

**Situation professionnelle en PPE 3 : Filtrage des accès internet  
vers internet via un PROXY**



**Documentation n°1 : Installation de la solution Pfsense.**

**Auteur :** Guillaume Orlando  
**Date :** 13/11/2017

## I. Introduction :

La mise en place d'un outil permettant d'effectuer un suivi des connexion est obligatoire au sein des organisations. Nous avons été sollicité par l'entreprise EPOKA pour la mise en place d'un tel service. En dehors des fonctionnalités obligatoires légales, le responsable informatique de la société nous a fournis un cahier des charges stipulant que :

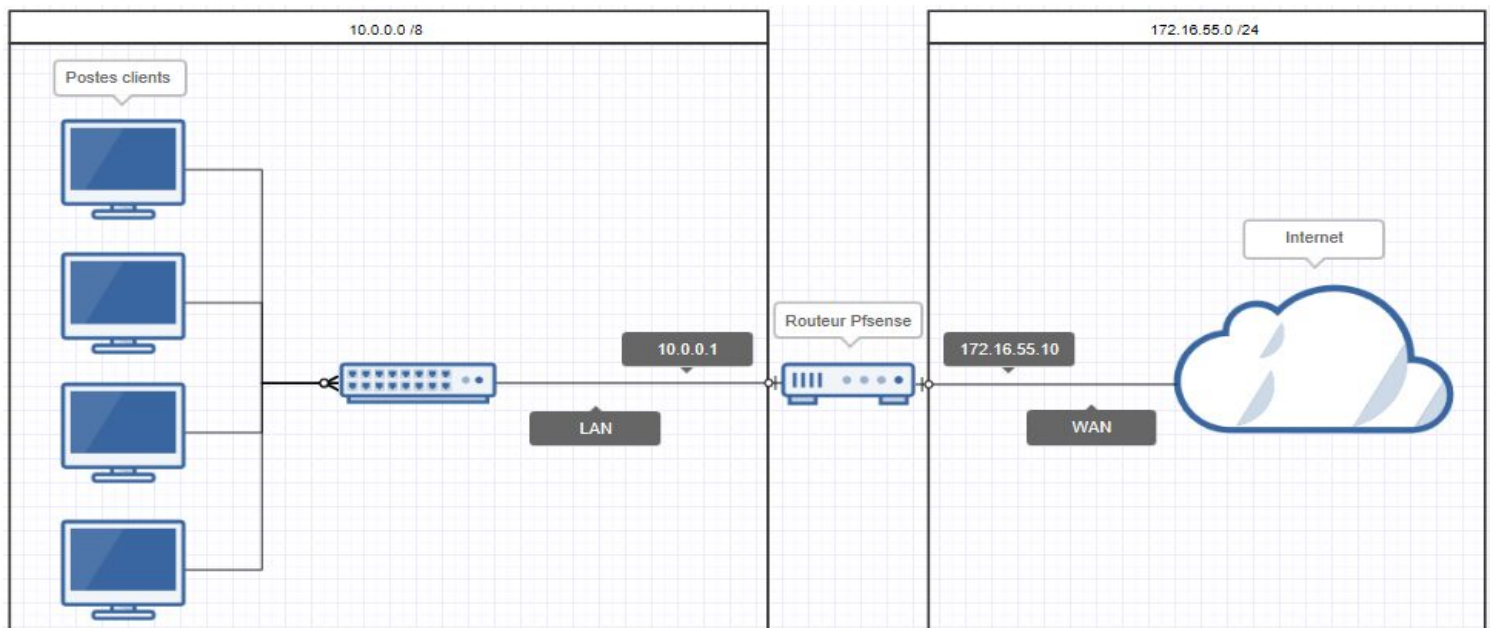
- La connexion des utilisateurs doit être filtrée sur un modèle de blacklist. Cette blacklist doit être celle de la ville de Toulouse.
- Les machines clientes des utilisateurs ne doivent pas être atteignables depuis internet, sauf en passant par un accès à distance OpenVPN.
- Les machines clientes des utilisateurs ne peuvent utiliser qu'un certain nombre de protocoles pour sortir du LAN, à savoir les protocoles suivants : Ping, dns, ftp, smtp, pop3, imap, rdp, http et https.

Après comparaison de plusieurs solutions, le service retenu sera le proxy open-source "Squid", qui tournera sous l'OS PfSense.

## II. Paramétrage de VMWare Workstation :

Puisque la mise en place d'un prototype de Proxy sous PfSense nécessite de mettre en place un réseau LAN virtualisé, nous allons utiliser le logiciel VMWare Workstation Pro par soucis de simplicité. En effet, l'outil de virtualisation de VMWare permet de gérer des fonctionnalités de configurations réseaux avancés bien plus facilement que sous les autres softs de virtualisations.

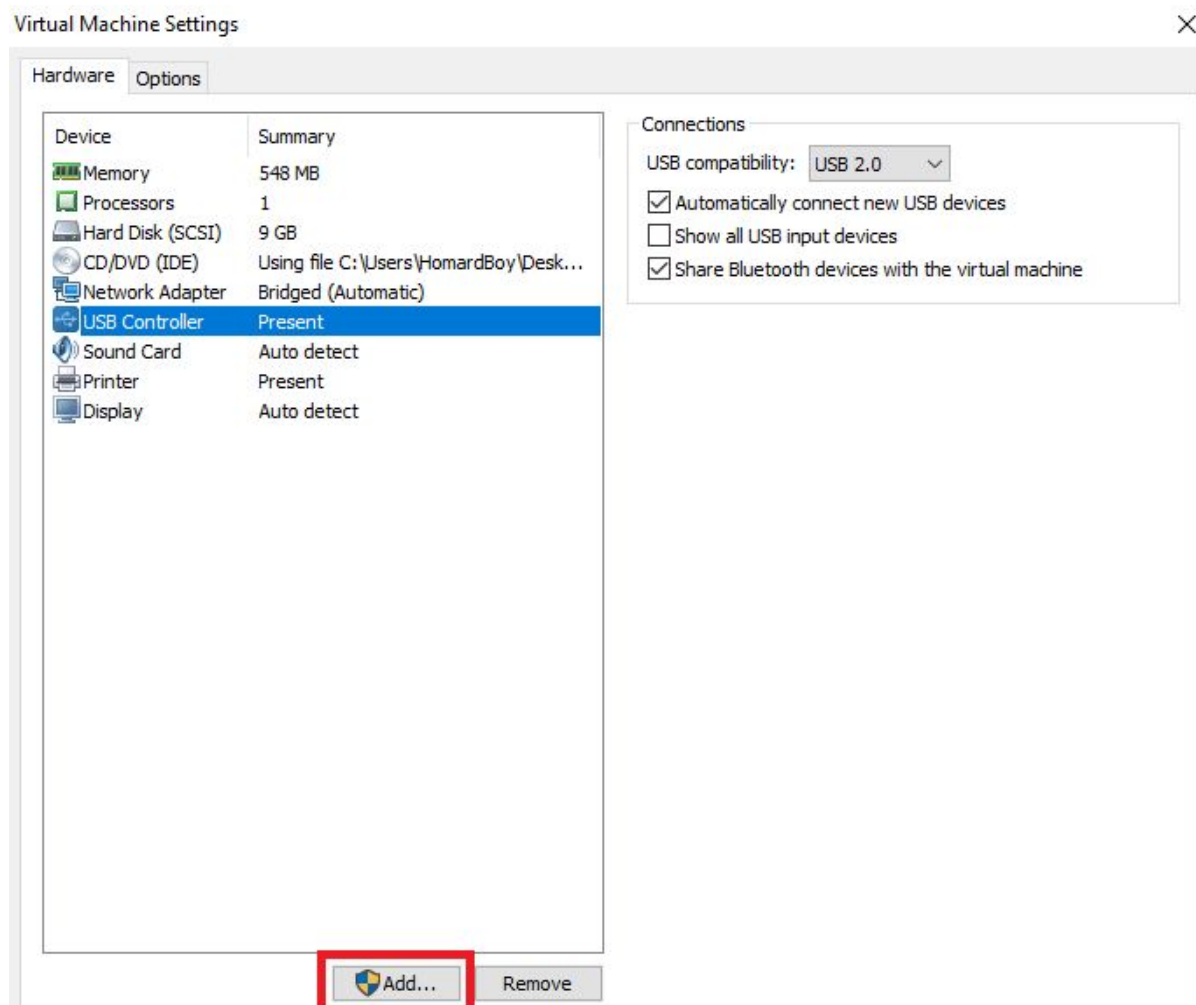
L'architecture du prototype sera la suivante :



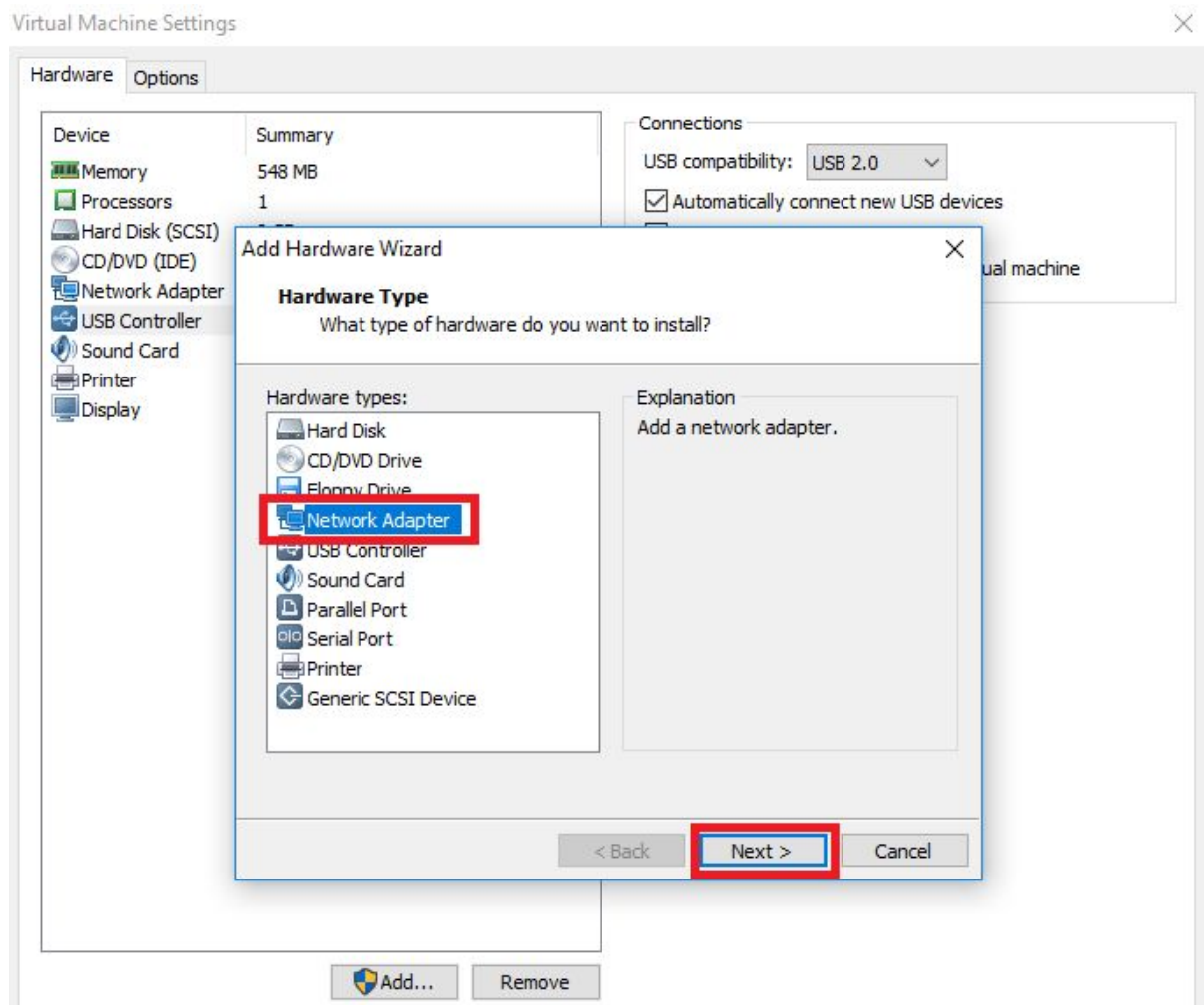
Dans un premier temps, nous allons créer la machine qui nous servira de routeur PfSense :

L'ISO utilisé est disponible gratuitement sur le site officiel du projet Pfsense : <https://www.pfsense.org/download/>. La version utilisée est la dernière en date, à savoir la version communautaire stable 2.4.1.

Pfsense étant un système d'exploitation très léger, nous n'avons pas besoin de booster les capacités de la machine virtuelle. Un processeur à un coeur et 512 Mo de mémoires vives sont amplement suffisants. En ce qui concerne l'espace disque, 10Go nous sont largement suffisants, même en tenant compte de l'archivage des logs utilisateurs. Attention aussi à disposer la carte réseau en mode accès par pont. Maintenant que la machine est faite, il faudra se rendre dans la partie de configuration matériel, et ajouter un nouveau périphérique :

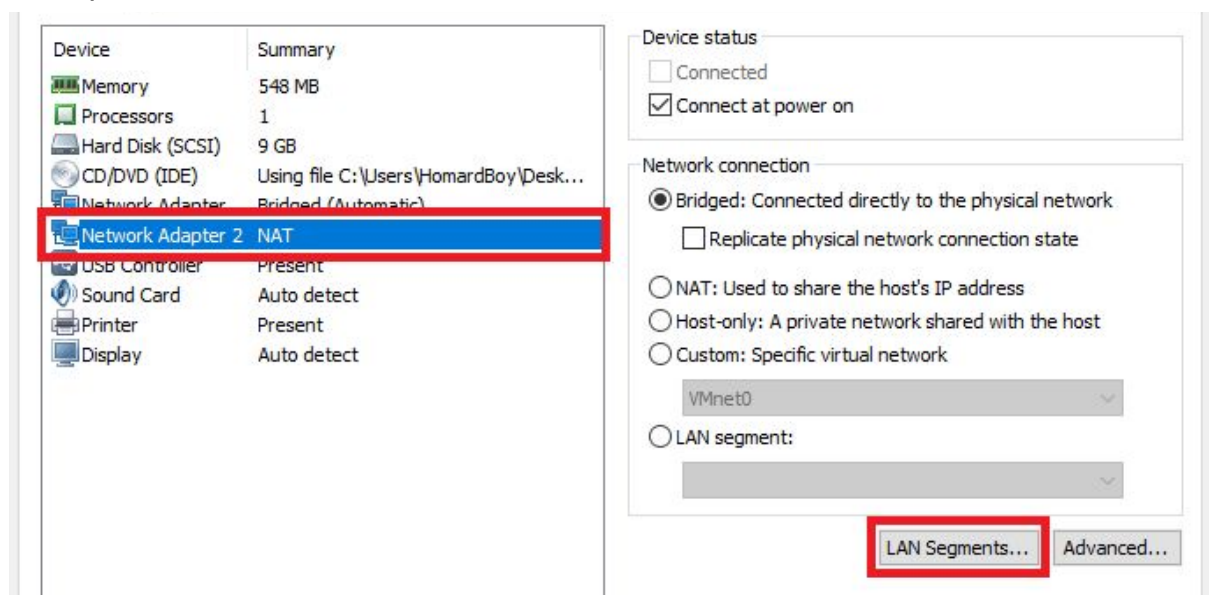


Nous ajoutons une carte réseau, puisque notre machine sera un routeur, il lui faut alors obligatoirement 2 cartes réseaux. La première carte réseau en accès par pont sera la carte connecté au WAN. La carte que nous ajoutons sera connecté au LAN et servira donc d'adresse de passerelle aux postes clients.

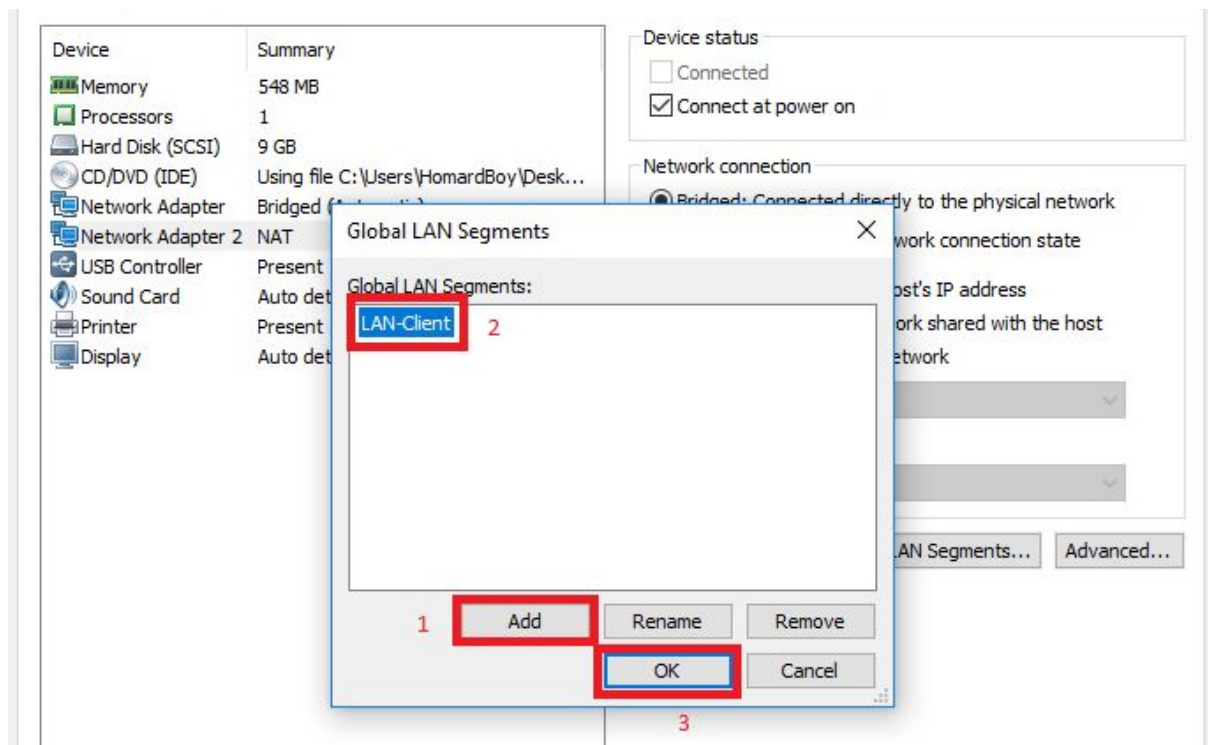


Nous laissons la carte en accès par pont pour le moment, en veillant tout de même à ce que la nouvelle carte soit connectée à la machine.

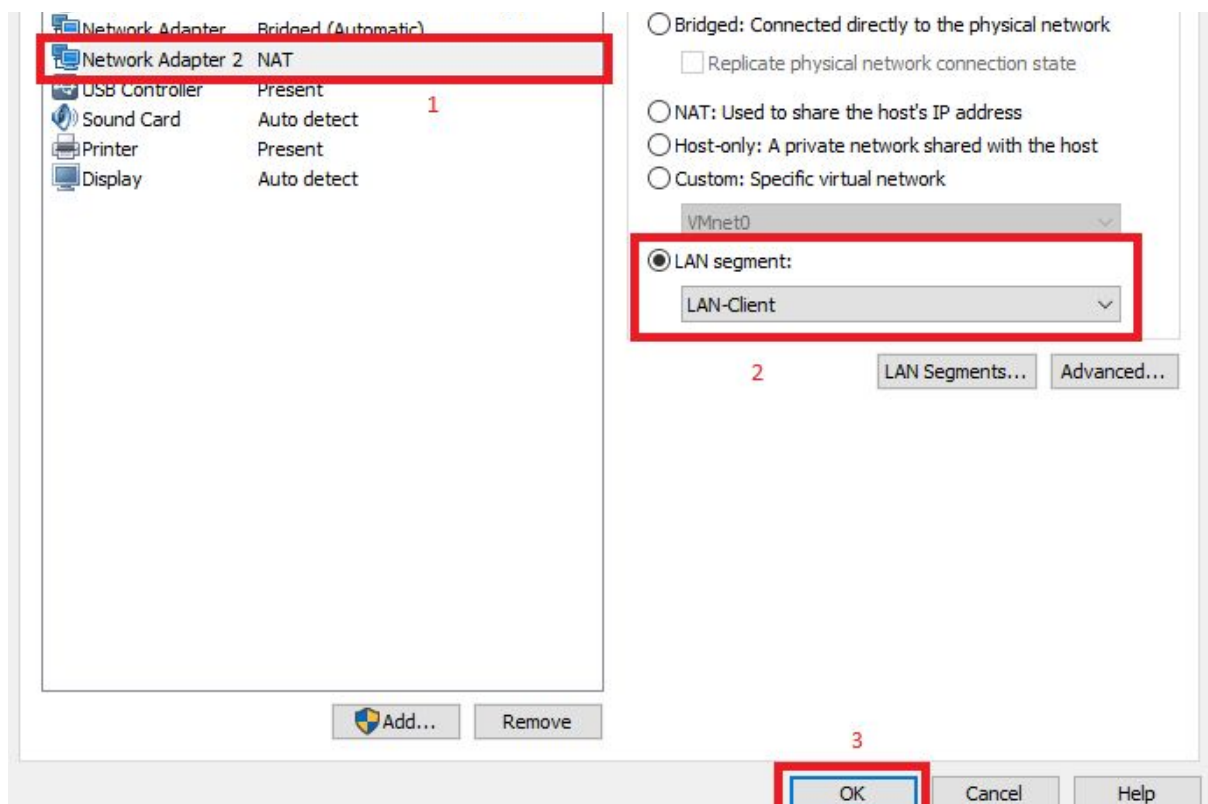
Nous pouvons maintenant créer notre réseau LAN :



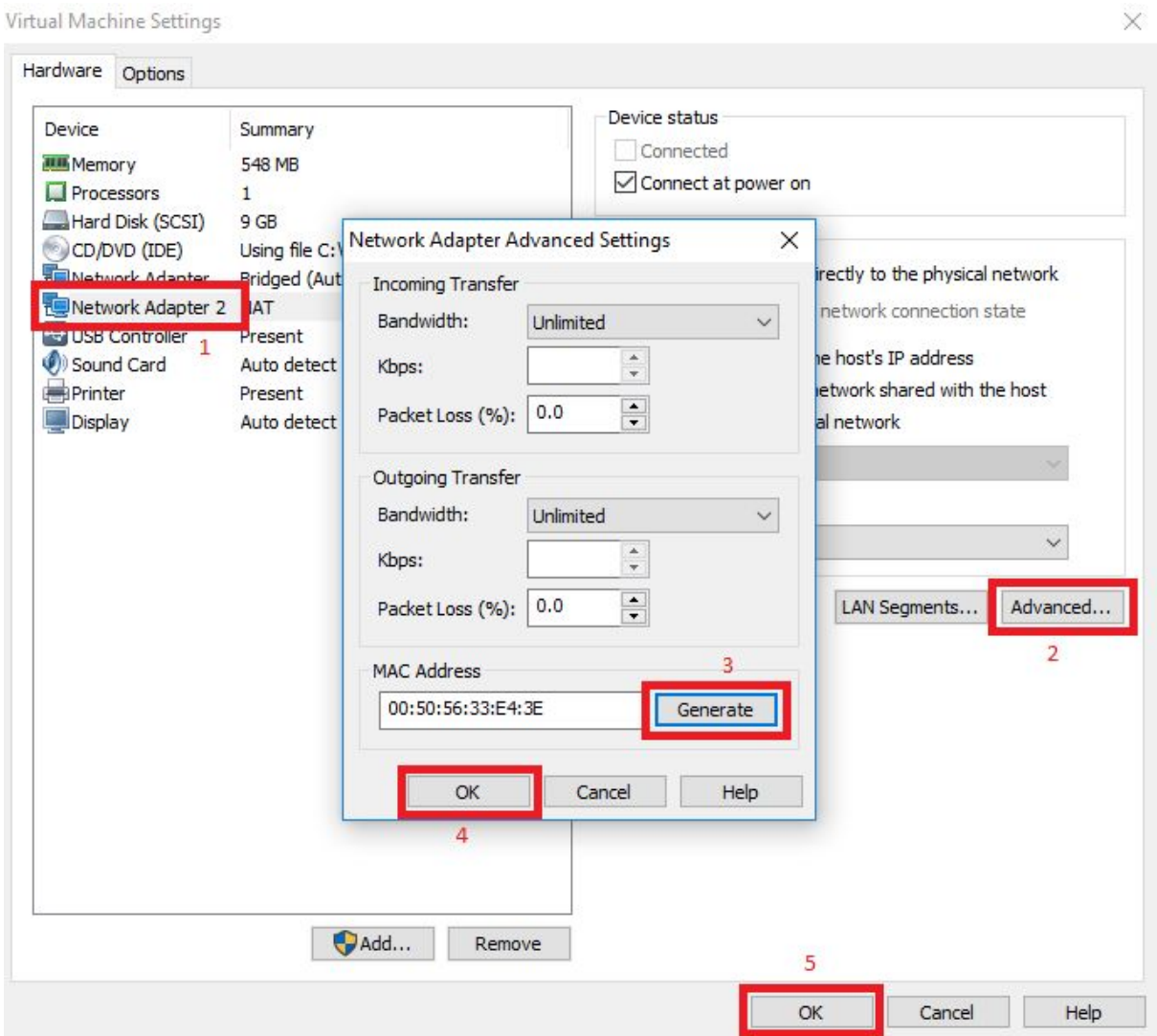
Nous ajoutons un nouveau réseau LAN. attention à bien le nommer pour pouvoir l'identifier plus tard :



Toujours sur notre nouvelle carte réseau, nous pouvons désormais sélectionner le mode "Segment LAN" pour les options de connexions réseaux. Dans le menu déroulant du segment LAN, nous devrions retrouver le réseau LAN créé juste avant :



Enfin, il ne reste plus qu'à générer une adresse MAC pour ce nouveau périphérique qu'est la carte réseau :



Il est préférable de noter les adresse MAC des cartes réseaux pour les identifier avec précision par la suite. Le tableau suivant résume les cartes réseaux en places pour le prototype :

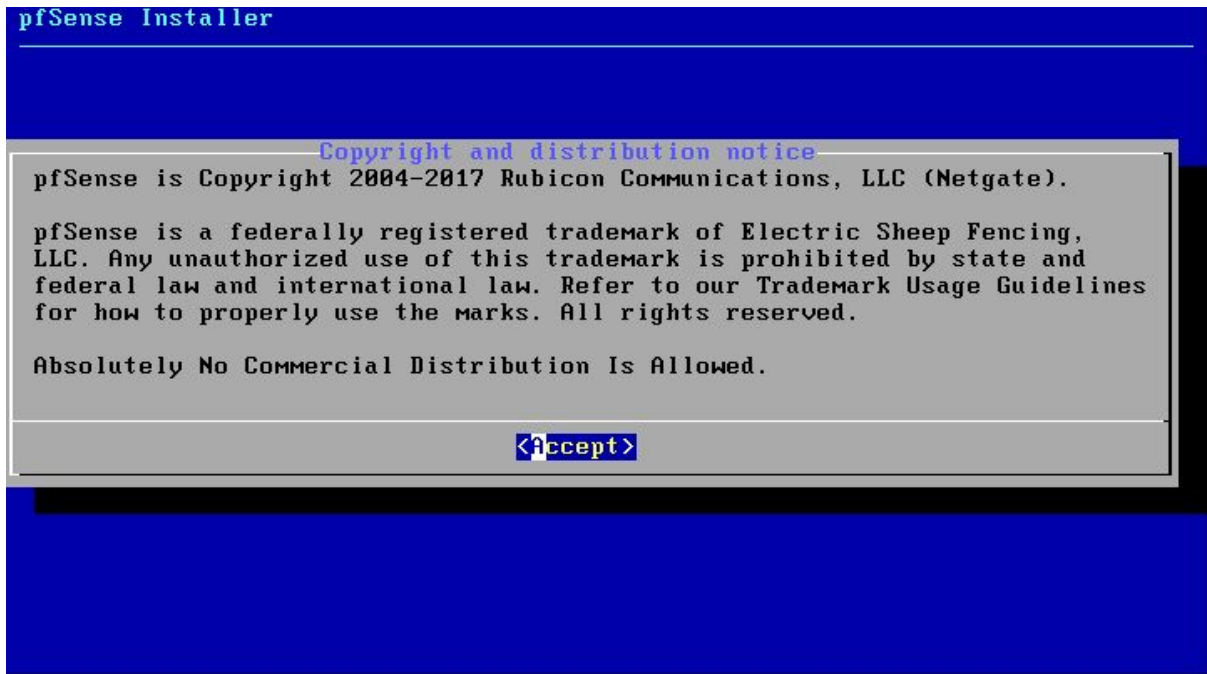
<b>Nom :</b>	em0	em1
<b>Mode réseau :</b>	Bridged	LAN Segment "Client"
<b>Adresse MAC :</b>	00:50:56:3A:5D:E7	00:50:56:30:74:FC
<b>Interface :</b>	WAN	LAN

La configuration des interfaces de la machine est maintenant terminé. Nous pouvons maintenant continuer avec la phase d'installation de l'OS Pfsense.

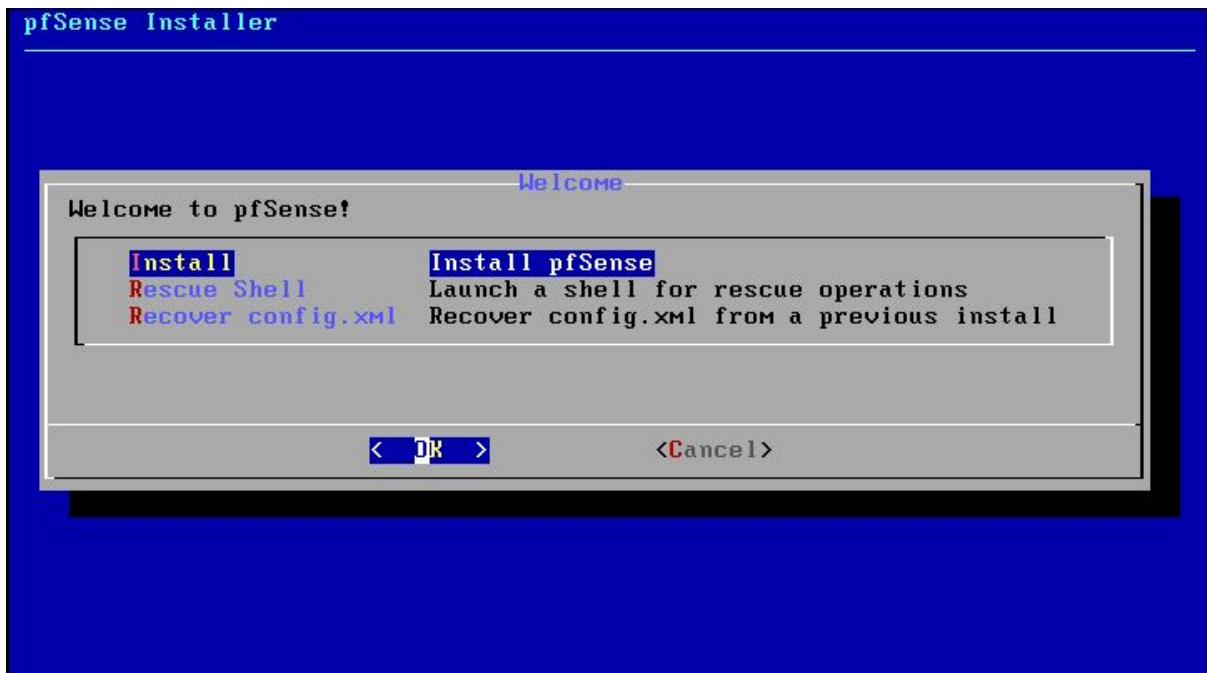


### III. Installation de la machine Pfsense :

Nous pouvons maintenant démarrer notre machine. Le boot est très rapide, et nous arrivons sur l'installation de l'OS. les options de configurations sont pour le moment très limitées, et il est possible d'accélérer le processus en gardant toutes les options par défaut. la première des tâches sera de lire et d'accepter le contrat d'utilisation de l'OS :

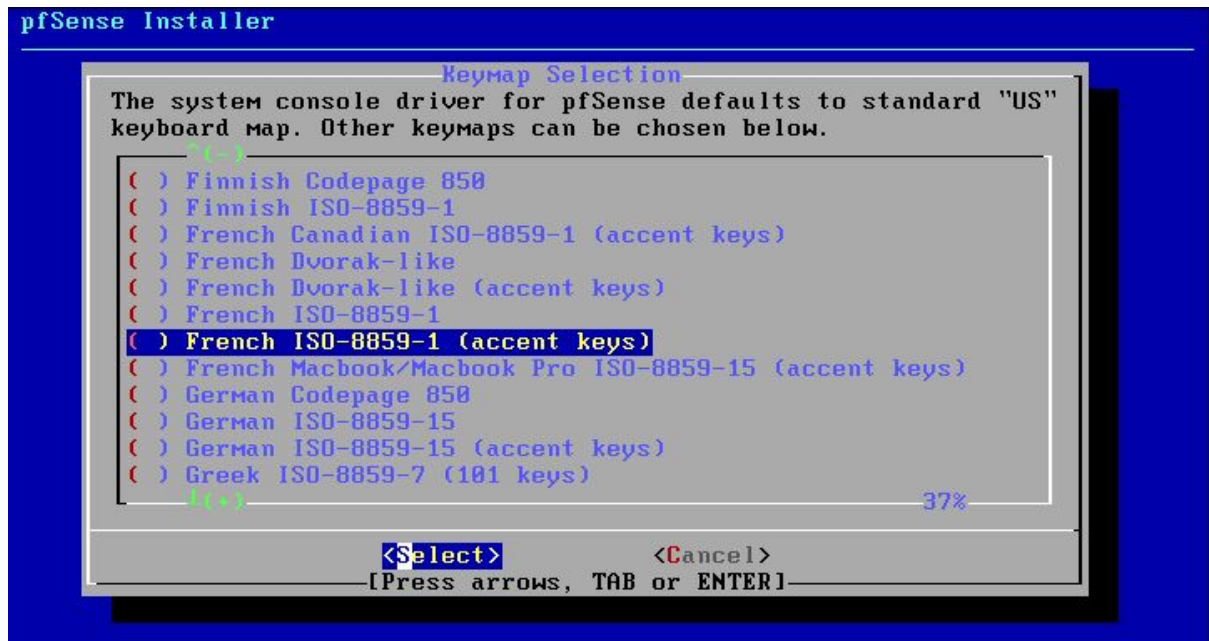


Nous allons ensuite indiquer que nous souhaitons installer Pfsense sur cette machine :

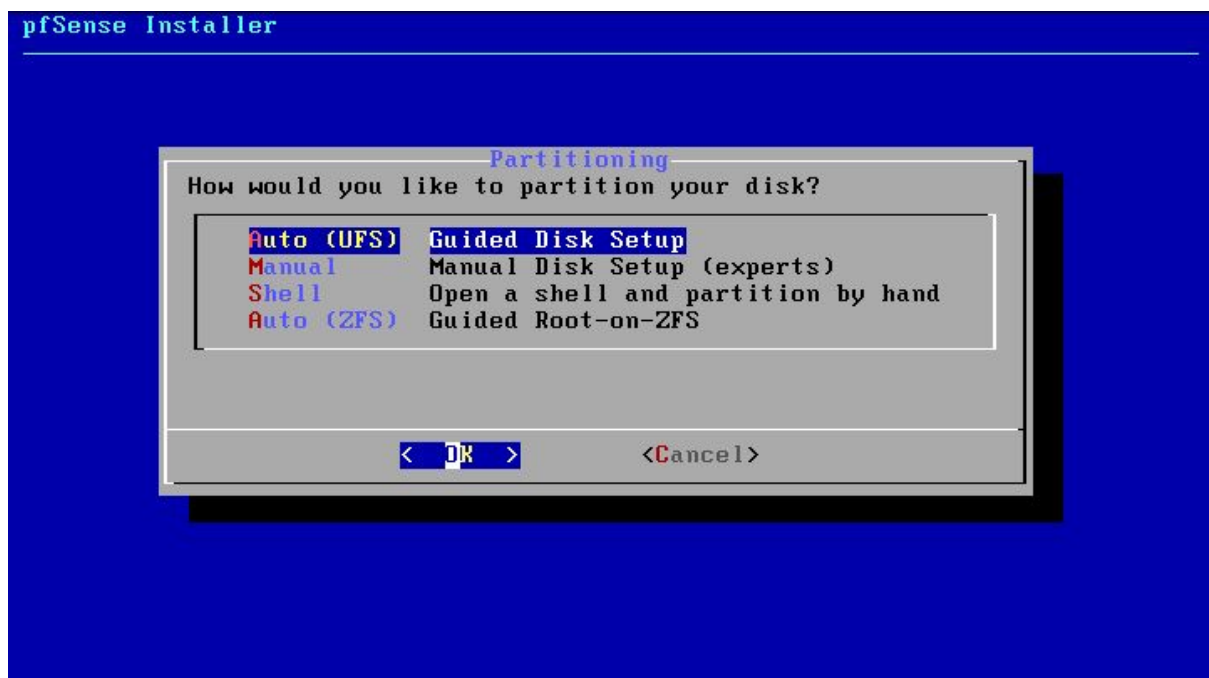


L'étape suivant consistera à sélectionner le type de mappage clavier à utiliser pour cette machine.

Attention à bien sélectionner la mappage avec la touche espace, avant de valider la sélection avec la touche “Entrer”



Enfin, nous allons indiquer que la répartition des fichiers sur le disque se fera de manière automatique :

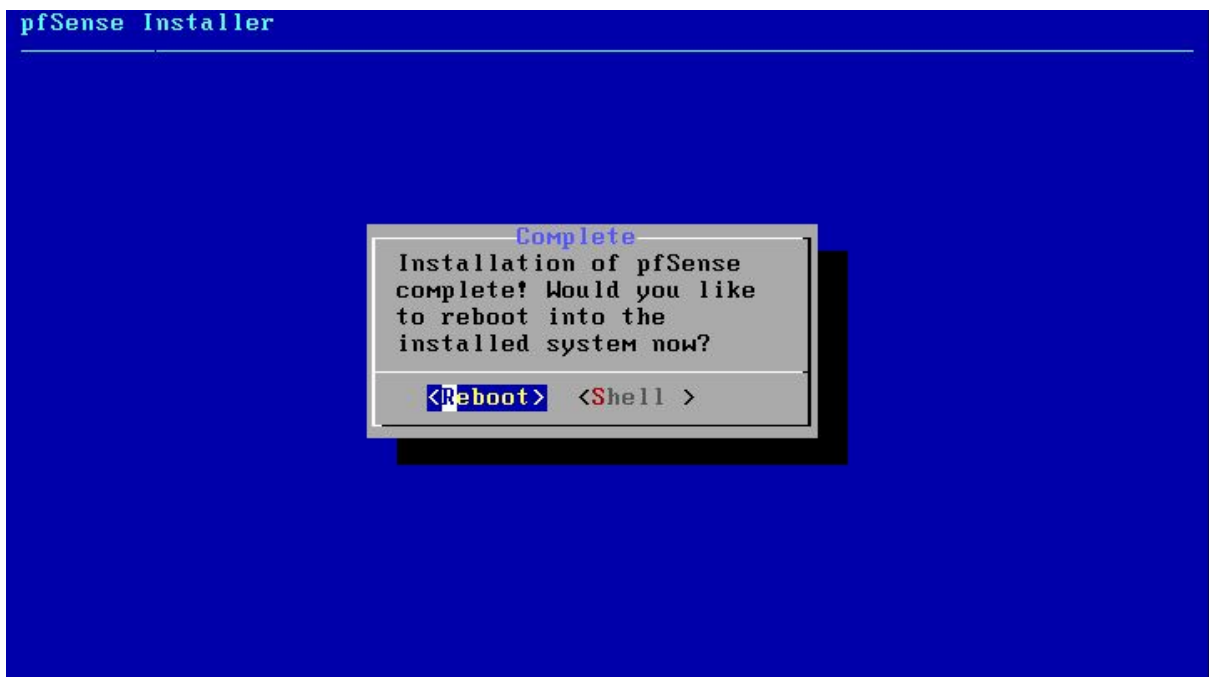


L'installation en elle même va ensuite débiter d'elle même. Celle-ci est très rapide, en effet, Pfsense est un système très léger basé sur linux.





Pour terminer, l'installation nous proposera d'ouvrir un shell pour vérifier la configuration automatique, ce que nous refusons. Enfin, il ne nous restera qu'à redémarrer la machine en veillant à retirer l'ISO pendant le redémarrage.



Le système d'exploitation est maintenant installé. Après un premier démarrage plutôt long, nous arrivons sur le menu de configuration general de Pfsense.

#### IV. Paramétrage des interfaces :

Maintenant que le système est installé, il nous faut paramétrer les deux interfaces réseaux. D'un côté, l'interface EM0 connectée au segment LAN "Client" avec une adresse réseau en 192.168.1.0/24. De l'autre, une interface EM1 en accès par pont, connecté au réseau 172.16.30.0/22.

Commençons par configurer l'interface LAN. il est recommandé d'avoir un poste client disponible pour la suite. Ce poste client virtuel doit avoir une carte réseau dans le même segment LAN que la carte EM0 de la machine Pfsense. Nous utiliserons ici un poste sous Linux Mint.

Le menu de configuration Pfsense est le suivant :

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.4.1-RELEASE amd64 Sun Oct 22 17:26:33 CDT 2017
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 01f8e9cd6bbaf82ae429

*** Welcome to pfSense 2.4.1-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: █
```

Par défaut, au vu des informations de la carte réseau VMWare, l'interface LAN à été configurée automatiquement avec une adresse valide appartenant au segment LAN "Client". Effectuons maintenant un test de validation de cet interface depuis le poste client sur le LAN. Ce poste devrait dans un premier temps obtenir une adresse IP cohérente avec celle du routeur Pfsense. Un Ifconfig nous confirme que le poste et l'interface Pfsense sont dans le même sous-réseau logique :

```
user@user ~ $ ifconfig
ens33: Link encap:Ethernet HWaddr 00:0c:29:9d:e4:dc
       inet addr:192.168.1.100 Bcast:192.168.1.255 Mask:255.255.255.0
       inet6 addr: fe80::a711:db8a:bec:9d0b/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:269 errors:0 dropped:0 overruns:0 frame:0
       TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:30854 (30.8 KB) TX bytes:14540 (14.5 KB)
```

Nous pouvons maintenant essayer de contacter l'interface LAN Pfsense avec un ping :

```
user@user ~ $ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.247 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.230 ms
^C
--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1020ms
rtt min/avg/max/mdev = 0.230/0.238/0.247/0.017 ms
```

Si l'interface est capable de nous répondre, nous en avons terminé avec la configuration de l'interface LAN.

Attaquons nous maintenant à l'interface WAN. Dans notre cas il s'agira du réseau 172.16.30.0/22 sur lequel notre poste physique est actuellement. Ce réseau possède un DHCP actif.

De retours sur le panneau de configuration Pfsense, nous allons sélectionner l'option 2, "Set interface(s) Ip address" :

```
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: █
```

Nous sélectionnons ensuite l'interface numéro 1, à savoir l'interface WAN. L'adresse de cet interface sera attribué via un DHCP :

```
Available interfaces:

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

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

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

Des options IPv6 sont ensuite paramétrables. Ne souhaitant pas y toucher, nous refusons le DHCP IPv6 et nous n'attribuons pas d'IP sur l'interface WAN IPv6 :

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

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

Enfin, nous activons l'interface de configuration graphique en ligne :

```
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y
Please wait while the changes are saved to WAN...
Reloading filter...
Reloading routing configuration...
DHCPD...█
```

Après quelques temps, l'interface WAN devrait apparaître comme ayant une adresse IP depuis le menu de configuration :

```
*** Welcome to pfSense 2.4.1-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4/DHCP4: 172.16.30.17/22
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 tester si l'interface est active et si l'adresse attribuée est valide, nous allons vérifier la connectivité entre notre poste physique et l'interface WAN. Notre poste physique à une adresse IP en 172.16.30.13 :

```
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: 7

Enter a host name or IP address 172.16.30.13

PING 172.16.30.13 (172.16.30.13): 56 data bytes
64 bytes from 172.16.30.13: icmp_seq=0 ttl=128 time=0.176 ms
64 bytes from 172.16.30.13: icmp_seq=1 ttl=128 time=0.478 ms
64 bytes from 172.16.30.13: icmp_seq=2 ttl=128 time=0.881 ms

--- 172.16.30.13 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.176/0.512/0.881/0.289 ms

Press ENTER to continue.
█
```

L'option de ping est disponible à l'option n°7.

Les deux interfaces sont donc désormais capables de contacter leurs réseaux respectifs. Cette dernière phase de configuration Pfsense est maintenant terminée.

#### V. Première connexion :

La suite des interactions avec Pfsense se fera via la machine cliente dans le segment LAN "Client". Il suffira d'ouvrir un navigateur et d'accéder à l'adresse IP de l'interface LAN du routeur Pfsense : 192.168.1.1 :

Nous tombons normalement sur la page d'administration web de routeur Pfsense.

Les identifiants de connexions par défauts sont :

admin	pfsense
-------	---------



[Login to pfSense](#)

A screenshot of the pfSense web interface login page. It has a dark blue background with the text 'SIGN IN' in white. Below it are two input fields labeled 'Username' and 'Password' in a light blue font. At the bottom is a green button with the text 'SIGN IN' in white.

La suite de la configuration se fera entièrement via cet interface web.

Attention à vérifier que notre machine cliente

#### VI. Conclusion :

Notre machine Pfsense est maintenant configurée de façon basique, avec des interfaces correctement configurées :

EM0	WAN	172.16.30.230
EM1	LAN	192.168.1.1

Les postes clients sont maintenant capables de se connecter à internet et d'échanger correctement avec le futur serveur proxy. Nous pourrions commencer à configurer les règles d'accès à internet, la blacklist de sites webs, et les sports de connexions valides.