

PETIT Antoine
10/03/2023
Mise à jour le 10/03/2023
BTS SIO 1

DMZ

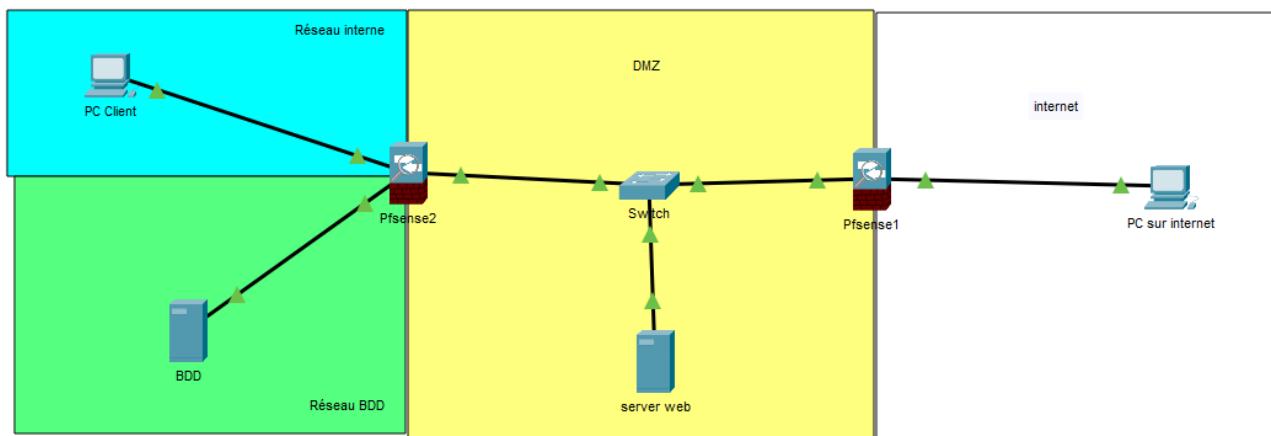
Sommaire

Problématique.....	2
Infrastructure réseaux.....	2
Paramètres de configuration.....	2
Tuto d'installation.....	3
Installation de Pfsense.....	3
Configuration terminal du Pfsense1.....	13
Configuration terminal du Pfsense2.....	20
Pré-configuration graphique des Pfsense.....	30
Configuration graphique du Pfsense1.....	37
Configuration graphique du Pfsense2.....	52
Notice d'utilisation.....	57
Annexes.....	57
Fiche recette.....	59

Problématique

Nous voulons pouvoir accéder aux site web depuis l'extérieur de notre réseau privé et depuis l'intérieur sans que l'extérieur n'est accès au reste du réseau priver .

Infrastructure réseaux



Paramètres de configuration

Pfsense1	IP Wan : DHCP	
	IP Lan :10.0.0.254 /24	
Serveur web	IP :10.0.0.1 /24	Passerelle :10.0.0.254
Pfsense2	IP Wan:10.0.0.253 /24	Passerelle :10.0.0.254
	IP Lan :192.168.10.254 /24	
	IP OPT1 :192.168.20.254 /24	
PC client	IP :192.168.10.1 /24	Passerelle : 192.168.10.254
BDD	IP :192.168.20.1 /24	Passerelle : 192.168.20.254

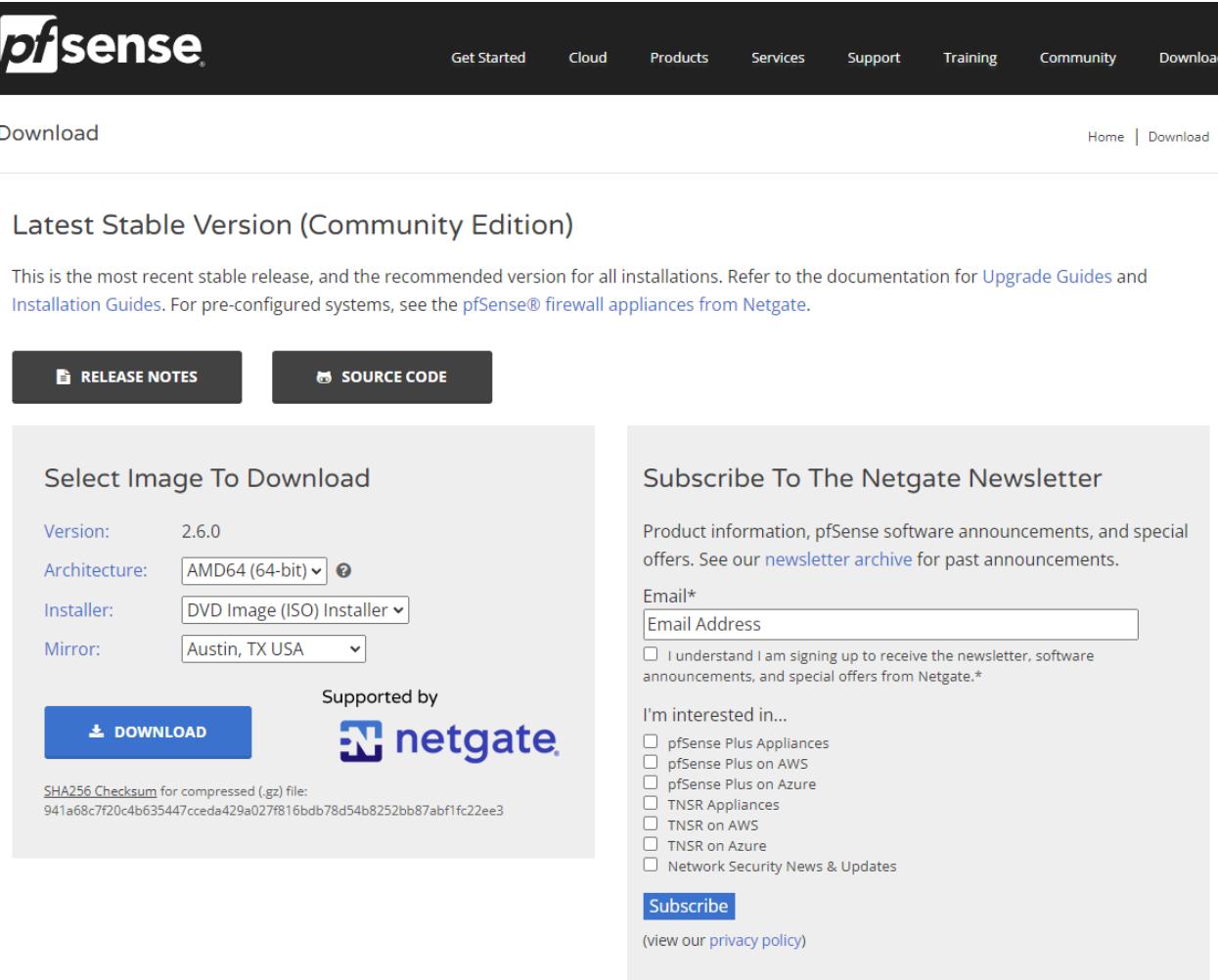
Tuto d'installation

Installation de Pfsense

Pour commencer nous allons aller chercher l'ISO de Pfsense sur leur site :

<https://www.pfsense.org/download/>

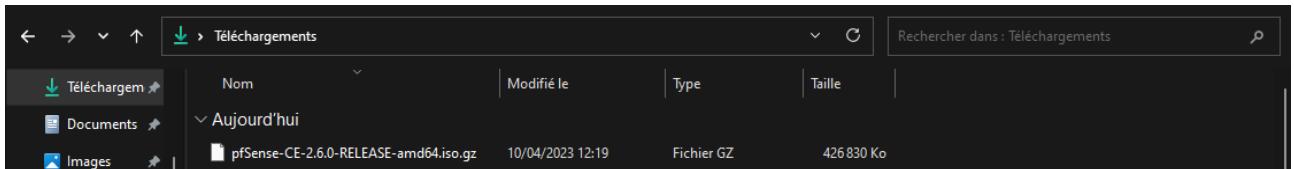
Vous tomberez sur cette page.



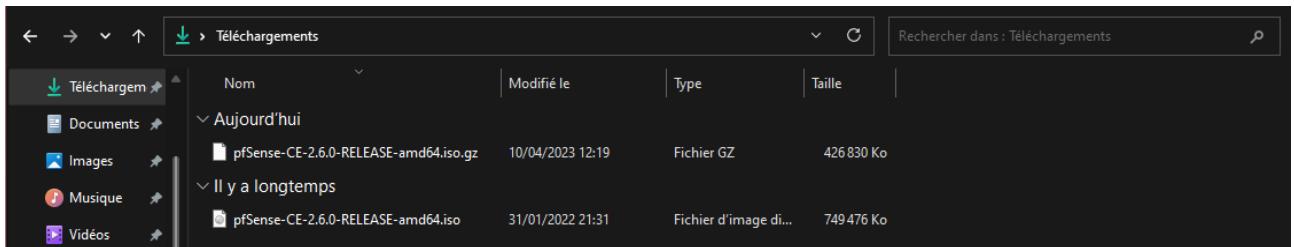
The screenshot shows the pfSense download page. At the top, there is a navigation bar with links for Get Started, Cloud, Products, Services, Support, Training, Community, and Download. Below the navigation bar, there is a 'Download' button and a 'Home | Download' link. The main content area is titled 'Latest Stable Version (Community Edition)'. It states that this is the most recent stable release and the recommended version for all installations. It also mentions 'Upgrade Guides' and 'Installation Guides'. Below this, there are two buttons: 'RELEASE NOTES' and 'SOURCE CODE'. The main download section is titled 'Select Image To Download' and shows the following configuration: Version: 2.6.0, Architecture: AMD64 (64-bit), Installer: DVD Image (ISO) Installer, and Mirror: Austin, TX USA. A large blue 'DOWNLOAD' button is present. Below the download section, there is a note about SHA256 Checksum for compressed (.gz) file: 941a68c7f20c4b635447cceda429a027f816bdb78d54b8252bb87abf1fc22ee3. To the right of the download section, there is a sidebar titled 'Subscribe To The Netgate Newsletter'. It contains a description of the newsletter, a 'Email*' input field, a 'Email Address' input field, a checkbox for accepting the newsletter terms, and a list of interests with checkboxes for pfSense Plus Appliances, pfSense Plus on AWS, pfSense Plus on Azure, TNSR Appliances, TNSR on AWS, TNSR on Azure, and Network Security News & Updates. A 'Subscribe' button and a link to the privacy policy are also in the sidebar.

Dans architecture choisissez bien AMD64 puis dans installer choisissez DVD Image, dans mirror choisissez celui que vous désirez il n'y a pas d'importance et n'oublier pas cliquer sur le bouton download.

Le fichier apparaîtra dans vos téléchargements.



il est actuellement dans une archive .gz vous pouvez l'extraire avec 7zip ce qui vous donne ceci.

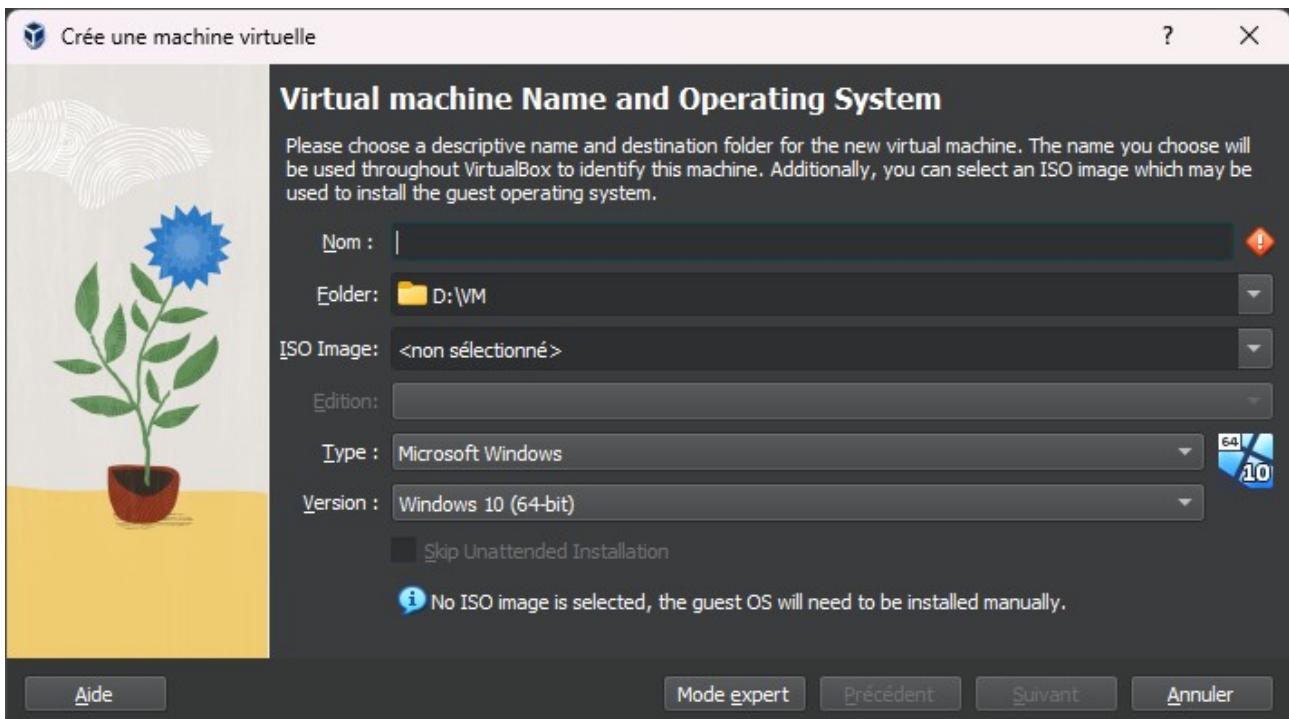


Maintenant il y a 2 possibilité qui s'offre à vous faire ce TP sous VM Virtual Box ou sur des machine physique pour ma pare n'ayant pas le matériel pour le faire en machine physique je vais donc choisir la première option si vous faites la seconde option je vous explique comment faire en ANNEXES.

Nous allons donc créer une machine virtuel.

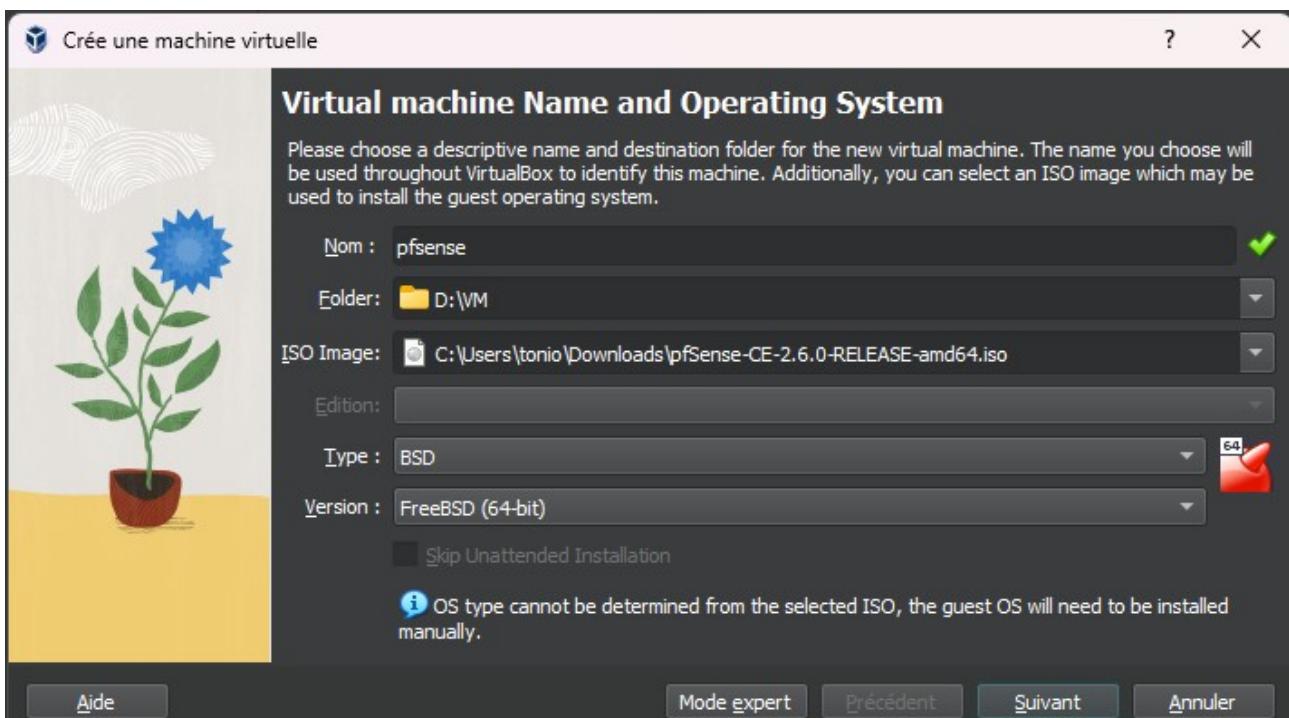


Vous allez donc cliquer sur nouvelle vous tomberez sur la page suivant.



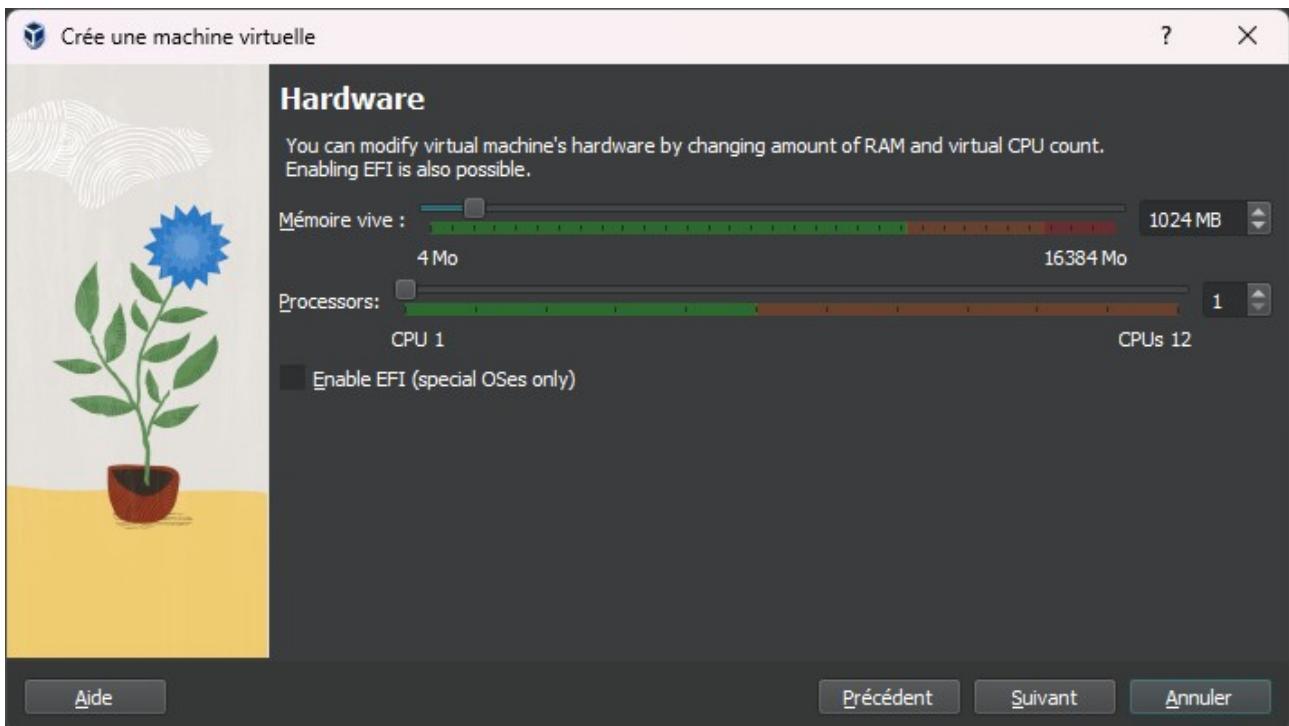
Dans la case nom taper le nom que vous désirez donner à votre machine, dans la case ISO image vous sélectionnez l'image présentement téléchargée puis dans type sélectionnez BSD et dans version sélectionnez FreeBSD (64bits).

Ce qui donne ceci.

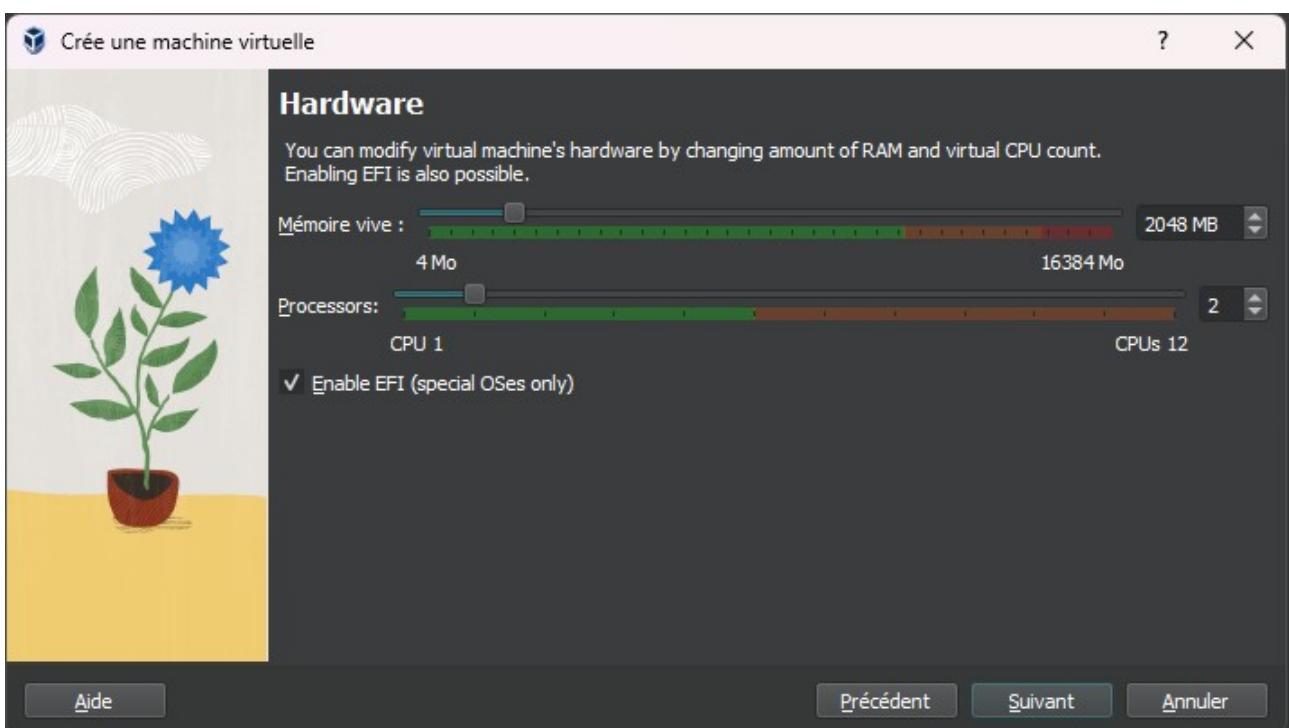


Cliquer ensuite sur suivant.

Vous arriverez sur la page suivante.

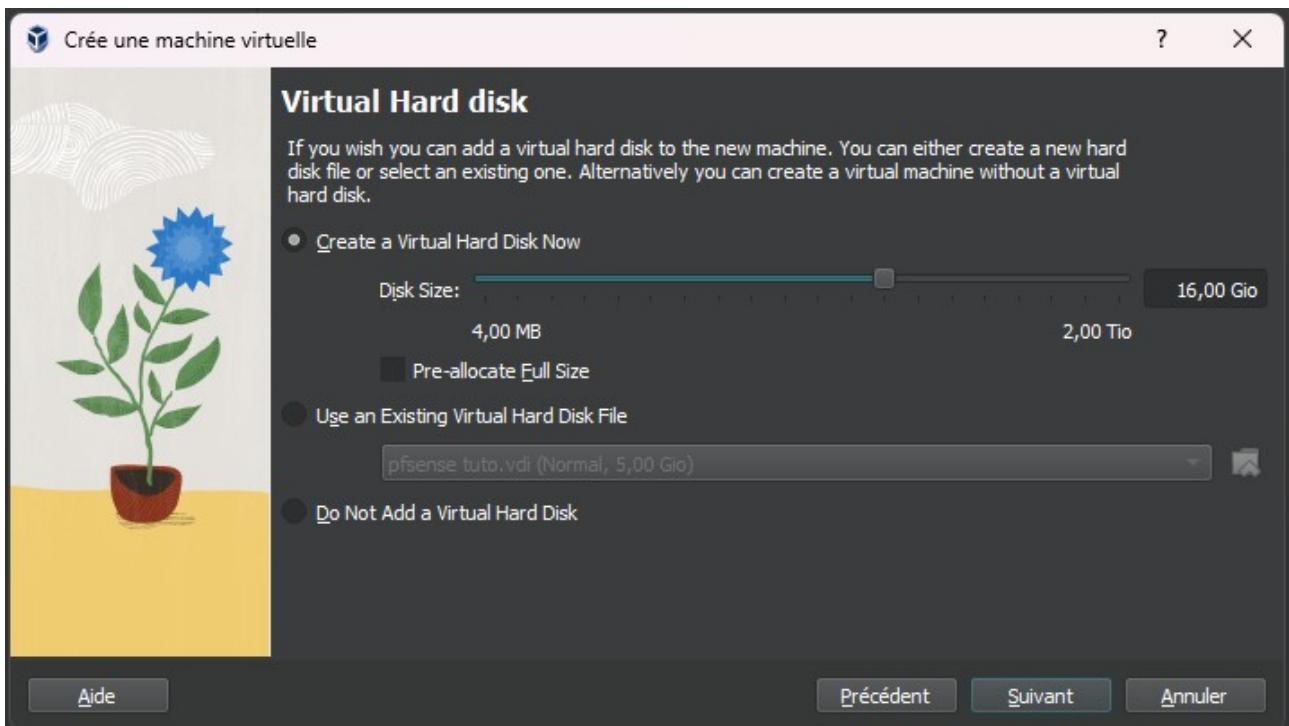


Vous choisirez dans Mémoire vive 2048 MB puis dans Processors Vous choisisrez 2 et cocherai Enable EFI comme ceci.



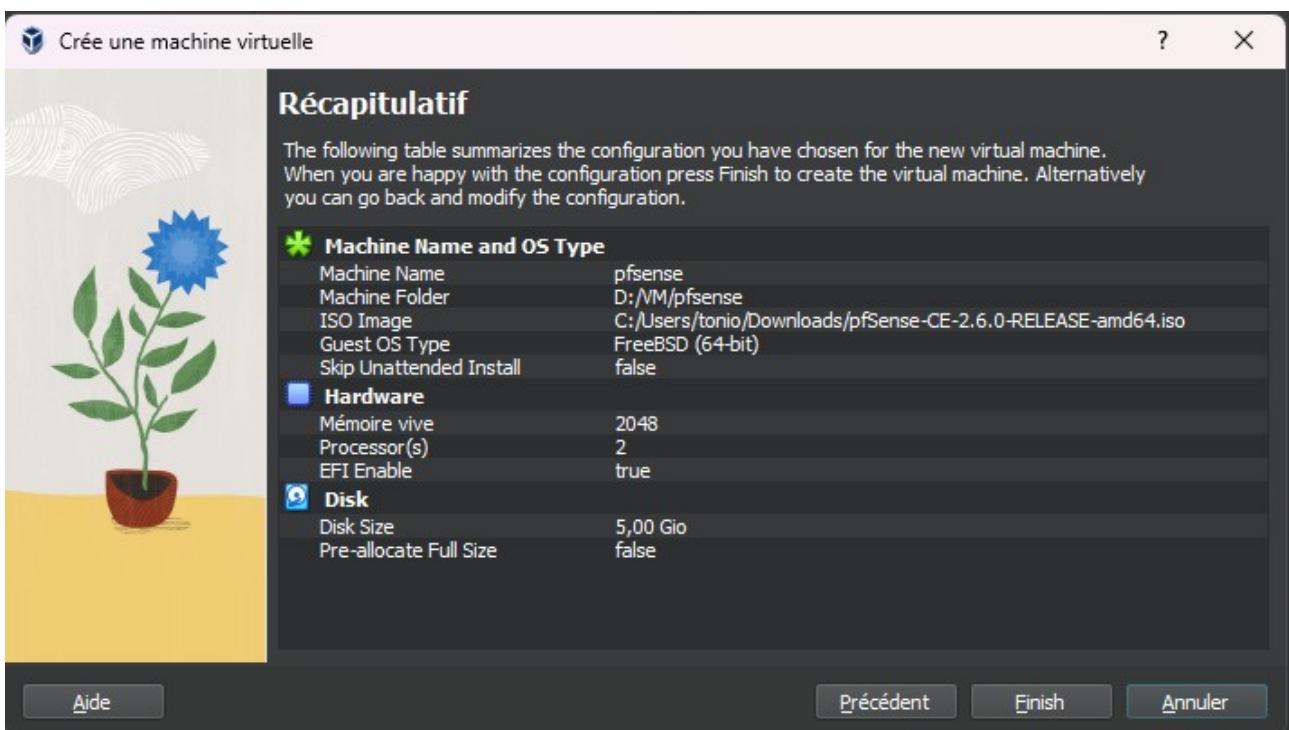
Cliquer ensuite sur suivant.

Vous arriverez sur la page suivent.

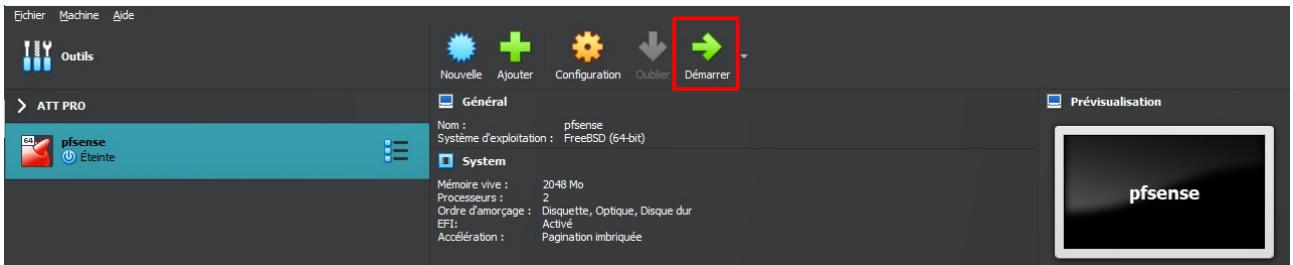


Vous choisirez 5 Gio et faites suivant.

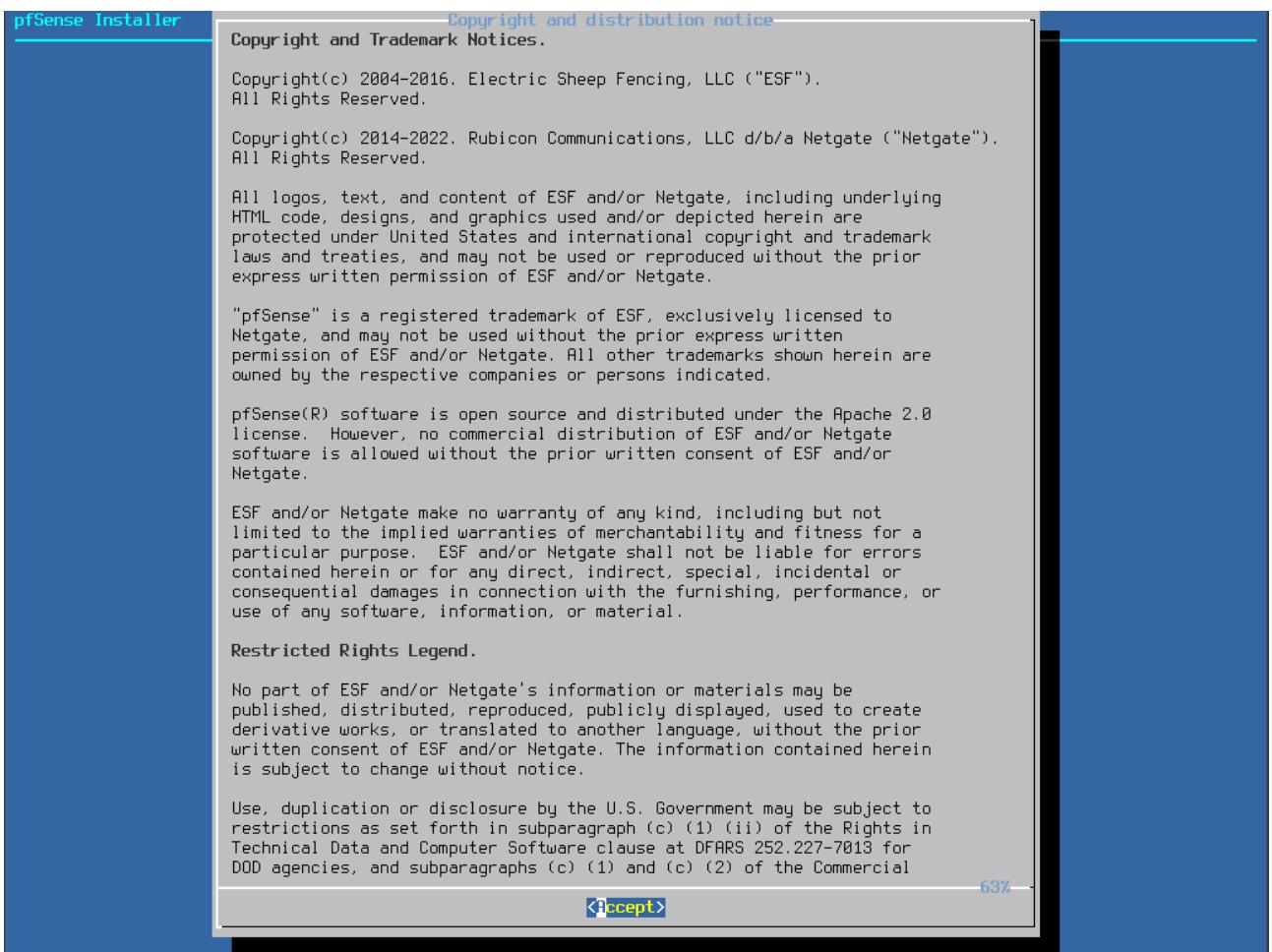
Vous arriverez sur la page suivent.



Puis cliquer sur finish.

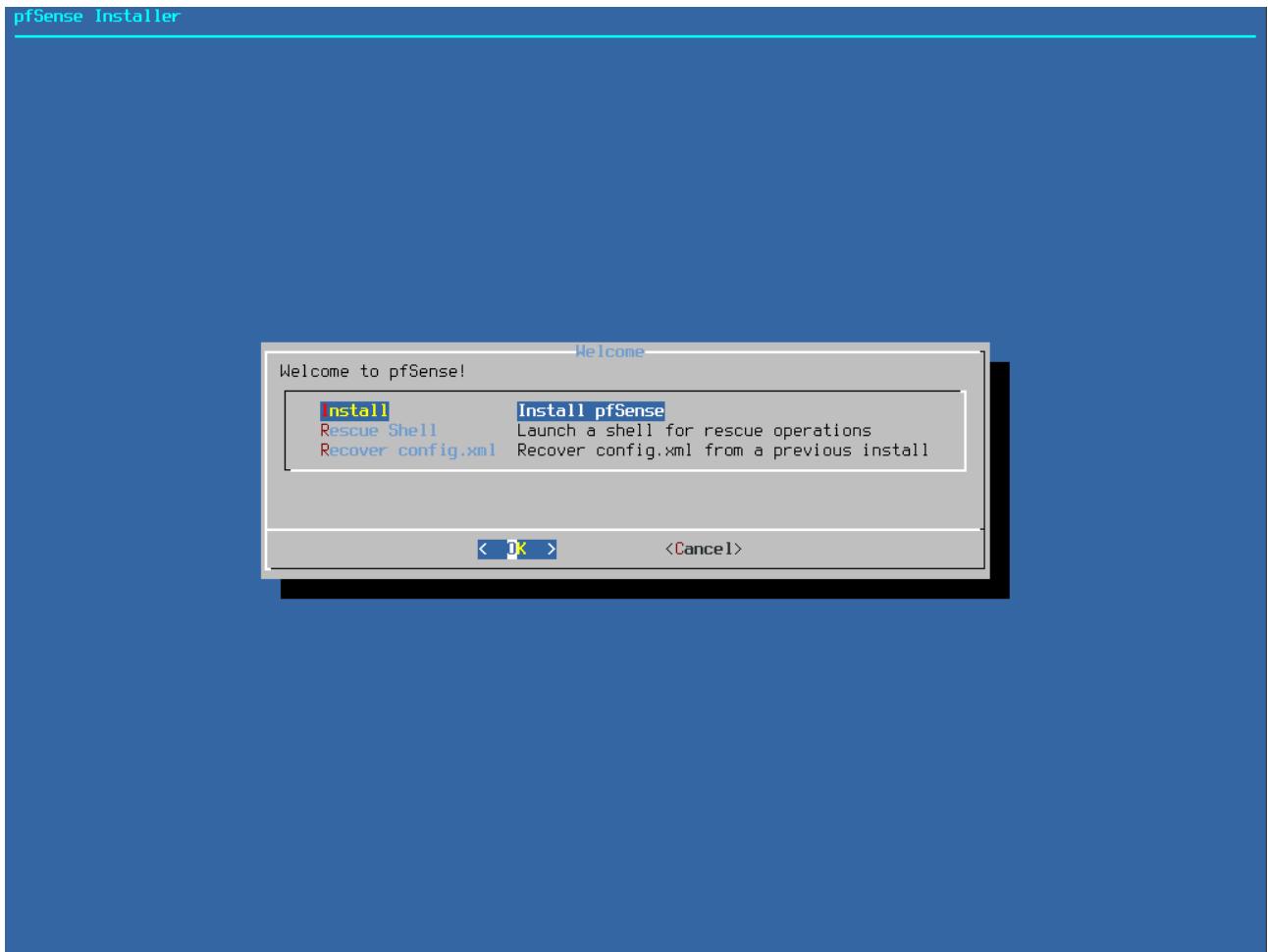


Vous double cliquer sur votre machine ou cliquer sur démarrer.



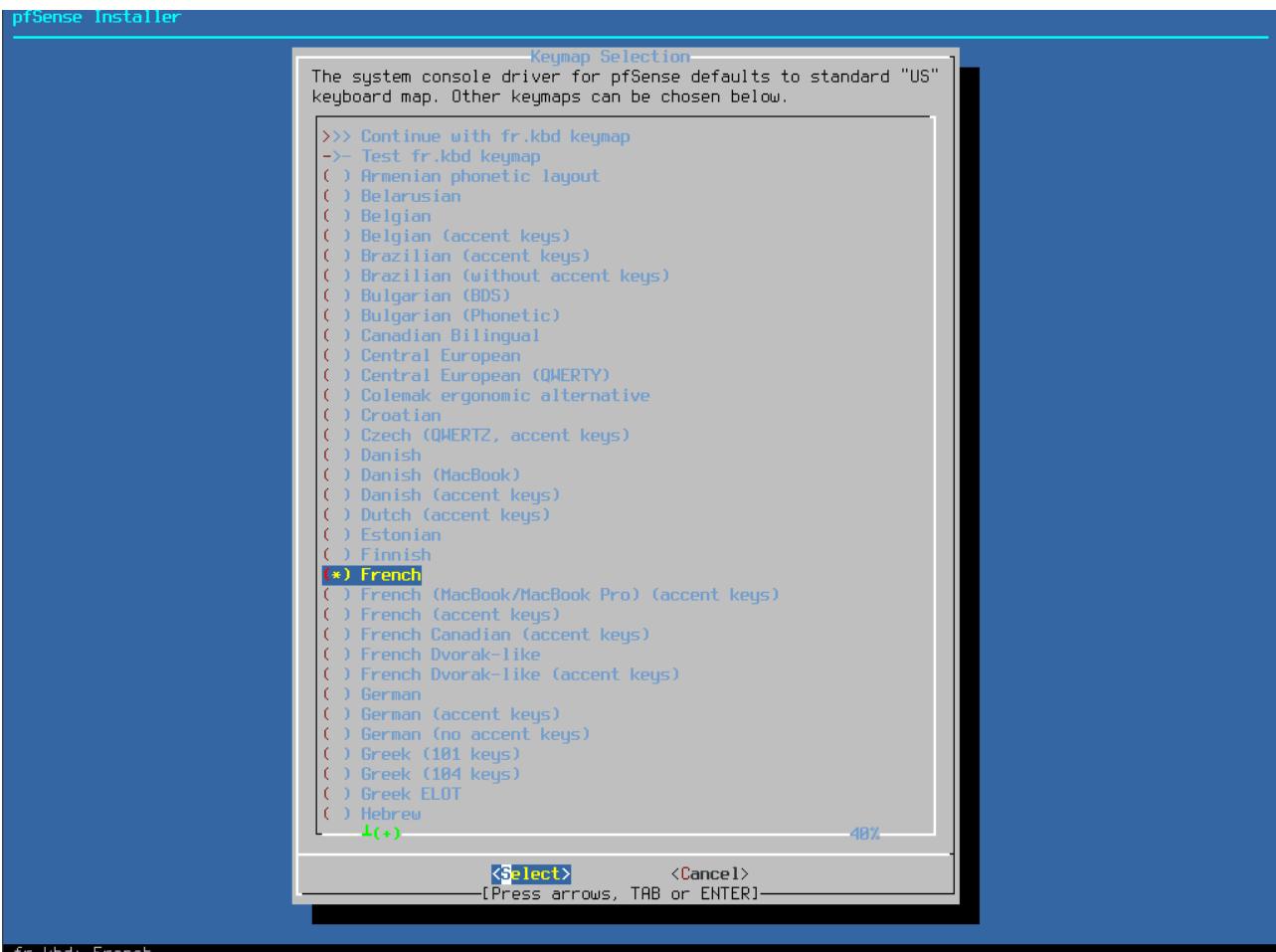
Vous arriverez sur cette page appuyer sur votre touche espace pour accepter.

Vous arriverez sur cette page.

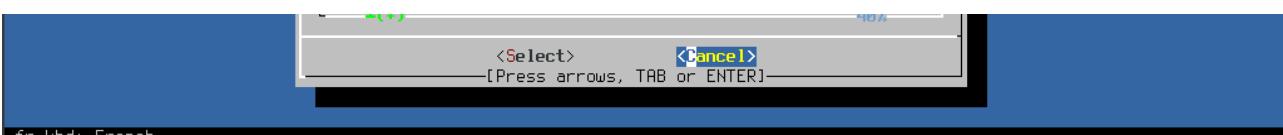


Appuyer sur votre touche entrer en étant sur Install.

Vous arriverez sur la page suivante.



Avec les flèche directionnel vous descendrez jusqu'à French apurai sur entrer.

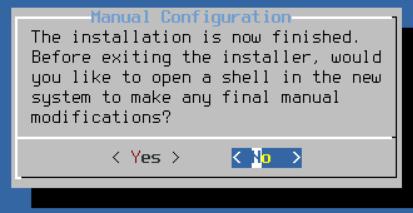


Puis apurai sur espace pour avoir Cancel de sélectionner et apurai sur entrer.

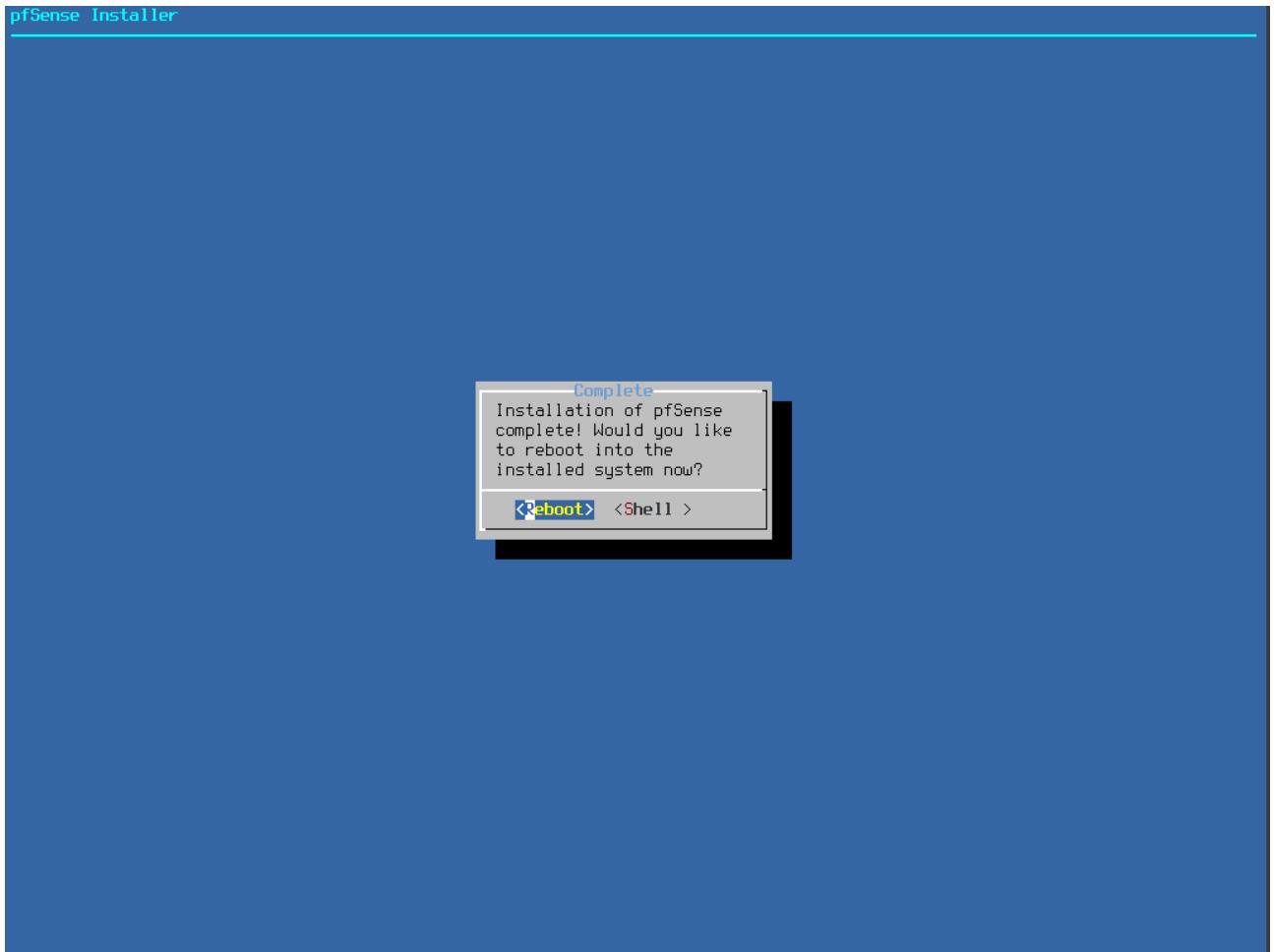
Vous arriverez ici.



Puis sélectionnerai avec les flèche directionnel UEFI et appuierai sur entrer.



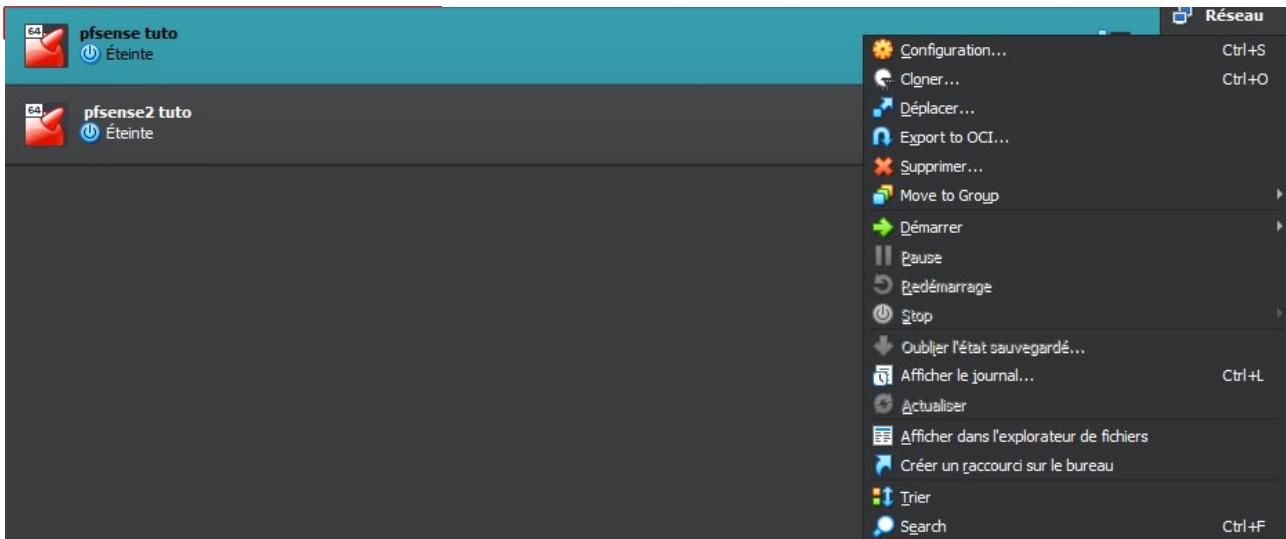
Puis sélectionnerai avec les flèche directionnel no et apurai sur entrer.



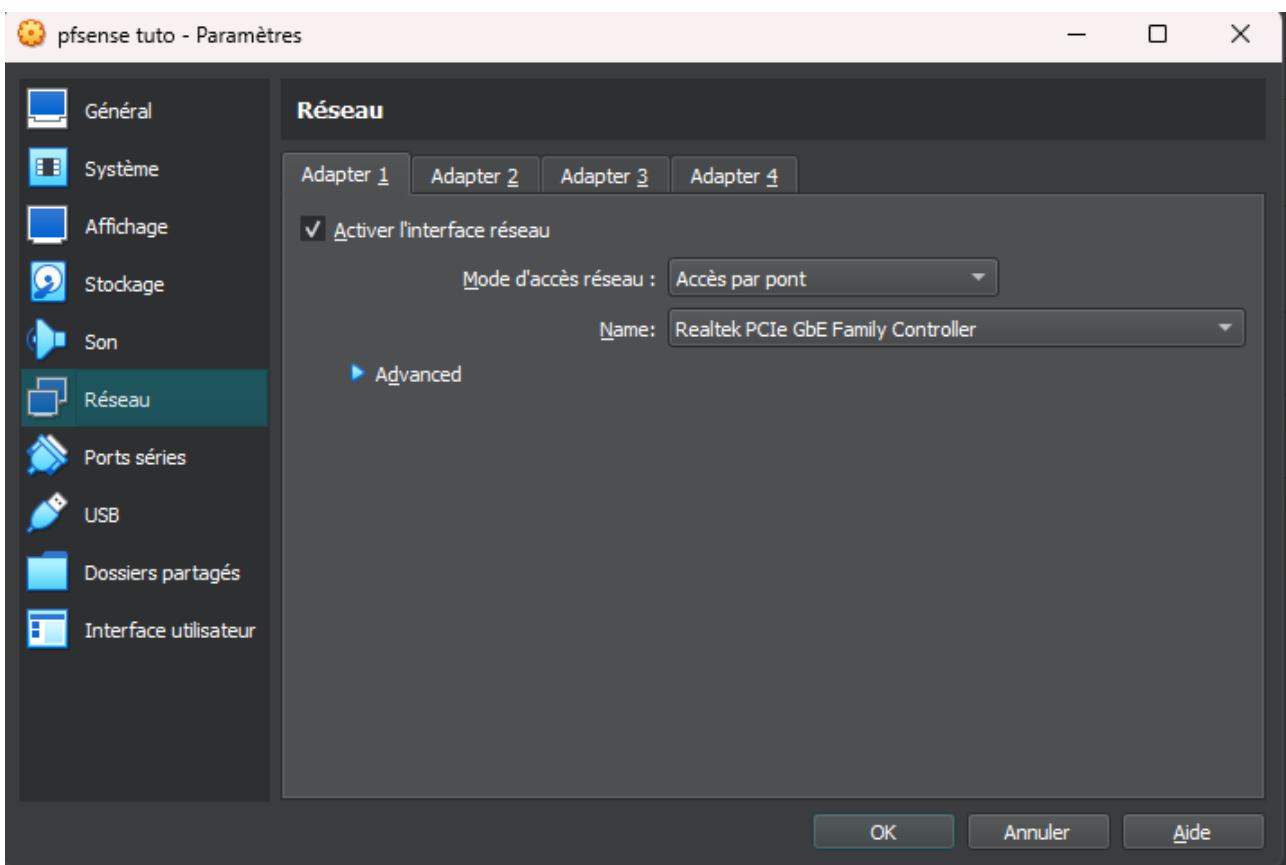
Et apurai sur espace et éjecterai le disque (en bas a droite de la fenêtre) / retiré la clef bootable pour ce qui on choisie la deuxième option .

Configuration terminal du PfSense1

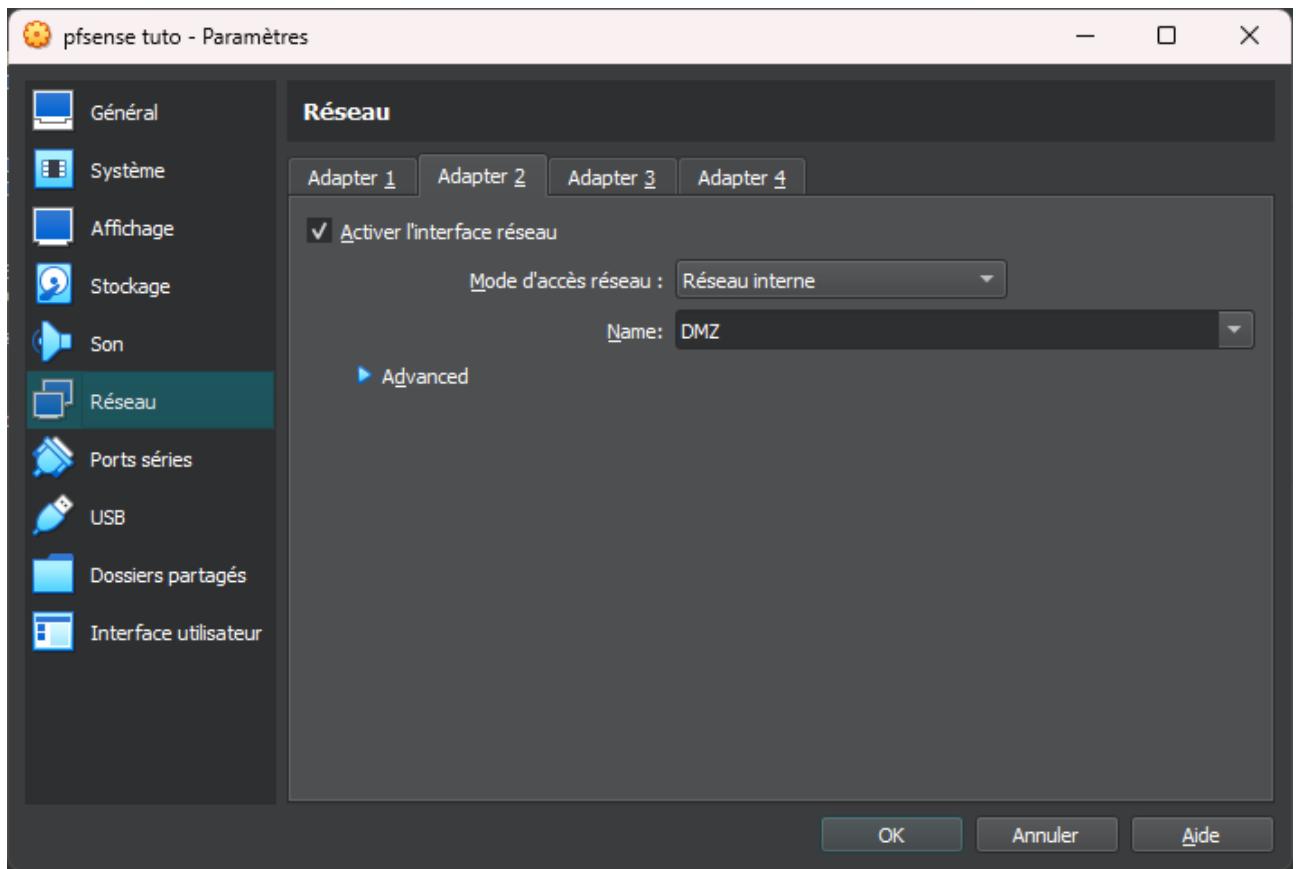
A partir de la vous éteignez la machine.



Vous faites un clique droit sur votre machine et cliquer sur configuration.



Vous cliquer sur Réseau puis configurer le mode d'accès réseau comme si dessus la section name est différent pour tout le monde ne vous en occuper pas



cliquer sur adapter 2 cocher la case Activer l'interface réseau mettez ensuite le mode d'accès réseau en Réseau interne puis dans name écrivez « DMZ » appuyer sur OK et démarrer la machine.

```

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.
Generating RRD graphs...done.
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)

VirtualBox Virtual Machine - Netgate Device ID: ef372f60b46595a3fccb

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.200/24
                           v6/DHCP6: 2a01:e0a:5c1:8d40:a00:27ff:fed6:ac6e/64
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: 1

```

Vous arrivez ici. Nous allons configurer le Pfsense1 de manière suivant taper 1 pour accéder a l'assignement des interface.

```

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.200/24
                           v6/DHCP6: 2a01:e0a:5c1:8d40:a00:27ff:fed6:ac6e/64
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: 1

Valid interfaces are:

em0      08:00:27:c6:ac:6e  (up) Intel(R) Legacy PRO/1000 MT 82540EM
em1      08:00:27:d9:d5:2e  (up) Intel(R) Legacy PRO/1000 MT 82540EM

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y/n]? n

```

Le Pfsense vous demande si vous voulez créeé des VLAN vous mettez n pour non car dans notre cas nous n'en avons pas

```
Valid interfaces are:
em0      08:00:27:c6:ac:6e  (up) Intel(R) Legacy PRO/1000 MT 82540EM
em1      08:00:27:d9:d5:2e  (up) Intel(R) Legacy PRO/1000 MT 82540EM

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y\?n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 or a): em0
```

Le Pfsense vous demande quel interface voulez vous entent qu'interface WAN mettez la em0 ou pc0 ou tout autre chose 0 sa peut variez.

```
If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 a or nothing if finished): em1
```

Le Pfsense vous demande quel interface voulez vous entent qu'interface LAN mettez la em1.

```
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 a or nothing if finished): em1

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1

Do you want to proceed [y\?n]? y
```

Le Pfsense vous demande si l'assignement vous convient vous mettez y pour oui.

```
The interfaces will be assigned as follows:
WAN  -> em0
LAN  -> em1

Do you want to proceed [y\?n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
VirtualBox Virtual Machine - Netgate Device ID: ef372f60b46595a3fccb

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.200/24
                           v6/DHCP6: 2a01:e0a:5c1:8d40:a00:27ff:fe6:ac6e/64
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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

Enter an option: 2
```

Nous allons configurer l'assignement des IP aux interface tapez 2

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.200/24
                           v6/DHCP6: 2a01:e0a:5c1:8d40:a00:27ff:fea6:ac6e/64
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: 1
```

On choisie l'interface WAN tapez 1.

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

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

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

le Pfsense demande si l'interface doit prendre son IPv4 en DHCP dit oui (y).

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

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

le Pfsense demande si l'interface doit prendre son IPv6 en DHCP dit non (n).

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

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

le Pfsense demande de configurer l'assignement d'une IPv6 statique vous passez.

```
Enter the new WAN IPv6 address. Press <ENTER> for none:  
>  
Disabling IPv4 DHCPD...  
Disabling IPv6 DHCPD...  
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

le Pfsense demande si il doit déplacer l'interface Web dite non (n).

```
Enter the new WAN IPv6 address. Press <ENTER> for none:  
>  
Disabling IPv4 DHCPD...  
Disabling IPv6 DHCPD...  
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n  
Please wait while the changes are saved to WAN...  
Reloading filter...  
Reloading routing configuration...  
DHCPD...  
The IPv4 WAN address has been set to dhcp  
Press <ENTER> to continue.
```

Appuyez sur entre.

```
Please wait while the changes are saved to WAN...  
Reloading filter...  
Reloading routing configuration...  
DHCPD...  
The IPv4 WAN address has been set to dhcp  
Press <ENTER> to continue.  
VirtualBox Virtual Machine - Netgate Device ID: ef372f60b46595a3fccb  
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***  
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.200/24  
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
```

Tapez 2 une nouvelle fois.

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***  
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.200/24  
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)  
2 - LAN (em1 - static)  
Enter the number of the interface you wish to configure: 2
```

Mais cette fois on configure l'interface LAN donc tapez 2.

```
Available interfaces:  
1 - WAN (em0 - dhcp)  
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:  
> 10.0.0.254
```

le Pfsense demande de taper l'IPv4 statique dans notre cas c'est 10.0.0.254.

Il vous demande le masque tapez 24.

```
Enter the new LAN IPv4 address. Press <ENTER> for none:  
> 10.0.0.254  
  
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
```

```
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:  
> 
```

Il vous demande une passerelle ne mettez rien et passez.

```
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:  
> 
```

le Pfsense demande de taper l'IPv6 statique passez.

```
Enter the new LAN IPv6 address. Press <ENTER> for none:  
>  
  
Do you want to enable the DHCP server on LAN? (y/n) n
```

Il vous demande si il doit servir de DHCP dites non (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) n
```

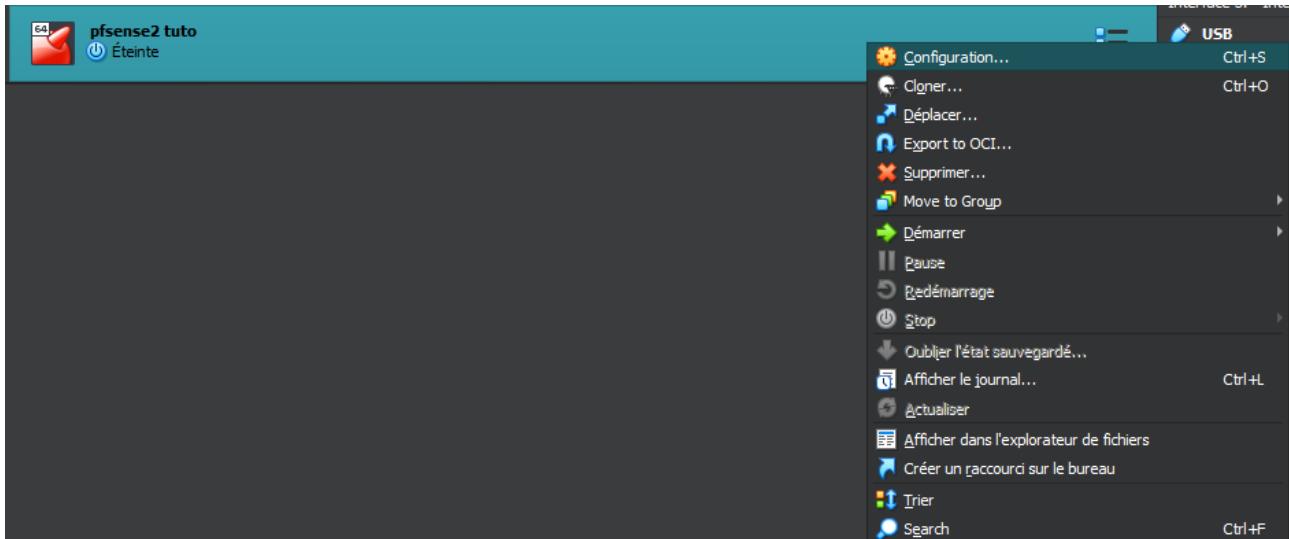
Il vous redemande si il doit déplacer l'interface web dite non (n).

```
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n  
  
Please wait while the changes are saved to LAN...  
  Reloading filter...  
  Reloading routing configuration...  
  DHCPD...  
  
The IPv4 LAN address has been set to 10.0.0.254/24  
You can now access the webConfigurator by opening the following URL in your web browser:  
  https://10.0.0.254/  
  
Press <ENTER> to continue.
```

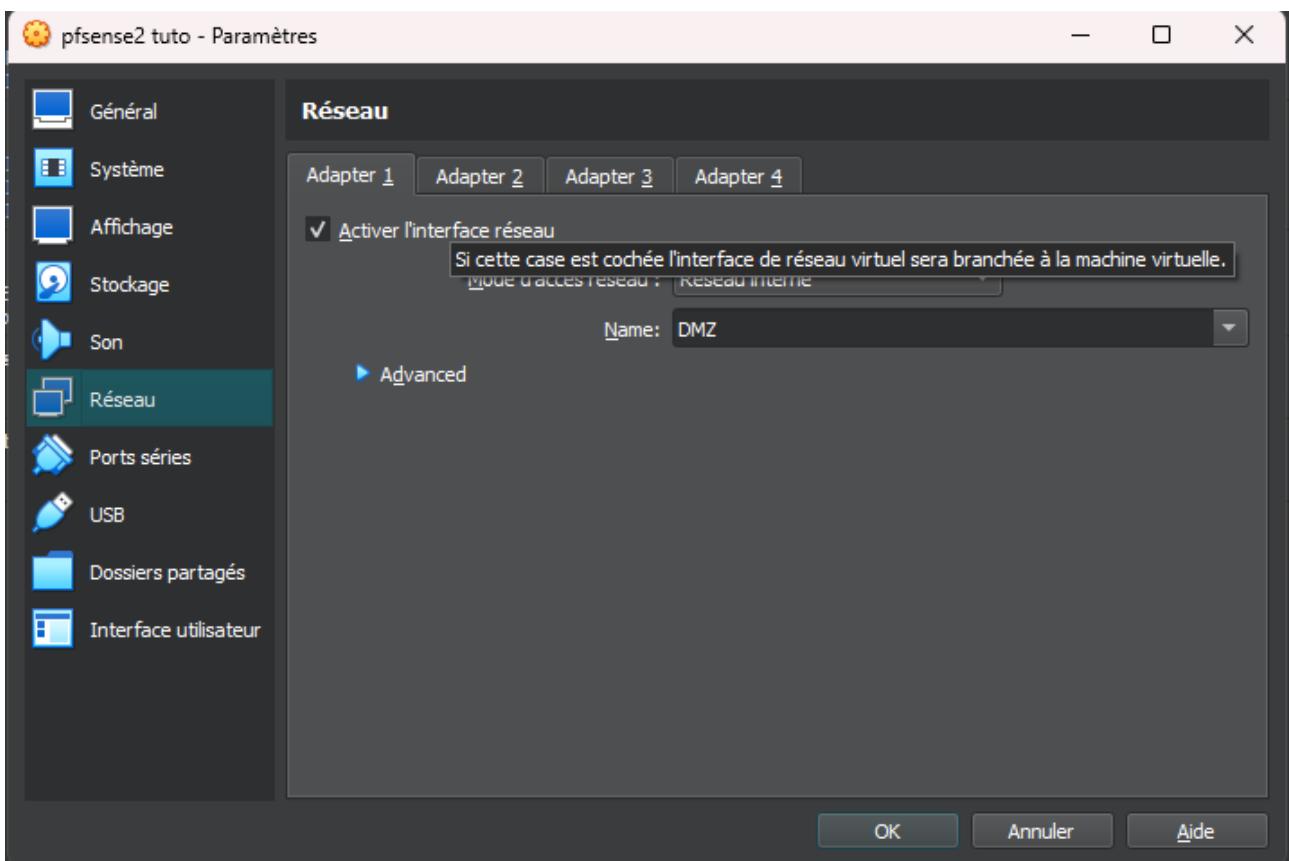
Appuyez sur entrer et ne pas éteindre la machine.

Configuration terminal du PfSense2

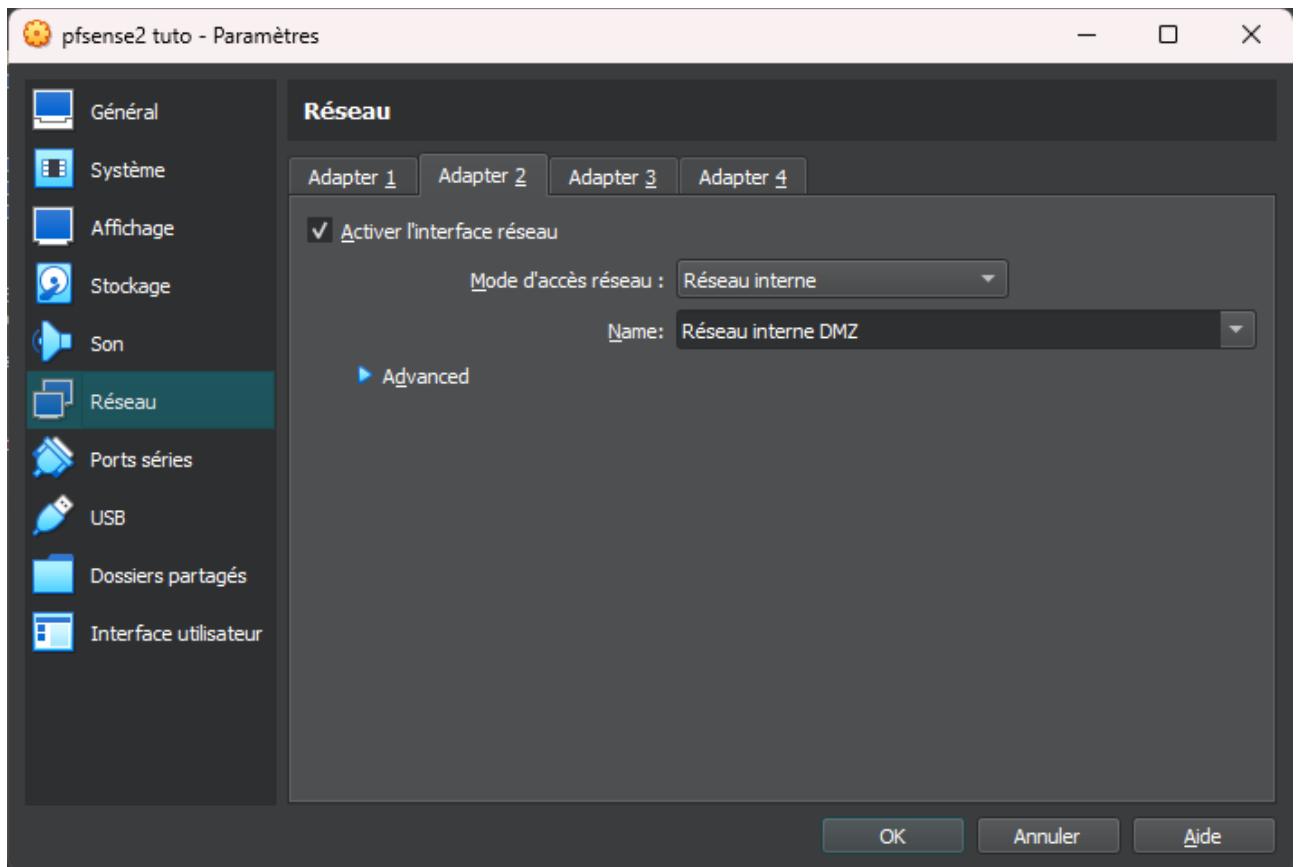
Installer un 2ème PfSense.



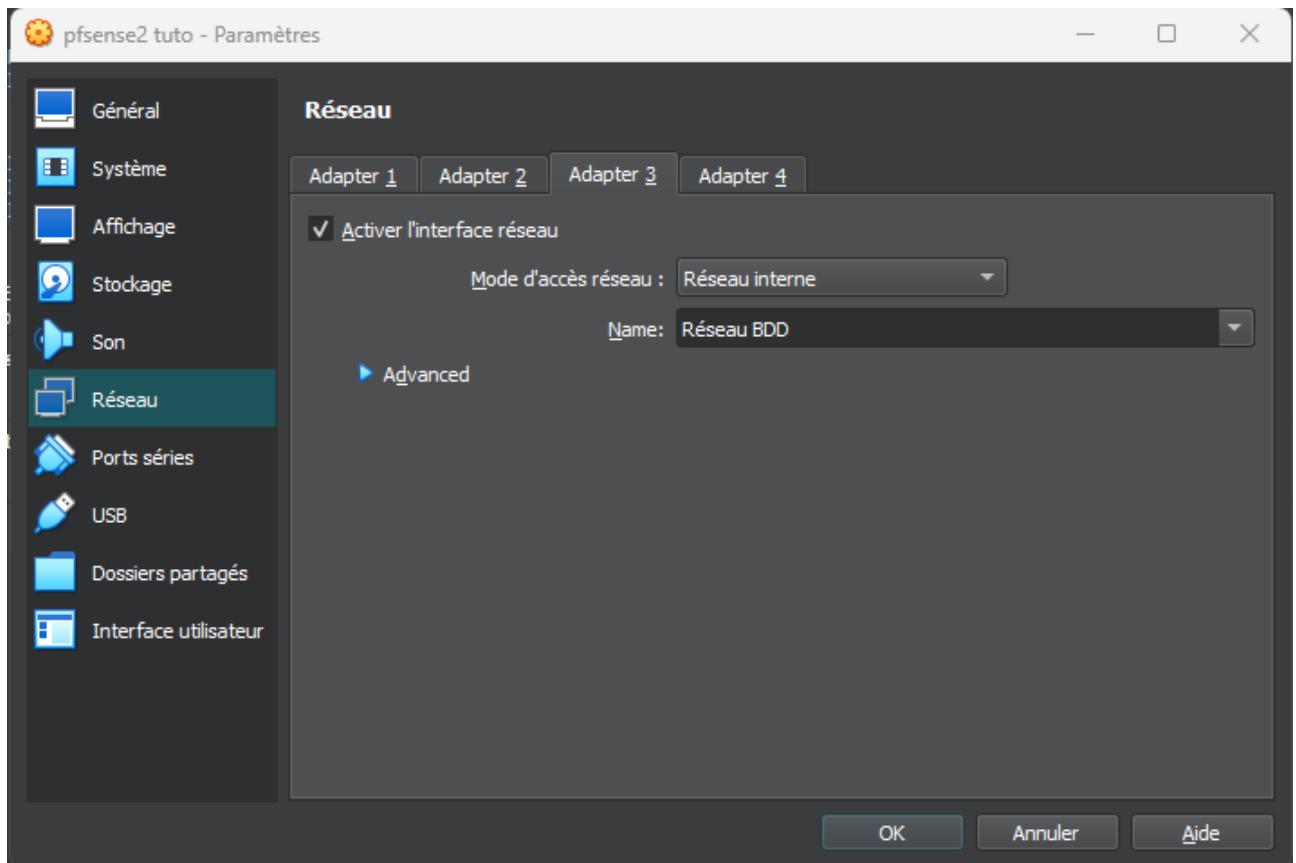
Allez dans configuration.



Dans mode d'accès réseau mettez réseau interne et sectionnez DMZ.



cliquer sur adapter 2 cocher la case Activer l'interface réseau mettez ensuite le mode d'accès réseau en Réseau interne puis dans name écrivez «Réseau interne DMZ»



cliquer sur adapter 3 cocher la case Activer l'interface réseau mettez ensuite le mode d'accès réseau en Réseau interne puis dans name écrivez «Réseau BDD» appuyer sur OK et démarrer la machine.

```
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.
Generating RRD graphs...done.
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)
```

```
VirtualBox Virtual Machine - Netgate Device ID: acd6bef04f88b5b9f1a
```

```
*** 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: 1
```

Tapez 1 pour assigner les interfaces.

```
*** 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: 1
```

```
Valid interfaces are:
```

```
em0      08:00:27:c6:ac:6e  (up) Intel(R) Legacy PRO/1000 MT 82540EM
em1      08:00:27:0b:13:96  (up) Intel(R) Legacy PRO/1000 MT 82540EM
em2      08:00:27:38:ec:7b (down) Intel(R) Legacy PRO/1000 MT 82540EM
```

```
Do VLANs need to be set up first?
```

```
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.
```

```
Should VLANs be set up now [y/n]? n
```

Tapez n puis que nous n'avons pas de VLAN.

```
Should VLANs be set up now [y\ln]? n
If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 or a): em0
```

Tapez em0 pour assigner l'interface 1 à l'interface WAN.

```
Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 a or nothing if finished): em1
```

Tapez em1 pour assigner l'interface 2 à l'interface LAN.

```
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 a or nothing if finished): em1

Enter the Optional 1 interface name or 'a' for auto-detection
(em2 a or nothing if finished): em2
```

Tapez em2 pour assigner l'interface 3 à l'interface OPT1.

```
Enter the Optional 1 interface name or 'a' for auto-detection
(em2 a or nothing if finished): em2

The interfaces will be assigned as follows:
WAN -> em0
LAN -> em1
OPT1 -> em2

Do you want to proceed [y\ln]? y
```

Le Pfsense vous demande si sa vous va tapez y.

```
The interfaces will be assigned as follows:
WAN -> em0
LAN -> em1
OPT1 -> em2

Do you want to proceed [y\ln]? y

Writing configuration...done.
One moment while the settings are reloading... done!
VirtualBox Virtual Machine - Netgate Device ID: acd6bef04f88b5b9f1a

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

WAN (wan)      -> em0      ->
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
OPT1 (opt1)    -> em2      ->

 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

Enter an option: 2
```

Tapez 2 pour assigner des IP aux interfaces.

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

WAN (wan)      -> em0      ->
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
OPT1 (opt1)    -> em2      ->

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)
2 - LAN (em1 - static)
3 - OPT1 (em2)

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

Tapez 1 pour assigner une IP a l'interface WAN.

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

WAN (wan)      -> em0      ->
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
OPT1 (opt1)    -> em2      ->

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)
2 - LAN (em1 - static)
3 - OPT1 (em2)

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

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

Le Pfsense vous propose d'assigner une IPv4 par DHCP dites non (n).
le Pfsense demande de taper l'IPv4 statique dans notre cas c'est 10.0.0.253.

```
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 10.0.0.253

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
```

le Pfsense demande un masque tapez 24.

```
Enter the new WAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 10.0.0.254
```

le Pfsense demande la passerelle du WAN tapez 10.0.0.254

```
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 10.0.0.254

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

Le Pfsense vous propose d'assigner une IPv6 par DHCP dites non (n).

```
Configure IPv6 address WAN interface via DHCP6? (y/n) n
Enter the new WAN IPv6 address. Press <ENTER> for none:
> █
```

le Pfsense demande de taper l'IPv6 statique passez.

```
Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n █
```

Le Pfsense demande si vous voulez déplacer l'interface Web dite non (n).

```
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
Please wait while the changes are saved to WAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
The IPv4 WAN address has been set to 10.0.0.253/24
Press <ENTER> to continue. █
```

Appuyer sur entrer.

```
Please wait while the changes are saved to WAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
The IPv4 WAN address has been set to 10.0.0.253/24
Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: acd6bef04f88b5b9f1a
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4: 10.0.0.253/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
OPT1 (opt1)    -> em2      ->
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 █
```

Tapez 2 pour assigner des IP aux interfaces.

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

```
WAN (wan)      -> em0      -> v4: 10.0.0.253/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
OPT1 (opt1)    -> em2      ->

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)
3 - OPT1 (em2)
```

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

Tapez 2 pour assigner une IP a l'interface LAN.

```
Available interfaces:
```

```
1 - WAN (em0 - static)
2 - LAN (em1 - static)
3 - OPT1 (em2)
```

```
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
```

le Pfsense demande de taper l'IPv4 statique dans notre cas c'est 192.168.10.254.

```
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:
> 
```

le Pfsense demande la passerelle du LAN passez.

```
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:
> 
```

le Pfsense demande de taper l'IPv6 statique passez.

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

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

Le Pfsense demande si il doit servir de DHCP dites non (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) n
```

Le Pfsense demande si vous voulez déplacer l'interface Web dite non (n).

```
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

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:
  https://192.168.10.254/

Press <ENTER> to continue.
```

Appuyer sur entrer.

```
Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

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:
  https://192.168.10.254/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: acd6bef04f88b5b9f1a

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

WAN (wan)      -> em0      -> v4: 10.0.0.253/24
LAN (lan)      -> em1      -> v4: 192.168.10.254/24
OPT1 (opt1)    -> em2      ->

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
```

Tapez 2 pour assigner l'IP à la dernière interface.

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

WAN (wan)      -> em0      -> v4: 10.0.0.253/24
LAN (lan)      -> em1      -> v4: 192.168.10.254/24
OPT1 (opt1)    -> em2      ->

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)
3 - OPT1 (em2)

Enter the number of the interface you wish to configure: 3
```

Tapez 3 pour assigner une IP a l'interface OPT1.

```
Available interfaces:  
1 - WAN (em0 - static)  
2 - LAN (em1 - static)  
3 - OPT1 (em2)  
  
Enter the number of the interface you wish to configure: 3  
Enter the new OPT1 IPv4 address. Press <ENTER> for none:  
> 192.168.20.254
```

le Pfsense demande de taper l'IPv4 statique dans notre cas c'est 192.168.20.254.

```
Enter the new OPT1 IPv4 address. Press <ENTER> for none:  
> 192.168.20.254  
  
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 OPT1 IPv4 subnet bit count (1 to 32):  
> 24
```

le Pfsense demande un masque tapez 24.

```
Enter the new OPT1 IPv4 subnet bit count (1 to 32):  
> 24  
  
For a WAN, enter the new OPT1 IPv4 upstream gateway address.  
For a LAN, press <ENTER> for none:  
> █
```

le Pfsense demande la passerelle du OPT1 passez.

```
For a WAN, enter the new OPT1 IPv4 upstream gateway address.  
For a LAN, press <ENTER> for none:  
>  
  
Enter the new OPT1 IPv6 address. Press <ENTER> for none:  
> █
```

le Pfsense demande de taper l'IPv6 statique passez.

```
Enter the new OPT1 IPv6 address. Press <ENTER> for none:  
>  
Do you want to enable the DHCP server on OPT1? (y/n) n
```

Le Pfsense demande si il doit servir de DHCP dites non (n).

```
Do you want to enable the DHCP server on OPT1? (y/n) n  
Disabling IPv4 DHCPD...  
Disabling IPv6 DHCPD...  
  
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

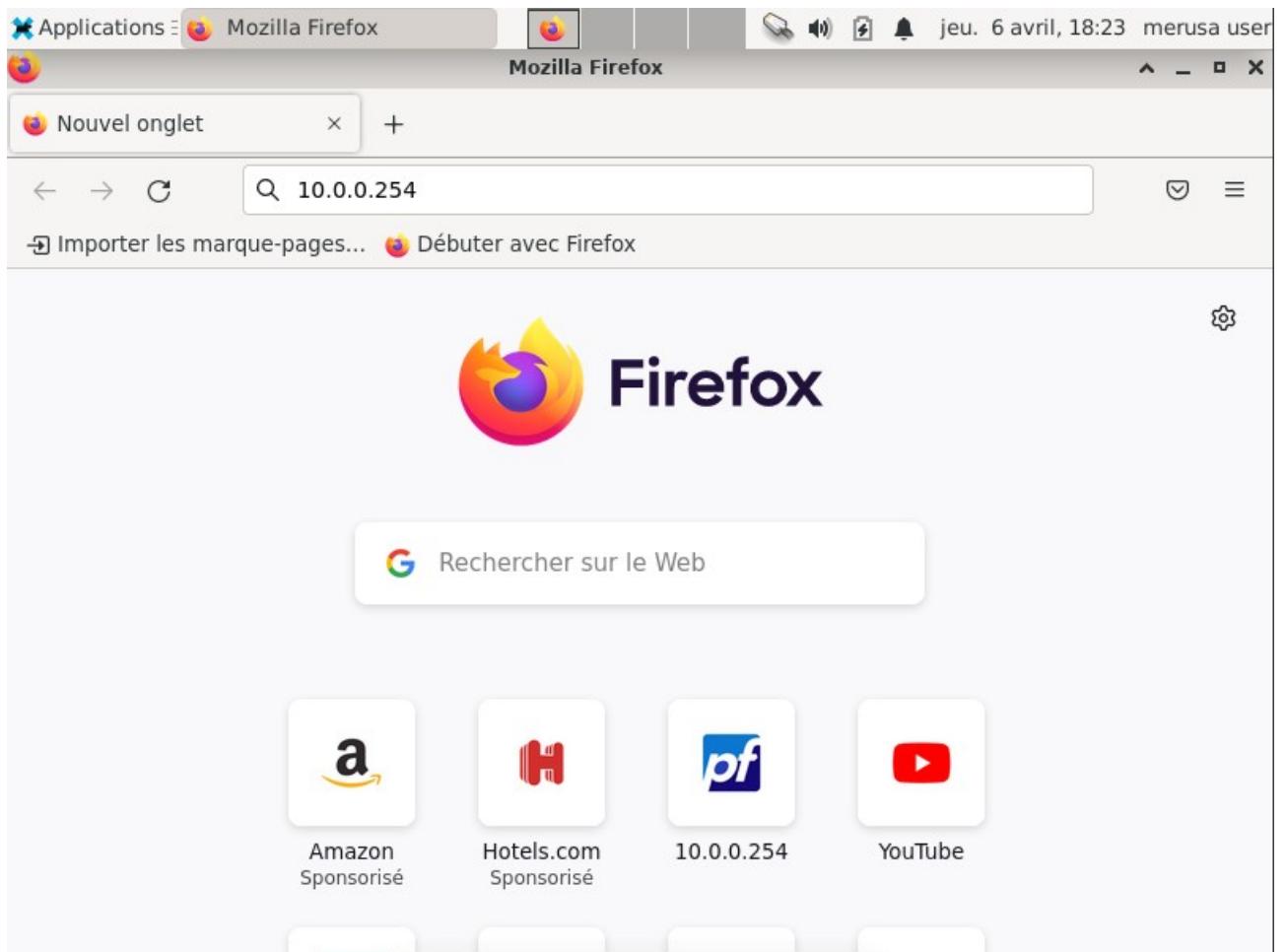
Le Pfsense demande si vous voulez déplacer l'interface Web dite non (n).

Appuyez sur entrer et ne pas éteindre la machine.

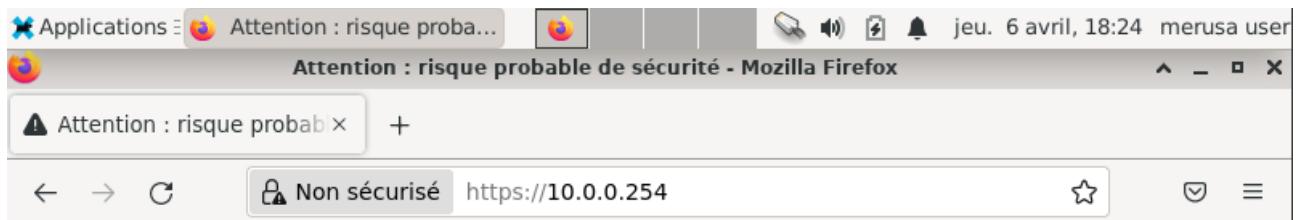
```
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n  
  
Please wait while the changes are saved to OPT1...  
  Reloading filter...  
  Reloading routing configuration...  
  DHCPD...  
  
The IPv4 OPT1 address has been set to 192.168.20.254/24  
  
Press <ENTER> to continue. █
```

Pré-configuration graphique des Pfsense

Pour commencer brancher vous sur le réseau LAN du Pfsense que vous voulez configurer.



Ouvrir un navigateur et taper l'IP LAN du Pfsense à configurer et taper sur entrer.



Attention : risque probable de sécurité

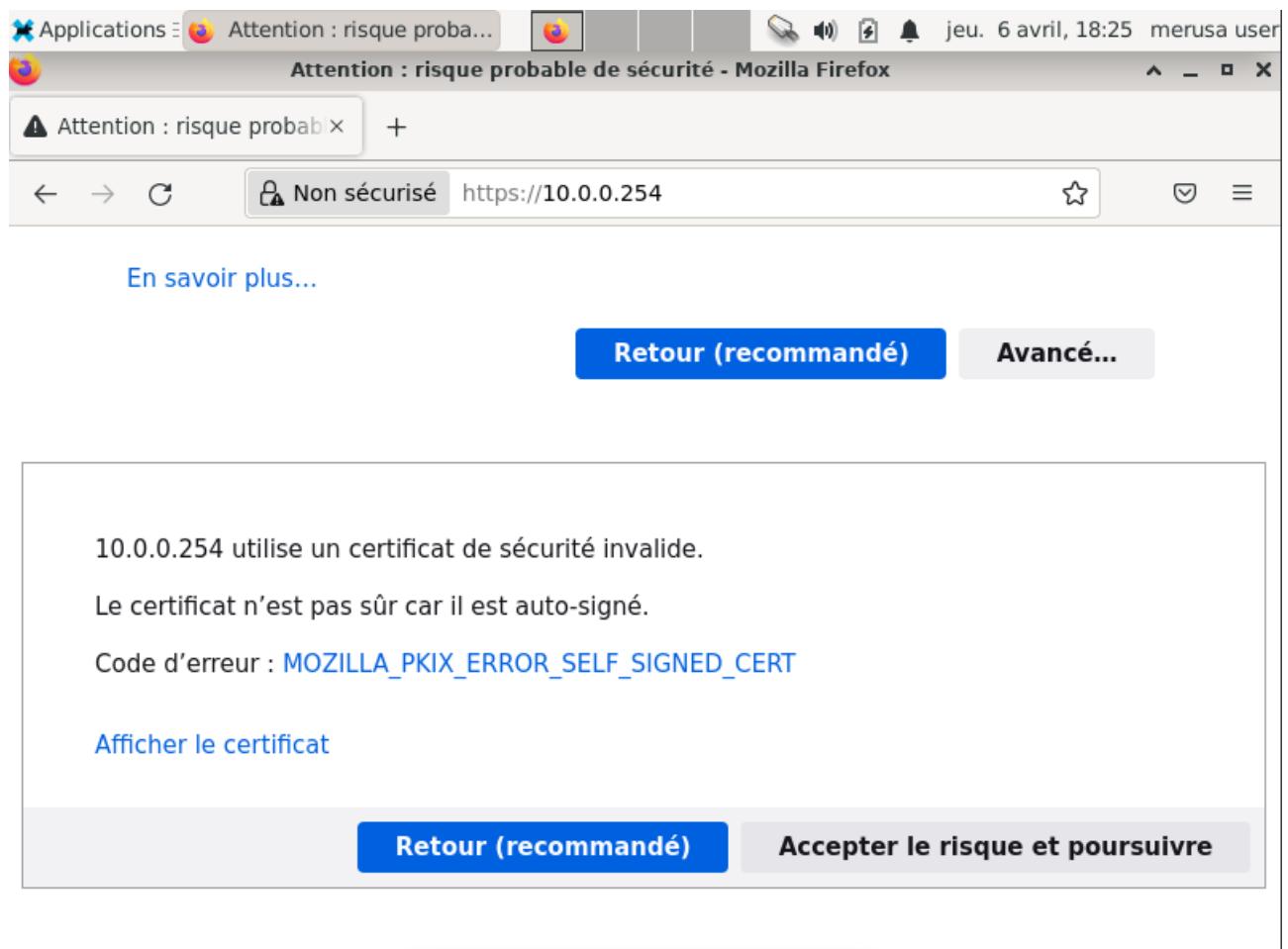
Firefox a détecté une menace de sécurité potentielle et n'a pas poursuivi vers 10.0.0.254. Si vous accédez à ce site, des attaquants pourraient dérober des informations comme vos mots de passe, e-mails, ou données de carte bancaire.

[En savoir plus...](#)

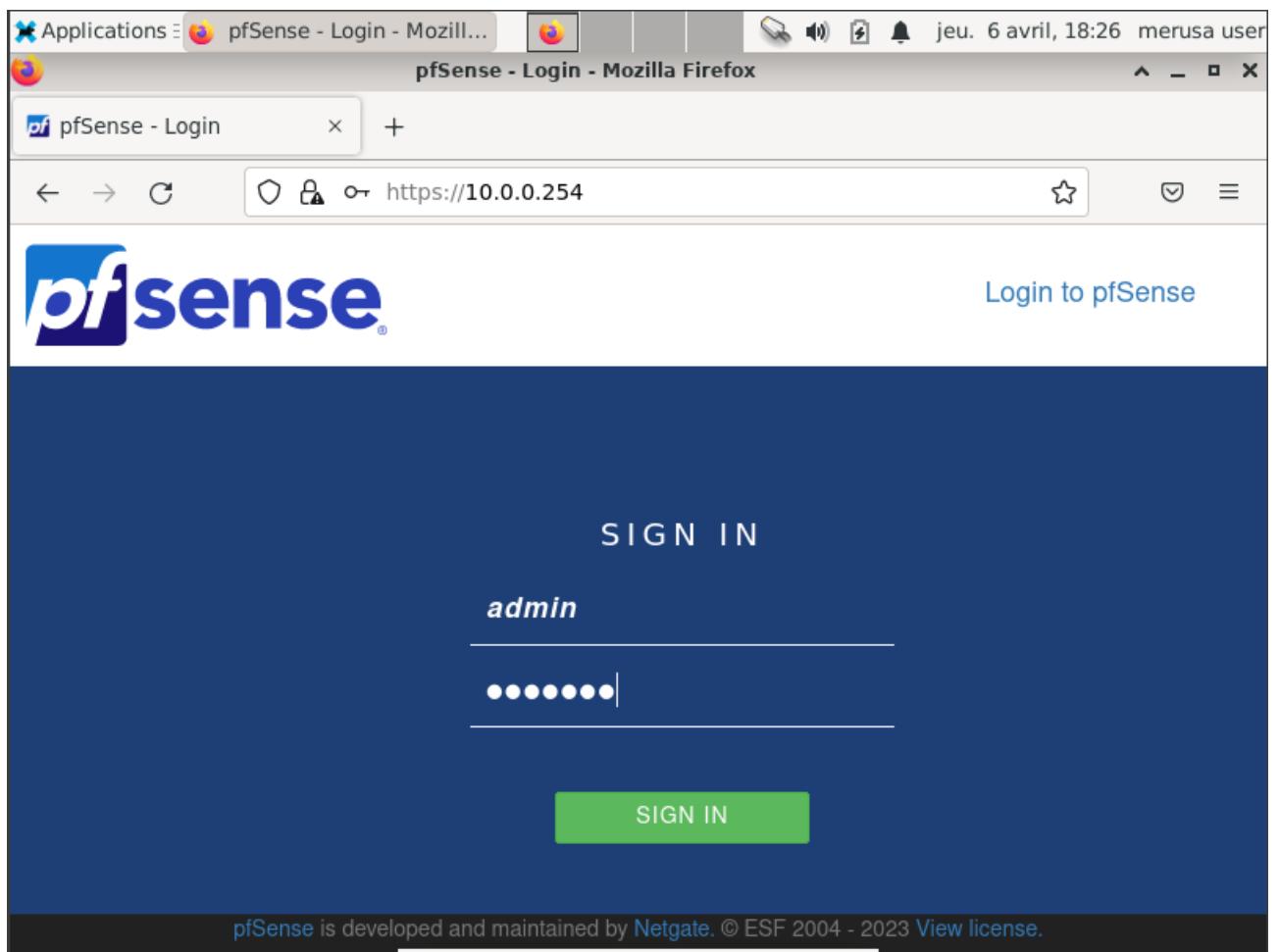
[Retour \(recommandé\)](#)

[Avancé...](#)

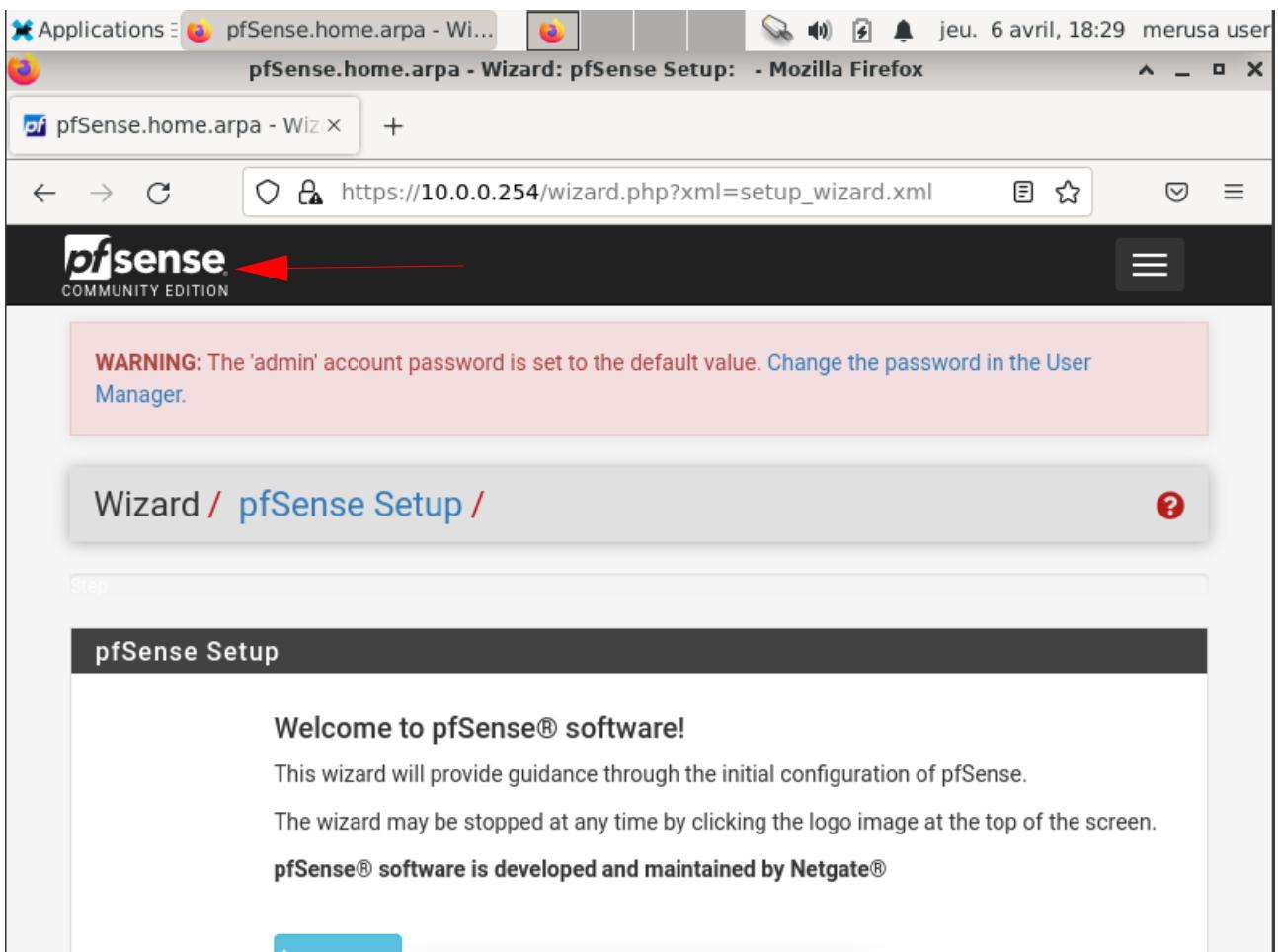
Cliquer sur avancé.



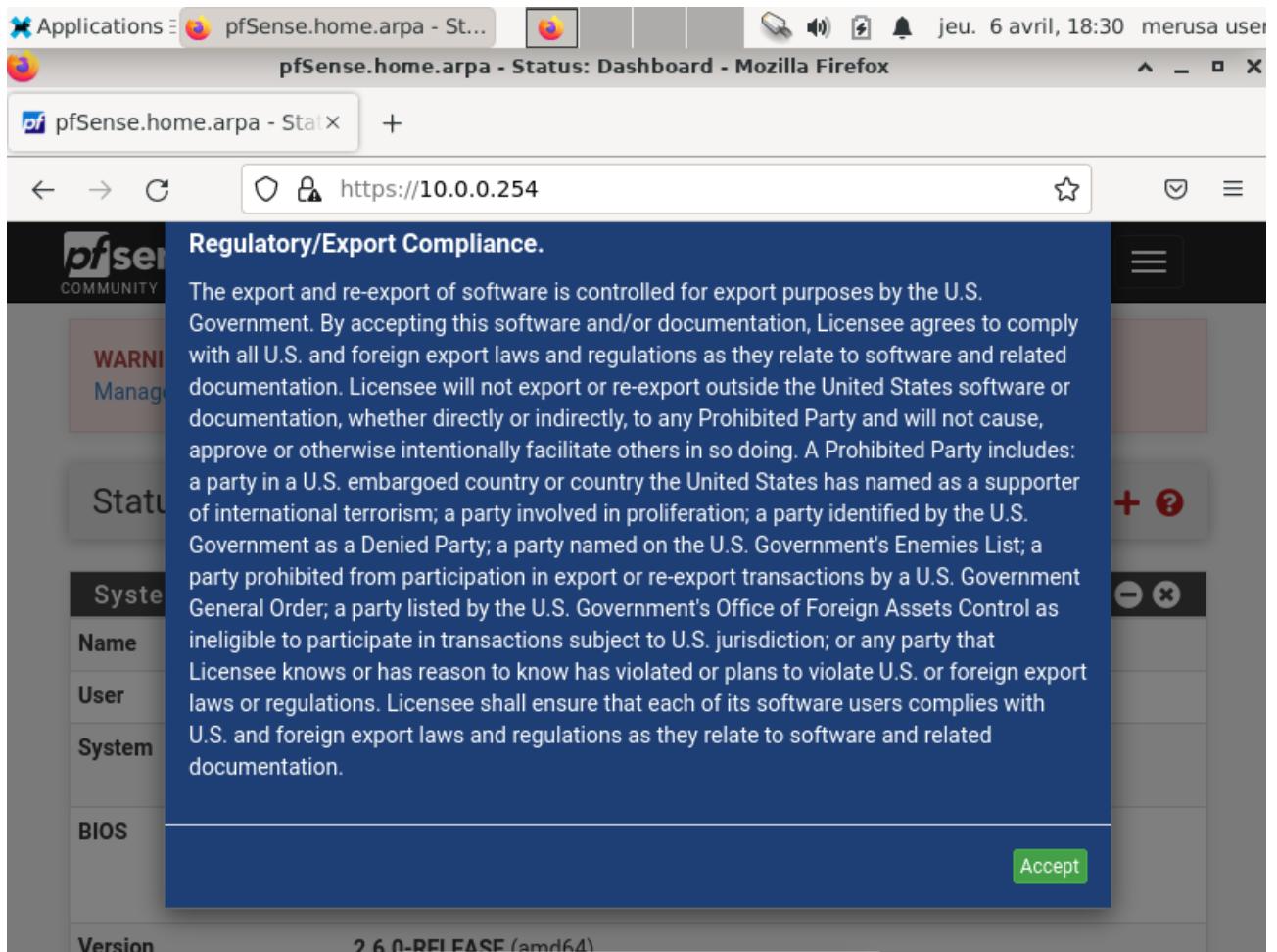
Cliquer sur accepter le risque et poursuivre.



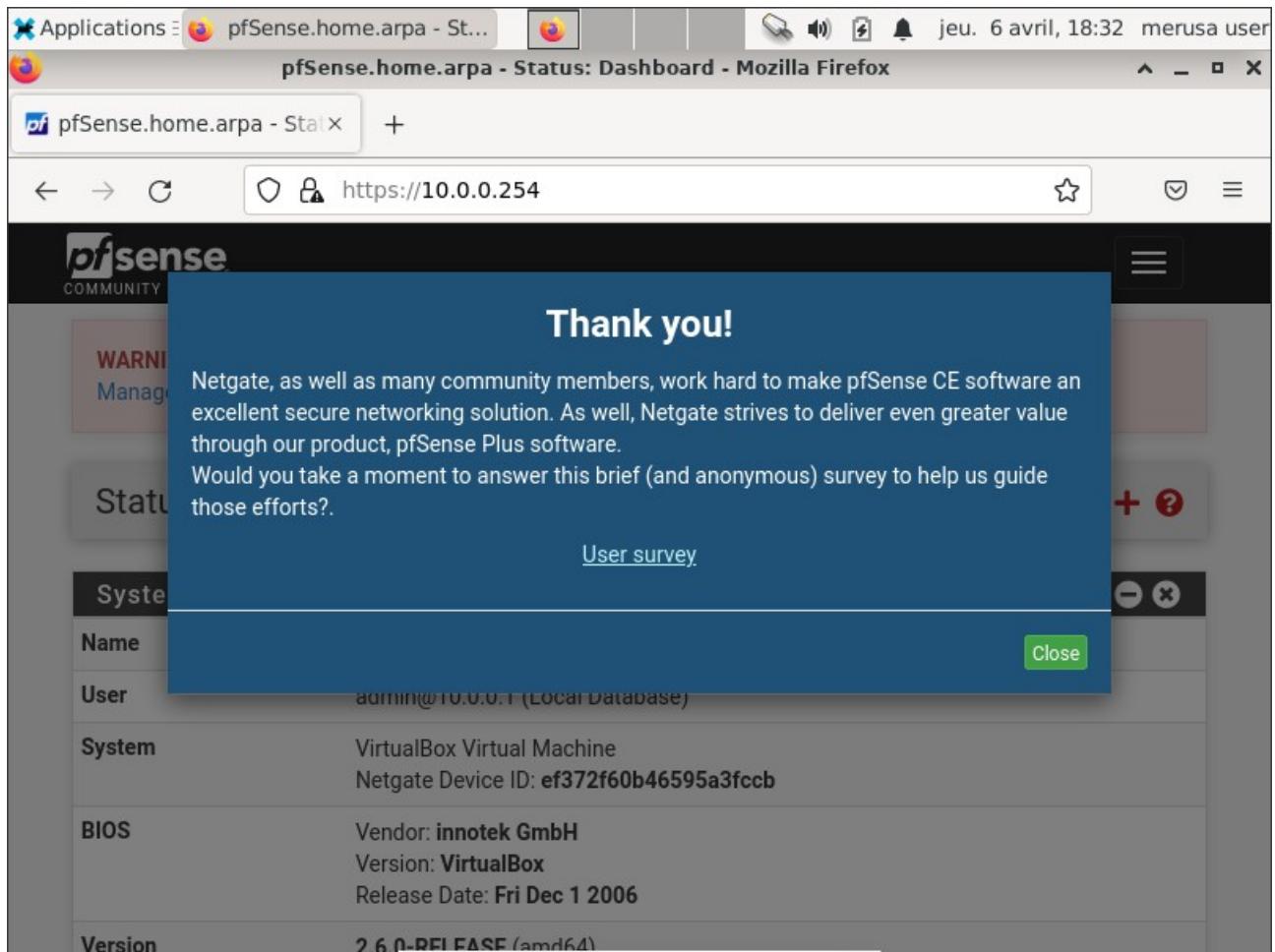
le login est admin et le mot de passe est pfsense.



Cliquer sur le logo de Pfsense en haut a gauche.

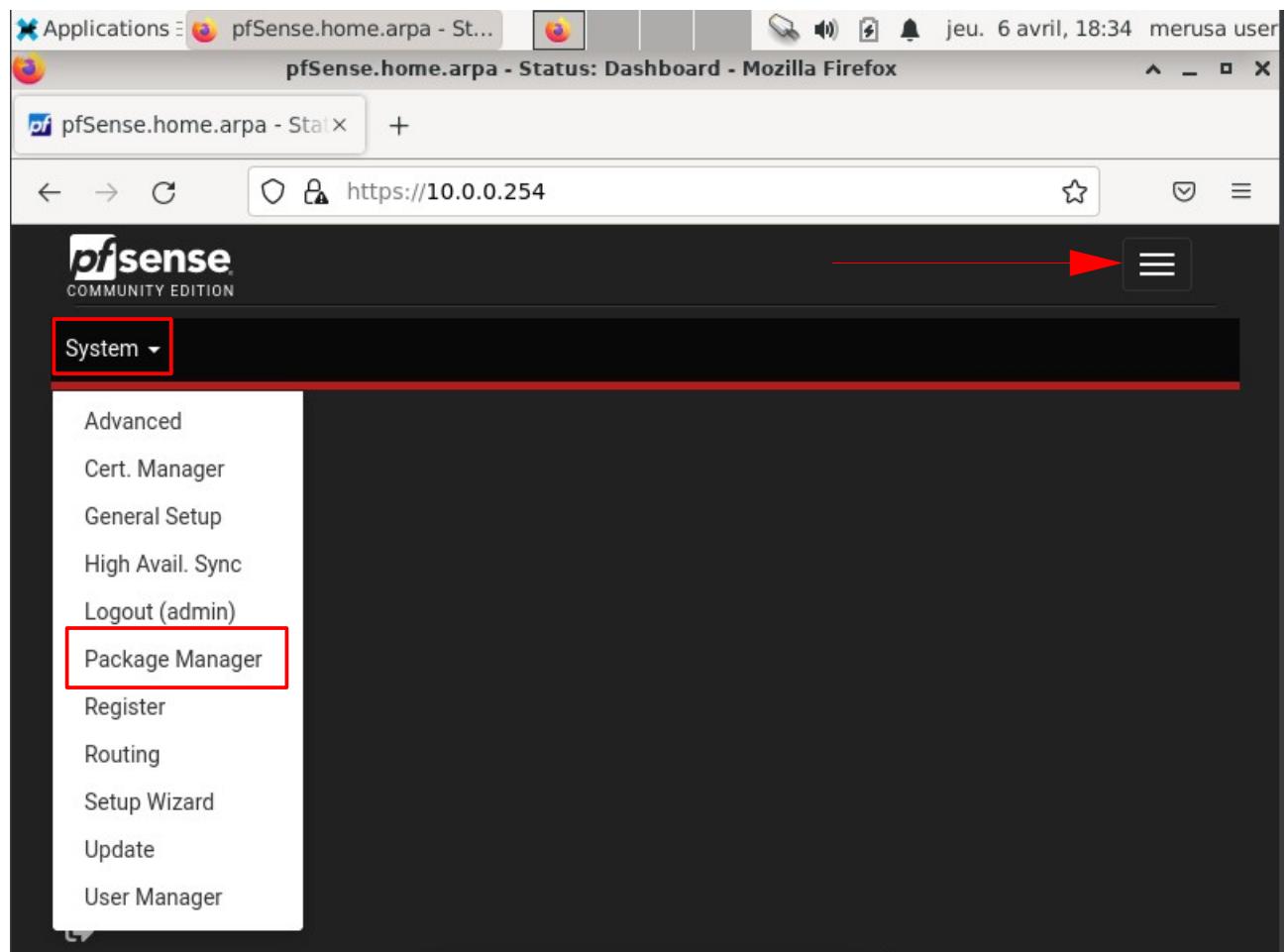


Cliquez sur accept

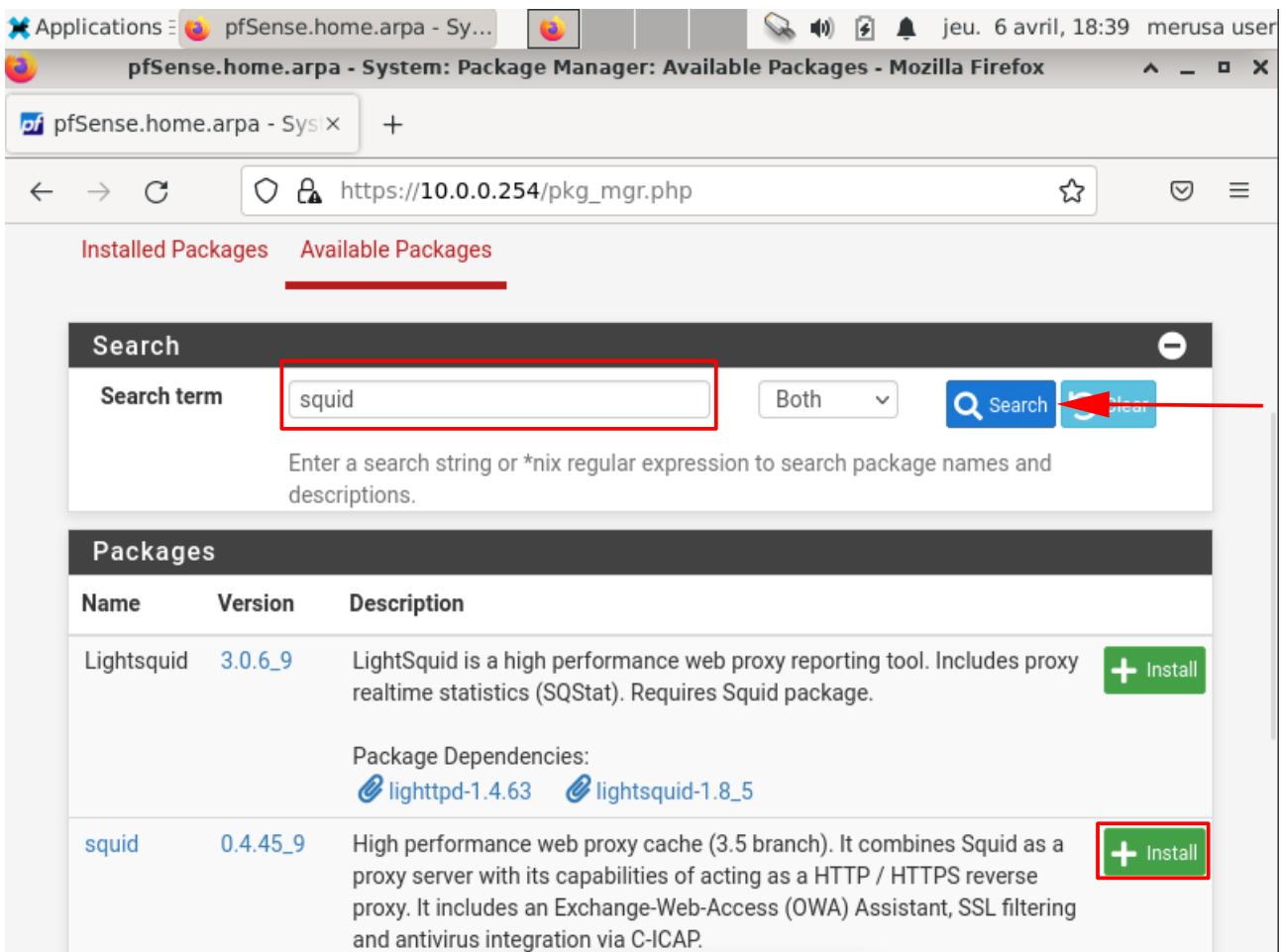


Cliquer sur close

Configuration graphique du PfSense1



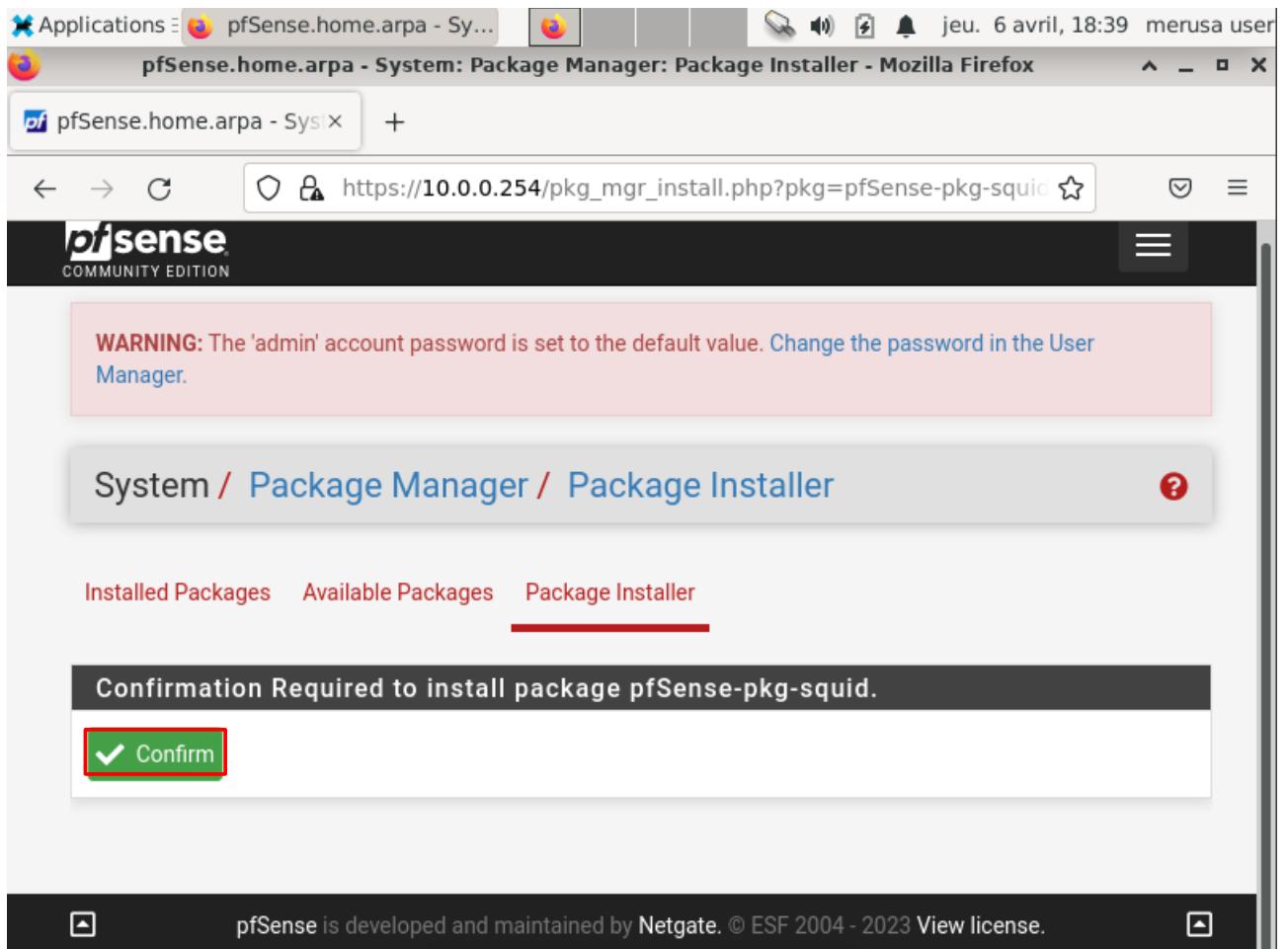
Cliquer sur le menu en haut a droite puis System puis Package Manager.



The screenshot shows a Mozilla Firefox browser window titled "pfSense.home.arpa - System: Package Manager: Available Packages - Mozilla Firefox". The address bar shows the URL https://10.0.0.254/pkg_mgr.php. The page displays the "Available Packages" tab. A search bar at the top has "squid" typed into it. A red box highlights the search term, and a red arrow points to the "Search" button. Below the search bar, a message says "Enter a search string or *nix regular expression to search package names and descriptions." The main table, titled "Packages", lists two entries:

Name	Version	Description	Action
Lightsquid	3.0.6_9	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package.	+ Install
squid	0.4.45_9	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP.	+ Install

Dans la bar de recherche tapez squid cliquer sur search puis cliquer sur install



cliquer sur confirm



pfSense-pkg-squid installation successfully completed.

Installed Packages Available Packages Package Installer

Package Installation

```
/usr/local/etc/squid/squid.conf.documented is a fully annotated  
configuration file you can consult for further reference.
```

```
Additionally, you should check your configuration by calling  
'squid -f /path/to/squid.conf -k parse' before starting Squid.
```

=====

```
Message from pfSense-pkg-squid-0.4.45_9:
```

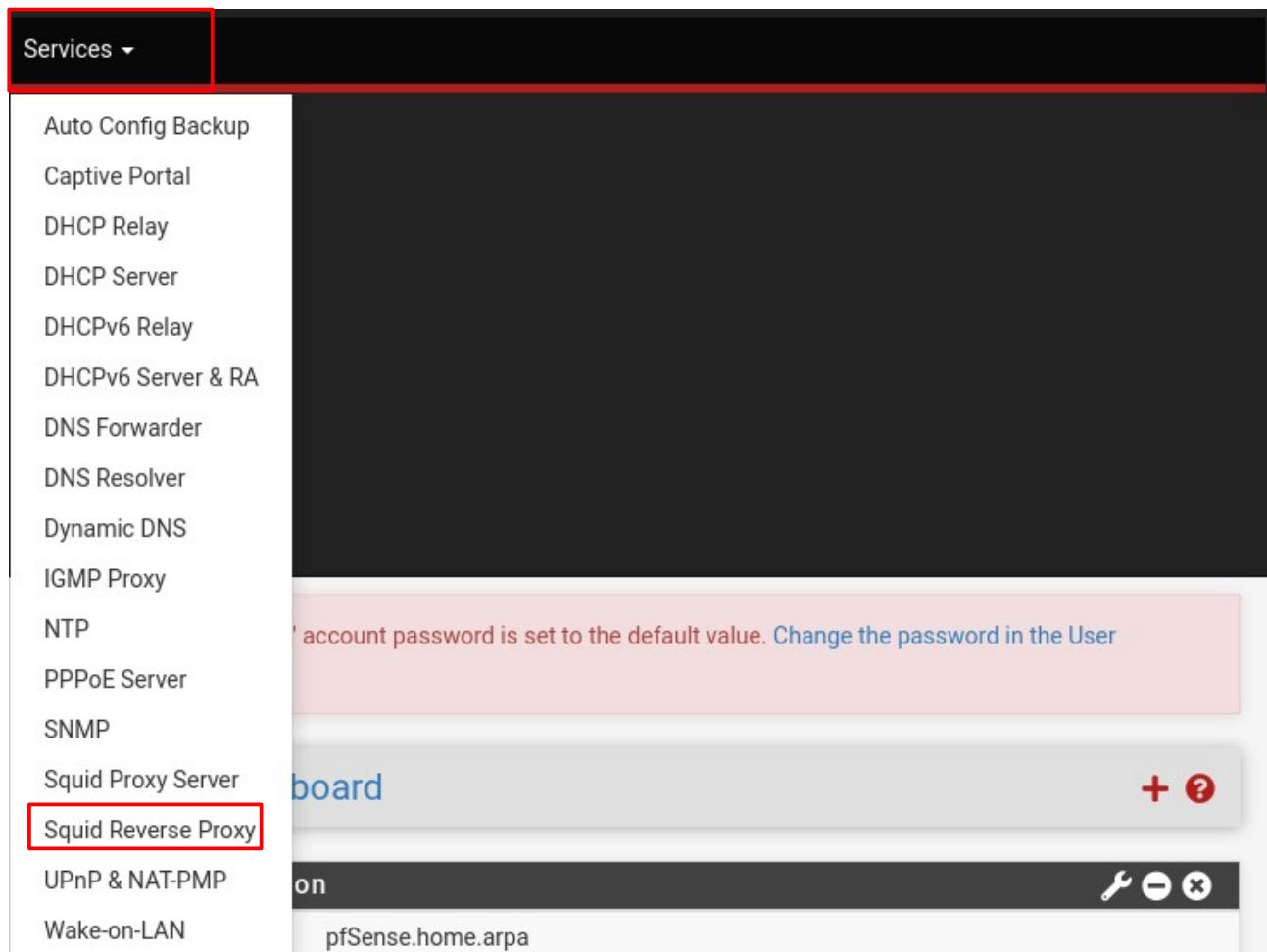
--

```
Please visit Services - Squid Proxy Server menu to configure the package and enable  
the proxy.
```

```
>>> Cleaning up cache... done.
```

```
Success
```

Attendre jusqu'à avoir cette page



Cliquer sur service puis sur squid Reverse Proxy

Squid Reverse Proxy General Settings

Listen IP

IPv4

Version

Select the IP version Squid Reverse Proxy will use to bind to.

Reverse Proxy Interface(s)

WAN

LAN

loopback

The interface(s) the reverse-proxy server will bind to (usually WAN). [Use CTRL + click to select multiple interfaces.](#) 

User Defined Reverse Proxy IPs

Squid will additionally bind to these user-defined IPs for reverse proxy operation. Separate entries by semi-colons (;) 

External FQDN

server_web

The external fully qualified domain name of the WAN IP address.

Reset TCP Connections on Unauthorized Requests

If checked, the reverse proxy will reset the TCP connection if the request is unauthorized.

Cliquer sur WAN puis assurez vous de remplir la ligne External FQDN

Squid Reverse HTTP Settings

Enable HTTP Reverse Proxy

If checked, the proxy server will act in HTTP reverse mode.

Important: You must add a proper firewall rule with destination matching the 'Reverse Proxy Interface(s)' address.

Reverse HTTP Port

80

This is the port the HTTP reverse proxy will listen on. Default: 80

Reverse HTTP Default Site

This is the HTTP reverse proxy default site. [Leave empty to use 'External FQDN' value specified above.](#)

Cocher la case Enable HTTP Reverse Proxy et enregistré

Package / Reverse Proxy Server: Peers / Web Servers



General Web Servers Mappings Redirects Real Time Sync

Status	Alias	IP Address	Port	Protocol	Description
					 Add

 Save

cliquer sur l'onglet Web Servers puis sur add

General Web Servers Mappings Redirects Real Time Sync

Squid Reverse Peer Mappings

Enable This Peer If checked, then this peer will be available for reverse proxy configuration.

Peer Alias server_web

Name to identify this peer on Squid reverse proxy configuration. Example: HOST1

Peer IP 10.0.0.1

IP address of this peer. Example: 192.168.0.1

Peer Port 80

Listening port of this peer. Example: 80

Peer Protocol HTTP

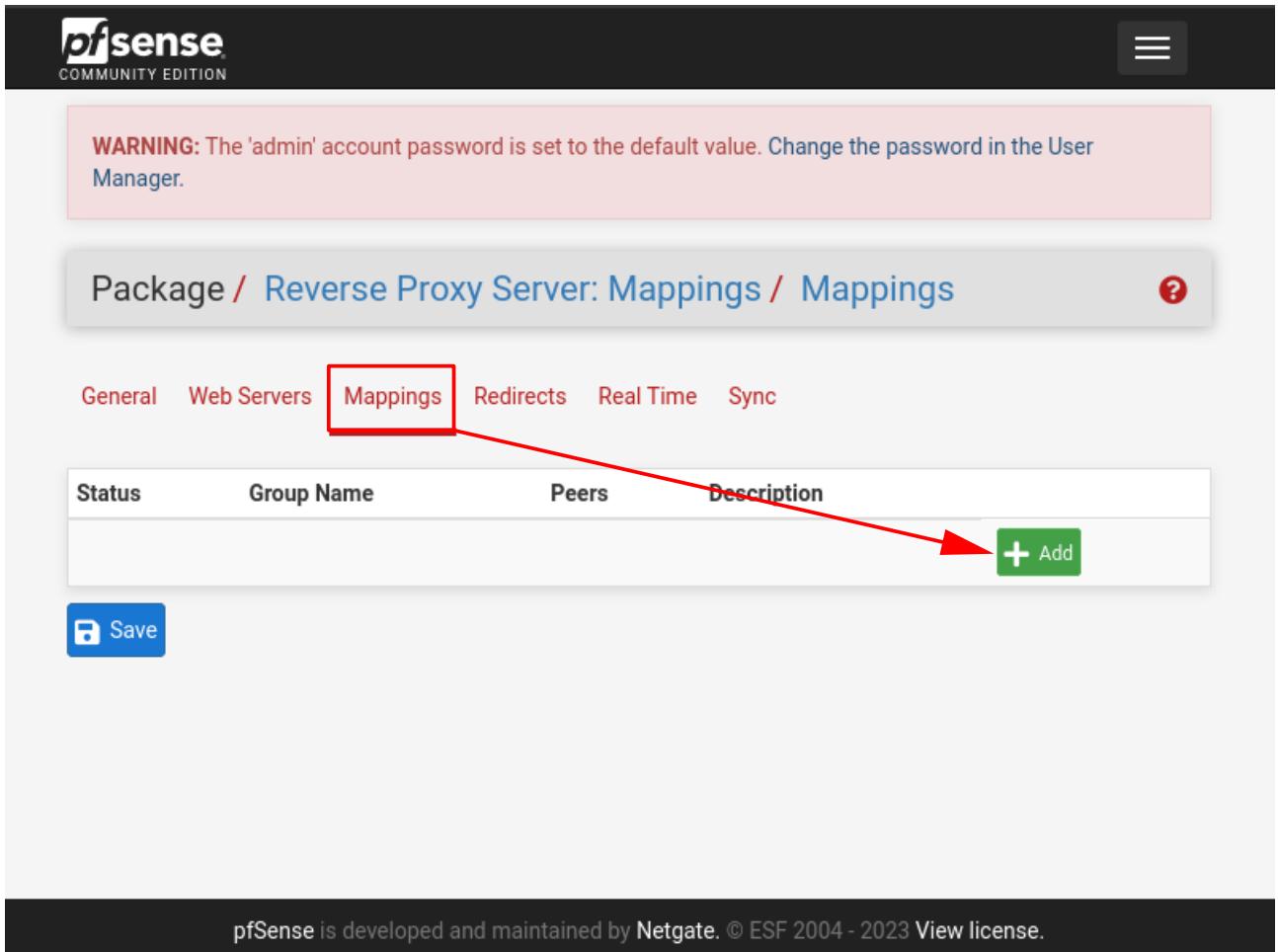
Select protocol listening on this peer port.

Peer Description Reverse proxy

Peer Description (Optional)

 Save

Remplir la section Alias comme vous le voulez dans la section Peer IP
mettre l'IP de votre serveur web et cliquer sur save.



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Package / Reverse Proxy Server: Mappings / Mappings

General Web Servers **Mappings** Redirects Real Time Sync

Status	Group Name	Peers	Description

Save **Add**

pfSense is developed and maintained by Netgate. © ESF 2004 - 2023 [View license](#).

cliquer sur l'onglet Mappings puis sur add

Squid Reverse Peer Mappings

Enable This URI If checked, then this URI (Uniform Resource Name) will be available for reverse proxy config.

Group Name

Name to identify this URI on Squid reverse proxy configuration. [Example: URI1](#)

Group Description
URI Group Description (Optional)

Peers

Apply these group mappings to the selected peers. [Use CTRL + click to select multiple peers.](#)

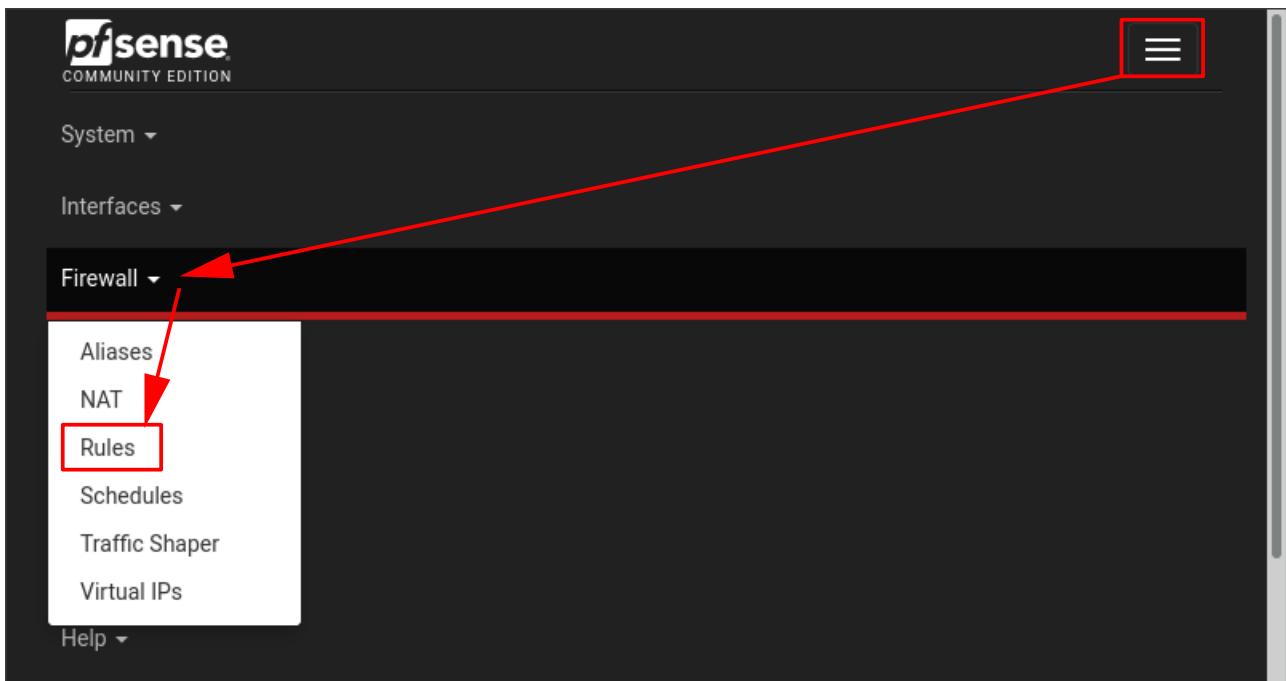
URI Settings Use URI row(s) below to add URL **regex** expression(s) to match (one per row). [i](#)

URI [Info](#)
Enter URL **regex** to match. [Click Info above for examples.](#)

Add 

 **Save**

Cochez Enable This URL dans groupe name écrive ce que vous voulez cliquer sur le peers que vous avez créée précédemment et dans URL écrivez votre http:// suivit de votre ip et cliquer ur save.



Cliquer sur le menu puis Firewall puis Rules.

A screenshot of the 'Firewall / Rules / WAN' interface. The top navigation bar shows 'Manager.', 'Firewall / Rules / WAN' (with 'WAN' selected), and icons for refresh, list, and help. Below the navigation is a toolbar with buttons for 'Floating', 'WAN', and 'LAN' (the 'WAN' button is highlighted with a red bar). The main area is titled 'Rules (Drag to Change Order)' and contains a table of rules:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/75 KiB	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks	
0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	

Below the table, a yellow box displays the message: 'No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.'

At the bottom are buttons for 'Add' (with up and down arrows), 'Delete', 'Save', and 'Separator'.

Cliquer sur l'écroue de la ligne RFC 1918 networks.

Reserved Networks

Block private networks and loopback addresses	<input type="checkbox"/> 	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	<input checked="" type="checkbox"/>	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

décoché tout en bas et décocher la case Block private networks and loopback addresses et cliquer sur save.

pfSense
COMMUNITY EDITION

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

Interfaces / WAN (em0)

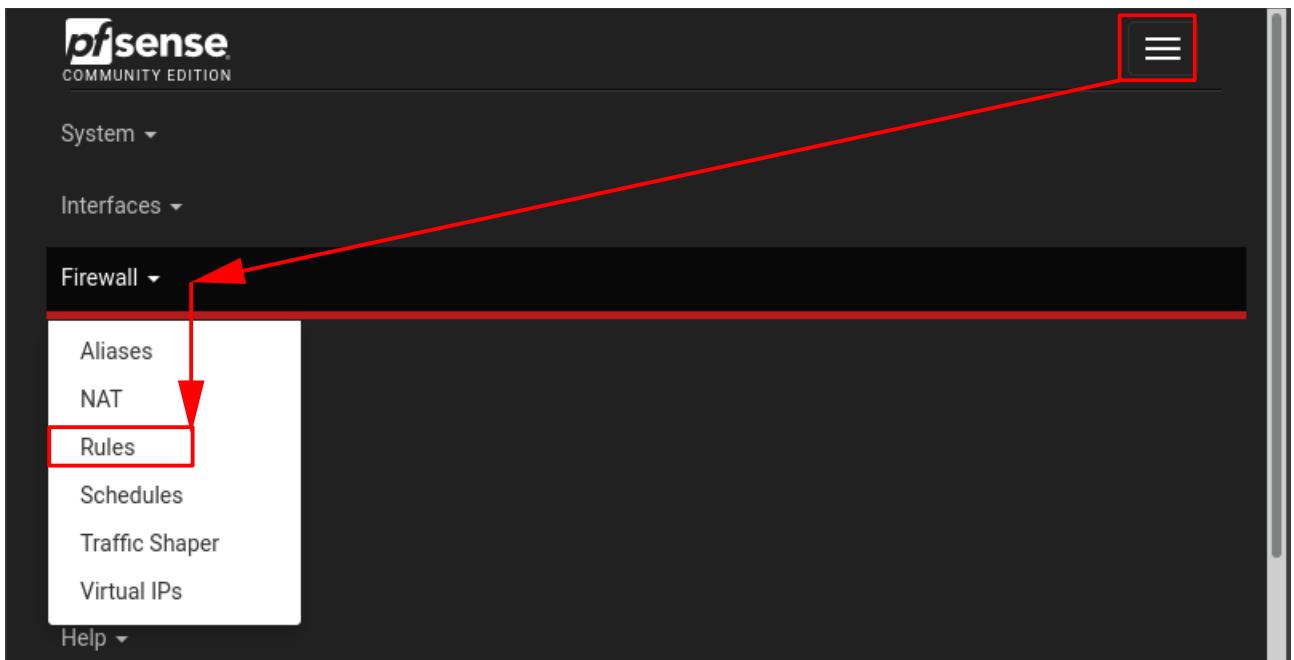
The WAN configuration has been changed.
The changes must be applied to take effect.
Don't forget to adjust the DHCP Server range if needed after applying.

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	WAN Enter a description (name) for the interface here.
IPv4 Configuration Type	DHCP
IPv6	None

Cliquer sur Apply changes.



Cliquer sur le menu puis Firewall puis Rules.

A screenshot of the 'Firewall / Rules / WAN' interface. The top navigation bar shows 'Firewall / Rules / WAN' with icons for list, table, and help. Below the navigation is a sub-navigation bar with tabs: 'Floating', 'WAN' (which is selected and highlighted in red), 'LAN', and 'OPT1'. The main content area is titled 'Rules (Drag to Change Order)'. A table lists a single rule: '0 /0 B' with state '*' and source 'Reserved Not assigned by IANA'. The table columns are: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. The 'Actions' column for this rule contains a gear icon. Below the table, a yellow box displays the message: 'No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.' At the bottom right of the interface are several buttons: a green 'Add' button with a '+' icon, a red 'Delete' button with a trash icon, a blue 'Save' button with a disk icon, and an orange 'Separator' button with a plus sign icon. A red arrow points to the 'Add' button.

Cliquer 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

WAN

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

Address

Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Dans protocol choisissez bien TCP.

Destination

Destination

Invert
match

any

Destination Address

/

Destination Port Range

HTTP (80)

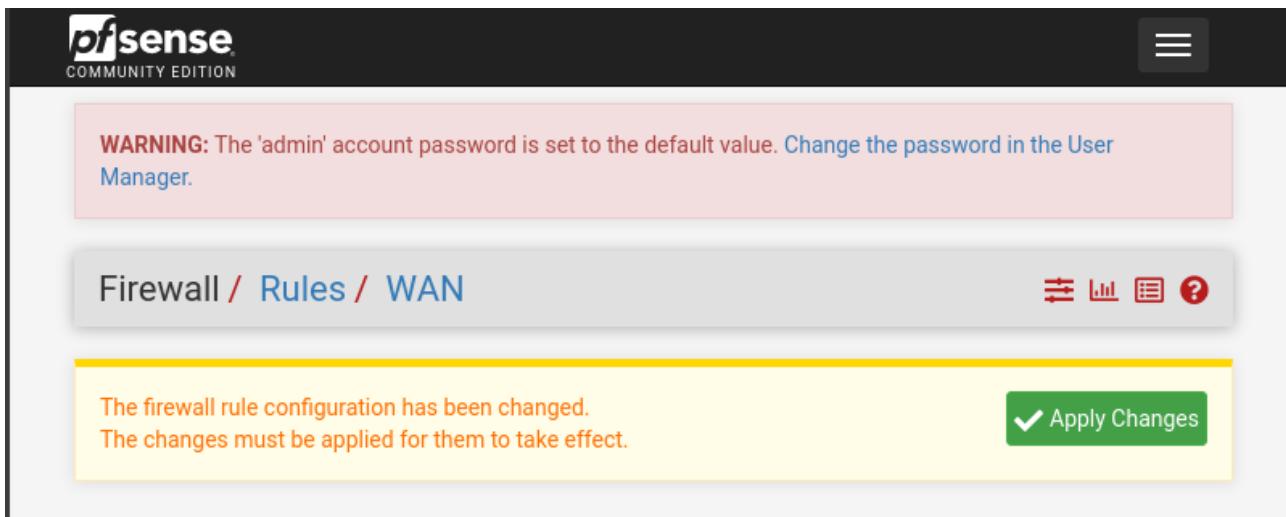
From

HTTP (80)

To

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

Dans Destination port range choisir HTTP dans from et to.

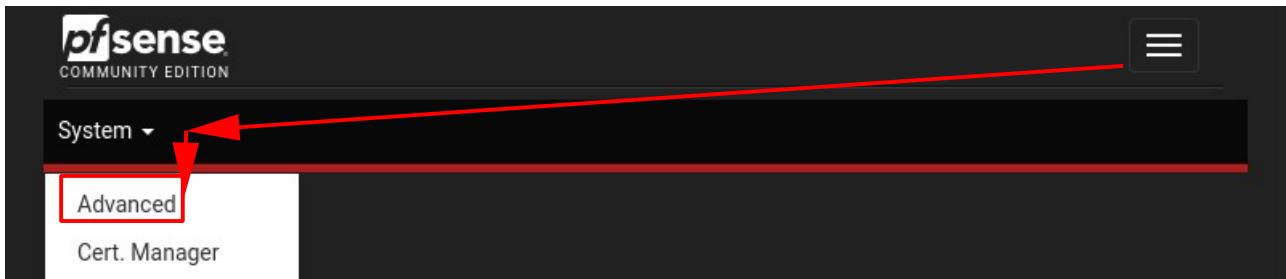


WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

[Apply Changes](#)

Cliquer sur Apply changes.

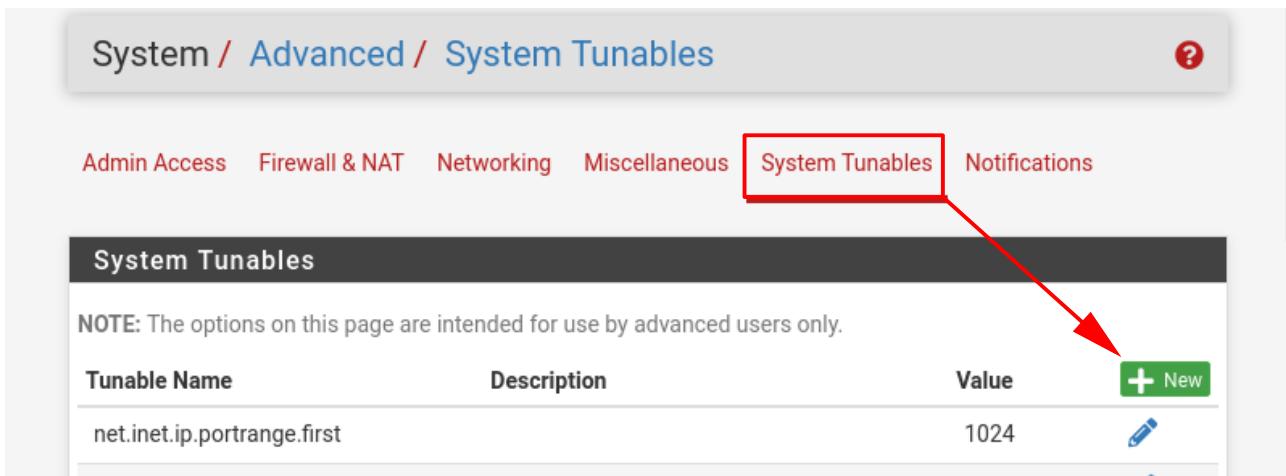


System ▾

Advanced

Cert. Manager

Cliquer sur le menu puis System puis Advanced.



System / Advanced / System Tunables

Admin Access Firewall & NAT Networking Miscellaneous System Tunables Notifications

System Tunables

NOTE: The options on this page are intended for use by advanced users only.

Tunable Name	Description	Value	
net.inet.ip.portrange.first		1024	<input checked="" type="button"/> New

Cliquer sur l'onglet System Tunables puis sur new



Admin Access Firewall & NAT Networking Miscellaneous System Tunables Notifications

Edit Tunable

Tunable

net.inet.ip.portrange.reservedhigh

Value

0

Description

Save

dans tunable taper net.inet.ip.portrange.reservedhigh puis remplire le champ value avec un 0 cliquer sur save.

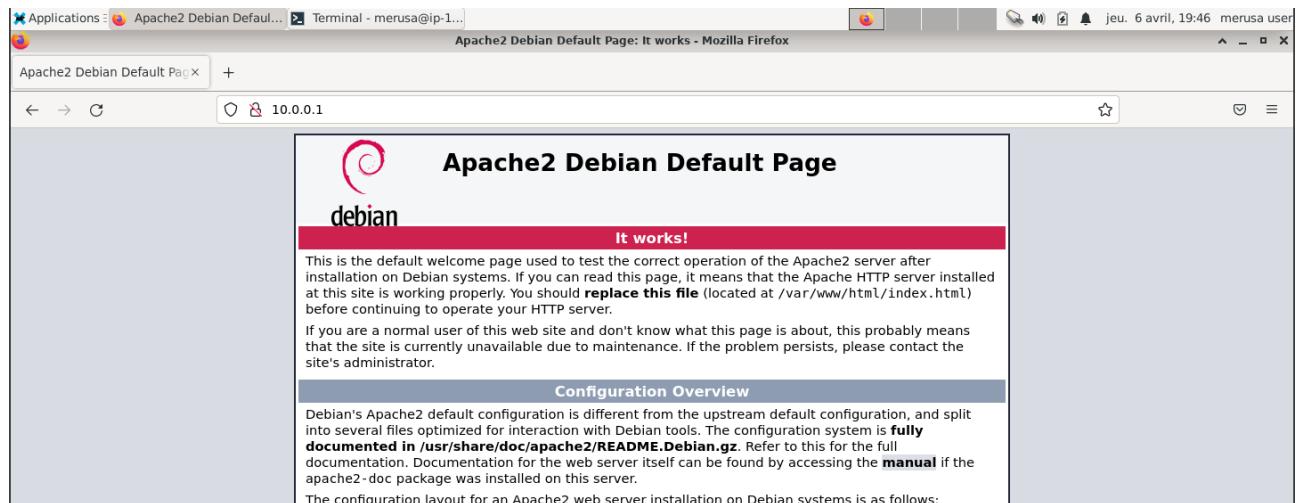


The firewall tunables have changed.

The changes must be applied for them to take effect.

Apply Changes

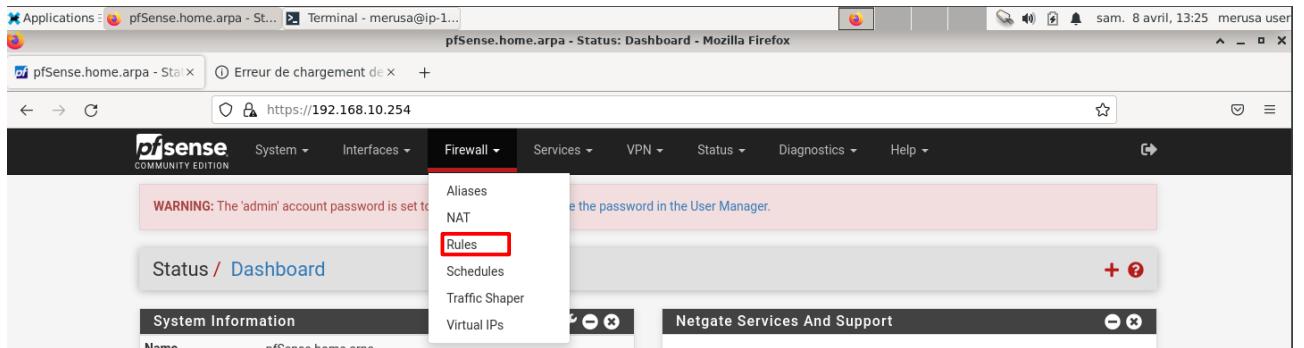
Cliquer sur Apply changes.



Puis allez sur un pc brancher sur l'interface WAN ou a internet et taper l'IP de votre serveur web.

Configuration graphique du Pfsense2

Je considérer que la partie près installé est déjà faite



Cliquer sur Firewall puis Rules.

A screenshot of the 'Firewall / Rules / WAN' page. The 'WAN' tab is selected. A table lists a single rule: '0 / 0 B * RFC 1918 networks * * * * * * Block private networks'. The 'Actions' column for this rule has a gear icon.

Cliquer sur l'écroue de la ligne RFC 1918 networks.

A screenshot of the 'Reserved Networks' configuration page. It shows two options: 'Block private networks and loopback addresses' (unchecked) and 'Block bogon networks' (checked). The 'Block bogon networks' section contains a note about blocking prefixes that should never appear in the Internet routing table.

décoché tout en bas et décocher la case Block private networks and loopback addresses et cliquer sur save.

A screenshot of the 'Interfaces / WAN (em0)' configuration page. A message at the top says 'The WAN configuration has been changed. The changes must be applied to take effect. Don't forget to adjust the DHCP Server range if needed after applying.' A green 'Apply Changes' button is visible on the right.

Cliquer sur Apply changes.

Cliquer sur Firewall puis Rules.

Cliquez sur add.

Dans protocol choisissez ICMP puis enregistré.

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Floating WAN LAN OPT1

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 0 B	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0 / 0 B	IPv4 ICMP any	*	*	*	*	*	none		

Add Add Delete Save Separator

Cliquez sur add.

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.

Source

Source

Invert match

any

Source Address

/

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

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.

Dans protocol choisissez UDP puis Destination port range mettez any pour From et To puis enregistré.

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Cliquez sur add.

Firewall / Rules / OPT1

Floating WAN LAN **OPT1**

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
No rules are currently defined for this interface All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.										

Add **Up** **Down** **Delete** **Save** **+** **Separator**

Cliquer sur l'onglet OPT1 puis sur add

Firewall / Rules / Edit

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 OPT1

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 **any** **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 **any** 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.

Dans protocol choisissez TCP/UDP puis Destination port range mettez any pour From et To puis enregistré.

Firewall / Rules / OPT1

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Floating WAN LAN OPT1

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	*	*	*	*	*	none			

Cliquer sur add.

Firewall / Rules / Edit

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: OPT1
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: ICMP
Choose which IP protocol this rule should match.

ICMP Subtypes: any
Alternate Host
Datagram conversion error
Echo reply
For ICMP rules on IPv4, one or more of these ICMP subtypes may be specified.

Source: Source: any
Destination: Destination: any

Dans protocol choisissez ICMP puis enregistré.

Firewall / Rules / OPT1

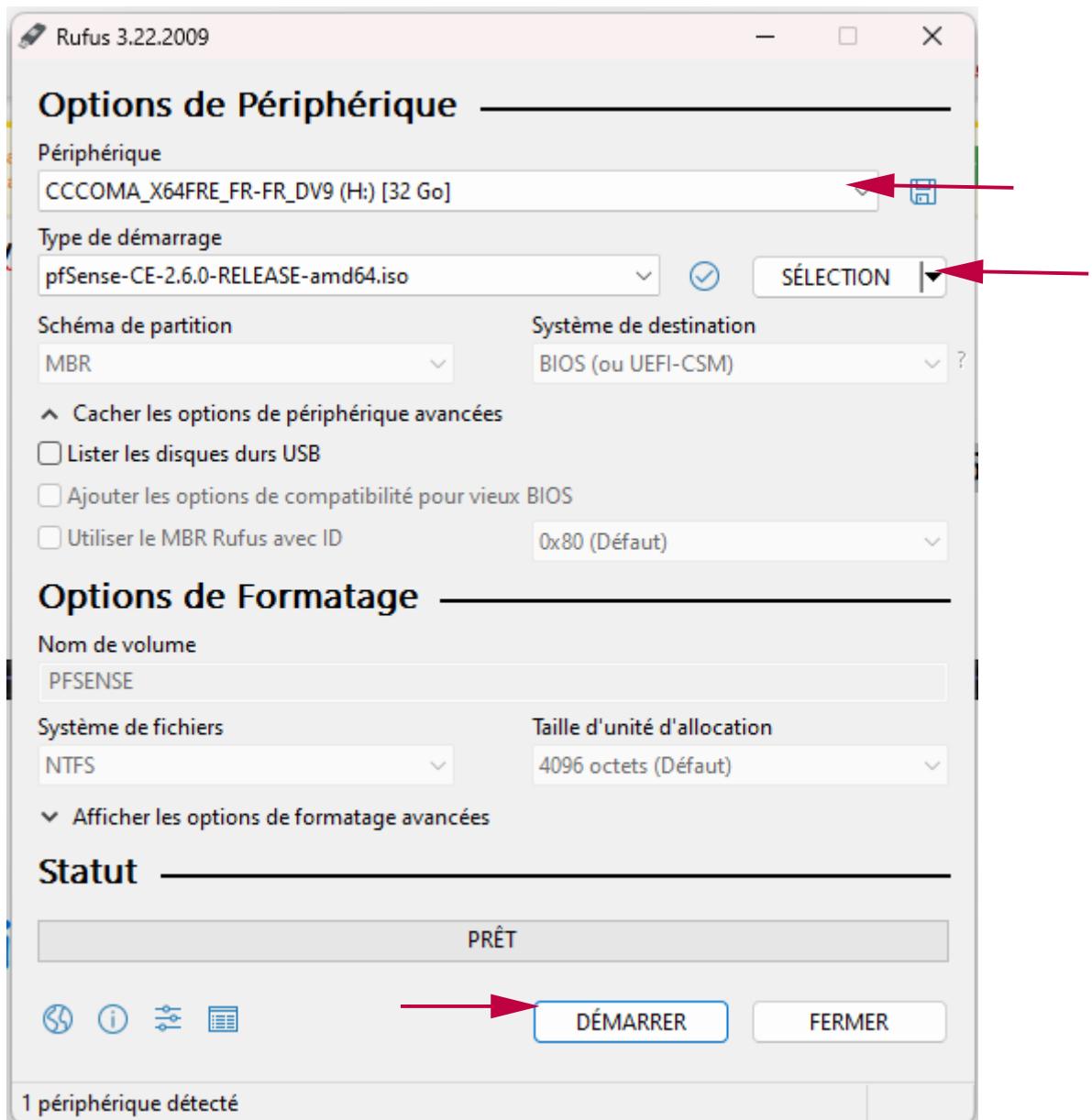
The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Cliquer sur Apply changes.

Notice d'utilisation

Annexes



Choisissez votre clef usb dans périphérique
dans sélection allez chercher votre iso
puis démarrer et pour finir placer votre clef usb sur une machine .
Retourner aux [tuto d'installation](#)

Fiche recette

Vérification de l'opérationnalité de la solution mise en œuvre : DMZ

Description du test :

1. *Ping le serveur web depuis l'extérieur*
2. *Ping refuser à l'extérieur sur le réseau interne DMZ*
3. *Ping de la BDD avec le Serveur web*

Résultats Attendus :

1. *Accès au site web depuis l'extérieur*
2. *Accès refuser à l'extérieur sur le réseau interne DMZ*
3. *Communication de la BDD avec le Serveur web*

Réception Globale :

Reçu :

Reçu avec réserve :

Refusé :

Commentaire :

Réception Étape 1 : Ping le serveur web depuis l'extérieur

Reçu :

Reçu avec réserve :

Refusé :

Commentaire :

Réception Étape 2 : Ping refuser à l'extérieur sur le réseau interne DMZ

Reçu :

Reçu avec réserve :

Refusé :

Commentaire :

Réception Étape 3 : Ping de la BDD avec le Serveur web

Reçu :

Reçu avec réserve :

Refusé :

Commentaire :