rules
- ☒ Firewall schedules
- ☒ Firewall aliases
- ☒ NAT configuration
- ☒ IPsec configuration
- ☒ OpenVPN configuration (Implies CA/Cert/CRL Sync)
- ☒ DHCP Server settings
- ☒ DHCP Relay settings
- ☒ DHCPv6 Relay settings
- ☒ WoL Server settings
- ☒ Static Route configuration
- ☒ Virtual IPs
- ☒ Traffic Shaper configuration
- ☒ Traffic Shaper Limiters configuration
- ☒ DNS Forwarder and DNS Resolver configurations
- ☒ Captive Portal

☒ Toggle All

**Save**

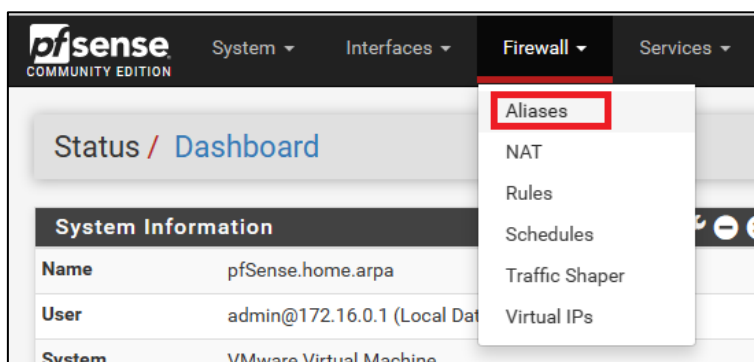
Laisser ces champs vides et cliquer sur « **Save** » pour terminer

## Autoriser la redondance

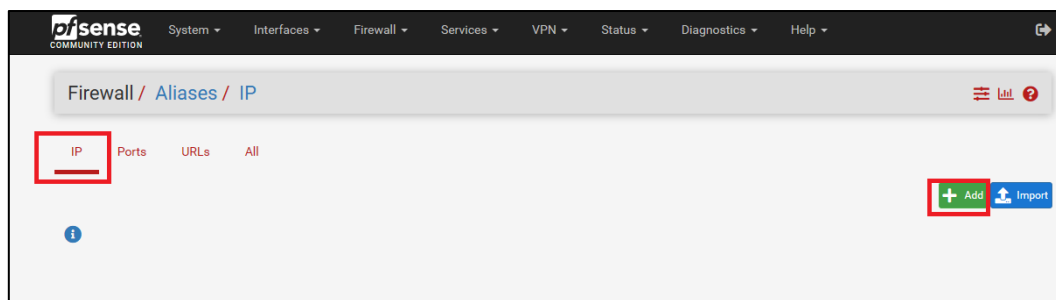
Il y a deux flux réseau à autoriser :

1. Le flux de synchronisation XML-RPC qui utilise le port 443.
2. Le flux de synchronisation du protocole pfsync.

## Création d'un alias



Aller sur « **Firewall** » puis « **Aliases** »



Cliquer « IP » puis « Add »

Name	<input type="text" value="pfsense_redondance"/>
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".	
Description	<input type="text"/>
A description may be entered here for administrative reference (not parsed).	

Indiquer le nom de l'alias et une description si vous le souhaitez

Type	<input type="text" value="Host(s)"/>
------	--------------------------------------

Sélectionner « Host(s) »

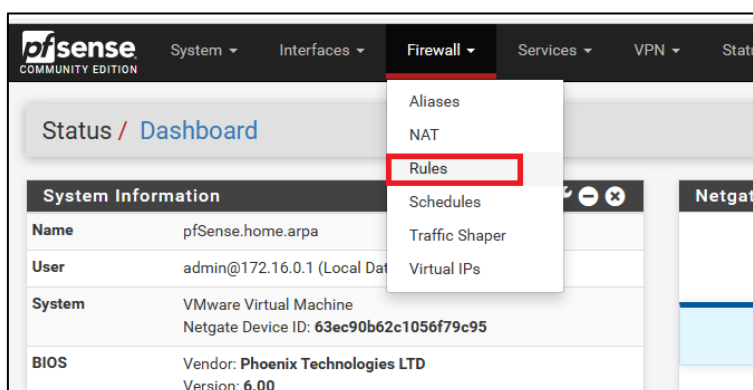
<b>Host(s)</b>			
Hint	Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.		
IP or FQDN	<input type="text" value="172.16.0.101"/>	<input type="text" value="pfsense principale"/>	<input type="button" value="Delete"/>
	<input type="text" value="172.16.0.102"/>	<input type="text" value="pfsense secondaire"/>	<input type="button" value="Delete"/>
<input type="button" value="Save"/> <input type="button" value="Export to file"/> <input type="button" value="+ Add Host"/>			

Indiquer les IP des serveurs Pfsense, pour ajouter des IP il faut cliquer sur « Add Host »  
Puis terminer en cliquant sur « Save »



Finaliser en cliquant sur « Apply Changes »

## Création des règles sur le pare feu



Se rendre dans « Firewall » puis « Rules »

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0 / 4.11 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙️
✓ 2 / 1.66 GiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	🔗 🛠️ 🗑️ 🔄
✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	🔗 🛠️ 🗑️ 🔄

⬆️ Add ⬇️ Add 🗑️ Delete 💾 Save ➕ Separator

Se rendre dans « **LAN** » puis « **Add** »

**Edit Firewall Rule**

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

**Disabled** ☐ Disable this rule  
Set this option to disable this rule without removing it from the list.

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

**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** TCP  
Choose which IP protocol this rule should match.

Dans « **Action** » sélectionner « **Pass** »  
Laisser décocher « **Disable this rule** »  
Choisir « **Lan** » dans « **Interface** »  
Sélectionner « **IPv4** » dans la section « **Address Family** »  
Puis sélectionner le protocole « **TCP** »

**Source**

**Source** ☐ Invert match Single host or alias pfsense\_redondance /

⚙️ Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Sélectionner la source « **Single host or alias** » et écrire le nom de l'alias

**Destination**

**Destination** ☐ Invert match This firewall (self) Destination Address /

**Destination Port Range** HTTPS (443) From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

En Destination sélectionner « **This firewall (self)** » et sélectionner uniquement le port 443

**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** Autorisation flux XML-RPC  
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

Renseigner une description puis cliquer sur « **Save** »

The alias list has been changed.  
The changes must be applied for them to take effect.

✓ Apply Changes

Finaliser en cliquant sur « **Apply Changes** »

Floating WAN LAN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 4 / 4.19 MIB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙️
✓ 0 / 0 B	IPv4 TCP	pfSense_ redondance	*	This Firewall	443 (HTTPS)	*	none		Autorisation flux XML-RPC	🔗 ⚙️ 📄 🗑️
✓ 5 / 1.66 GIB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	🔗 ⚙️ 📄 🗑️
✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	🔗 ⚙️ 📄 🗑️

⬆️ Add ⬇️ Add 🗑️ Delete 💾 Save ➕ Separator

Cliquer à nouveau sur « **Add** »

Edit Firewall Rule

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

**Disabled** ☐ Disable this rule  
Set this option to disable this rule without removing it from the list.

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

**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** PFSYNC  
Choose which IP protocol this rule should match.

Dans « **Action** » sélectionner « **Pass** »  
Laisser décocher « **Disable this rule** »  
Choisir « **Lan** » dans « **Interface** »  
Sélectionner « **IPv4** » dans la section « **Address Family** »  
Puis sélectionner le protocole « **PFSYNC** »

Source

**Source** ☐ Invert match Single host or alias pfSense\_redondance /

Sélectionner la source « **Single host or alias** » et écrire le nom de l'alias

Destination

**Destination** ☐ Invert match This firewall (self) Destination Address /

En Destination sélectionner « **This firewall (self)** »

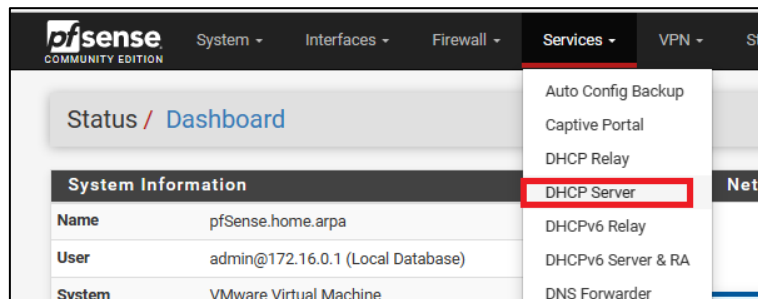
Extra Options	
<b>Log</b>	<input type="checkbox"/> Log packets that are handled by this rule <small>Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the <a href="#">Status: System Logs: Settings</a> page).</small>
<b>Description</b>	<input type="text" value="Autorisation flux pfsync"/> <small>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.</small>
<b>Advanced Options</b>	<input checked="" type="checkbox"/> Display Advanced
<input checked="" type="button" value="Save"/>	

Renseigner une description puis cliquer sur « **Save** »

<small>The alias list has been changed. The changes must be applied for them to take effect.</small>	<input checked="" type="button" value="Apply Changes"/>
--	---

Finaliser en cliquant sur « **Apply Changes** »

## Configuration du DHCP



Se rendre dans « **Services** » et « **DHCP Server** »

Services / DHCP Server / LAN	
<b>WAN</b>	<b>LAN</b>
<b>General Options</b>	
<b>Enable</b>	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
<b>BOOTP</b>	<input type="checkbox"/> Ignore BOOTP queries
<b>Deny unknown clients</b>	<input type="text" value="Allow all clients"/> <small>When set to <b>Allow all clients</b>, any DHCP client will get an IP address within this scope/range on this interface. If set to <b>Allow known clients from any interface</b>, any DHCP client with a MAC address listed on <b>any</b> scope(s)/interface(s) will get an IP address. If set to <b>Allow known clients from only this interface</b>, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.</small>
<b>Ignore denied clients</b>	<input type="checkbox"/> Denied clients will be ignored rather than rejected. <small>This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.</small>
<b>Ignore client identifiers</b>	<input type="checkbox"/> If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease. <small>This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.</small>
<b>Subnet</b>	172.16.0.0
<b>Subnet mask</b>	255.255.0.0
<b>Available range</b>	172.16.0.1 - 172.16.255.254
<b>Range</b>	<input type="text" value="172.16.0.10"/> <input type="text" value="172.16.0.50"/> <small>From To</small>

Se positionner dans l'onglet « **LAN** »  
Indiquer l'étendue d'adresse IP dans « **Range** »  
Laisser le reste des options par défaut

Additional Pools							
<div>Add <a href="#">+ Add pool</a></div> <p>If additional pools of addresses are needed inside of this subnet outside the above Range, they may be specified here.</p> <table><thead><tr><th>Pool Start</th><th>Pool End</th><th>Description</th><th>Actions</th></tr></thead><tbody></tbody></table>				Pool Start	Pool End	Description	Actions
Pool Start	Pool End	Description	Actions				

*Vous pouvez ajouter des pools d'adresses ici en cliquant sur « **Add Pool** »  
Nous ne l'utiliserons pas*

Servers	
WINS servers	WINS Server 1
	WINS Server 2
DNS servers	1.1.1.1
	1.0.0.1
	DNS Server 3
	DNS Server 4
Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.	

*Indiquer dans « **Servers** » les serveurs WINS et DNS à utiliser  
Dans notre cas nous utilisons les DNS de Cloudflare donc « **1.1.1.1** » et « **1.0.0.1** »*

OMAPI	
OMAPI Port	OMAPI Port Set the port that OMAPI will listen on. The default port is 7911, leave blank to disable. Only the first OMAPI configuration is used.
OMAPI Key	OMAPI Key Enter a key matching the selected algorithm to secure connections to the OMAPI endpoint. <input type="checkbox"/> Generate New Key Generate a new key based on the selected algorithm.
Key Algorithm	HMAC-SHA256 (current bind9 default) Set the algorithm that OMAPI key will use.

*Nous n'utiliserons pas OMAPI, laisser vide par défaut*



### Other Options

**Gateway**


The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.

**Domain name**


The default is to use the domain name of this system as the default domain name provided by DHCP. An alternate domain name may be specified here.

**Domain search list**


The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.

**Default lease time**


This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.

**Maximum lease time**


This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.

**Failover peer IP**


Leave blank to disable. Enter the interface IP address of the other machine. Machines must be using CARP. Interface's advskew determines whether the DHCPd process is Primary or Secondary. Ensure one machine's advskew < 20 (and the other is > 20).

**Static ARP**
☐ Enable Static ARP entries
 

This option persists even if DHCP server is disabled. Only the machines listed below will be able to communicate with the firewall on this interface.

**Time format change**
☐ Change DHCP display lease time from UTC to local time
 

By default DHCP leases are displayed in UTC time. By checking this box DHCP lease time will be displayed in local time and set to the time zone selected. This will be used for all DHCP interfaces lease time.

**Statistics graphs**
☐ Enable RRD statistics graphs
 

Enable this to add DHCP leases statistics to the RRD graphs. Disabled by default.

**Ping check**
☐ Disable ping check
 

When enabled dhcpd sends a ping to the address being assigned, and if no response has been heard, it assigns the address. Enabled by default.

**Dynamic DNS**

**MAC address control**

**NTP**

**TFTP**

**LDAP**

**Network Booting**

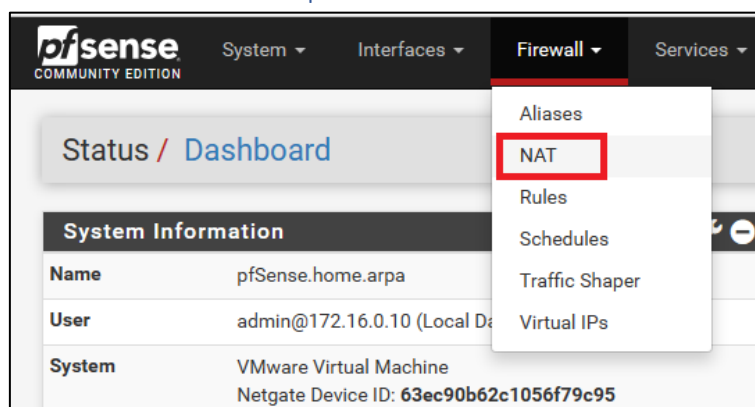
**Additional BOOTP/DHCP Options**

#### DHCP Static Mappings for this Interface

Static ARP	MAC address	IP address	Hostname	Description
<input type="button" value="+ Add"/>				

Dans « **Gateway** » indiquer l'adresse IP virtuelle utilisé par l'interface LAN, dans notre cas : « **172.16.0.100** »  
Laisser le reste par défaut ou configurer à sa convenance et terminer en cliquant sur « **Save** »

## Configuration de l'adresse IP virtuelle pour le trafic sortant



Se rendre dans « **Firewall** » puis « **NAT** »

Firewall / NAT / Outbound

Port Forward 1:1 **Outbound** NPt

**Outbound NAT Mode**

Mode

- ☐ Automatic outbound NAT rule generation. (IPsec passthrough included)
- ☒ **Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)**
- ☐ Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
- ☐ Disable Outbound NAT rule generation. (No Outbound NAT rules)

**Save**

Se positionner sur l'onglet « **Outbound** »  
Puis sélectionner « **Hybrid Outbound NAT rule generation** »  
Sauvegarder en cliquant sur « **Save** »

Mappings

<input type="checkbox"/>	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<b>Add</b>	<b>Add</b>	<b>Delete</b>	<b>Save</b>							

Cliquer ensuite sur « **Add** »

**Edit Advanced Outbound NAT Entry**

**Disabled** ☐ Disable this rule

**Do not NAT** ☐ Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules. In most cases this option is not required.

**Interface** **WAN**  
The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.

Sélectionner l'interface dans « **Interface** » et choisir « **WAN** »

**Address Family** **IPv4**  
Select the Internet Protocol version this rule applies to.

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

Choisir « **IPv4** » dans « **Address Family** »  
Choisir « **Any** » dans « **Protocol** »

**Source** **Network** **172.16.0.0 / 16**  
Type Source network for the outbound NAT mapping. Port or Range

**Destination** **Any** **/ 24**  
Type Destination network for the outbound NAT mapping. Port or Range

☐ Not  
Invert the sense of the destination match.

Indiquer le reseau source dans « **Source** » dans notre cas « **172.16.0.0/16** »  
En « **Destination** » sélectionner « **Any** »

**Translation**

**Address** 192.168.75.200 (CARP WAN)  
Connections matching this rule will be mapped to the specified Address.  
The Address can be an Interface, a Host-type Alias, or a Virtual IP address.

**Port or Range**  
Enter the external source Port or Range used for remapping the original source port on connections matching the rule.  
Port ranges are a low port and high port number separated by "-".  
Leave blank when Static Port is checked.

☐ Static Port

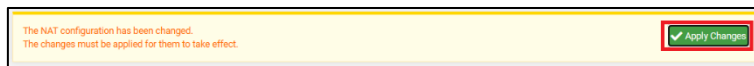
**Misc**

**No XMLRPC Sync** ☐  
Prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

**Description** Utilisation de l'adresse IP virtuelle pour le trafic sortant  
A description may be entered here for administrative reference (not parsed).

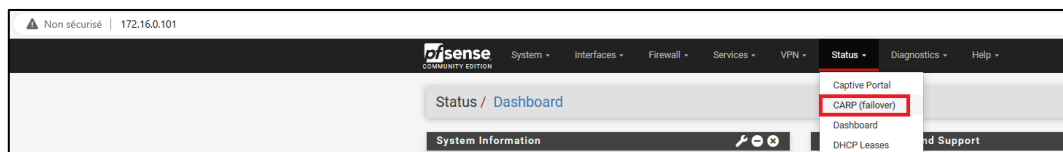
**Save**

Indiquer l'adresse IP virtuelle à utiliser dans « **Address** »  
Renseigner une description dans « **Description** »  
Terminer en cliquant sur « **Save** »

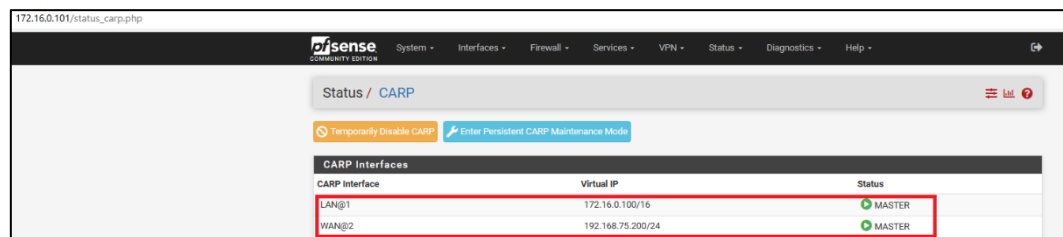


Appliquer la configuration en cliquant sur « **Apply Changes** »

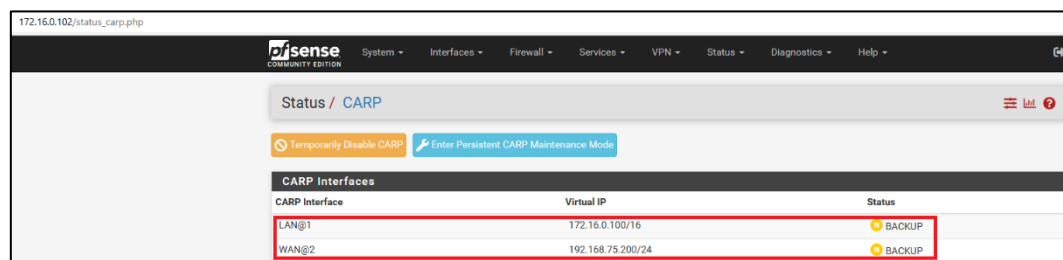
## Vérification de la configuration de la redondance



Se rendre dans « **Status** » puis « **CARP (failover)** »

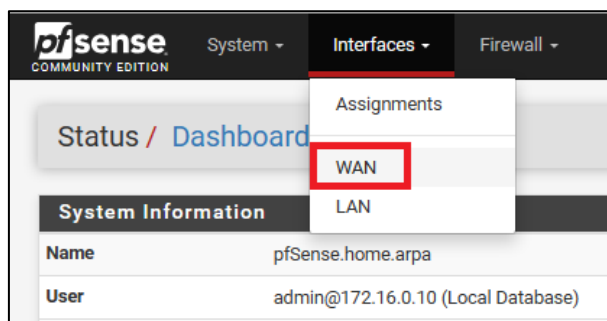


On peut voir que le pfSense principal est bien considéré comme MASTER



Le pfSense secondaire est bien en BACKUP

## Règles de filtrage



Se rendre dans « **Interfaces** » puis « **WAN** »

**General Configuration**

Enable ☒ Enable interface

**Description**   
Enter a description (name) for the interface here.

**IPv4 Configuration Type**

**IPv6 Configuration Type**

**MAC Address**   
This field can be used to modify ("spoof") the MAC address of this interface.  
Enter a MAC address in the following format: xxxxxxxxxx or leave blank.

**MTU**   
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

**MSS**   
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

**Speed and Duplex**   
Explicitly set speed and duplex mode for this interface.  
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

**Static IPv4 Configuration**

**IPv4 Address**  /

**IPv4 Upstream gateway**  [+ Add a new gateway](#)  
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.  
On local area network interfaces the upstream gateway should be "none".  
Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).  
Gateways can be managed by [clicking here](#).

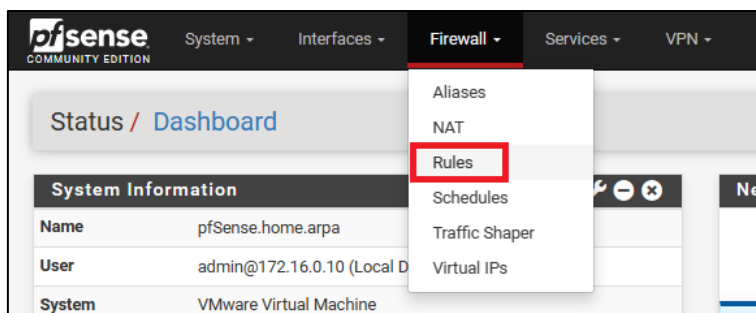
**Reserved Networks**

**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.

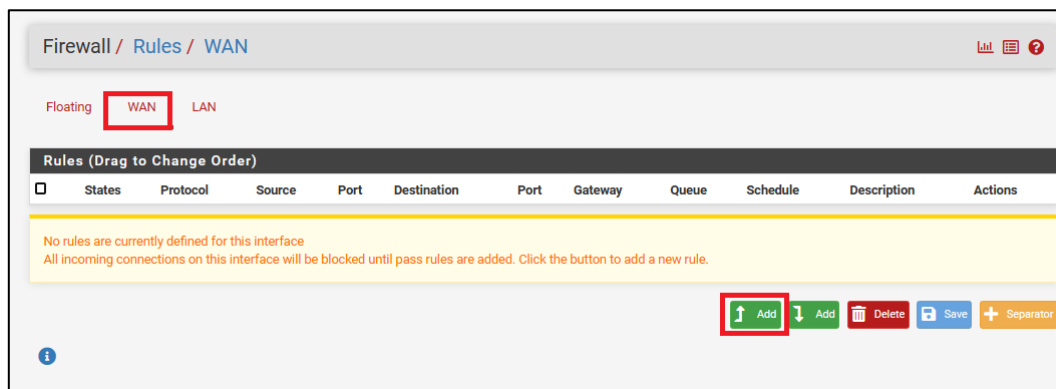
**Block bogon networks** ☐  
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.  
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.  
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

[Save](#)

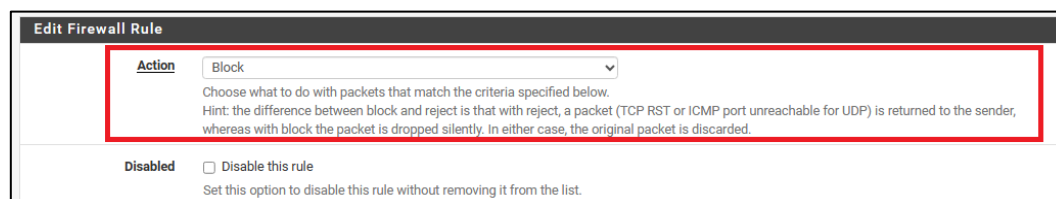
Décocher les 2 dernières cases puis faire « **Save** »  
La configuration est à faire sur les 2 pfsenses



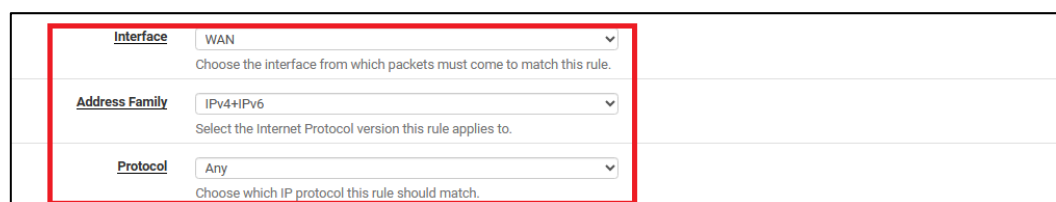
Se rendre ensuite dans « **Firewall** » puis « **Rules** »



Se mettre sur l'onglet « **WAN** » et cliquer sur « **Add** »



Dans « **Action** » choisir « **Block** »  
Ne pas cocher la case « **Disabled** »



Dans « **Interface** » choisir « **WAN** »  
Choisir « **IPv4+IPv6** » dans « **Address Family** »  
Choisir « **Any** » dans « **Protocol** »

<b>Source</b>	
Source <input type="checkbox"/> Invert match any	Source Address /
<b>Destination</b>	
Destination <input type="checkbox"/> Invert match any	Destination Address /
<b>Extra Options</b>	
<b>Log</b> <input type="checkbox"/> Log packets that are handled by this rule <small>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).</small>	
<b>Description</b> Blocage total <small>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.</small>	
<b>Advanced Options</b> <input type="button" value="Display Advanced"/>	
<input type="button" value="Save"/>	

Dans « **Source** » et « **Destination** » sélectionner « **Any** »  
Renseigner une description  
Finaliser en cliquant sur « **Save** »

The firewall rule configuration has been changed. The changes must be applied for them to take effect.	<input type="button" value="✓ Apply Changes"/>
---	--

On termine en cliquant sur « **Apply Changes** »