

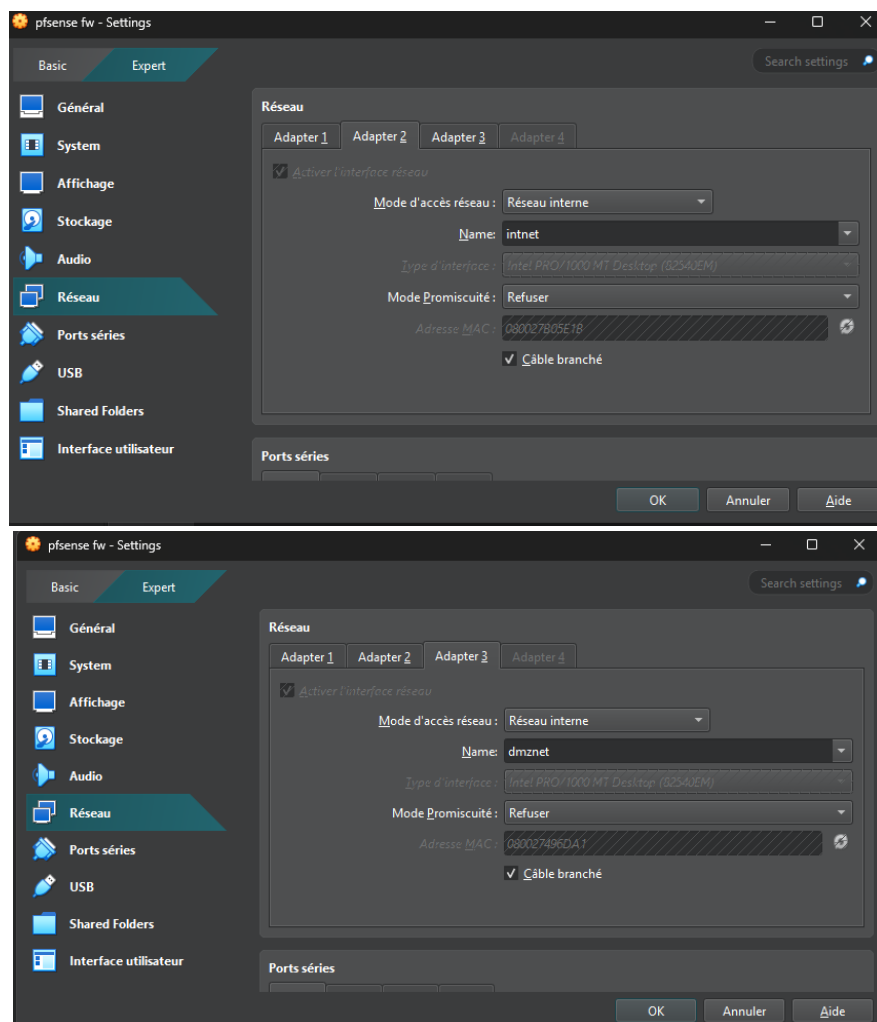
Compte rendu de l'installation de pfsense :

Outils :

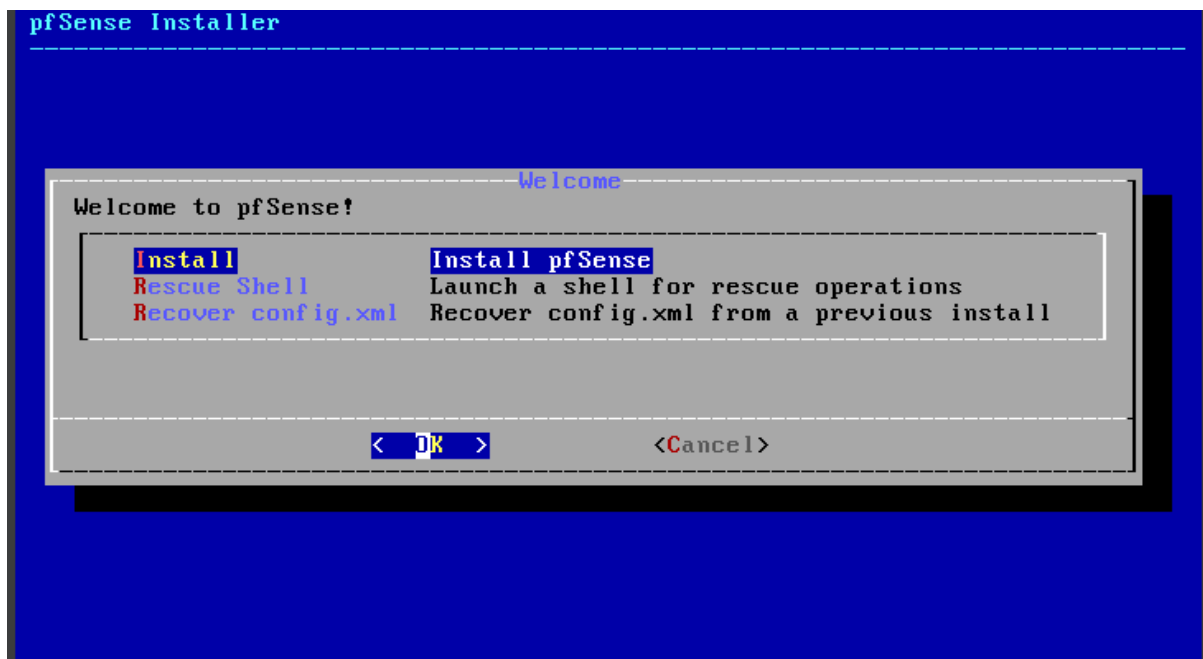
- Virtualbox (une vm pfsense et une vm Ubuntu Desktop)

Mise en place et installation de pfsense :

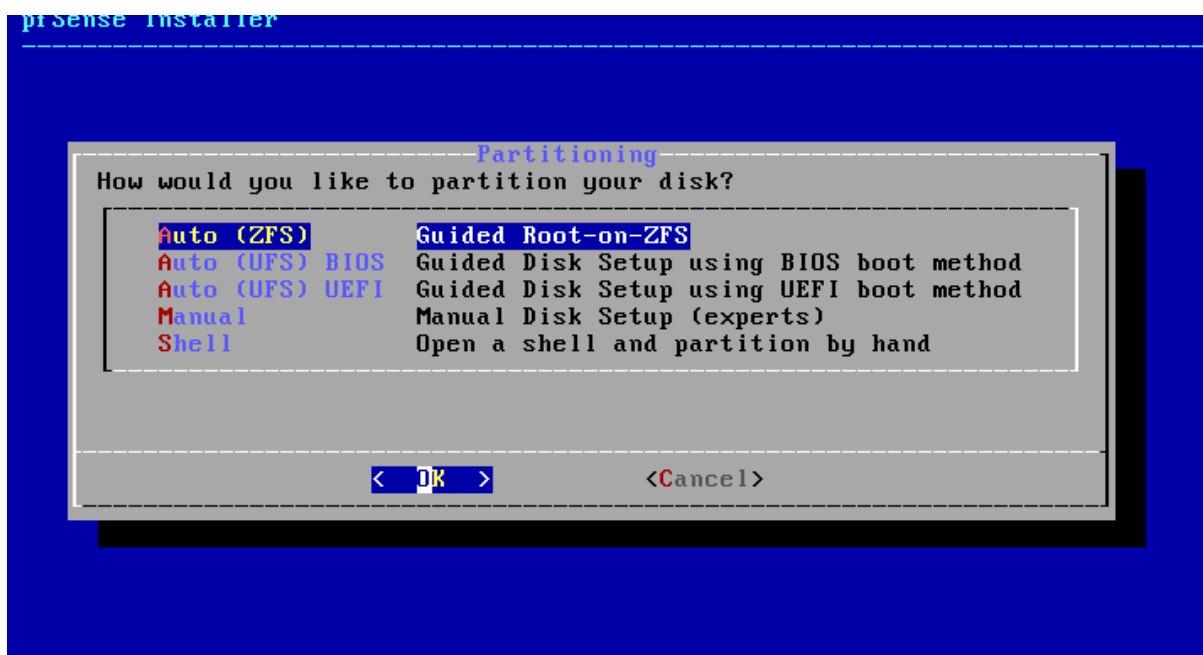
Pour commencer, nous devons créer une nouvelle machine virtuelle avec l'ISO pfsense en prenant soin de mettre le type BSD (pfsense étant une distribution FreeBSD) en 64 bits. Avant de lancer la machine virtuelle, il faut activer deux interfaces supplémentaires afin de pouvoir connecter pfsense à notre réseau interne pour pouvoir le configurer sur son interface web plus tard et une autre interface pour créer la DMZ plus tard.



On lance ensuite notre machine virtuelle puis on accepte la licence avant de pouvoir sélectionner l'installation de pfsense comme ci-dessous :



Ensuite, il nous suffit de suivre ces diverses étapes dans ce sens :



On sélectionne ZFS car il permet de faciliter l'installation

pfSense Installer

ZFS Configuration

Select Virtual Device type:

stripe	Stripe - No Redundancy
mirror	Mirror - n-Way Mirroring
raid10	RAID 1+0 - n x 2-Way Mirrors
raidz1	RAID-Z1 - Single Redundant RAID
raidz2	RAID-Z2 - Double Redundant RAID
raidz3	RAID-Z3 - Triple Redundant RAID

< OK > <Cancel>

-----[Press arrows, TAB or ENTER]-----

[1+ Disks] Striping provides maximum storage but no redundancy

On choisit "stripe" pour une installation sur un seul disque puis on lance l'installation.

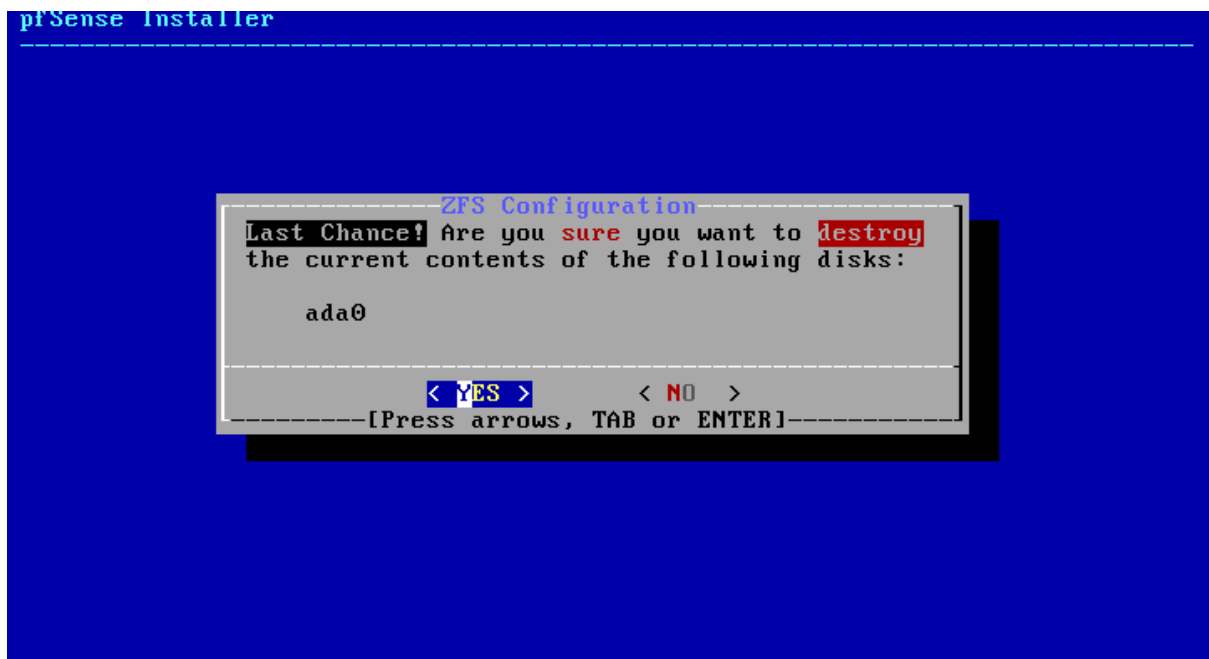
pfSense Installer

ZFS Configuration

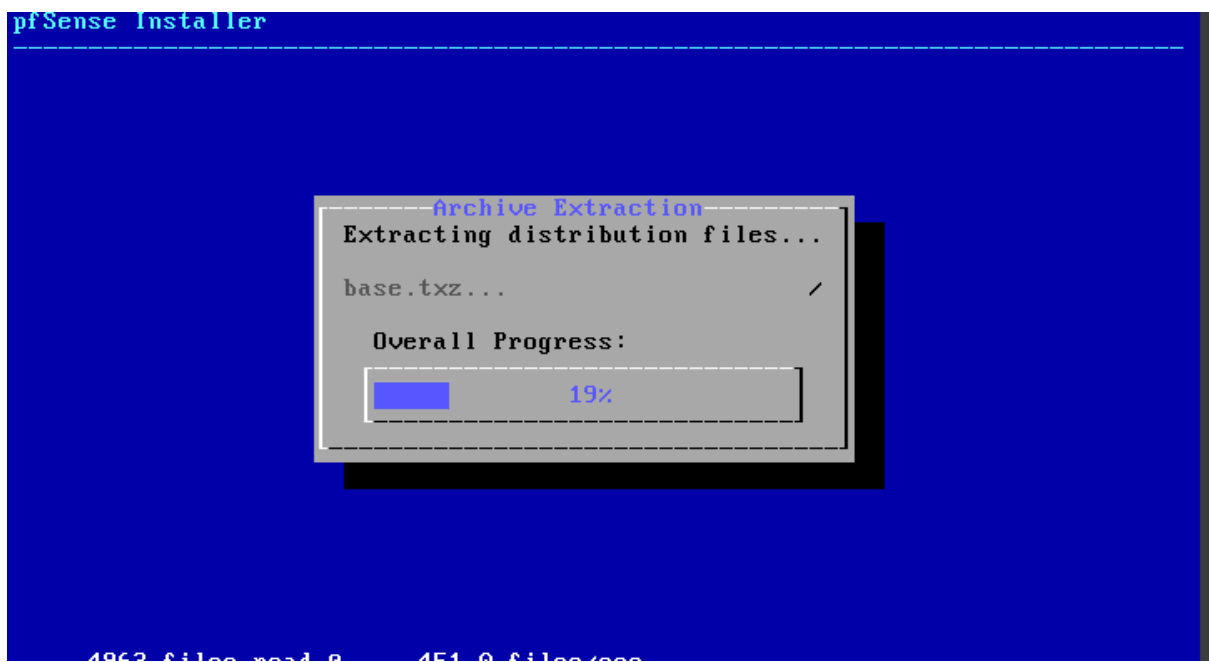
Configure Options:

>>> Install	Proceed with Installation
T Pool Type/Disks:	stripe: 0 disks
- Rescan Devices	*
- Disk Info	*
N Pool Name	pfSense
4 Force 4K Sectors?	YES
E Encrypt Disks?	NO
P Partition Scheme	GPT (BIOS)
S Swap Size	1g
M Mirror Swap?	NO
W Encrypt Swap?	NO

<Select> <Cancel>



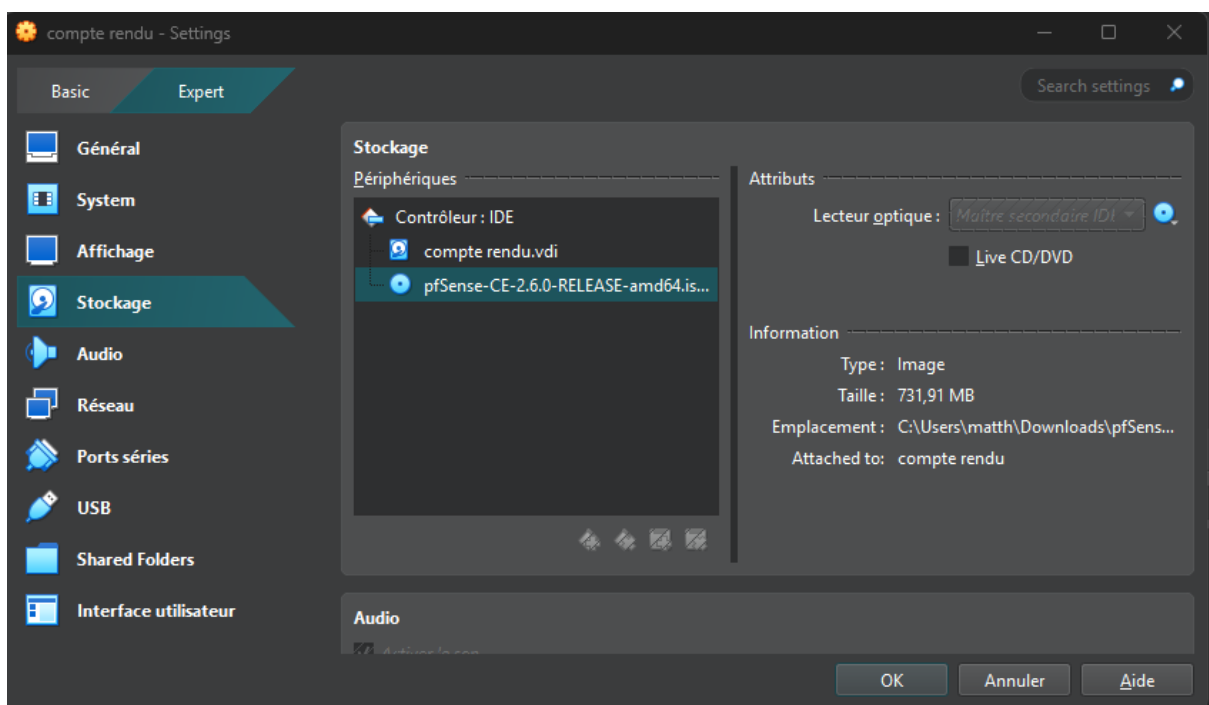
Puis on laisse l'installation se faire :



On refuse l'installation manuelle car nous n'avons rien à modifier là-dessus :



Avant de reboot la machine, il faut supprimer le périphérique optique et garder le .vdi car sinon l'installation risque d'être compromise :



Une fois supprimé, on peut relancer la machine et accéder au menu de pfsense dès que c'est chargé :

```

FreeBSD/amd64 (pfsense-fw.firewalling.com) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: 4074fb5081d01906f1d6

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

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
                v6/DHCP6: fd00::a00:27ff:fe28:1cf7/64
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
DMZ (opt1)     -> em2      -> v4: 10.1.1.1/32

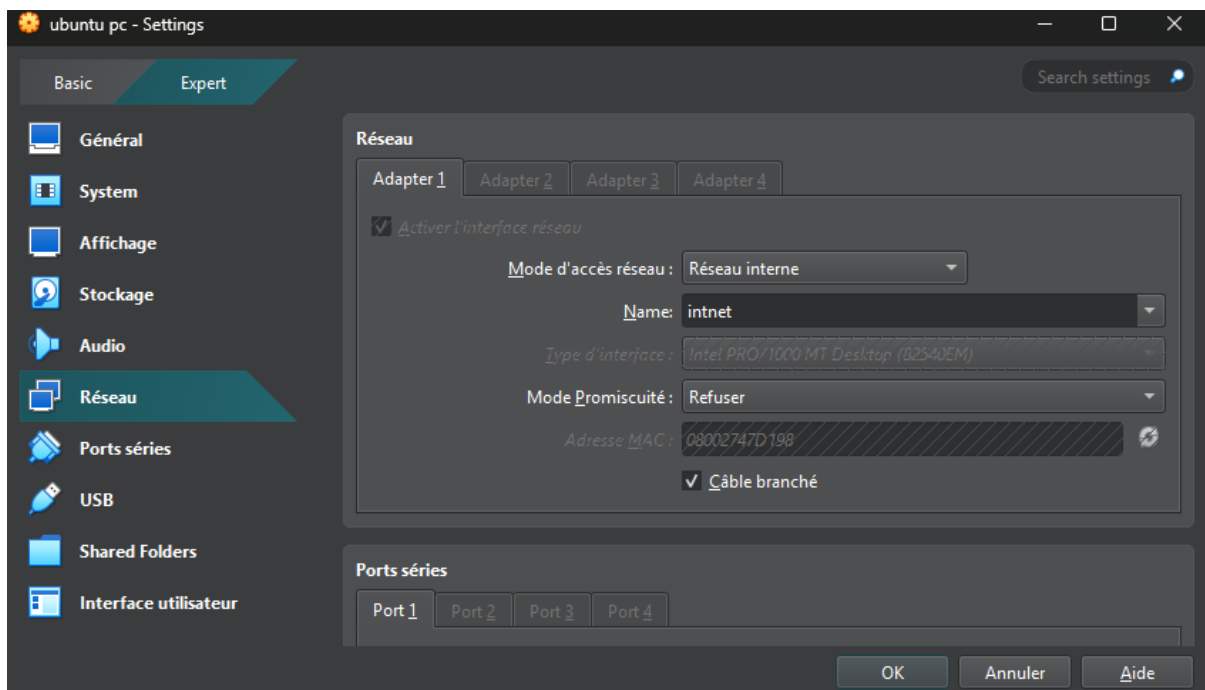
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable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

Enter an option: █

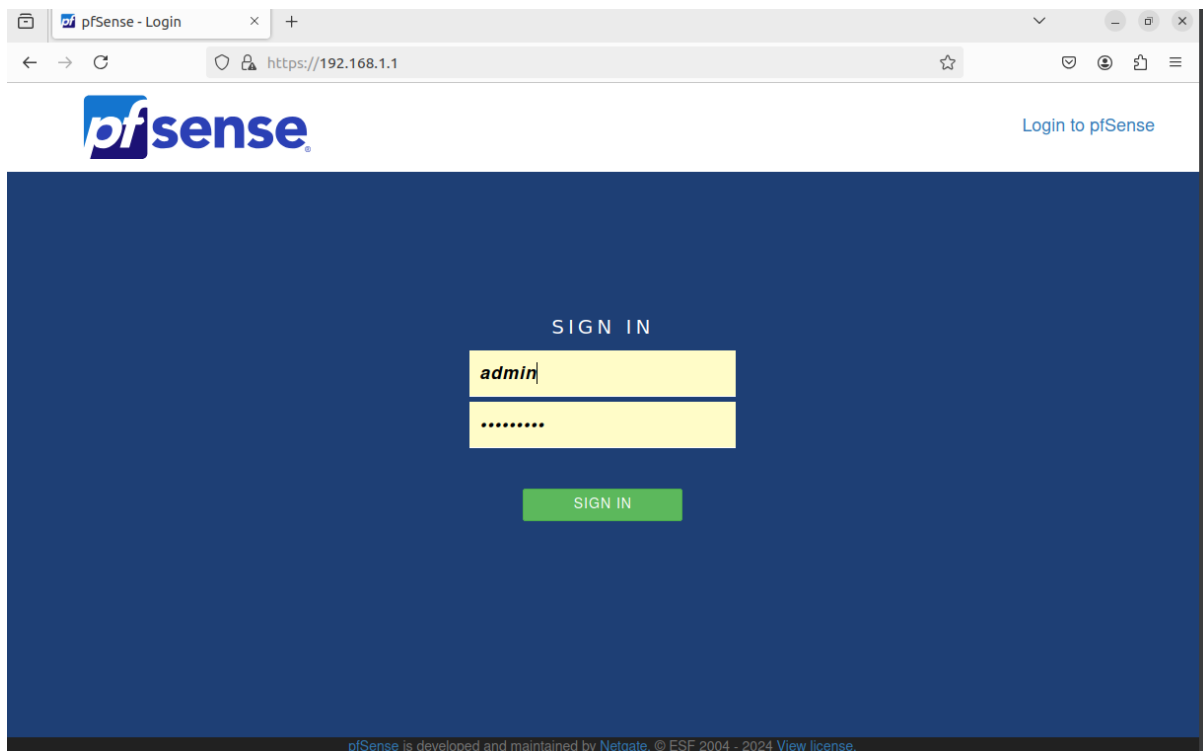
```

Installation de la machine Ubuntu :

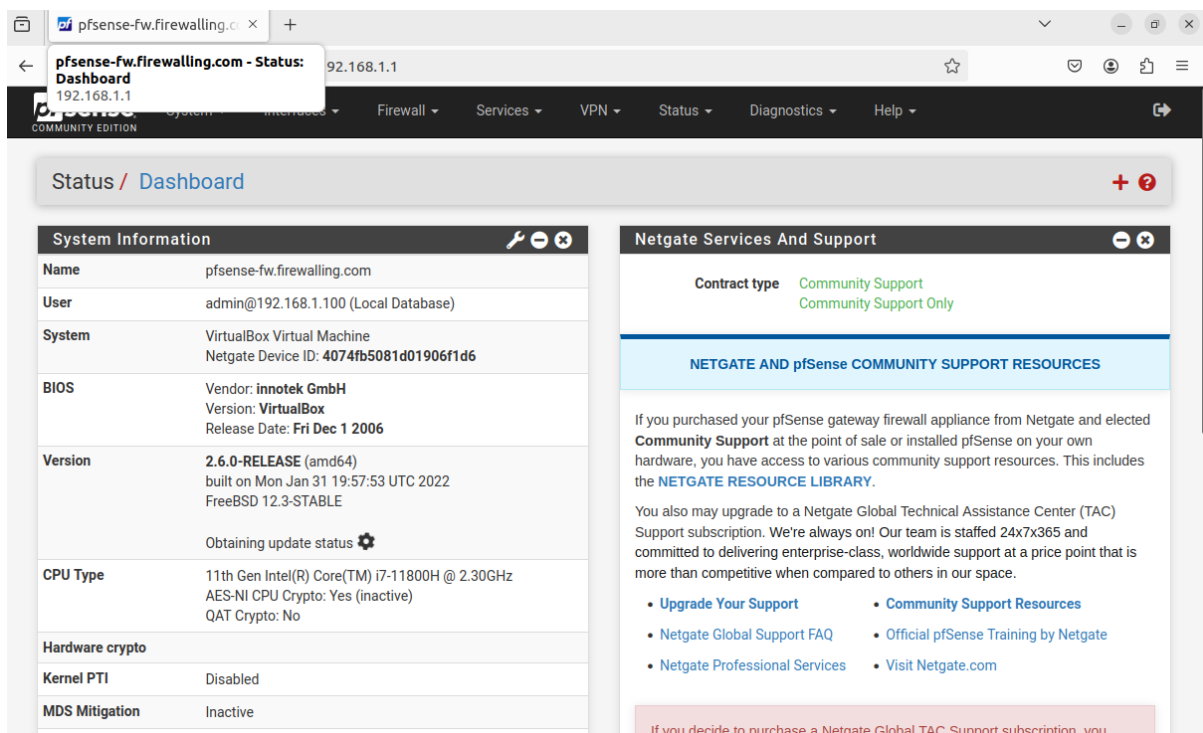
Nous créons une nouvelle machine virtuelle avec l'ISO Ubuntu Desktop en modifiant l'interface réseau pour la passer en réseau interne. L'installation prendra un peu de temps mais une fois effectué, on pourra vérifier que l'ip soit bien celle du réseau interne avec pfsense.



Configuration de pfsense via son interface Web :



On se connecte sur l'interface Web de pfSense qui a pour adresse 192.168.1.1 et une fois connecté, nous nous retrouvons sur le dashboard.



On se dirige ensuite dans l'onglet "Interfaces" afin de vérifier si nos interfaces sont bien présentes (la DMZ doit être ajoutée avec l'interface OPT1 où l'on clique sur le bouton add en sélectionnant l'interface correspondante).

Interfaces / Interface Assignments

Interface Assignments

Interface Groups

Wireless

VLANs

QinQs

PPPs

GREs

GIFs

Bridges

LAGGs

Interface	Network port
WAN	em0 (08:00:27:28:1c:f7)
LAN	em1 (08:00:27:b0:5e:1b) <div>Delete</div>
DMZ	em2 (08:00:27:49:6d:a1) <div>Delete</div>

Save














Interfaces that are configured as members of a lagg(4) interface will not be shown.

Wireless interfaces must be created on the Wireless tab before they can be assigned.

Puis on se dirige dans l'onglet "Firewall" puis "Rules" en sélectionnant l'interface que l'on souhaite afin de rajouter les règles correspondantes à nos normes de sécurité.

Floating WAN LAN DMZ







Rules (Drag to Change Order)






<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓	0/410 KiB	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓	0/720 KiB	IPv4 TCP	LAN net	*	*	*	*	none	allow to access WAN	   
<input type="checkbox"/>	✓	2/488 KiB	IPv4 *	LAN net	*	*	*	*	none	Default allow LAN to any rule	   
<input type="checkbox"/>	✓	0/0 B	IPv6 *	LAN net	*	*	*	*	none	Default allow LAN IPv6 to any rule	   

 Add  Add  Delete  Save  Separator

Floating WAN LAN DMZ









Rules (Drag to Change Order)






<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗	0/0 B	*		RFC 1918 networks	*	*	*	*	Block private networks	
<input type="checkbox"/>	✗	0/0 B	*		Reserved Not assigned by IANA	*	*	*	*	Block bogon networks	
<input type="checkbox"/>	✗	0/0 B	IPv4 TCP	*	*	*	*	none		block external traffic	   

 Add  Add  Delete  Save  Separator

Floating WAN LAN DMZ

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	*	80 (HTTP)	*	none		allow access DMZ (80/HTTP)	   
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	*	DMZ net	443 (HTTPS)	*	none		allow access DMZ	   

 Add  Add  Delete  Save  Separator