

Installation, configuration,
paramétrage de Pfsense.



Créé par : **HENRY Alexis,**

Le *15/06/2022.*

Modifié par : **HENRY Alexis,**

Le *15/06/2022.*

Version du document : **v1.**

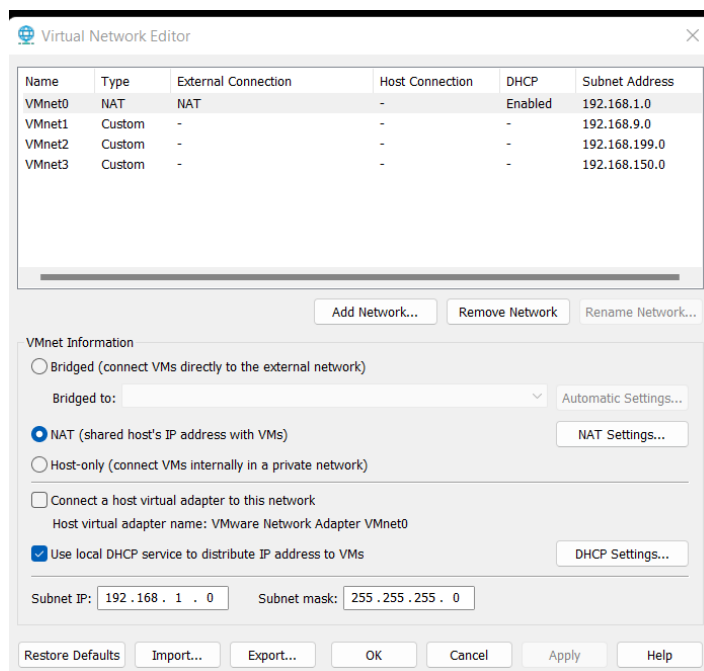
Table des matières

INSTALLATION DE PFSense	2
Configuration de la machine virtuelle.....	2
Installation du système d'exploitation	3
Welcome.....	3
Keymap Selection	4
Partitioning.....	5
CONFIGURATION DE PFSense.....	9
Set interface(s) IP address.....	10
Résultats.....	12
Reboot.....	12
CONFIGURATION D'UNE MACHINE CLIENTE	14
Configuration via IP statique	14
Configuration via IP dynamique	15
PARAMETRAGE DE PFSense	17
Setup pfSense.....	18
Admin Password.....	21
Serveur DHCP	22
Filtrages	23
Filtrage « deny all »	23
Filtrage internet.....	25
Création d'un Alias pour Internet.....	25
Création de la règle d'activation pour Internet.....	26

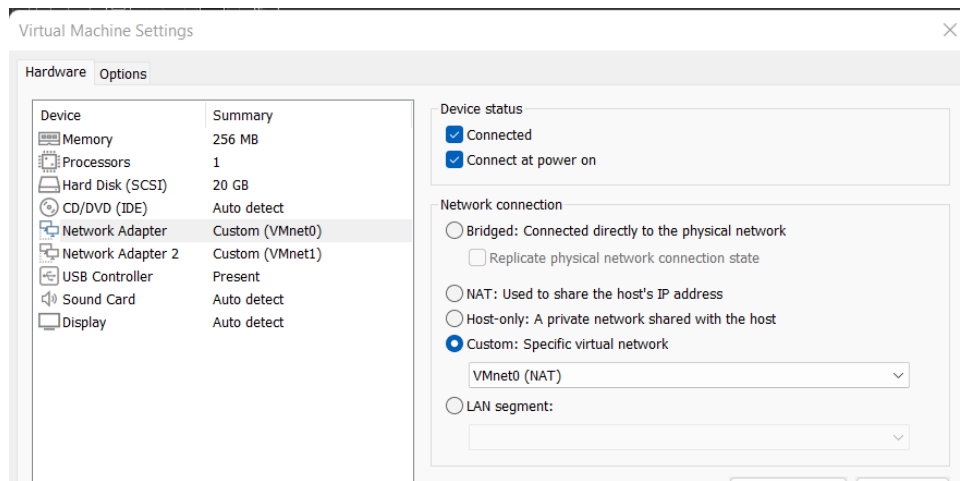
Installation de Pfsense

Configuration de la machine virtuelle.

Création d'un VMnet0 en NAT, ainsi qu'un VMnet1 en host-only.



Attribution d'une deuxième carte réseaux à la machine virtuelle, la première étant en VMnet0, la seconde VMnet1.



Installation du système d'exploitation

Welcome

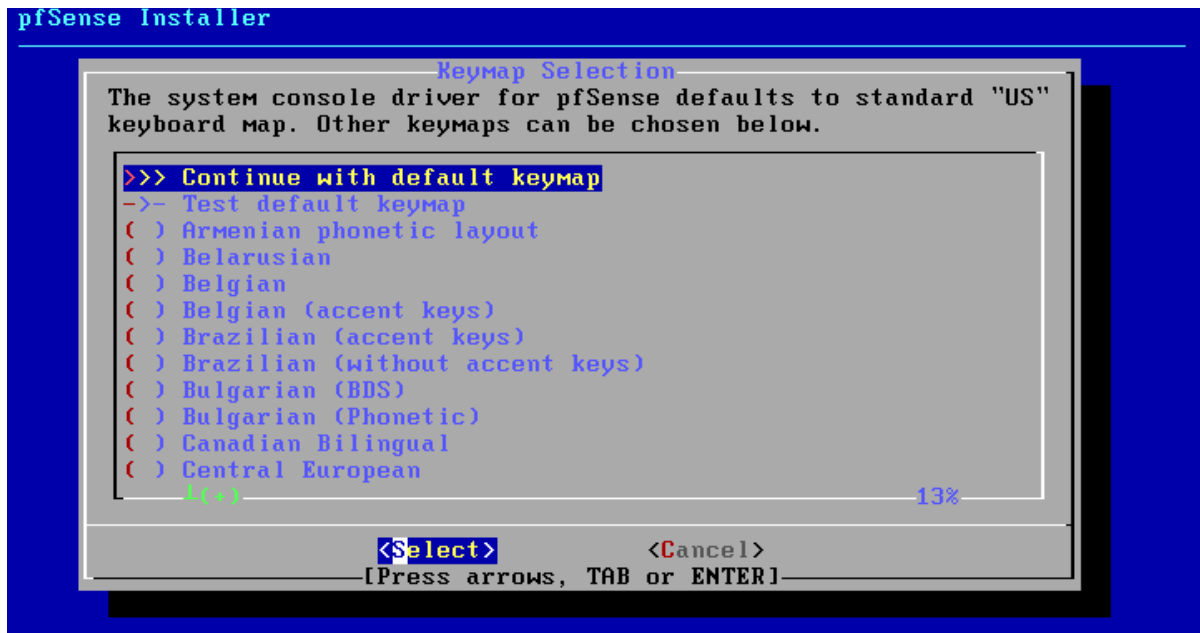
La première page qui apparaît lors de l'installation va nous demander ce que nous voulons faire. Nous avons différents choix :



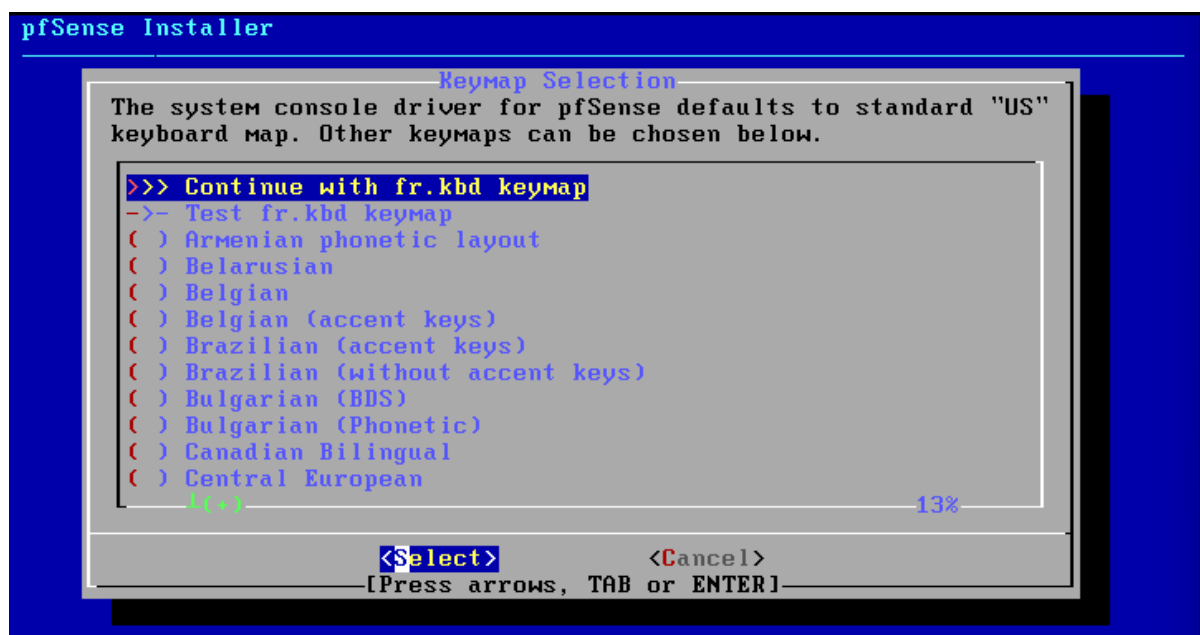
Pour ce qui est de l'installation, il faudra sélectionner « Install » puis appuyer sur « Ok ».

Keymap Selection

Cette étape correspond à la sélection de la langue du clavier, il faudra se rendre à la langue voulue, puis la sélectionner.

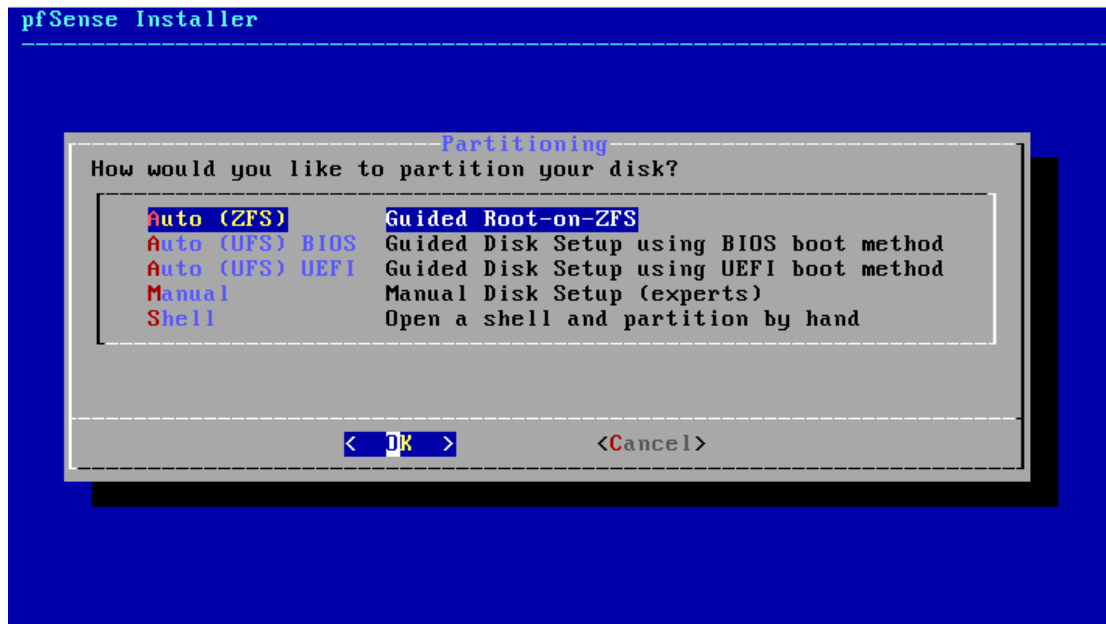


Une fois sélectionné, il faudra appuyer sur « Continue with ... ».



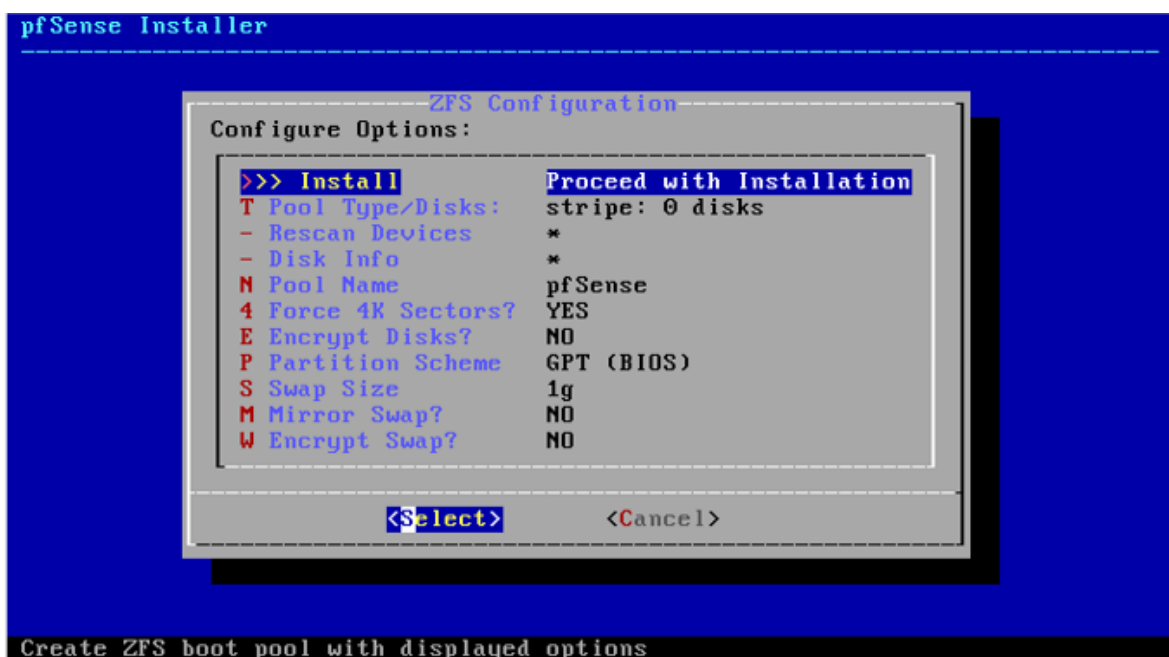
Partitioning

Nous arrivons ensuite sur la partie « Partitioning », il faut garder l'options par défaut, c'est-à-dire « Auto (ZFS) Guided Root-on-ZFS ».

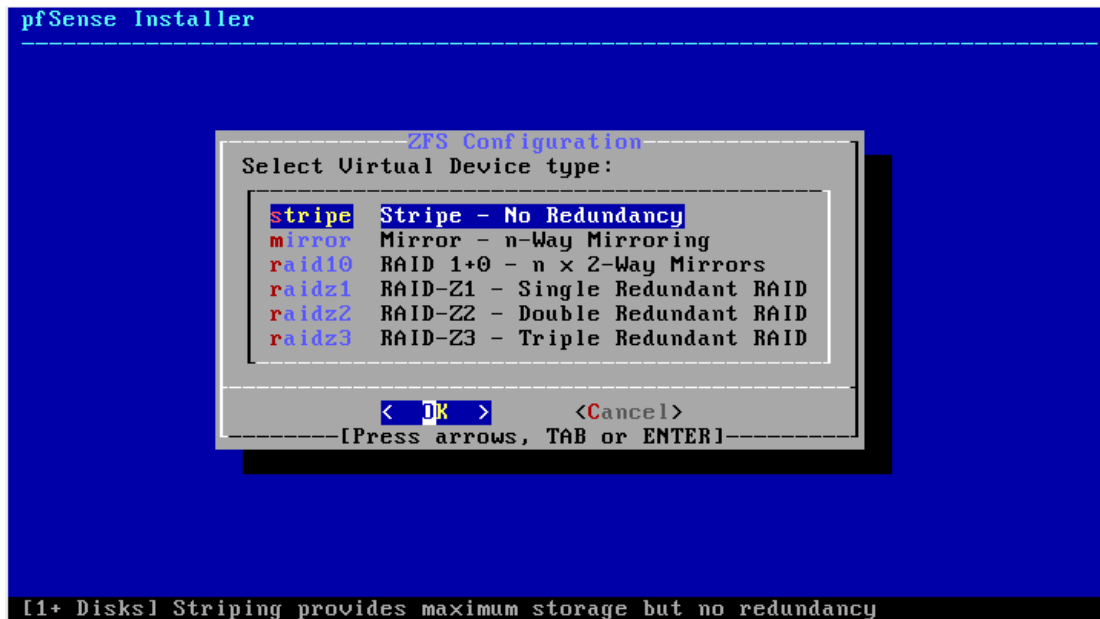


ZFS Configuration

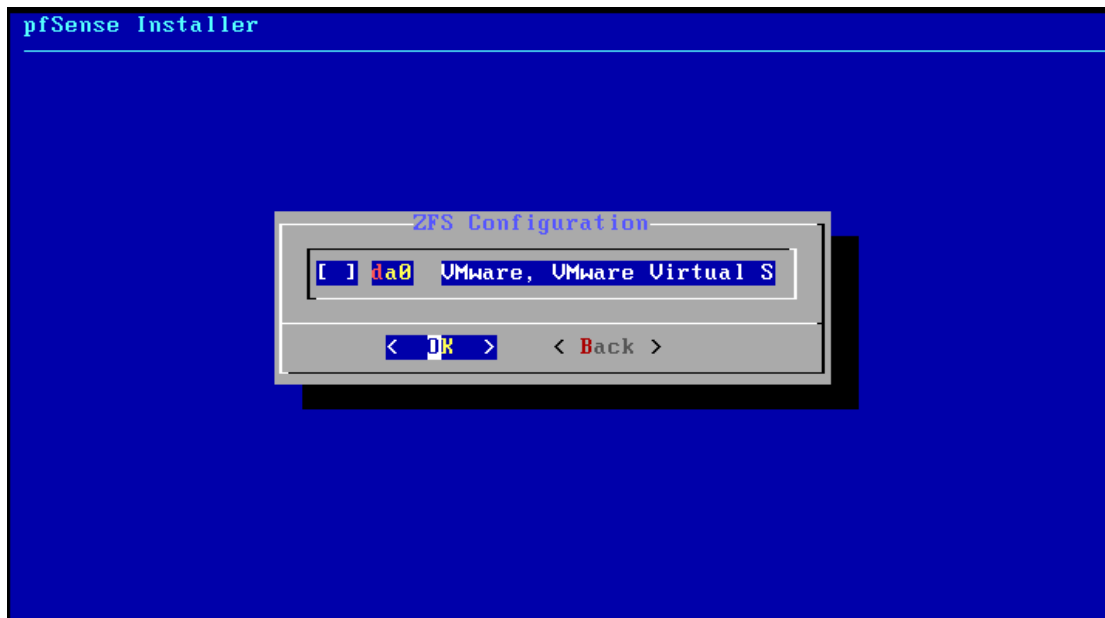
Pour ce qui est de la configuration de ZFS, il faut la laisser par défaut.



Ci-dessous, il faut garder la sélection de base « Stripe | Stripe – No Redundancy ».

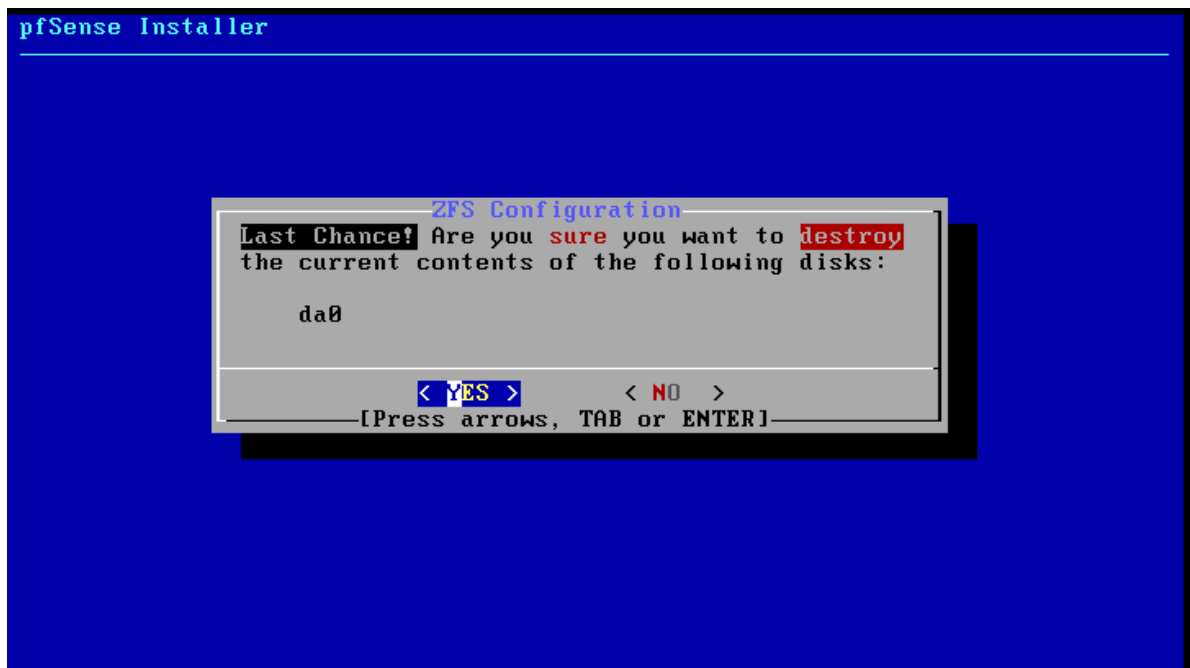


Ci-dessous, la fenêtre nous permet de sélectionner le disque à formater. Pour le sélectionner appuyer sur espace. Puis sur « OK ».



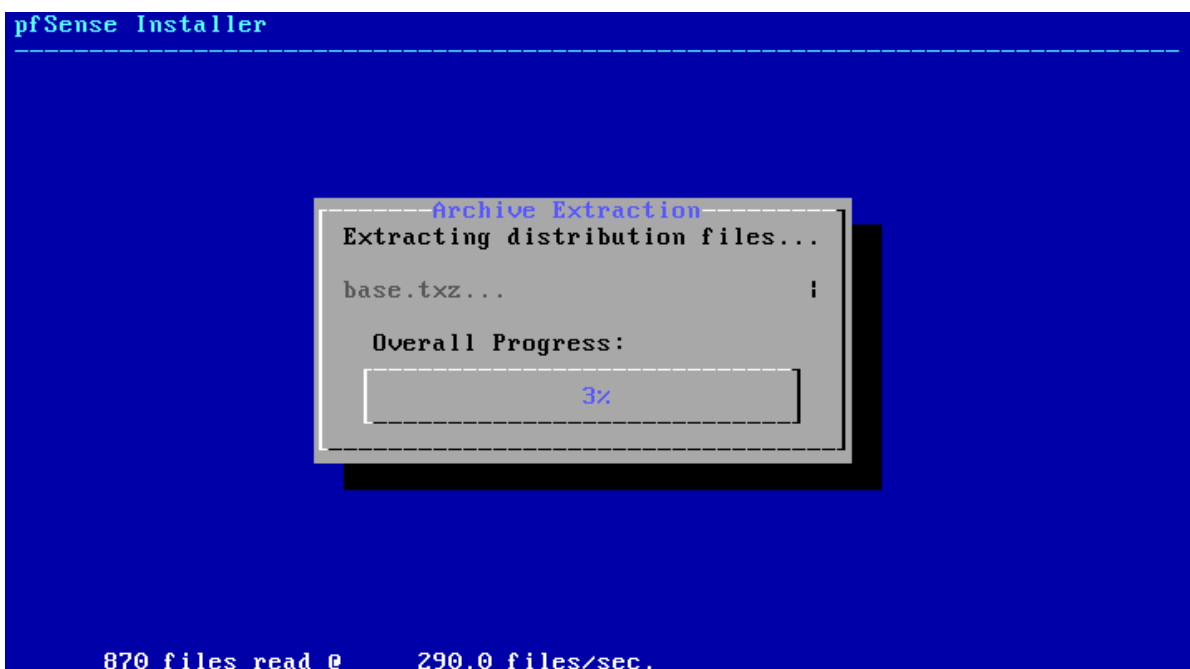
Ci-dessous, il demande confirmation pour la destruction du contenu du disque sélectionné.

Vous pouvez confirmer en appuyant sur « YES ».

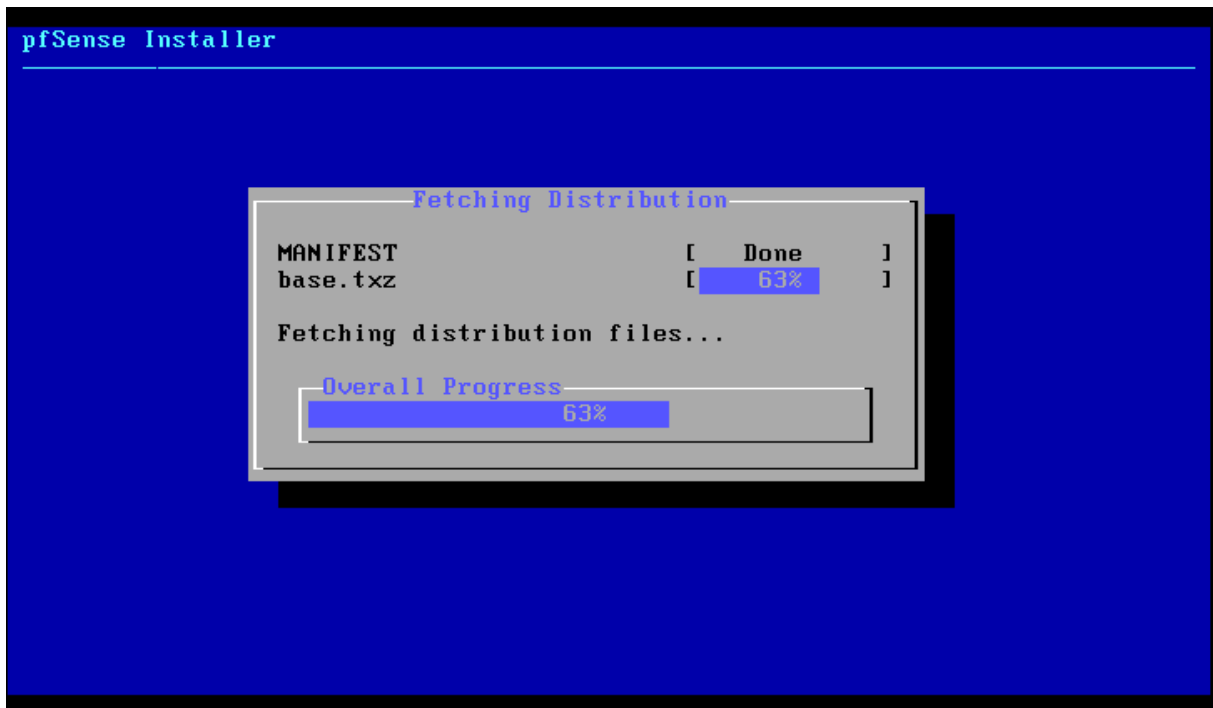


Archive Extraction

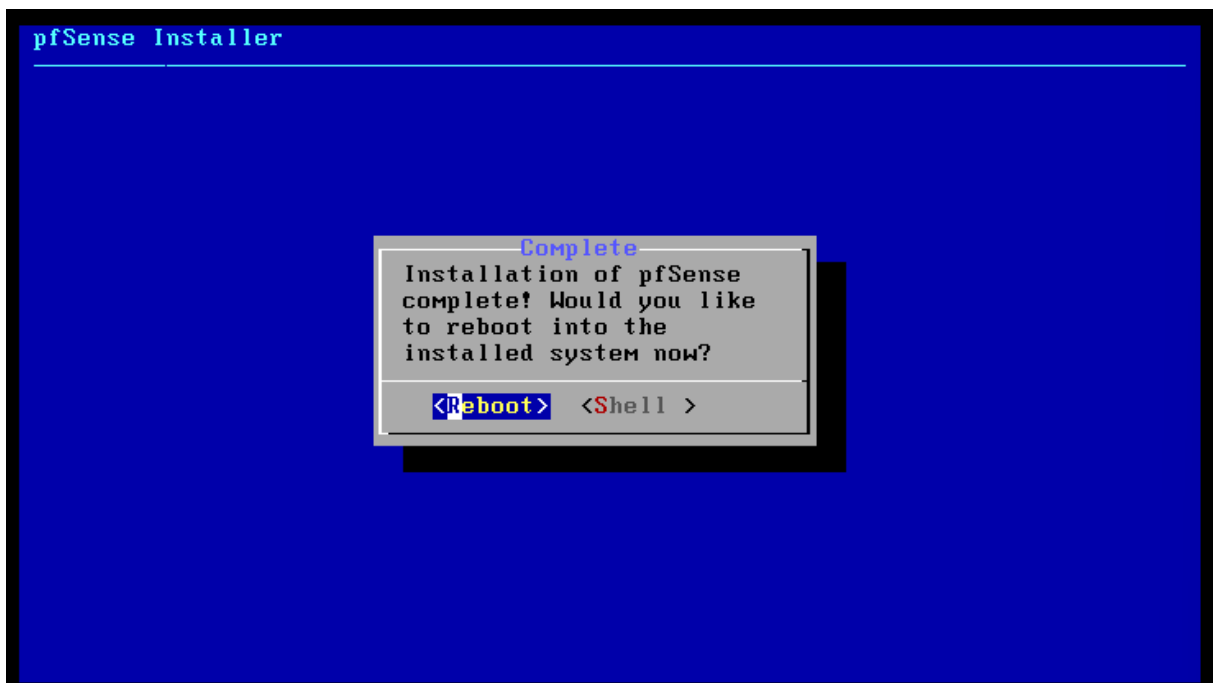
Ci-dessous, après avoir validé la dernière étape, on peut voir qu'il débute le formatage du disque.



Si cela se passe bien, vous devrez voir la barre de progression se remplir.



Si le formatage se termine avec succès, pfSense devrez vous proposer de redémarrer le système. Appuyer sur « Reboot ».



Ci-dessous, on voit que Pfsense redémarre.

```

Setting up extended sysctls...done.
Setting timezone...done.
Configuring loopback interface...done.
Starting syslog...done.
Setting up interfaces microcode...done.
Configuring loopback interface...done.
Configuring LAN interface...done.
Configuring WAN interface...done.
Configuring CARP settings...done.
Syncing OpenVPN settings...done.
Configuring firewall.....done.
Starting PFLOG...done.
Setting up gateway monitors...done.
Setting up static routes...done.
Setting up DNSs...
Starting DNS Resolver...done.
Synchronizing user settings...done.
Configuring CRON...done.
Bootstrapping clock...done.
Starting NTP Server...done.
Starting webConfigurator...done.
Starting DHCP service...done.
Starting DHCPv6 service...done.
Configuring firewall.....done.
█

```

Après le redémarrage du système, vous devriez arriver sur la page d'accueil de Pfsense, c'est-à-dire la page qui va vous proposer les différentes fonctionnalités proposées.

```

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: 1820d0b65807cc97f8e7

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.128/24
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: █

```

Configuration de PFSens

Ci-dessous, la liste de toutes les fonctionnalités que propose Pfsense pour sa configuration :

```

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

```

Set interface(s) IP address

Nous allons commencer par attribuer une IP à Pfsense, cela correspond à la seconde option.

```

VMware Virtual Machine - Netgate Device ID: 1820d0b65807cc97fbe7

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.128/24
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: █

```

Il faudra donc appuyer sur « 2 », puis sur « Enter ».

```

Available interfaces:

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

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

```

Nous souhaitons configurer le LAN, il faut donc entrer 2, pour configurer cette interface.

```
Available interfaces:
```

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

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

Suite à cela, il faut entrer l'IP que nous souhaitons lui attribuer.

```
Enter the new LAN IPv4 address. Press <ENTER> for none:  
> 192.168.1.254
```

Ensuite, il nous demande le masque, il faut indiquer 24,16,8 ...

```
Enter the new LAN IPv4 address. Press <ENTER> for none:  
> 192.168.1.254
```

```
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
```

Pour les deux étapes suivantes, nous n'avons pas besoin de les configurer, il vous suffira donc d'appuyer sur « Enter », sans entrer quelconque donnée.

```
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:  
>
```

Ci-dessous, il demande si nous souhaitons activé le DHCP Server sur le LAN, pour la suite nous n'en avons pas besoin. Vous pouvez écrire « n », puis appuyer sur « Enter ».

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

Ci-dessous, la dernière étape, à laquelle il faudra répondre par « y ».

```
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█
```

Résultats

```
The IPv4 LAN address has been set to 192.168.9.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
```

```
http://192.168.9.254/
```

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

```
VMware Virtual Machine - Netgate Device ID: 1820d0b65807cc97fbe7
```

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

```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.128/24
LAN (lan)      -> em1      -> v4: 192.168.9.254/24
```

```
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: █
```

Reboot

Pour prendre en compte tous les changements réalisés, vous pouvez redémarrer la machine.

```

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

```

Ci-dessus, nous pouvons apercevoir que l'option pour redémarrer la machine est la 5.

Il faut donc entrer « 5 », puis valider.

Il va vous proposer une liste d'options de redémarrage, nous souhaitons faire un redémarrage normal, de ce fait il faut écrire « y » ou « Y », puis valider.

```

Enter an option:
Message from syslogd@pfSense at Jun 15 07:38:03 ...
php-fpm[43186]: /index.php: Successful login for user 'admin' from: 192.168.9.10
(Local Database)
5

pfSense will reboot. This may take a few minutes, depending on your hardware.
Do you want to proceed?

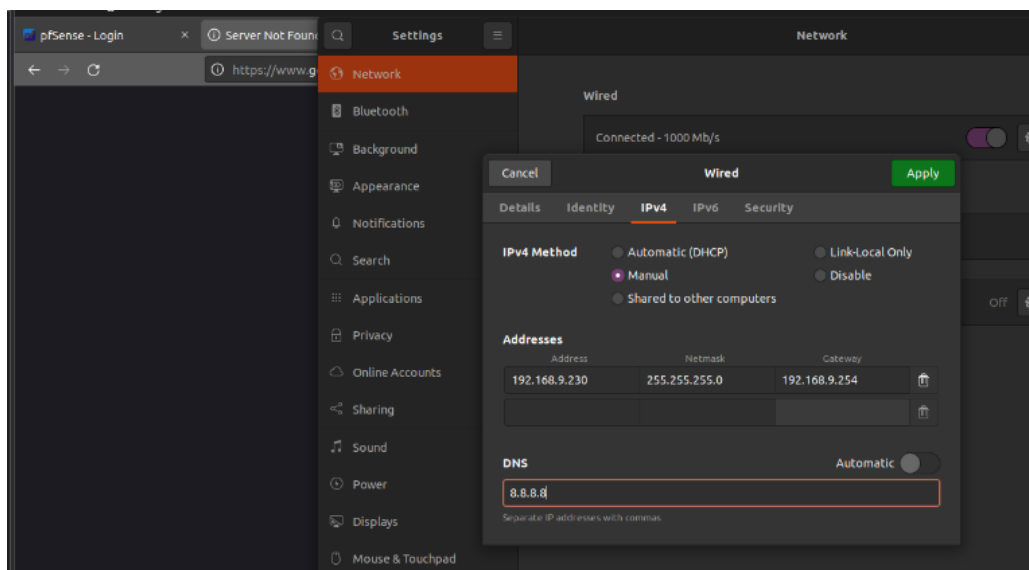
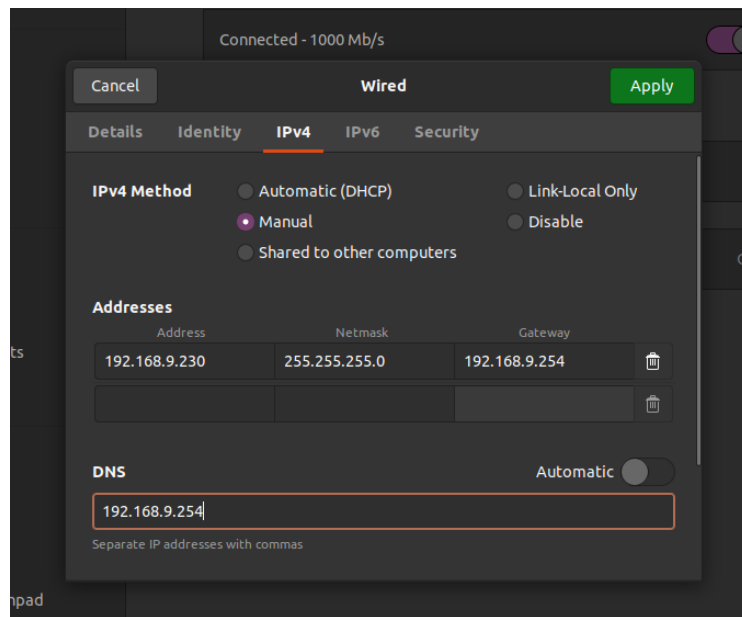
Y/y: Reboot normally
R/r: Reroot (Stop processes, remount disks, re-run startup sequence)
S: Reboot into Single User Mode (requires console access!)
Enter an option: y

```

Configuration d'une machine cliente

Configuration via IP statique

Ci-dessous, la configuration d'une machine cliente en IP statique :

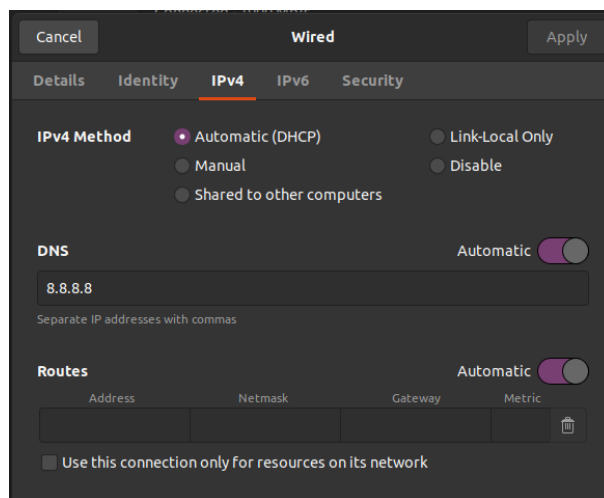


Configuration via IP dynamique

La machine cliente utilisée est une Ubuntu 20.04.

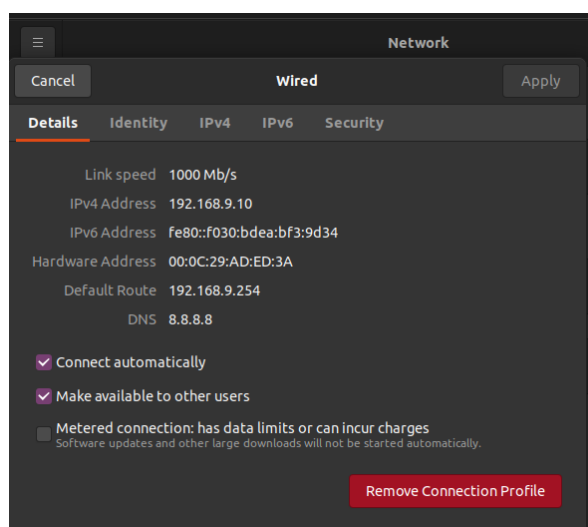
Dans les paramètres réseaux de la machine, on voit qu'elle est en « Automatic (DHCP) ».

Une fois, la mise en place du Serveur DHCP de Pfsense, il est possible de passer la machine cliente en DHCP. Comme ci-dessous :



La machine contient donc la configuration ci-dessous :

On peut voir que la « Default route » est bien l'IP de la machine Pfsense. Ainsi que l'adresse IP de la machine cliente est bien comprise dans la plage du VMnet1.



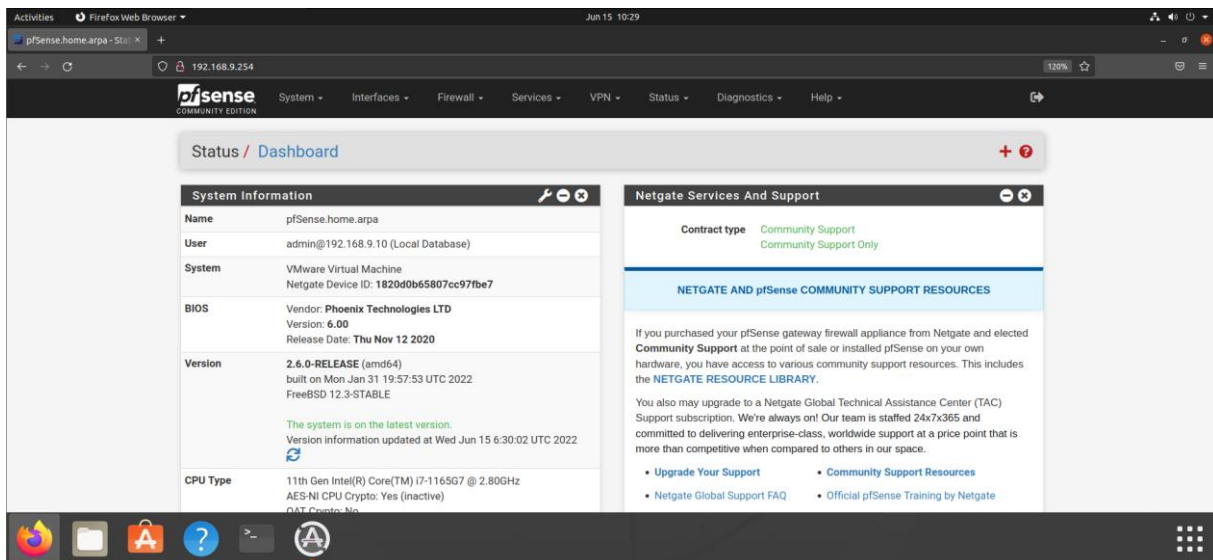
Par exemple, ci-dessous, on peut voir que la machine client est bien connectée au réseau.



Ci-dessous, la machine cliente peut ping la machine pfSense.

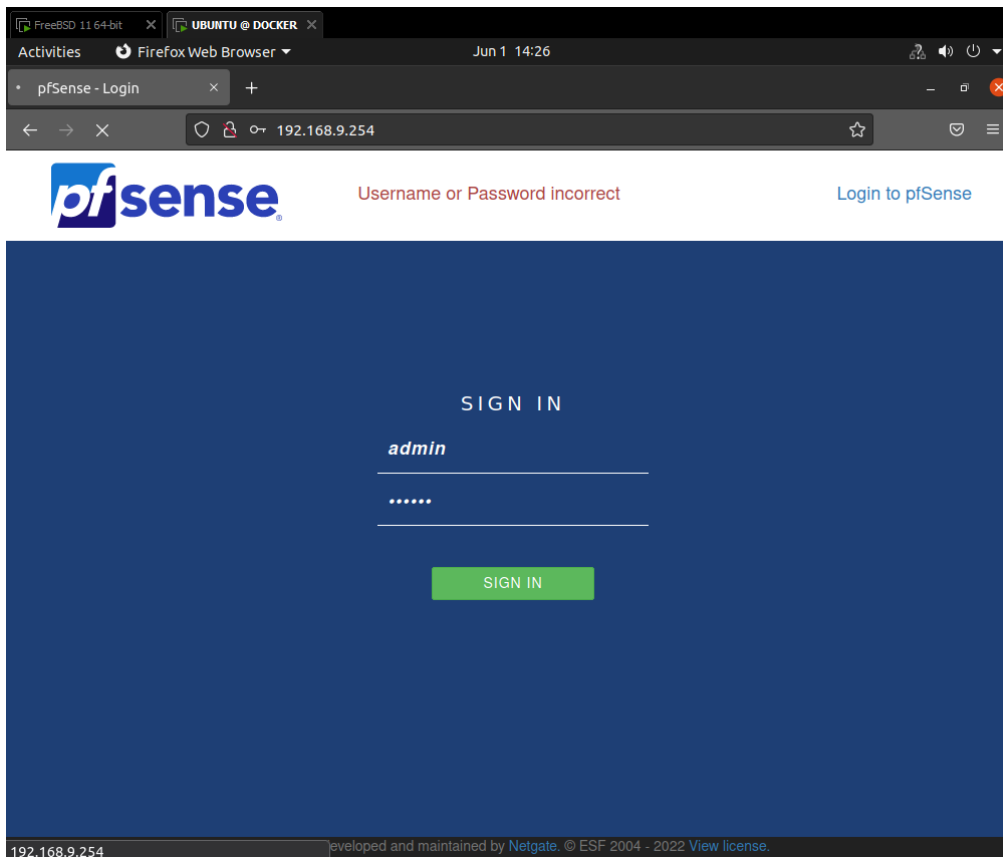
```
docker@ubuntu:~$ ping 192.168.9.254
PING 192.168.9.254 (192.168.9.254) 56(84) bytes of data:
64 bytes from 192.168.9.254: icmp_seq=1 ttl=64 time=0.625 ms
64 bytes from 192.168.9.254: icmp_seq=2 ttl=64 time=0.584 ms
```

Dernière étape, la machine cliente a bien accès via internet à l'interface pfSense.



Paramétrage de PfSense

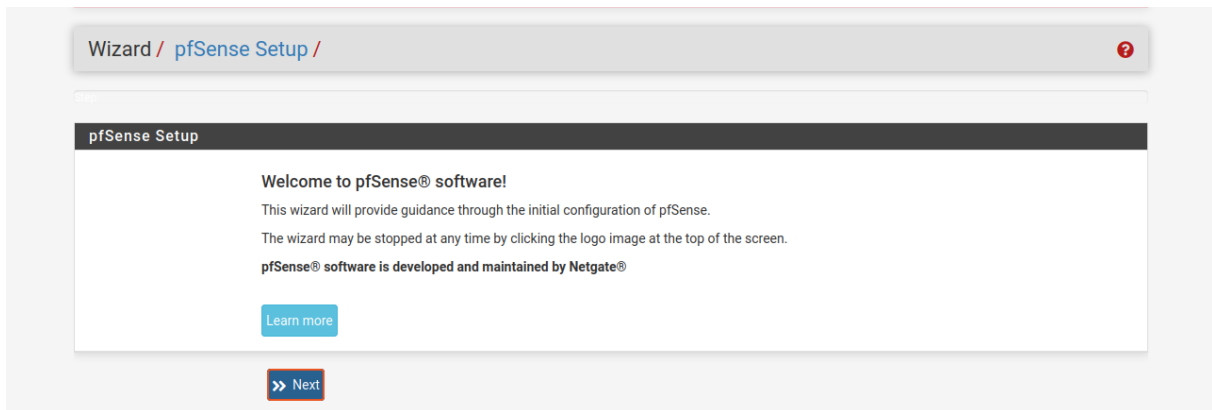
Une fois que l'on arrive à accéder à l'interface de pfSense, nous pouvons commencer à le paramétrer.



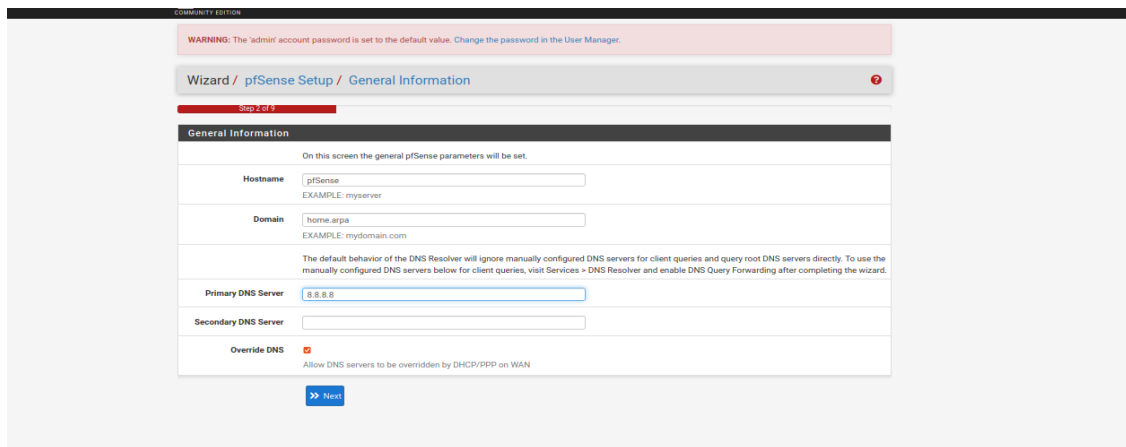
Les identifiants par défauts sont : admin / pfsense.

Setup pfSense

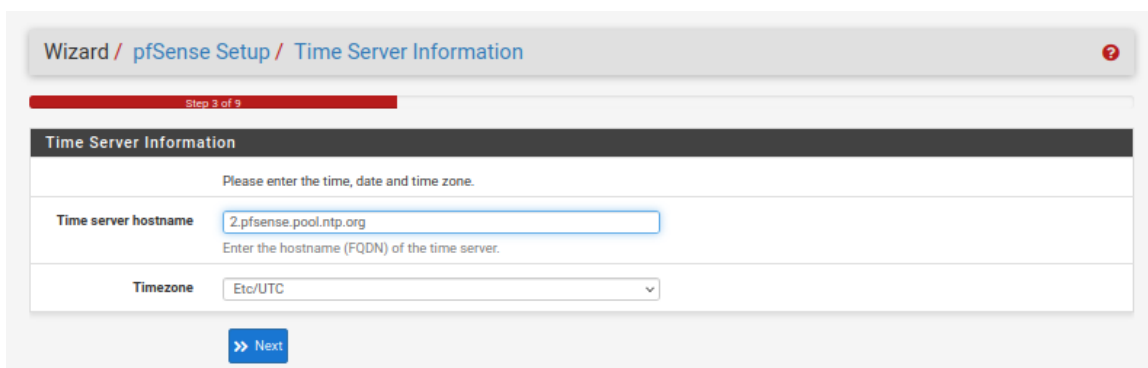
Après la première connexion, vous devez d'abord passer par le setup de pfSense. Cette étape est à nouveau réalisable à tout moment via le menu. Pour passer les étapes, il vous suffira d'appuyer sur « Next ».



Lors de la seconde étape, vous pouvez configurer les DNS, ainsi que le hostname, etc...



La troisième étape, vous permet de configurer les paramètres du temps sur le serveur. Vous pouvez les laisser par défauts.



La quatrième étape, contient énormément de paramètre, dont nous n'avons pas forcément l'utilité de les modifier pour l'instant.

The screenshot shows the 'Configure WAN Interface' step of the pfSense setup wizard. The breadcrumb trail is 'Wizard / pfSense Setup / Configure WAN Interface'. A progress bar indicates 'Step 4 of 9'. The page is divided into several sections for configuration:

- Configure WAN Interface:** A dropdown menu for 'SelectedType' is set to 'DHCP'. Below it, a note states: 'On this screen the Wide Area Network information will be configured.'
- General configuration:** Contains three input fields: 'MAC Address' (with a note about spoofing), 'MTU' (with a note about default values of 1492 for PPPoE and 1500 for others), and 'MSS' (with a note about MSS clamping).
- Static IP Configuration:** Contains three input fields: 'IP Address', 'Subnet Mask' (set to 32), and 'Upstream Gateway'.
- DHCP client configuration:** Contains one input field: 'DHCP Hostname' (with a note about client identification).
- PPPoE configuration:** Contains four input fields: 'PPPoE Username', 'PPPoE Password', 'PPPoE Service name' (with a hint: 'Hint: this field can usually be left empty'), and a checkbox for 'PPPoE Dial on demand' (checked).

L'étape 5, ci-dessous, vous permet de configurer l'adresse IP du LAN, ainsi que le masque de sous-réseaux.

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

Configure LAN Interface

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

LAN IP Address:

Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask:

[» Next](#)

Sur la prochaine étape, vous devez cliquer sur « Reload ».

Wizard / pfSense Setup / Reload configuration

Step 7 of 9

Reload configuration

Click 'Reload' to reload pfSense with new changes.

[» Reload](#)

La dernière étape, vous confirme que pfSense a bien été configuré.

Wizard / pfSense Setup / Wizard completed.

Step 9 of 9

Wizard completed.

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

[Check for updates](#)

Remember, we're here to help.

[Click here](#) to learn about Netgate 24/7/365 support services.

User survey

Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)

[Anonymous User Survey](#)

Useful resources.

- Learn more about Netgate's product line, services, and pfSense software from our [website](#)
- To learn about Netgate appliances and other offers, [visit our store](#)
- Become part of the pfSense community. Visit our [forum](#)
- Subscribe to our [newsletter](#) for ongoing product information, software announcements and special offers.

[Finish](#)

Admin Password

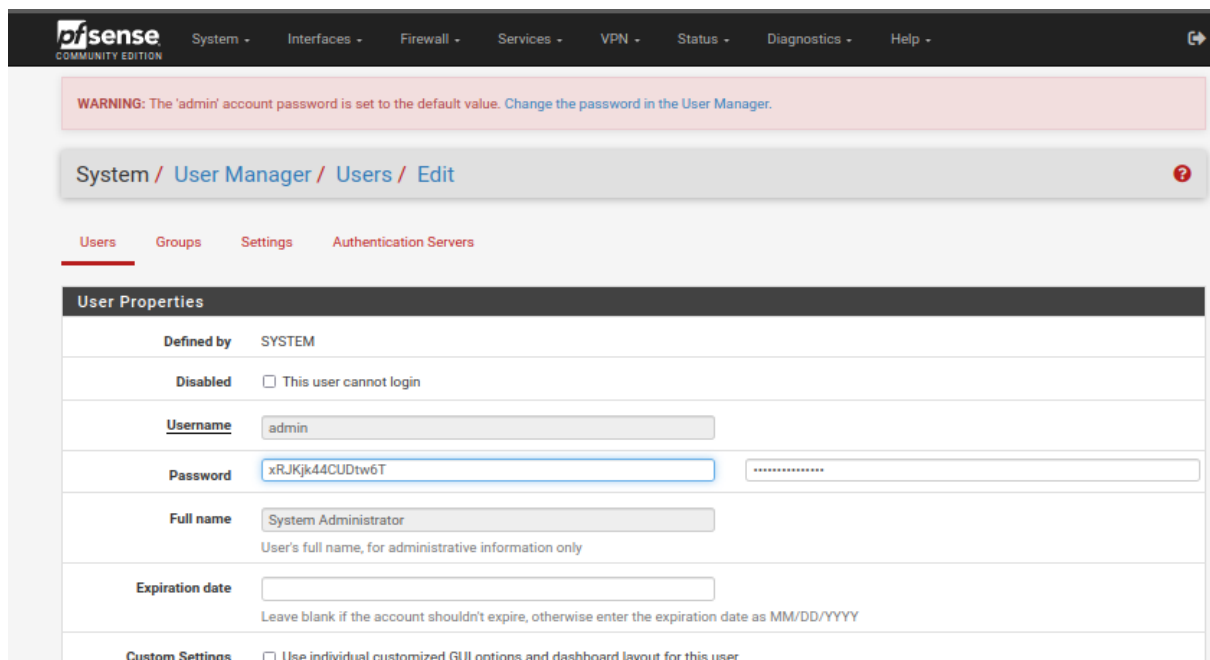
Lors de la première connexion, pfSense nous avertis que le mot de passe du compte administrateur est à sa valeur par défaut, de ce fait nous devons le modifier.

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

L'espace pour modifier le mot de passe se trouve dans :

- System / User Manager / Users / Edit

Comme ci-dessous:



The screenshot shows the pfSense web interface. At the top, there is a navigation bar with the pfSense logo and menu items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation bar, a warning message is displayed: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The main content area shows the breadcrumb "System / User Manager / Users / Edit" and a sub-menu with "Users", "Groups", "Settings", and "Authentication Servers". The "Users" sub-menu is selected, and the "User Properties" section is visible. The "User Properties" section contains the following fields:

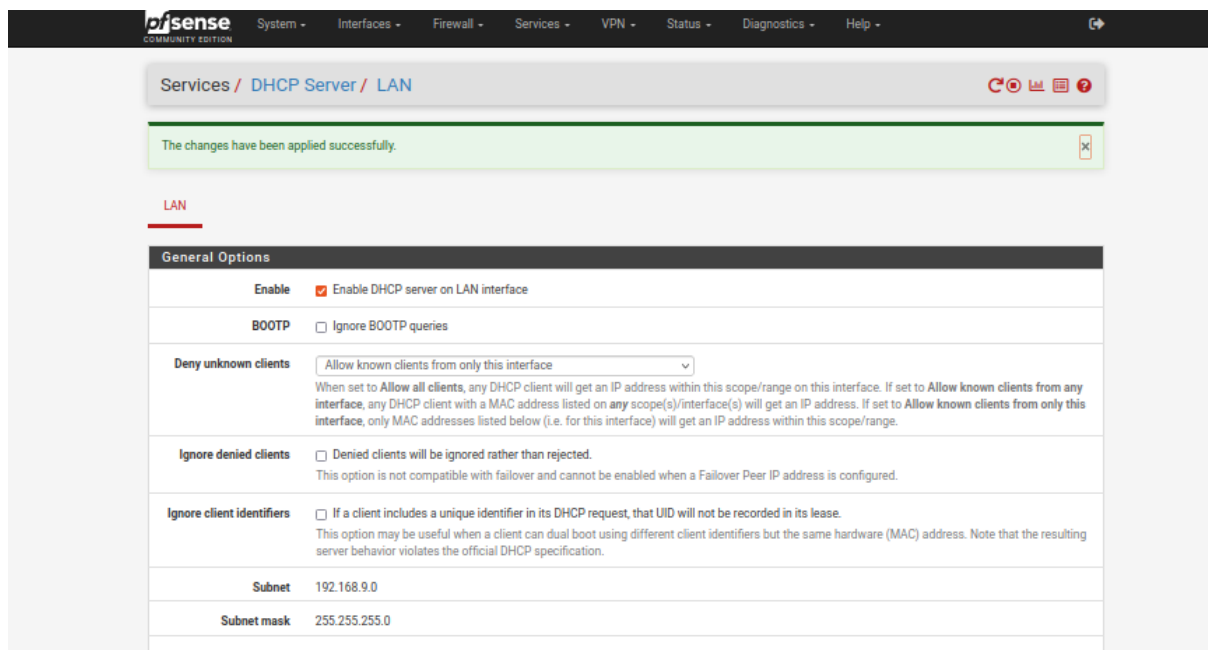
Defined by	SYSTEM
Disabled	<input type="checkbox"/> This user cannot login
Username	admin
Password	xRJkjk44CUDtw6T
Full name	System Administrator <small>User's full name, for administrative information only</small>
Expiration date	<input type="text"/> <small>Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY</small>
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.

Serveur DHCP

Dû au fait que nous n'avons pas activé le serveur DHCP lors de l'installation de pfSense, nous devons alors activer depuis l'interface web.

Pour ce faire, vous devez vous rendre dans l'onglet Services, puis dans :

- Services / DHCP Server / LAN



Dans l'étape de paramétrage ci-dessus, il faut aussi modifier la catégorie « Deny unknown clients » :



Mettre cette option sur: « Allow known clients from only this interface ».

Cette étape permet de faire passer notre machine cliente sous DHCP. C'est-à-dire qu'elle se fera attribuée une adresse IP dynamiquement.

Filtrages

Filtrage « deny all »

Création d'une règle pour bloquer tous les accès :

En action on met « Block », cela permet de dire que ce sera une règle qui va bloquer des ports.

The screenshot shows the 'Edit Firewall Rule' configuration page in WinBox. The rule is named 'deny all' and is configured with the following settings:

- Action:** Block
- Disabled:** Disable this rule
- Interface:** LAN
- Address Family:** IPv4
- Protocol:** TCP

Source: Invert match, Source Address: any

Destination: Invert match, Destination Address: any, Destination Port Range: From: any, To: any

Extra Options: Log packets that are handled by this rule

Description: Block all

Advanced Options: Display Advanced

Save:

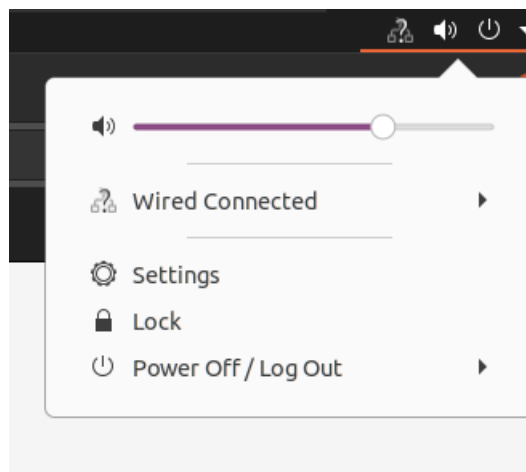
Ci-dessous, la règle après création :

The screenshot shows the Mikrotik WinBox interface for configuring Firewall Rules on the LAN interface. A green notification bar at the top states: "The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress." Below this, the "LAN" tab is selected. The "Rules (Drag to Change Order)" table is displayed with the following data:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 2 / 90 KIB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙️
✗ 0 / 0 B	IPv4 TCP	*	*	*	*	*	none		Block all	📌 ✎ 🗑️

At the bottom right, there are buttons for "Add", "Add", "Delete", "Save", and "Separator".

Une fois le changement sauvegardé, on voit que la machine cliente a perdu la connexion à internet.



Filtrage internet

Création d'un Alias pour Internet

Création d'un Alias (Firewall / Aliases / Edit), cela permet de créer une règle pour un groupe de ports, et ce à la place de faire une règle par ports.

Le port ci-dessous, permet donc de faire des règles pour tous les ports que requiert Internet. C'est-à-dire les ports 80, 443, et 53.

Firewall / Aliases / Edit

Properties

Name
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

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

Type

Port(s)

Hint Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.

Port	Protocol	Action
<input type="text" value="80"/>	<input type="text" value="HTTP"/>	<input type="button" value="Delete"/>
<input type="text" value="443"/>	<input type="text" value="HTTPS"/>	<input type="button" value="Delete"/>
<input type="text" value="53"/>	<input type="text" value="DNS"/>	<input type="button" value="Delete"/>

Ci-dessous, l'Alias une fois créé.

Firewall / Aliases / Ports

IP Ports URLs All

Firewall Aliases Ports

Name	Values	Description
Internet_access	80, 443, 53	Autorisation port 80,443,53

Création de la règle d'activation pour Internet

Il faut ensuite créer une règle qui va cibler l'alias que nous avons créé. C'est-à-dire les ports que nécessite Internet : 80, 443, 53.

Cette règle aura comme action « Pass », car elle permettra l'autorisation de certains ports.

Firewall / Rules / Edit

Edit Firewall Rule

Action
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
Choose the interface from which packets must come to match this rule.

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

Protocol
Choose which IP protocol this rule should match.

Elle permettra les protocoles TCP et UDP. Cela dû au fait que DNS utilise en général UDP.

Source

Source Invert match /

[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 /

Destination Port Range
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.

Ci-dessus, on indique alors notre Alias, en mettant les « Destination Port Range » à (other).

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	1655293374
Created	6/15/22 11:42:54 by admin@192.168.100.100 (Local Database)
Updated	6/15/22 11:42:54 by admin@192.168.100.100 (Local Database)

[Save](#)

En dernier, on ajoute un commentaire pour qu'on nous indique ce que fait la règle.

Ci-dessous, on peut apercevoir la règle que nous avons créé.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	3 / 1.47 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/>	14 / 3.16 MiB	IPv4 TCP/UDP	LAN net	*	*	Internet_access	*	none		Acces Internet	
<input checked="" type="checkbox"/>	0 / 0 B	IPv4 TCP	LAN net	*	*	*	*	none			

Add Add Delete Save Separator

Ci-dessous on voit que la connexion est établie, et que l'on a donc accès à internet.

