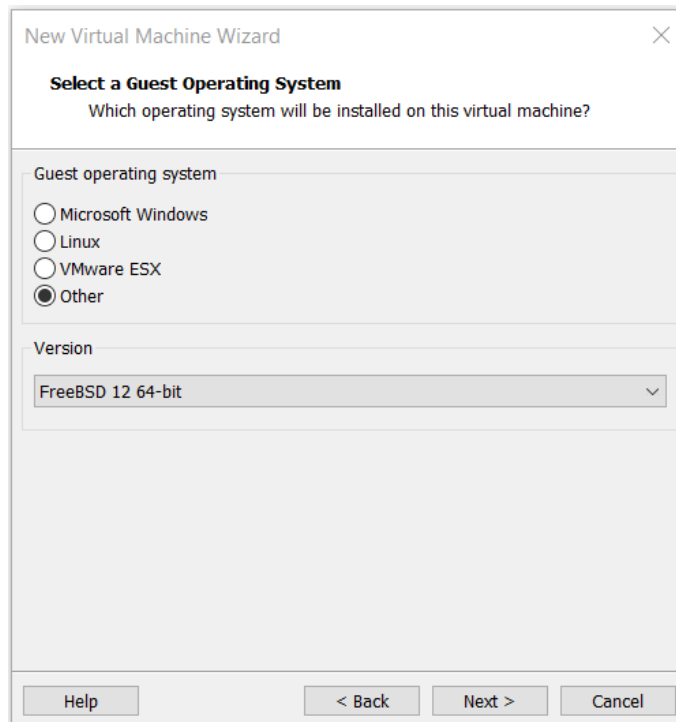


# Installation et configuration de Pfsense



## I. Paramétrages de la VM Pfsense

Lors de la création de la VM pour installer Pfsense, il est primordial de choisir le système d'exploitation suivant :



New Virtual Machine Wizard

**Select a Guest Operating System**  
Which operating system will be installed on this virtual machine?

Guest operating system

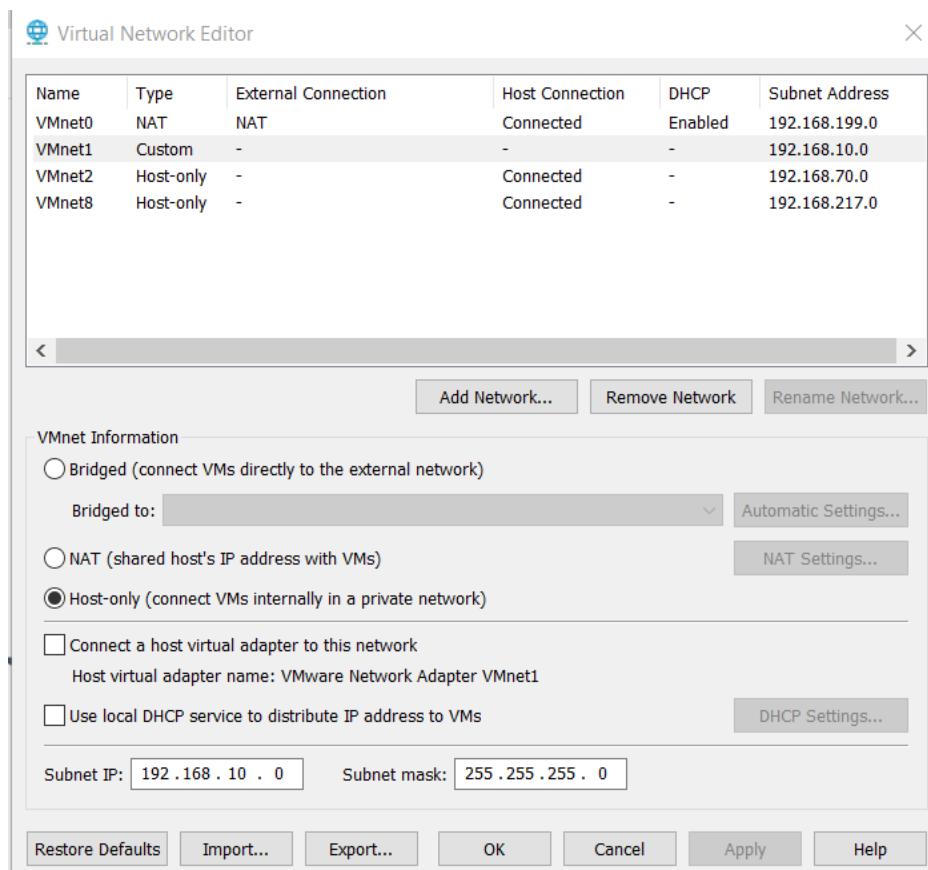
☐ Microsoft Windows  
☐ Linux  
☐ VMware ESX  
☒ Other

Version

FreeBSD 12 64-bit

Help < Back Next > Cancel

Et de paramétrer le réseau de cette façon : une carte en NAT et l'autre en Custom. Celle en custom sera réutilisée pour la carte réseau de la VM de Windows pro.



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	NAT	NAT	Connected	Enabled	192.168.199.0
VMnet1	Custom	-	-	-	192.168.10.0
VMnet2	Host-only	-	Connected	-	192.168.70.0
VMnet8	Host-only	-	Connected	-	192.168.217.0

Add Network... Remove Network Rename Network...

VMnet Information

☐ Bridged (connect VMs directly to the external network)  
 Bridged to:  Automatic Settings...

☐ NAT (shared host's IP address with VMs) NAT Settings...

☒ Host-only (connect VMs internally in a private network)

☐ Connect a host virtual adapter to this network  
 Host virtual adapter name: VMware Network Adapter VMnet1

☐ Use local DHCP service to distribute IP address to VMs DHCP Settings...

Subnet IP:  Subnet mask:

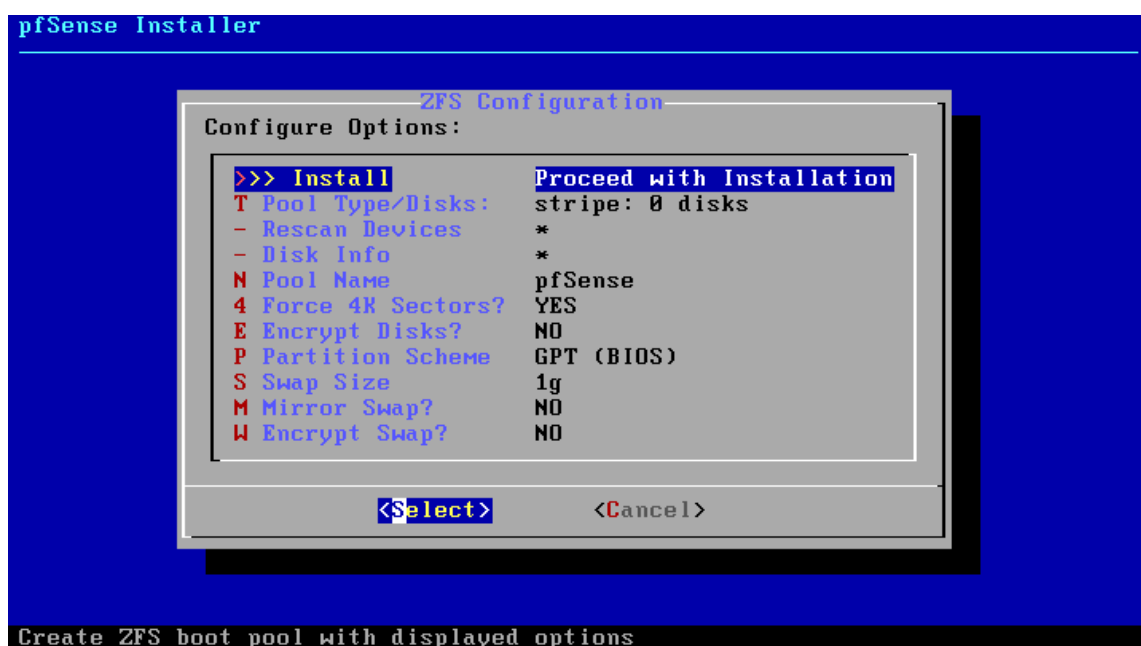
Restore Defaults Import... Export... OK Cancel Apply Help

## II. Installation de Pfsense

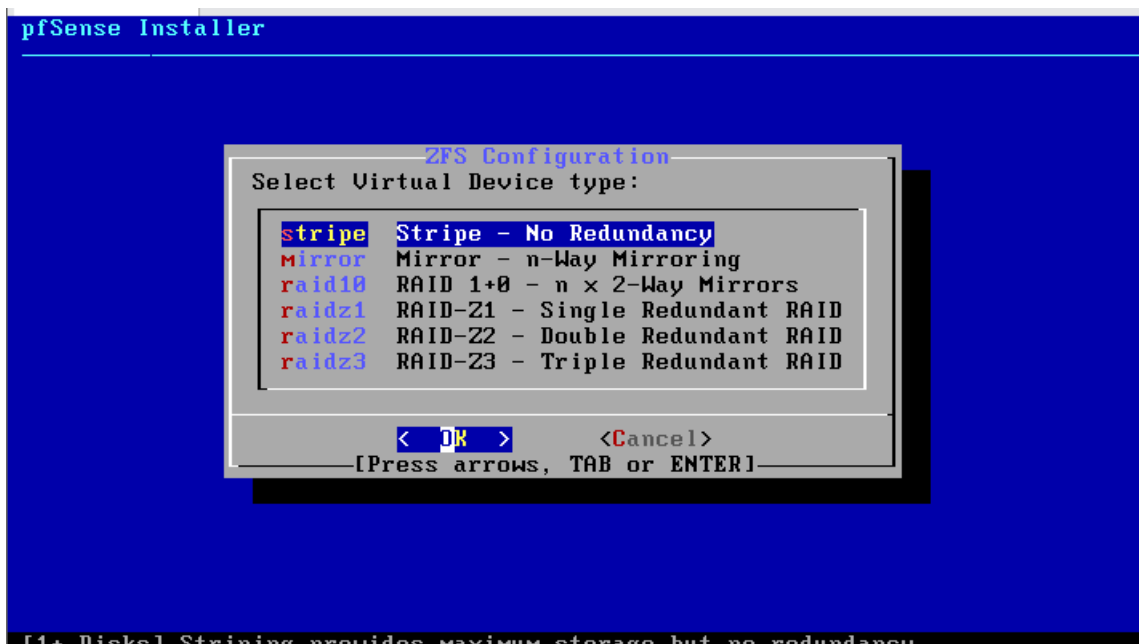
Pour pouvoir installer Pfsense, il faut dans un premier temps lui indiquer comment on souhaite partitionner le disque. Ici, nous choisissons la première option qui est une partition automatique.



Ensuite, on vérifie les paramètres de la configuration de la partition choisie et on fait « entrée » sur « Install »



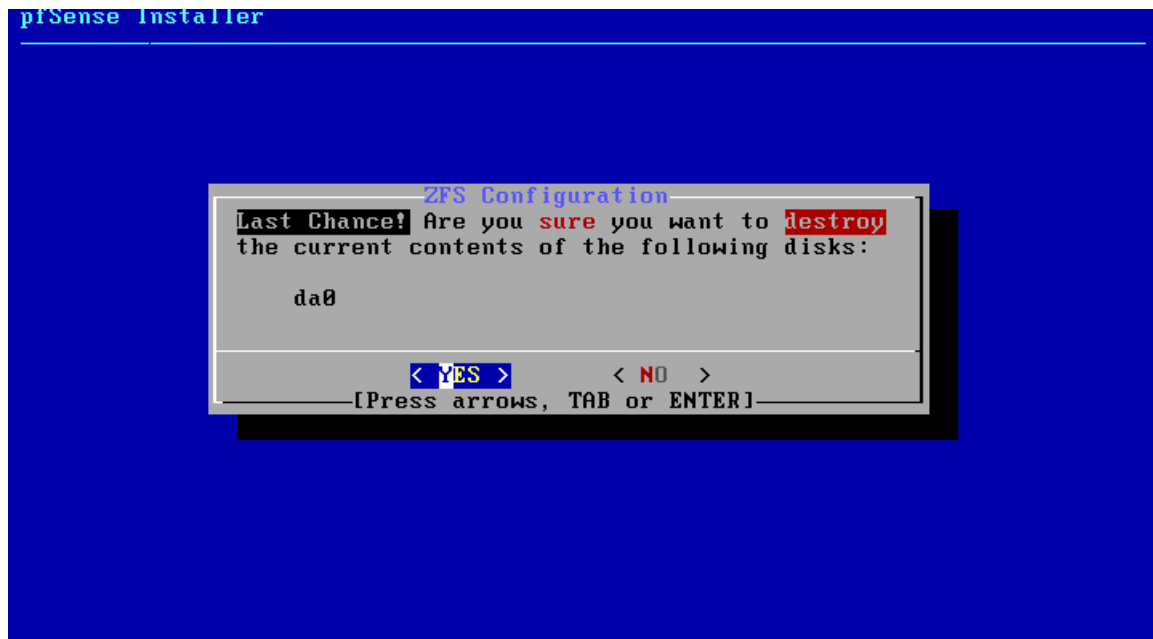
Puis on sélectionne le disque virtuel, ici on prend la première « stripe » qui est sans redondance. Il n'y a donc pas de RAID.



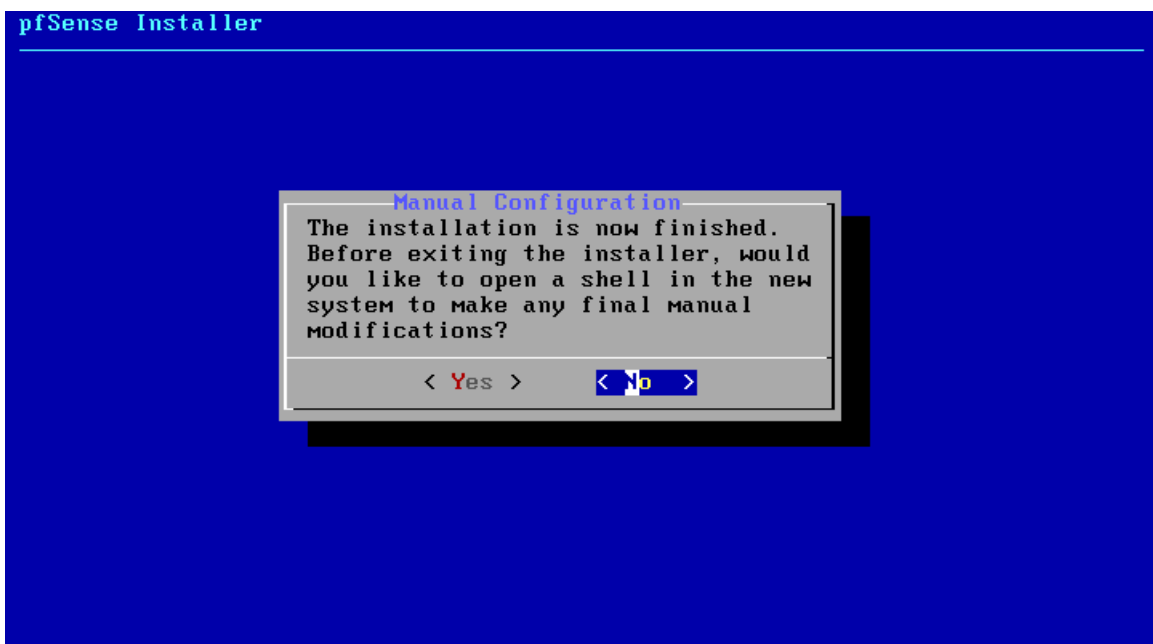
Etant sur une machine virtuelle, il me propose le disque virtuel de celui-ci :



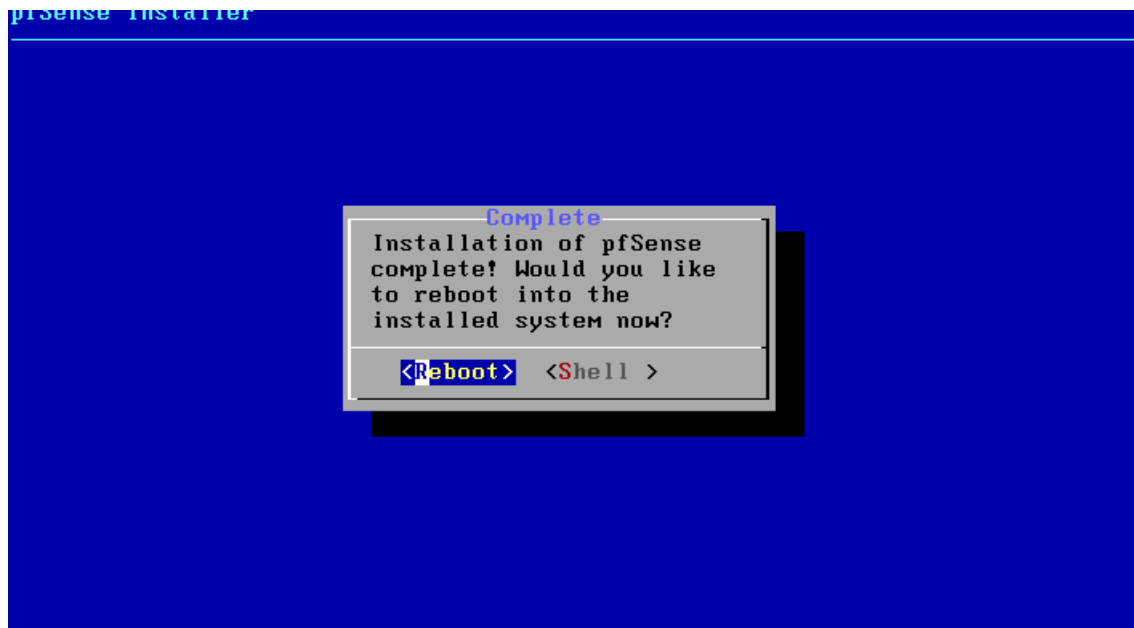
On nous demande ensuite si on est sûr de vouloir faire l'installation sur ce disque au risque de supprimer les données déjà présentes. Si vous n'avez pas de données alors vous pouvez cliquer sur « YES » :



Une fois l'installation finie, il nous propose d'ouvrir une ligne de commande pour terminer des paramètres manuellement. On dit tout simplement « No » puisque nous pourrions faire des modifications lorsqu'il redémarrera



On nous informe que l'installation est complète et on nous demande si on souhaite redémarrer le système : on clique sur « Reboot »



#### a. Paramétrage de l'adresse réseau

Une fois que le système a redémarré, l'interface suivant apparaît avec plusieurs fonctions :

```
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.arp) (ttyv0)
VMware Virtual Machine - Netgate Device ID: 33ba400d4ead543a5b17

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.199.128/24
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: █
```

Pour configurer l'adresse réseau, il suffit de taper l'option 2 :

```
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.arp) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 33ba400d4ead543a5b17

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.199.128/24
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
```

Ce qui fait apparaître les deux cartes réseaux disponibles sur la machine, une WAN et une LAN. Chacune à une adresse IP par défaut que nous allons modifier.

```
VMware Virtual Machine - Netgate Device ID: 33ba400d4ead543a5b17

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.199.128/24
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: 
```

:

Ici on nous indique qu'il faut qu'on choisisse quelle carte modifier. On a pas besoin de modifier la carte 1 ou WAN mais la carte 2, la LAN.

```
VMware Virtual Machine - Netgate Device ID: 33ba400d4ead543a5b17
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.199.128/24
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
```

Après l'interface à configurer choisie, on informe l'adresse qu'on souhaite que la machine dispose :

```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.199.128/24
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:
> 192.168.10.254
```



Ensuite on indique le masque de sous réseau, on a choisi le /24 :

```
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:
> 192.168.10.254

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):
> 24
```

En tapant sur « entrée », il nous propose deux options de paramétrages d'adresses, on tape sur « entrée » pour ignorer. Ensuite, il nous demande si nous souhaitons activer le serveur DHCP, nous lui indiquons « non »

```
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:
> 192.168.10.254

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):
> 24

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

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

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

```
Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
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...

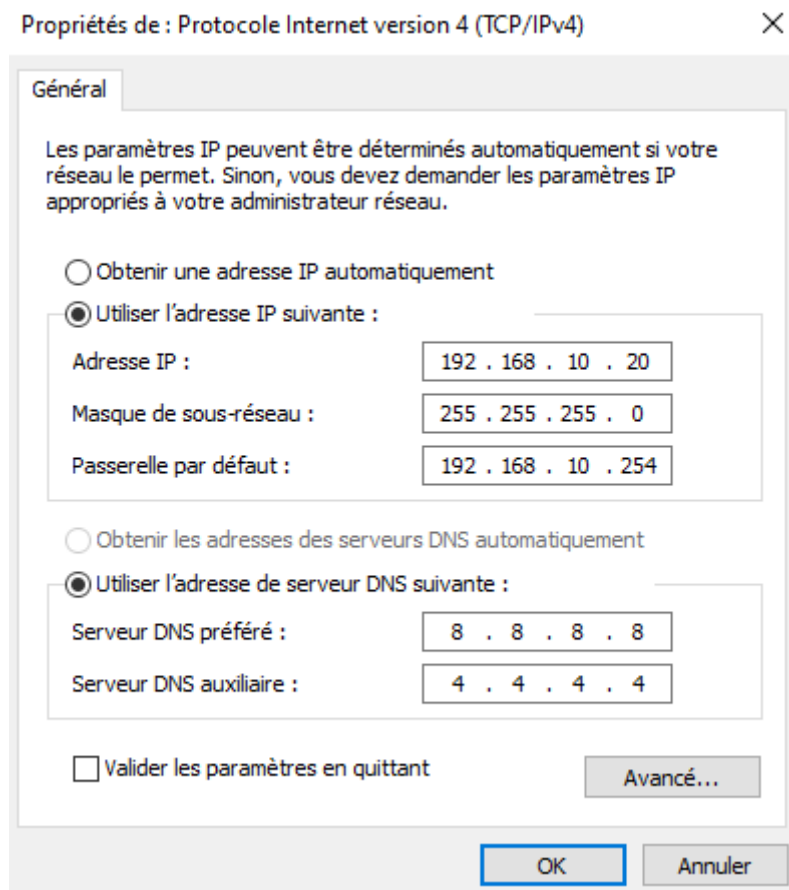
The IPv4 LAN address has been set to 192.168.10.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    http://192.168.10.254/

Press <ENTER> to continue.
```

### III. Paramétrage de la carte réseau du PC Windows

Nous paramétrons la carte de avec une adresse fixe :

- 192.168.10.20 puisque mon réseau est 192.168.10.0
- 255.255.255.0 puisque sur le serveur PfSense nous avons renseigné le masque en /24
- 192.168.10.254 car c'est notre serveur PfSense qui nous permet de nous connecter à Internet grâce à la seconde carte réseau en NAT



Je teste pour voir si nous arrivons à pinger google, si oui cela veut dire qu'on a accès à internet :

```
C:\Users\Client1>ping 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=10 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=11 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=10 ms TTL=127
Réponse de 8.8.8.8 : octets=32 temps=10 ms TTL=127
```

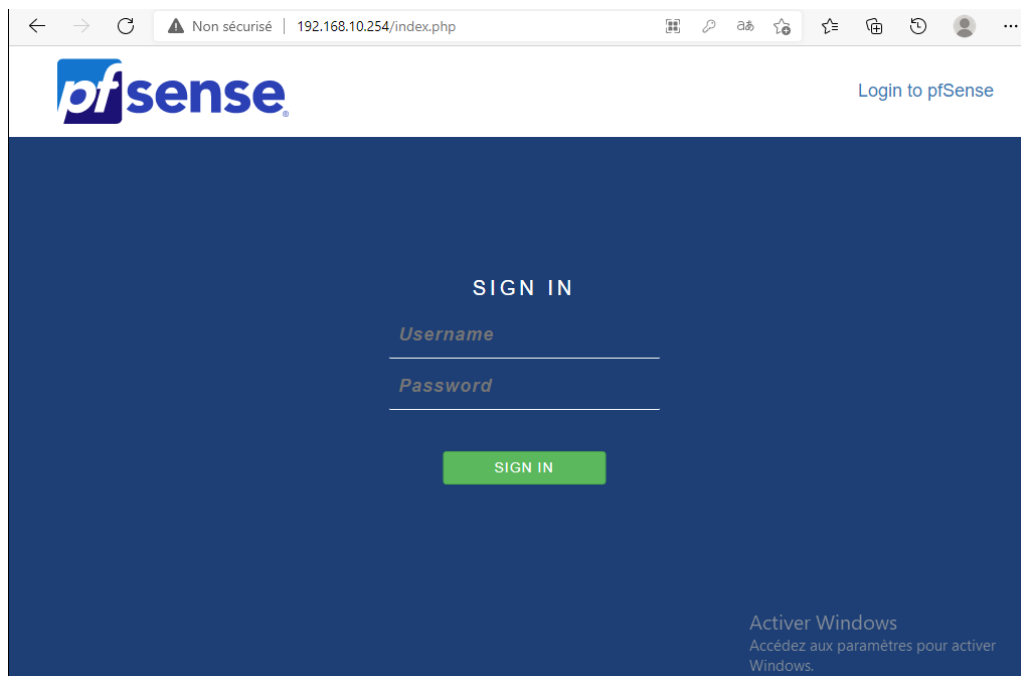
Cela fonctionne aussi si je teste ma passerelle alias mon serveur :

```
C:\Users\Client1>ping 192.168.10.254

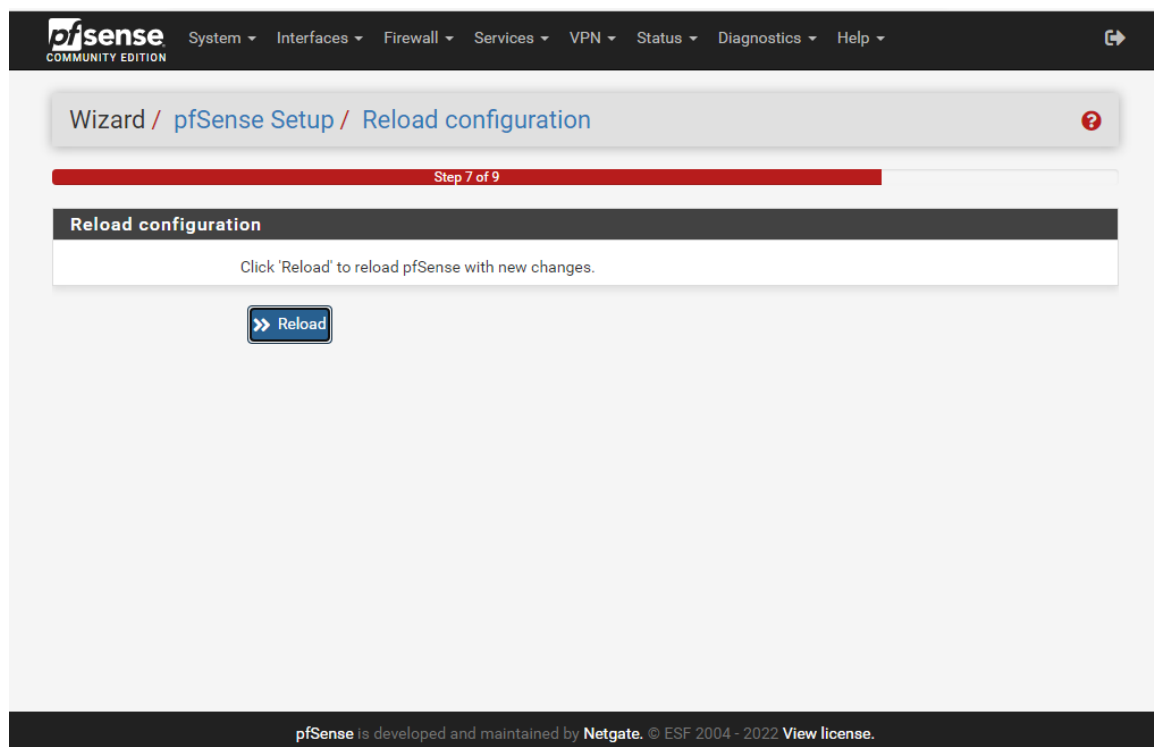
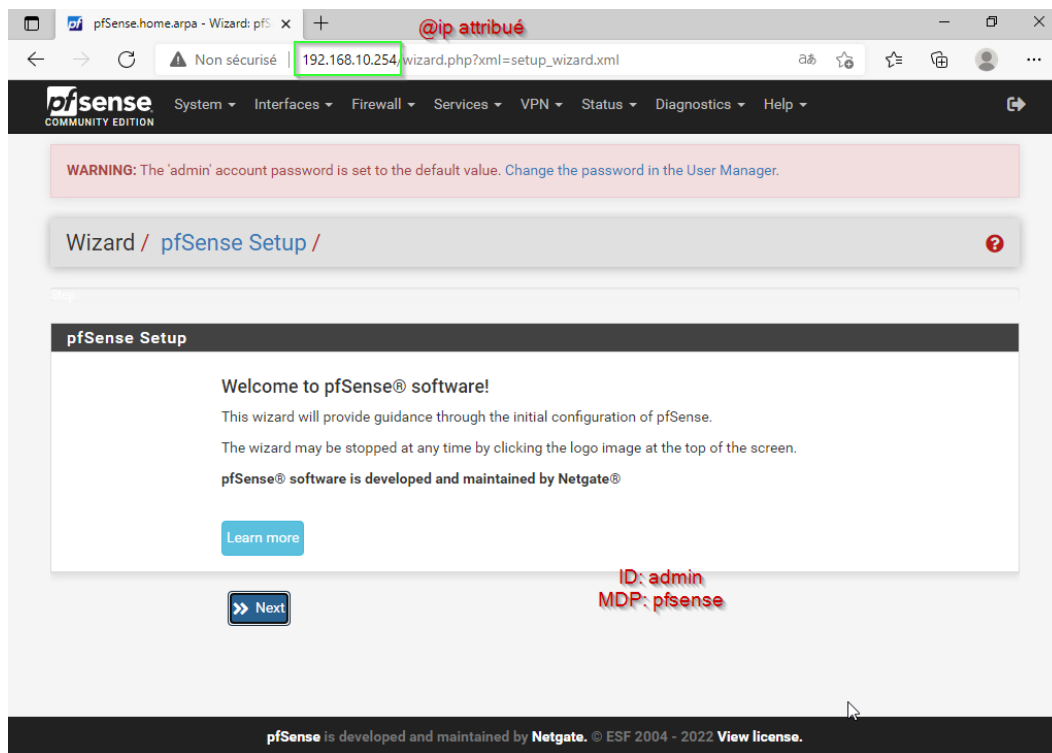
Envoi d'une requête 'Ping' 192.168.10.254 avec 32 octets de données :
Réponse de 192.168.10.254 : octets=32 temps<1ms TTL=64
Réponse de 192.168.10.254 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.10.254 : octets=32 temps=1 ms TTL=64
Réponse de 192.168.10.254 : octets=32 temps=1 ms TTL=64
```

## IV. Configuration de Pfsense

Le serveur qui détient Pfsense est enfin prêt, on peut aller sur le poste client et taper l'adresse IP renseigné à l'étape précédente. Vous arriverez sur cette page :



Reste plus qu'à indiquer l'identifiant (admin) et le mot de passe (pfsense) qui sont par défaut et vous vous connecterez sur le site de configuration de Pfsense.



On clique sur suivant jusqu'à atterrir sur cette page où on configure le nom de l'hôte, le domain, etc..

The screenshot shows the pfSense Community Edition interface. At the top, there's a navigation bar with links like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below this is a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The main heading is "Wizard / pfSense Setup / General Information". A red progress bar indicates "Step 2 of 9". The section is titled "General Information" and contains the following fields:

- Hostname:** A text box containing "pfSense". Below it, an example is given: "EXAMPLE: myserver".
- Domain:** A text box containing "home.arpa". Below it, an example is given: "EXAMPLE: mydomain.com".
- Primary DNS Server:** An empty text box.
- Secondary DNS Server:** An empty text box.
- Override DNS:** A checkbox that is checked.

Below the fields, there is a paragraph of text: "On this screen the general pfSense parameters will be set." and "The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query to servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver to enable DNS Query Forwarding after completing the wizard."

On active le DHCP via la page internet.

The screenshot shows the pfSense Community Edition interface. At the top, there's a navigation bar with links like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below this is a heading "Services / DHCP Server / LAN". The section is titled "General Options" and contains the following fields:

- Enable:** A checkbox that is checked, with the label "Enable DHCP server on LAN interface".
- BOOTP:** A checkbox labeled "Ignore BOOTP queries" which is unchecked.
- Deny unknown clients:** A dropdown menu set to "Allow all clients". Below it, a paragraph of text explains the options: "When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range."
- Ignore denied clients:** A checkbox labeled "Denied clients will be ignored rather than rejected." which is unchecked. Below it, a paragraph of text explains: "This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured."
- Ignore client identifiers:** A checkbox labeled "If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease." which is unchecked. Below it, a paragraph of text explains: "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."
- Subnet:** A text box containing "192.168.10.0".

L'interface WAN disposera du DHCP :

**pfSense**  
COMMUNITY EDITION

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

⌂

**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / **pfSense Setup** / **Configure WAN Interface** ?

Step 4 of 9

**Configure WAN Interface**

On this screen the Wide Area Network information will be configured.

**SelectedType** DHCP ▾

**General configuration**

**MAC Address**   
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

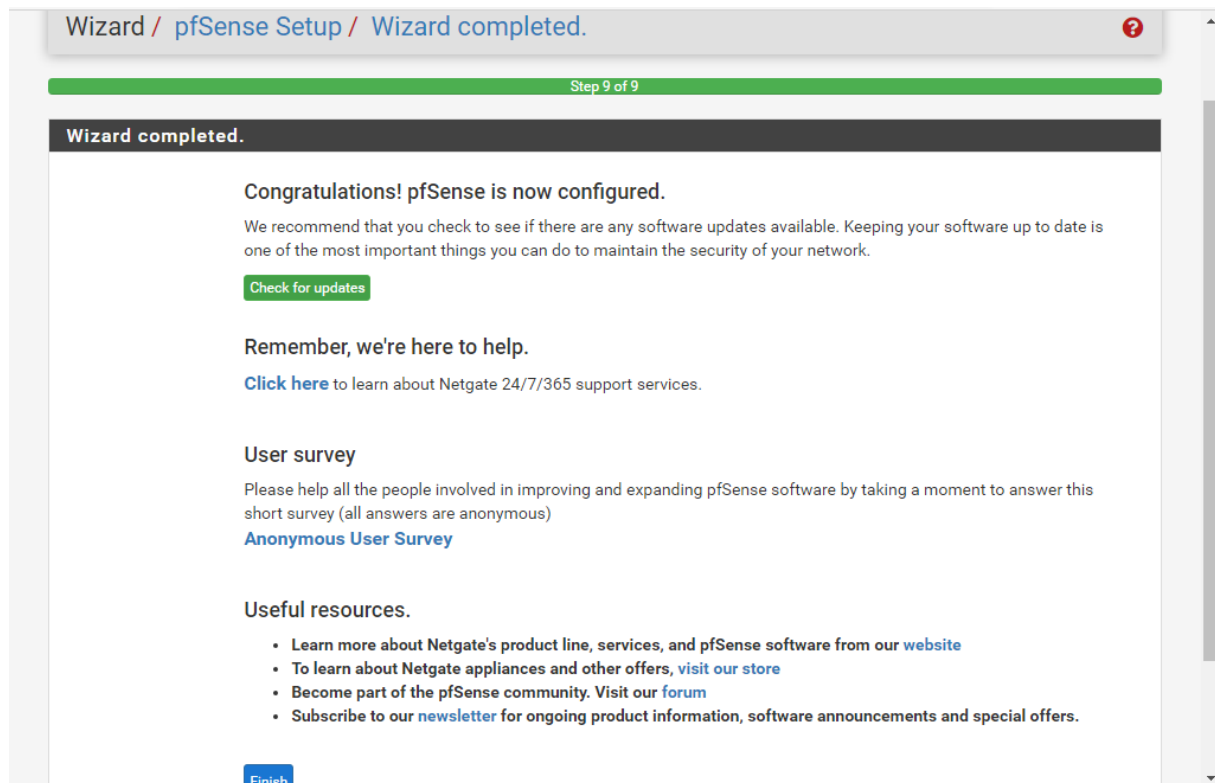
**MTU**   
Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

**MSS**   
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

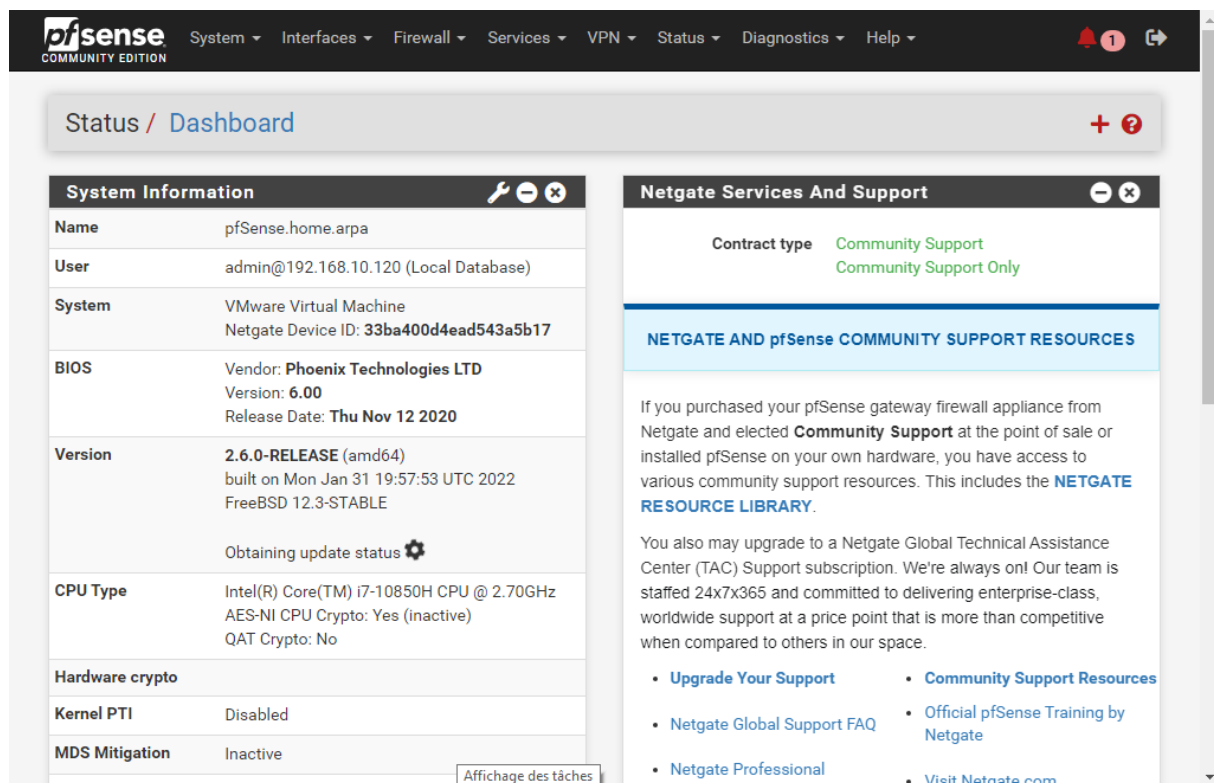
mercredi 1 juin 2022 ▾

DOBLER Tiffany

Ensuite le paramétrage sera complété :



Voici l'interface de base :



## a. Activation du protocole HTTP

pfSense COMMUNITY EDITION

System / Advanced / Admin Access

Admin Access Firewall & NAT Networking Miscellaneous System Tunables Notifications

**webConfigurator**

Protocol ☒ HTTP ☐ HTTPS (SSL/TLS)

TCP port   
Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.

Max Processes   
Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.

WebGUI redirect ☐ Disable webConfigurator redirect rule  
When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the listening port configured. Check this box to disable this automatically added redirect rule.

OCSP Must-Staple ☐ Force OCSP Stapling in nginx  
When this is checked, OCSP Stapling is forced on in nginx. Remember to upload your certificate as a full chain, not just the certificate, or this option will be ignored by nginx.

## b. Activation du port SSH

Secure Shell Server ☒ Enable Secure Shell

SSHd Key Only   
When set to *Public Key Only*, SSH access requires authorized keys and these keys must be configured for each user that has been granted secure shell access. If set to *Require Both Password and Public Key*, the SSH daemon requires both authorized keys and valid passwords to gain access. The default *Password or Public Key* setting allows either a valid password or a valid authorized key to login.

Allow Agent Forwarding ☐ Enables ssh-agent forwarding support.

SSH port   
Note: Leave this blank for the default of 22.

**Login Protection**

Threshold   
Block attackers when their cumulative attack score exceeds threshold. Most attacks have a score of 10.

Blocktime   
Block attackers for initially blocktime seconds after exceeding threshold. Subsequent blocks increase by a factor of 1.5. Attacks are unblocked at random intervals, so actual block times will be longer.

Detection time   
Remember potential attackers for up to detection\_time seconds before resetting their score.

Pass list  /   
Addresses added to the pass list will bypass login protection.

Add address

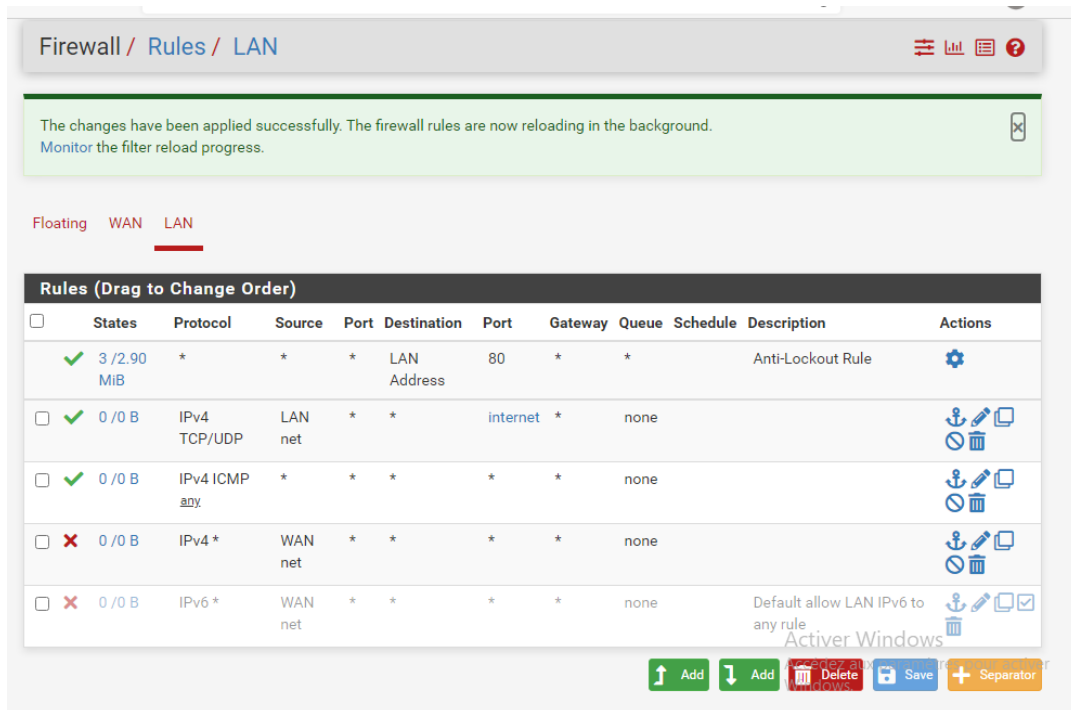
si connexion distance



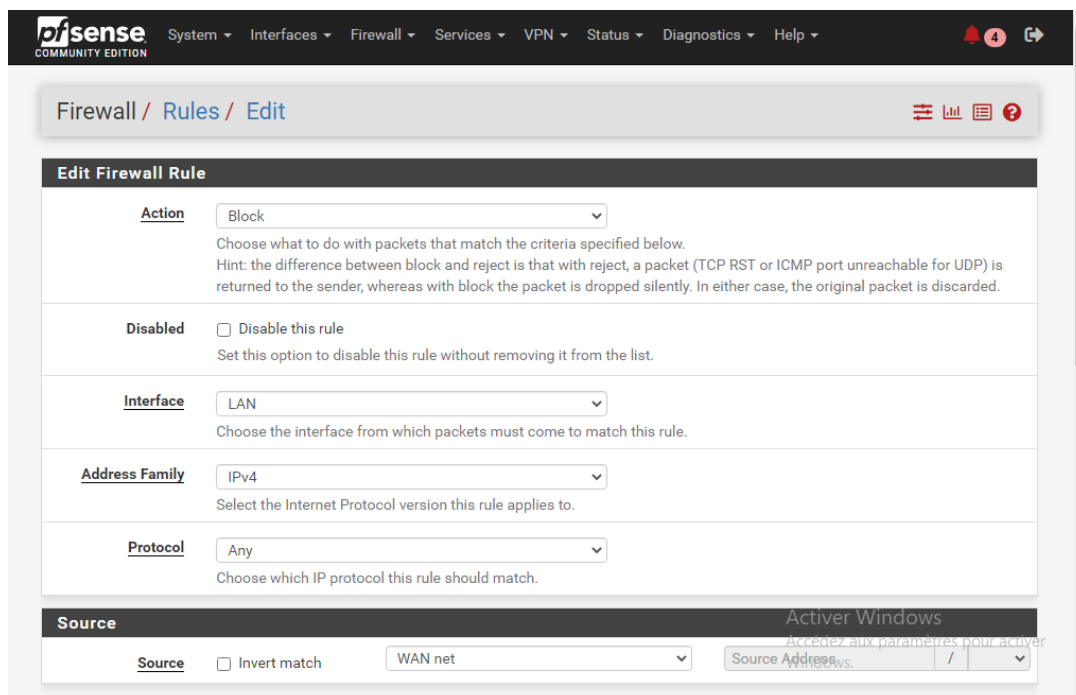
## V. Filtrer l'accès à internet

### a. Bloquer l'accès

Pour pouvoir bloquer l'accès internet de notre machine, il faut créer des règles de parefeu. Pour cela, nous devons nous rendre dans Firewall > Rules > LAN et on clique sur « Add » :



Puis configurer les paramètres de cette manière :



**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 WAN net Source Address /

**Destination**

**Destination** ☐ Invert match any Destination Address /

**Extra Options**

**Log** ☐ Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description**  
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options** [Display Advanced](#)

**Rule Information**

Tracking ID 1655277321

Et on valide avec « save » et voici la règle :

<input type="checkbox"/>	<span style="color: red;">X</span>	0 / 0 B	IPv4 *	WAN net	*	*	*	*	none
--------------------------	------------------------------------	---------	--------	---------	---	---	---	---	------

## b. Règles pour accéder à nouveau à internet

Tout d'abord il faut créer un alias qui nous permettra de faire une règle autorisant les ports pour accéder à internet.

**pfsense** COMMUNITY EDITION

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

Firewall / Rules / LAN

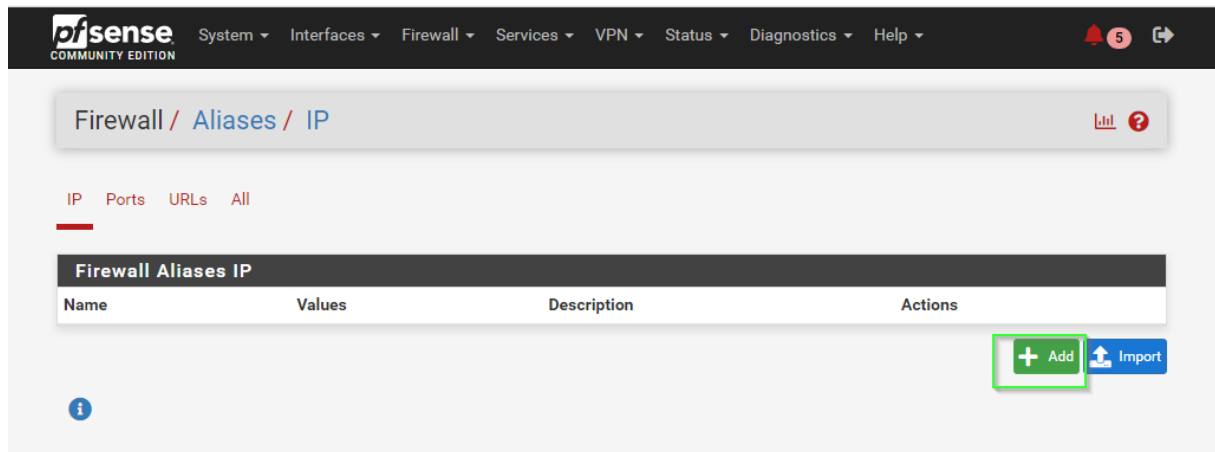
The changes have been applied successfully. [Monitor](#) the filter reload progress.

Now reloading in the background.

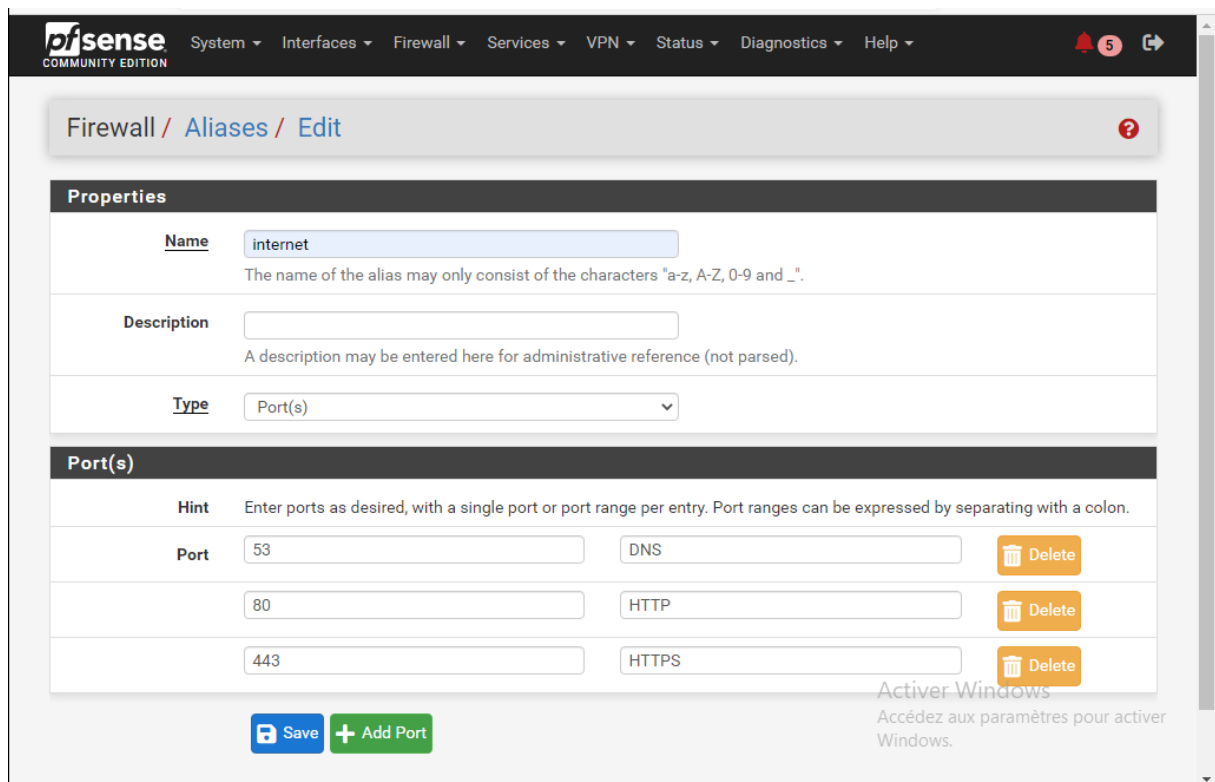
Floating WAN LAN

- Aliases
- NAT
- Rules
- Schedules
- Traffic Shaper
- Virtual IPs

Firewall > Aliases pour accéder à cette interface :



On clique sur « Add » et on paramètre l'alias de la manière suivante :



Puis on crée une règle qui contiendra l'alias créé :

### 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/UDP  
Choose which IP protocol this rule should match.

### Source

**Source** ☐ Invert match LAN net Source Address /   
[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**.

### Destination

**Destination** ☐ Invert match any Destination Address /

**Destination Port Range** (other) internet (other) internet  
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.

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

Firewall / Rules / LAN

Floating WAN LAN

#### Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	4 / 3.00 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	3 / 3.91 MiB	IPv4 TCP/UDP	LAN net	*	*	internet	*	none			
<input checked="" type="checkbox"/>	0 / 960 B	IPv4 ICMP any	*	*	*	*	*	none			
<input type="checkbox"/>	0 / 0 B	IPv4 *	WAN net	*	*	*	*	none			
<input type="checkbox"/>	0 / 0 B	IPv6 *	WAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Save Separator

Access aux paramètres pour activer Windows.