

Configuration



**MISTRAL
MARTHELY
PHAM**

02/05/2022

ARCHITECTURE CLIENT-SERVEUR

*Détail des configurations à réaliser
pour mettre en œuvre la solution
(système, réseau, services)*

01 Configuration pare-feu

Configuration pare-feu

Présentation pas à pas de la configuration du pare-feu sous PfSense

02 Configuration clients

Configuration clients

Présentation pas à pas de la configuration des clients sous Windows et Linux

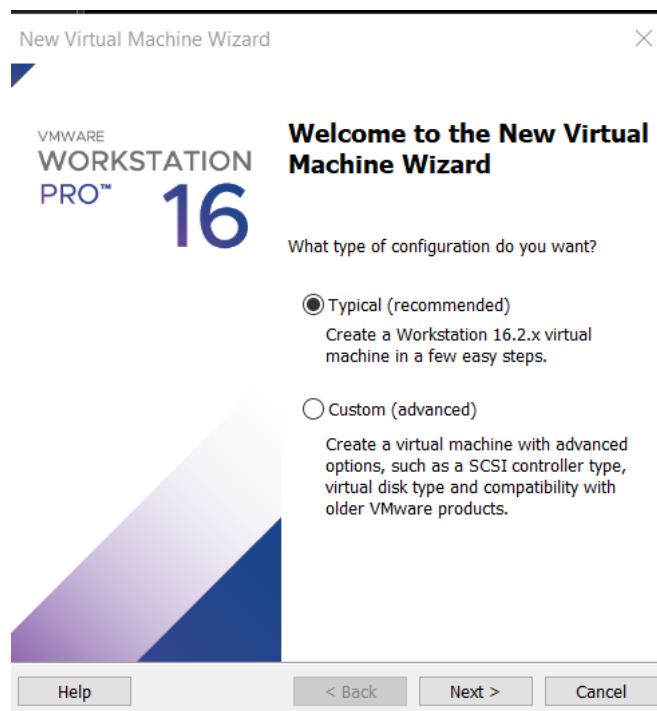
03 Configuration serveur

Configuration serveur

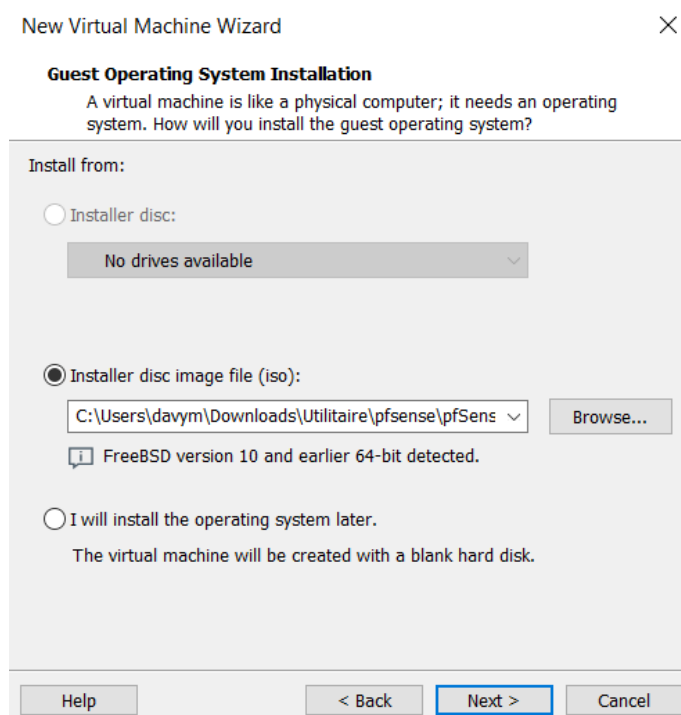
Présentation pas à pas de la configuration du serveur sous Nginx

Configuration pare-feu

Nous allons présenter ici la démarche de configuration du pare-feu étape par étape, ici à l'aide d'une nouvelle machine virtuelle.



Utiliser le type de configuration « Typical » qui est celle recommandée, pas besoin d'option avancée pour le moment



Après avoir préalablement télécharger l'iso PfSense, indiquer le chemin de ce dernier à la VM

New Virtual Machine Wizard
✕

Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name:

Location:

Browse...

The default location can be changed at Edit > Preferences.

< Back
Next >
Cancel

Ici il est possible de renommer directement le nom de la VM ainsi que son emplacement. L'emplacement n'est pas nécessaire à la modification cependant.

New Virtual Machine Wizard
✕

Specify Disk Capacity

How large do you want this disk to be?

The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.

Maximum disk size (GB):

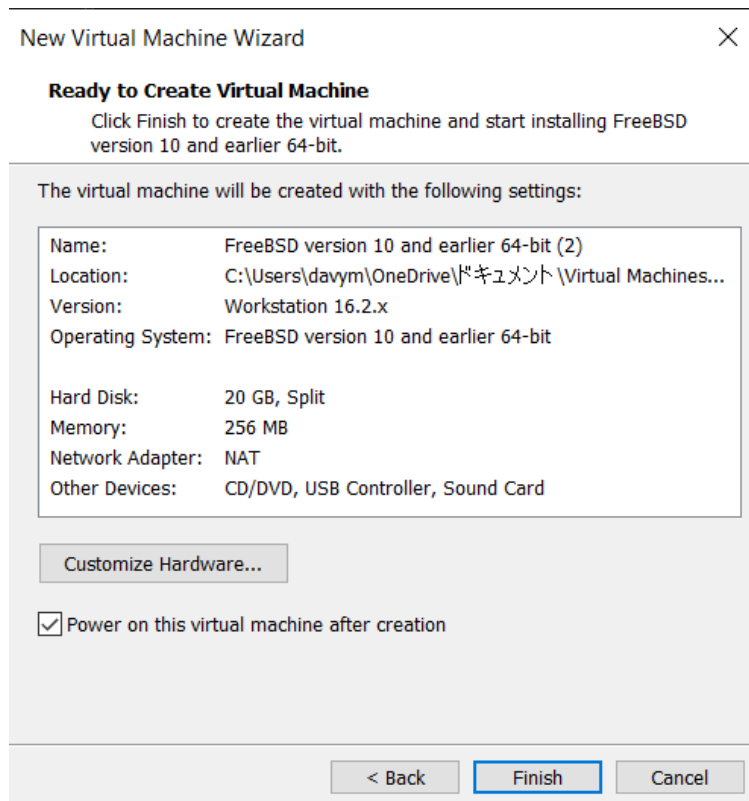
Recommended size for FreeBSD version 10 and earlier 64-bit: 20 GB

☐ Store virtual disk as a single file
☒ Split virtual disk into multiple files

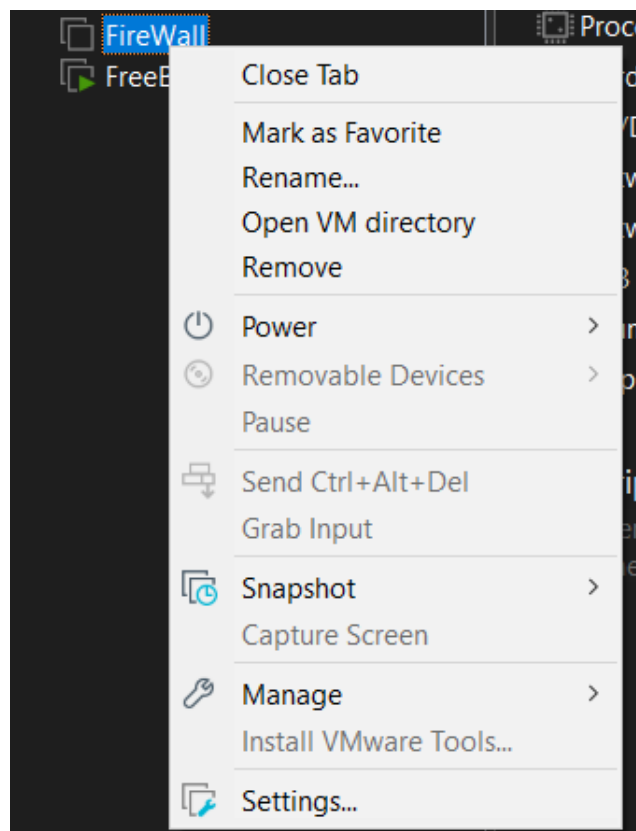
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Help
< Back
Next >
Cancel

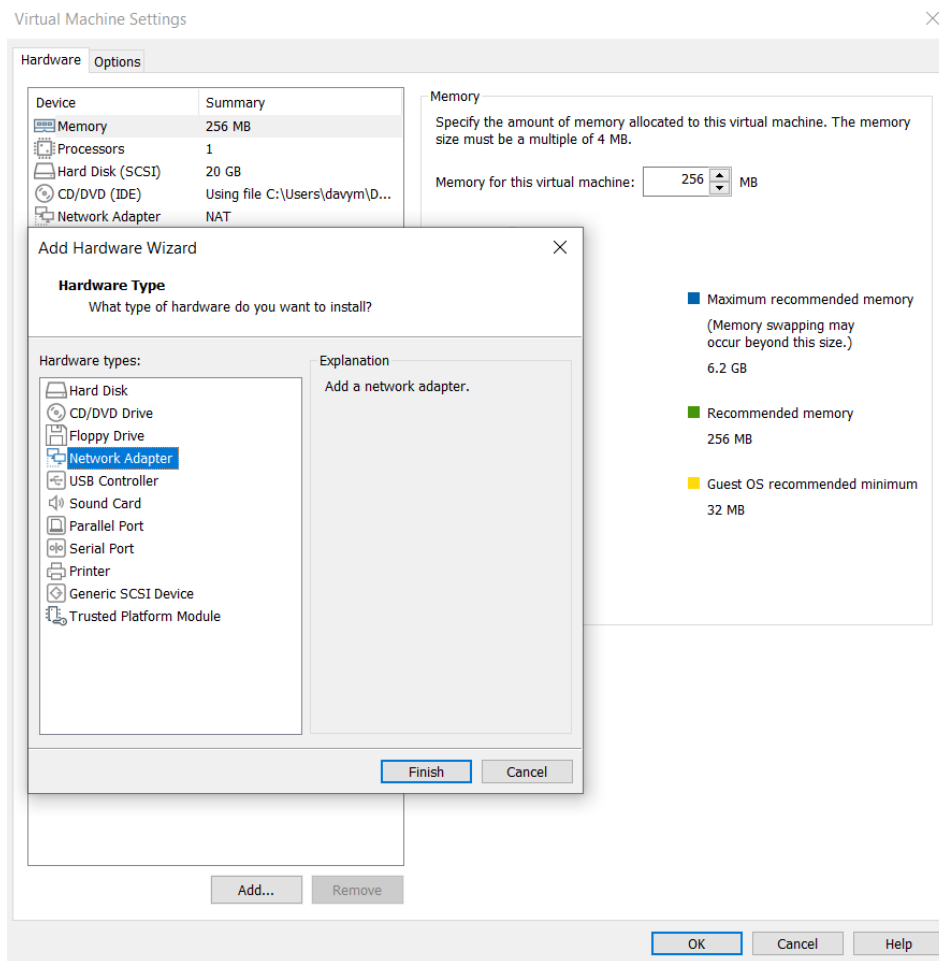
Vient ensuite la possibilité d'allocation de l'espace disque, ici nous mettons 20GB de façon à être large mais le pare-feu ne demande pas autant d'espace. Sélectionner l'option de séparation du disque virtuel en plusieurs fichiers.



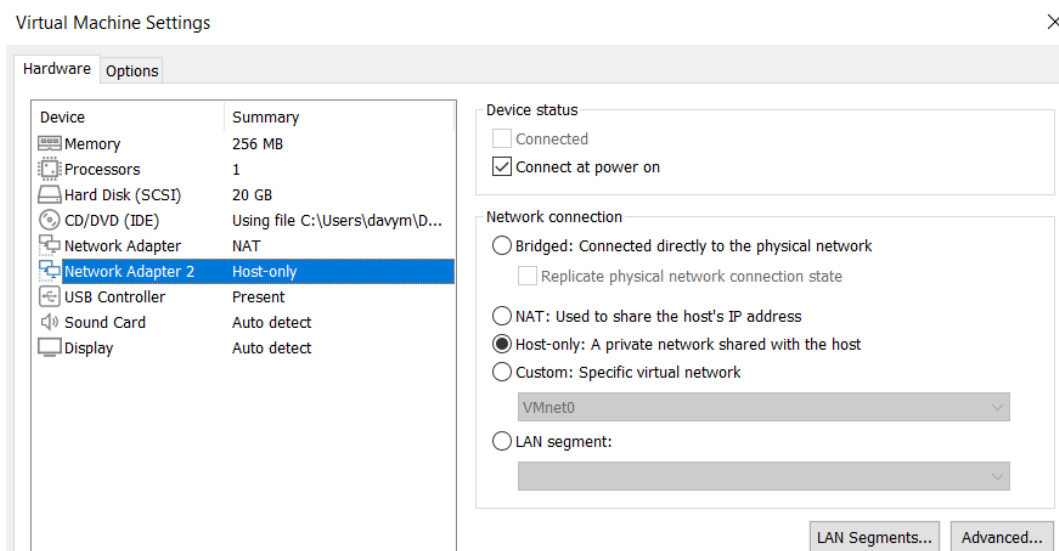
Ici vient le récap de la création de notre VM. Pour finir le processus appuyer tout simplement sur « Finish » si tous les éléments vous conviennent



Petite étape à ne pas oublier, notre pare-feu doit comporter 2 adaptateurs internet, car c'est ce dernier qui fera office de passerelle entre le WAN et le LAN. Pour ce faire sur la VM, effectuer un clic droit et ensuite sur « Settings ».

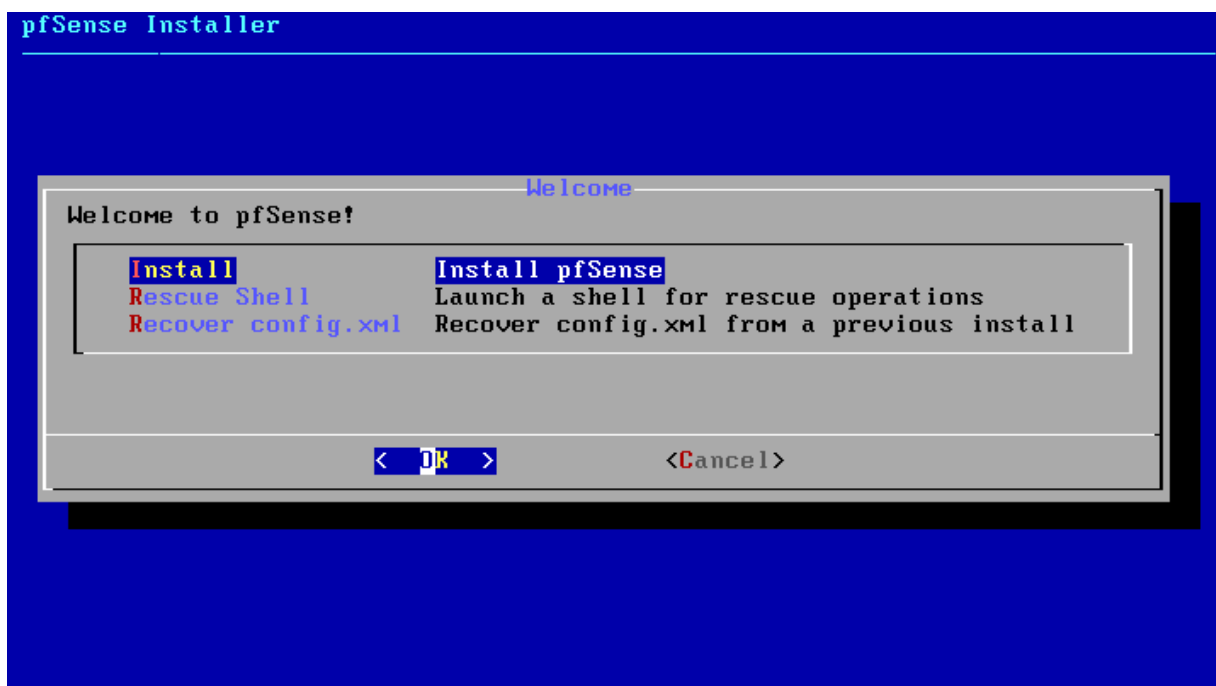
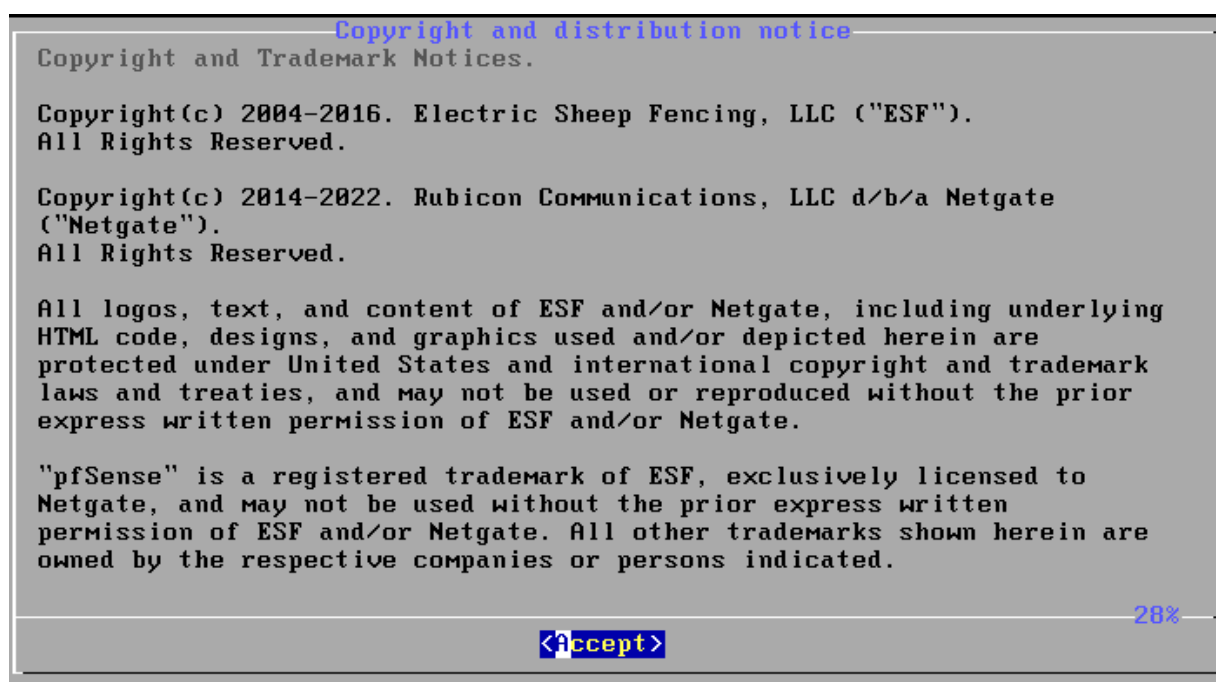


Appuyer sur « Add », ensuite sélectionner « Network Adpatater ».



Une fois ce nouvel adaptateur ajouté, mettre celui-ci en « host-only ». Il ne reste plus qu'à lancer maintenant le pare-feu.

Ci-joint une série de captures des étapes à suivre



Keymap Selection

The system console driver for pfSense defaults to standard "US" keyboard map. Other keymaps can be chosen below.

```
>>> Continue with default keymap
->- Test default keymap
( ) Armenian phonetic layout
( ) Belarusian
( ) Belgian
( ) Belgian (accent keys)
( ) Brazilian (accent keys)
( ) Brazilian (without accent keys)
( ) Bulgarian (BDS)
( ) Bulgarian (Phonetic)
( ) Canadian Bilingual
( ) Central European
```

L(+)

13%

<Select>

<Cancel>

[Press arrows, TAB or ENTER]

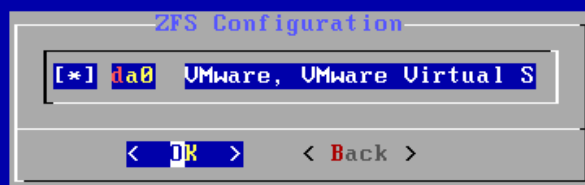
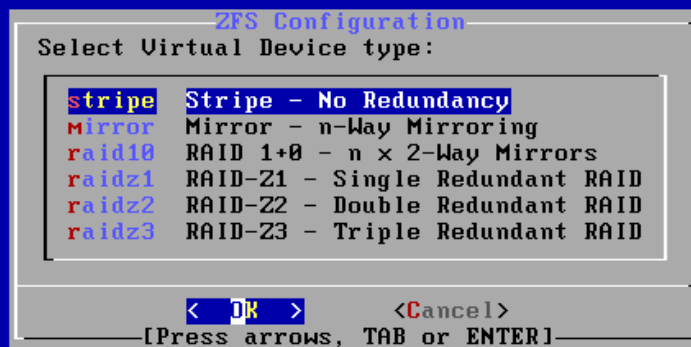
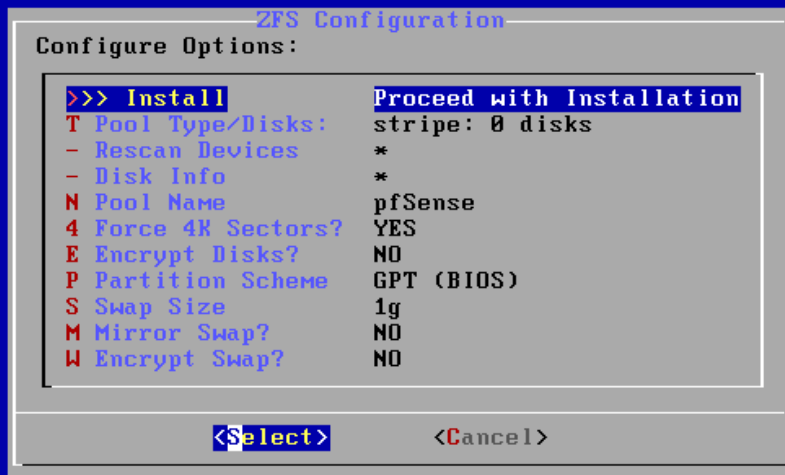
Partitioning

How would you like to partition your disk?

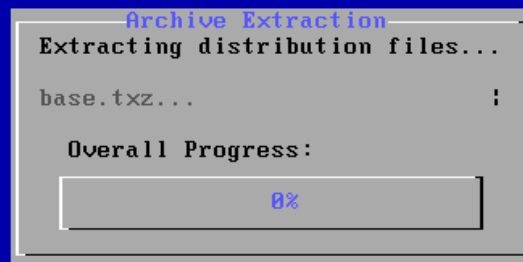
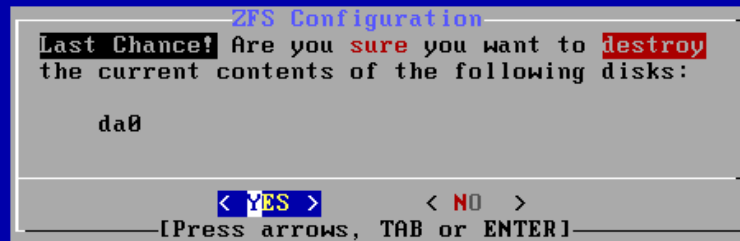
Auto (ZFS)	Guided Root-on-ZFS
Auto (UFS) BIOS	Guided Disk Setup using BIOS boot method
Auto (UFS) UEFI	Guided Disk Setup using UEFI boot method
Manual	Manual Disk Setup (experts)
Shell	Open a shell and partition by hand

< OK >

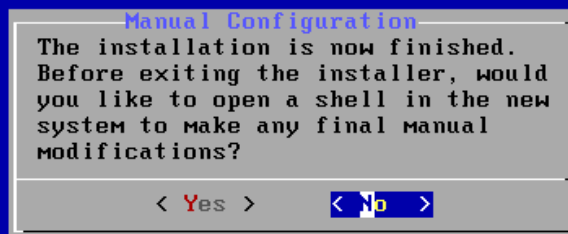
<Cancel>

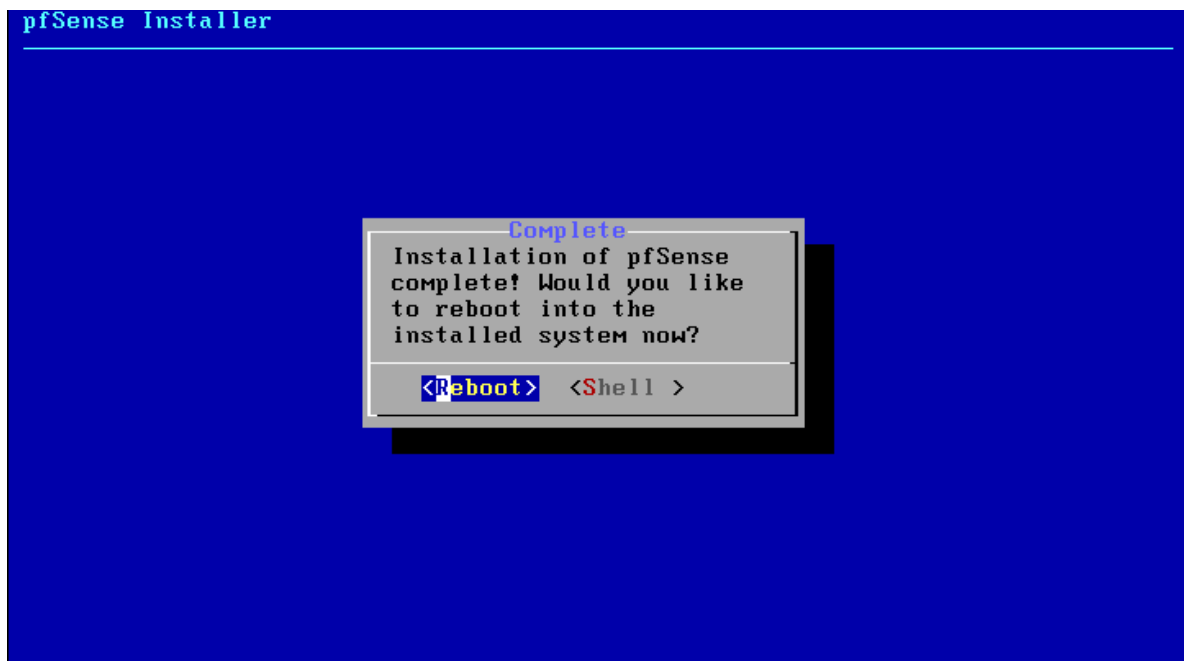


Ici appuyer sur la touche espace pour que l'étoile apparaisse signifiant ainsi « all »



173 files read @ 173.0 files/sec.





```
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: da27cc013a53124acad1

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

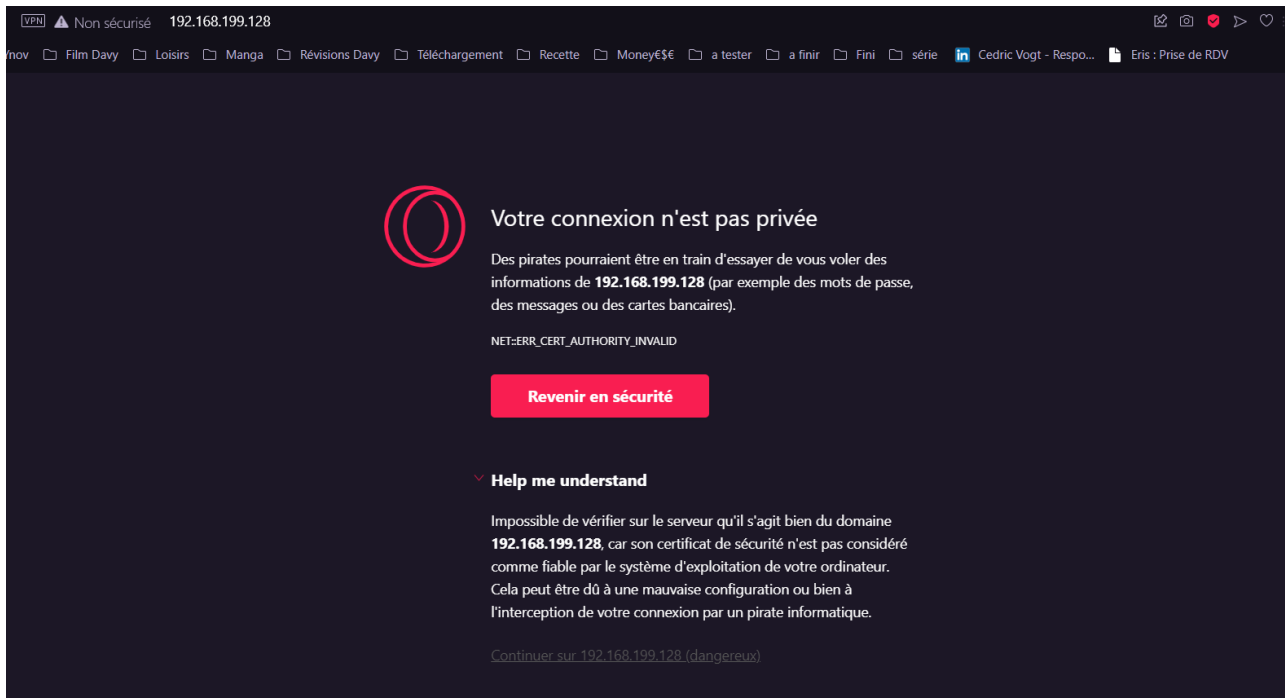
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.199.128/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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

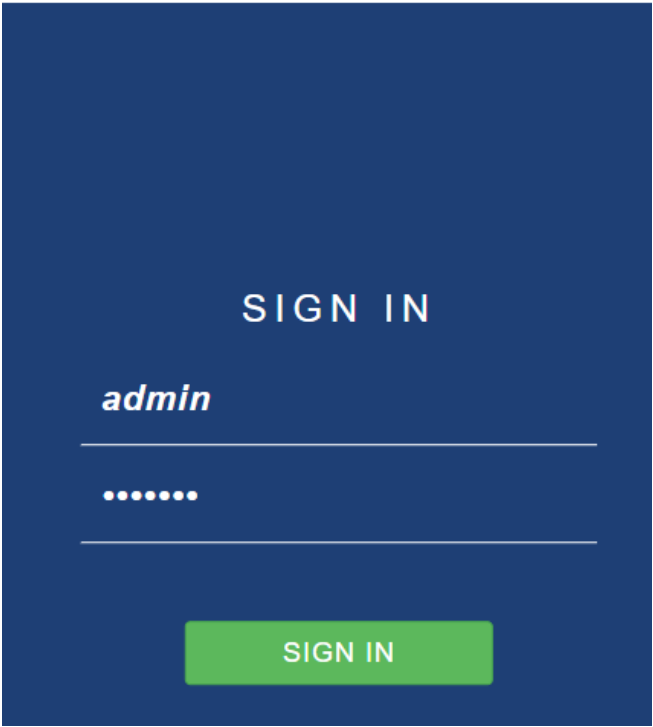
Enter an option: 8

[2.6.0-RELEASE][root@pfSense.home.arpa]/root: █
```

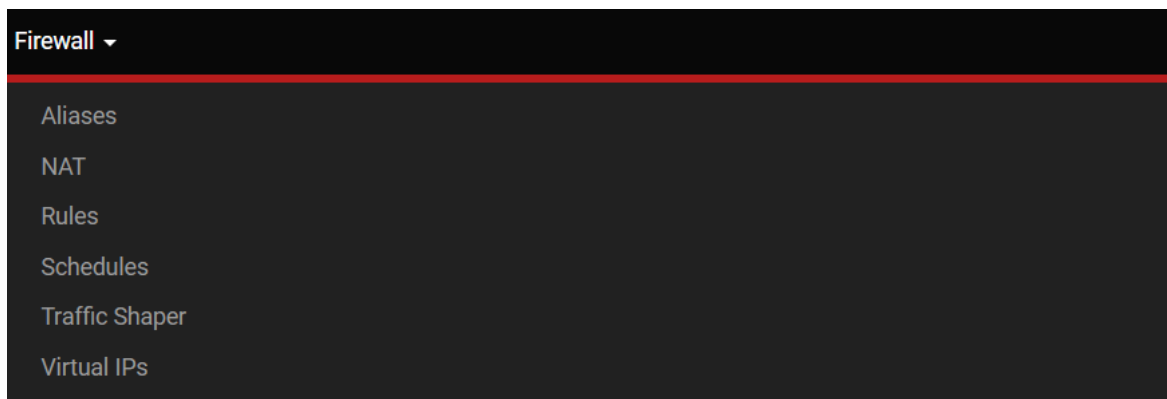
Nous remarquons ici la présence d'un WAN et d'un LAN avec chacun une adresse IP attribuée. Appuyer sur 8 pour accéder à l'interface de commande qui nous sera utile par la suite



Entrer l'adresse IP Em0 (WAN) dans le navigateur internet de votre choix. Il est normal de tomber sur cette page, sélectionner simplement « continuer sur *adresse_ip-em0* »



Une fois sur cette page ID : admin, Mot de passe : pfsense. Afin d'accéder à l'interface PfSense



Dans le menu dépliant sélectionner « Firewall » puis « Rules »

Firewall / Rules / WAN1

Floating WAN1 LAN1 WAN2 IPsec

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗ 0 /45 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙
✗ 0 /0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙

2 règles sont déjà ici prédéfinies, nous allons les supprimer. Pour ce faire, appuyer sur l'engrenage en fin de ligne de l'un ou de l'autre

Reserved Networks

Block private networks and loopback addresses ☐ 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 ☐ 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

Aller en bas de page et désélectionner ces 2 options. Puis appuyer sur « Save ».

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

Apply Changes

Appuyer ensuite sur « Apply Changes » pour littéralement appliquer les changements.

```
[2.6.0-RELEASE][root@pfSense.home.arpal/root: pfctl -d  
pf disabled
```

Cependant notre pare-feu va bloquer le rafraîchissement de notre page. Dans l'interface de notre VM taper la commande `pfctl -d` qui va désactiver le pare-feu pour nous permettre d'affecter nos changements.

The changes have been applied successfully.

En retournant sur notre navigateur nous avons ce message qui s'affiche nous confirmant notre opération



Juste en dessous de la liste des règles sélectionner l'un des boutons « Add »

Destination

Destination ☐ Invert match WAN address Destination Address /

Destination Port Range HTTP (80) 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 le champ « Destination », changer le type en « Wan adress » et le Port Range en « http ». Puis sur « Save »

Destination

Destination ☐ Invert match WAN address Destination Address /

Destination Port Range HTTPS (443) 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.






Réitérer l'opération pour le port « Htps » cette fois-ci afin de pouvoir complètement utiliser notre pare-feu sans avoir à le désactiver à chaque fois.

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

Apply Changes

Floating **WAN** LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPV4 TCP	*	*	WAN address	443 (HTTPS)	*	none			  
<input type="checkbox"/>	✓ 0/0 B	IPV4 TCP	*	*	WAN address	80 (HTTP)	*	none			  

```
[2.6.0-RELEASE][root@pfSense.home.arpa]/root: pfctl -d
pf disabled
```

The changes have been applied successfully.

Tout comme pour la suppression des règles principales après avoir fait la « Save », appuyer sur « Apply Changes » et taper dans l'interface de commande du pare-feu sur la VM la commande `pfctl -d` pour appliquer les changements. Une l'opération terminée le message de confirmation s'affichera.

Status / Dashboard

System Information

Name: pfSense.home.arpa

User: admin@192.168.199.1 (Local Database)

System: VMware Virtual Machine
Netgate Device ID: da27cc013a53124acad1

BIOS: Vendor: Phoenix Technologies LTD
Version: 6.00
Release Date: Thu Nov 12 2020

Version: 2.6.0-RELEASE (amd64)
built on Mon Jan 31 19:57:53 UTC 2022
FreeBSD 12.3-STABLE

The system is on the latest version.
Version information updated at Sun May 1 13:45:05 UTC 2022

CPU Type: Intel(R) Core(TM) i5-7300HQ CPU @ 2.50GHz
AES-NI CPU Crypto: Yes (inactive)
QAT Crypto: No

Hardware crypto

Kernel PTI: Enabled

MDS Mitigation: Inactive

Uptime: 01 Hour 33 Minutes 06 Seconds

Current date/time: Sun May 1 15:17:14 UTC 2022

DNS server(s):
• 127.0.0.1
• 192.168.199.2

Last config change: Sun May 1 14:21:03 UTC 2022

State table size: 0% (0/19000) Show states

Netgate Services And Support

Contract type: Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the [NETGATE RESOURCE LIBRARY](#).

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC support [here](#).

Interfaces

Interface	Speed	Duplex	IP Address
WAN	1000baseT	<full-duplex>	192.168.199.128
LAN	1000baseT	<full-duplex>	192.168.1.1

En appuyant sur le logo PfSense en haut a gauche, vous accédez au récapitulatif de votre pare-feu avec en bas à droite les règles d'interfaces que nous avons programmées.

```
The IPv4 LAN address has been set to 192.168.1.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
```

```
https://192.168.1.1/
```

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

```
VMware Virtual Machine - Netgate Device ID: da27cc013a53124acad1
```

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

```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.199.128/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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

```
Enter an option: 2
```

Une fois ces étapes passées, nous allons configurer notre adresse IP de notre LAN. Pour ce faire taper « 2 » dans l'interface de commande du pare-feu

```
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
```

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.10.10.6
```

```
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):
> 29
```

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

```
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:  
>
```

```
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
```

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

```
The IPv4 LAN address has been set to 10.10.10.6/29  
You can now access the webConfigurator by opening the following URL in your web  
browser:
```

```
https://10.10.10.6/
```

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

```
The IPv4 LAN address has been set to 10.10.10.6/29  
You can now access the webConfigurator by opening the following URL in your web  
browser:
```

```
https://10.10.10.6/
```

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

```
VMware Virtual Machine - Netgate Device ID: da27cc013a53124acad1
```

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

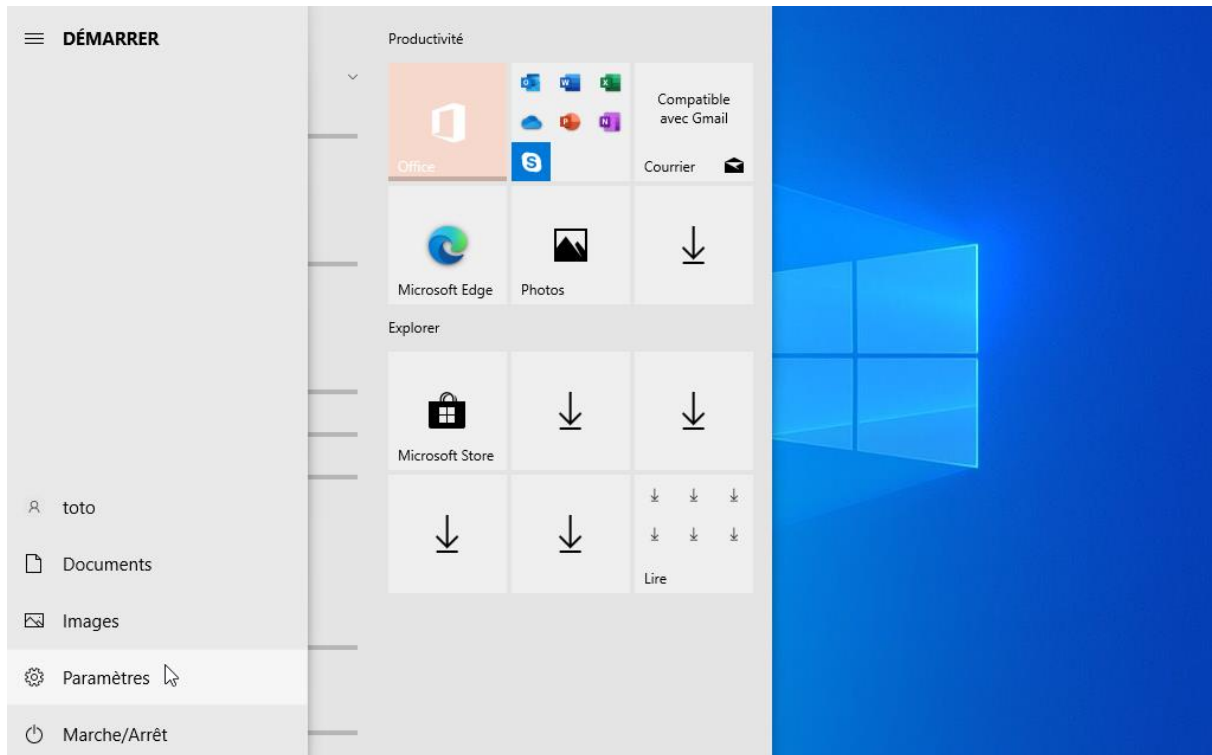
```
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.199.128/24  
LAN (lan)      -> em1      -> v4: 10.10.10.6/29
```

- | | |
|-----------------------------------|----------------------------------|
| 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 | |

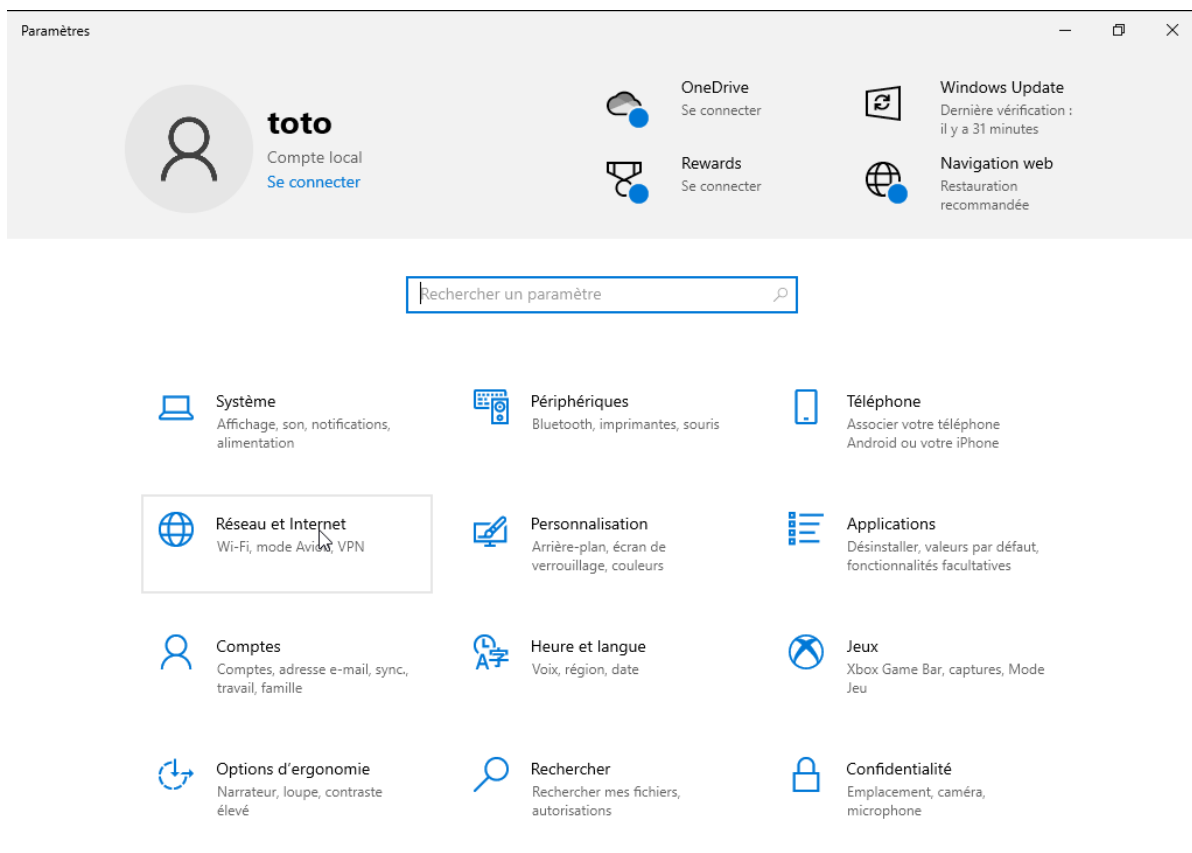
```
Enter an option: 
```

Configuration clients

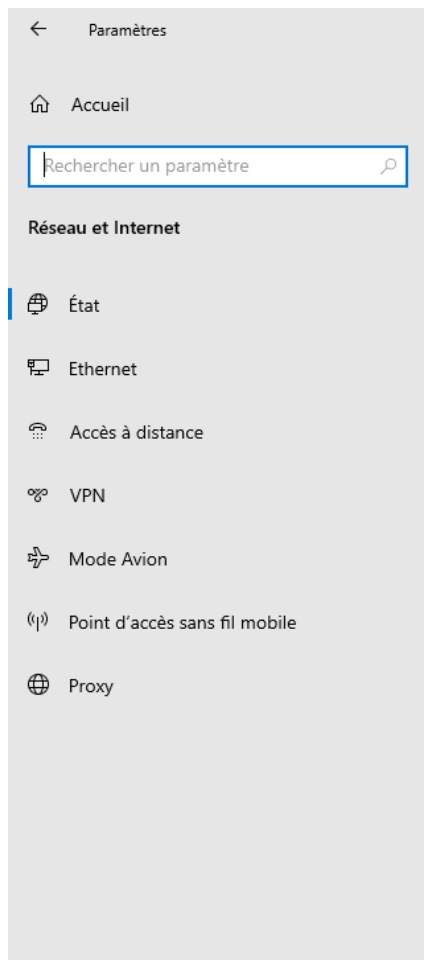
SOUS WINDOWS



Aller dans les paramètres

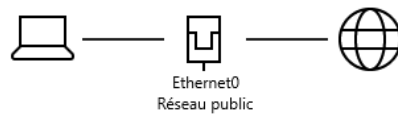


Sélectionner « réseau et Internet »



État

Statut du réseau




Vous êtes connecté à Internet

Si vous disposez d'un forfait de données limitées, vous pouvez configurer ce réseau en tant que connexion limitée ou modifier d'autres propriétés.


 Ethernet0 94 Mo
Depuis ces 30 derniers jours


Propriétés

Consommation des données

 Afficher les réseaux disponibles
Affichez les options de connexion qui vous entourent.

Paramètres réseau avancés

 Modifier les options d'adaptateur
Affichez les cartes réseau et modifiez les paramètres de connexion.

 Centre Réseau et partage
Décidez des contenus que vous souhaitez partager sur les réseaux auxquels vous vous connectez.

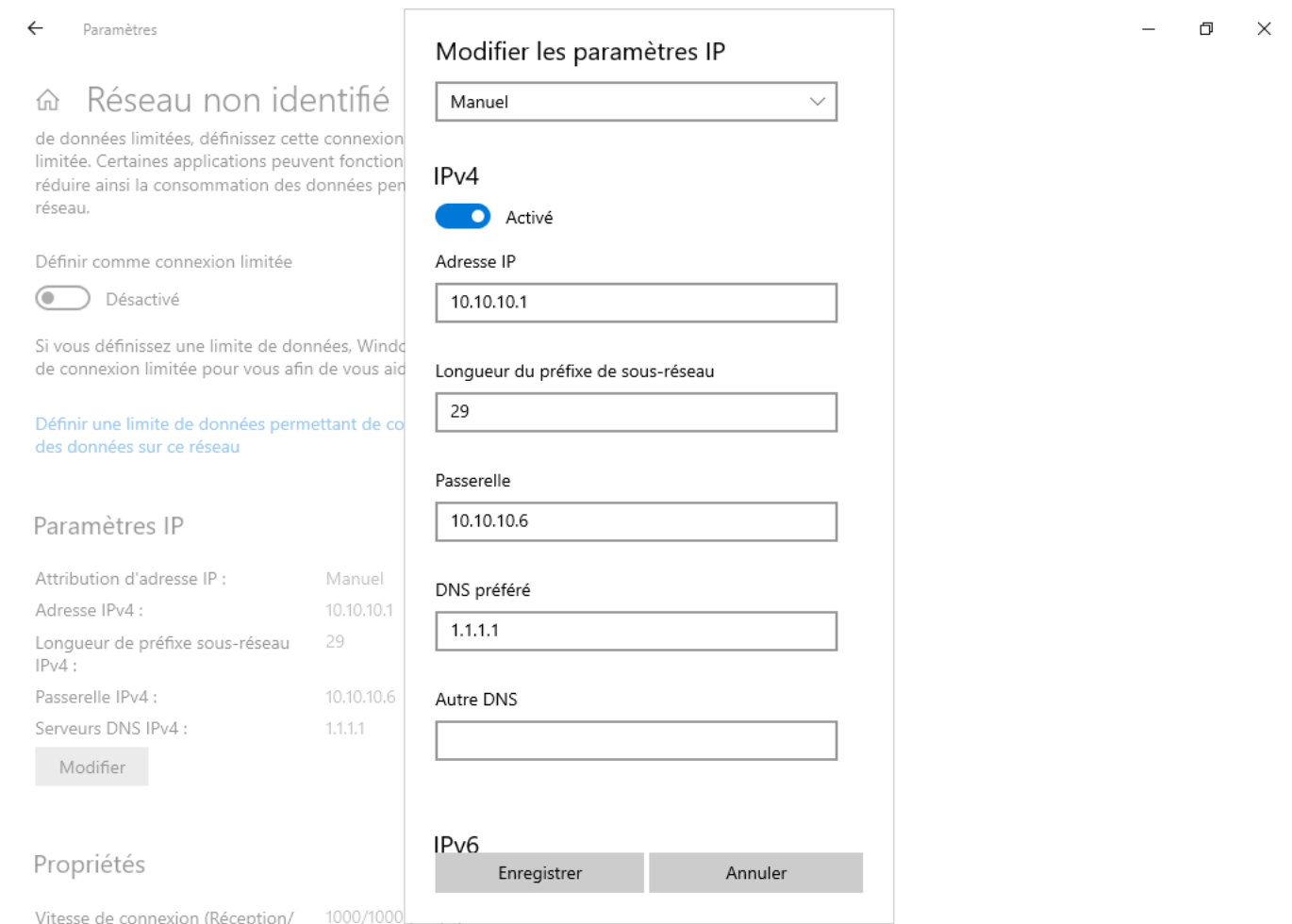
Puis aller dans « Propriétés »

Paramètres IP

Attribution d'adresse IP :	Manuel
Adresse IPv4 :	10.10.10.1
Longueur de préfixe sous-réseau IPv4 :	29
Passerelle IPv4 :	10.10.10.6
Serveurs DNS IPv4 :	1.1.1.1

Modifier

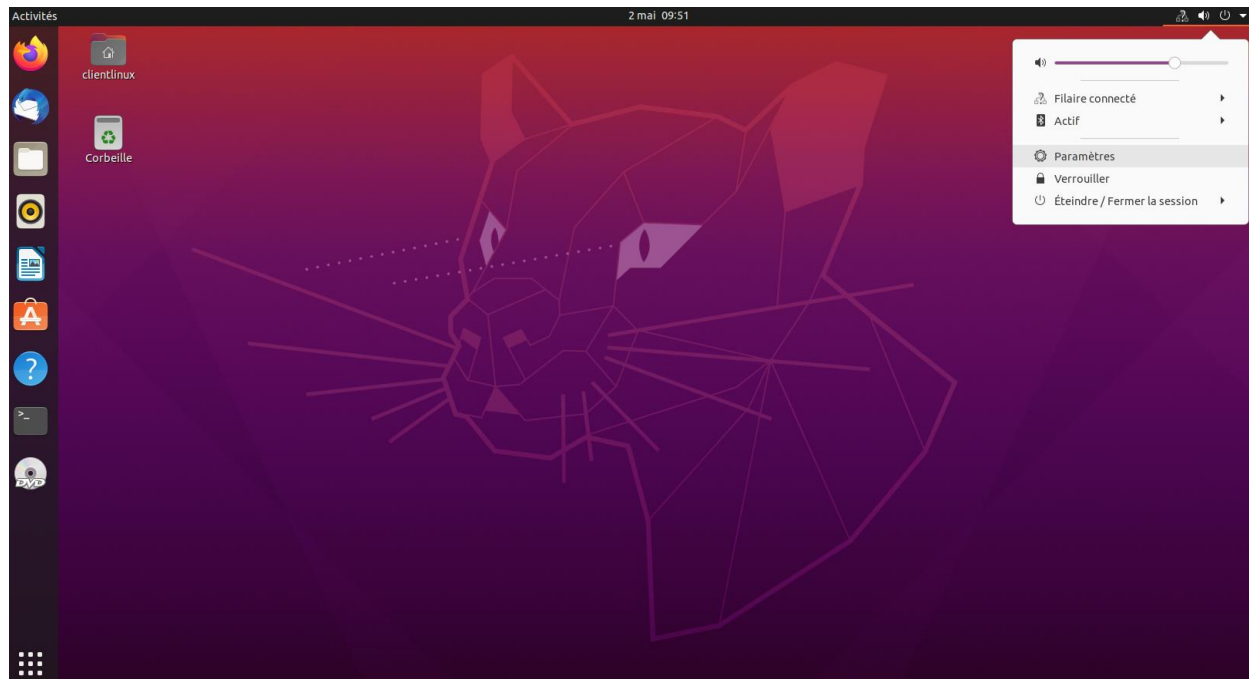
Ensuite sur « Modifier »



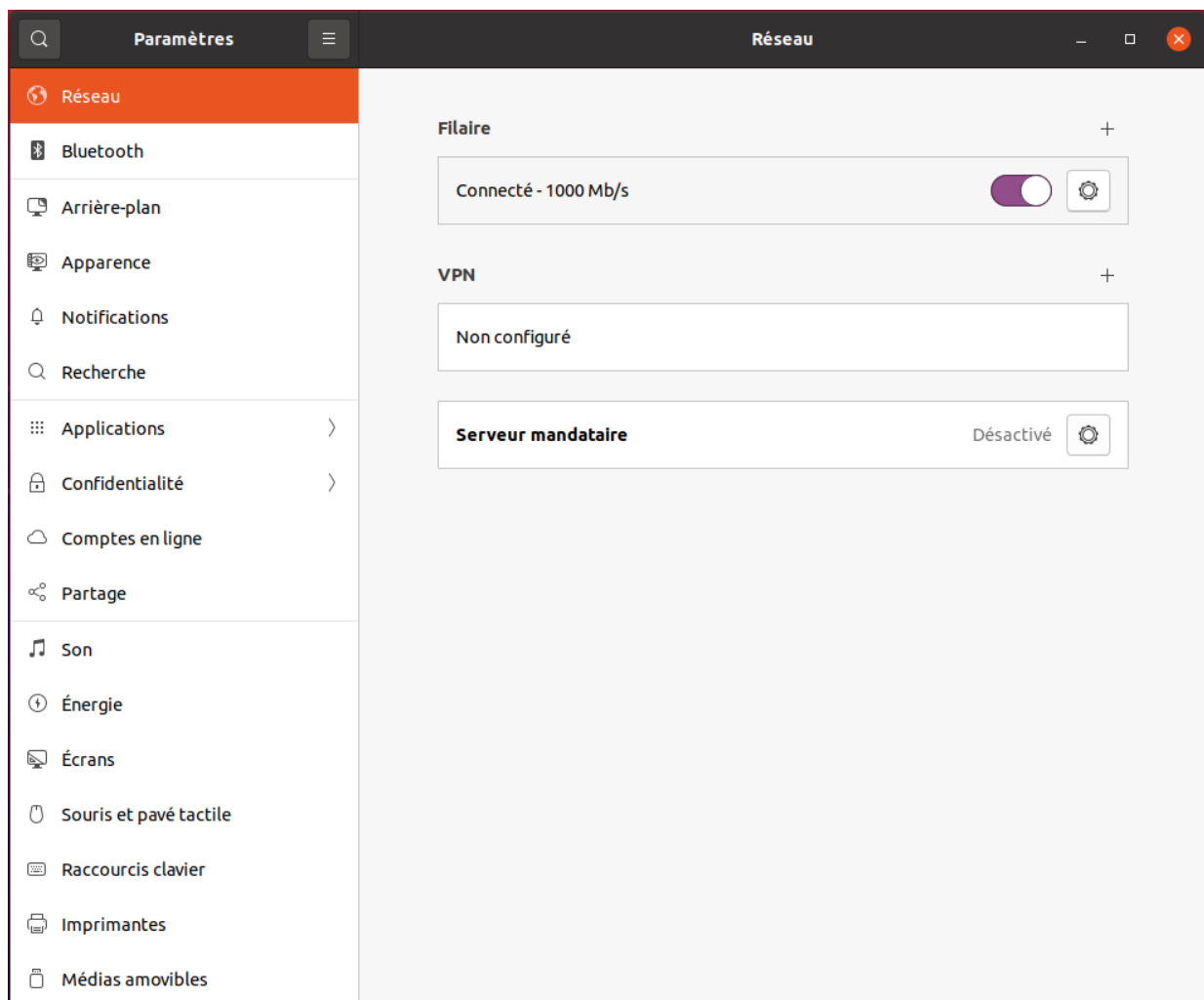
Basculer en mode « Manuel » si nécessaire et configurer l'adresse IP de votre Pc. La longueur du sous-réseau, de même que la passerelle correspondent à celles de votre pare-feu préalablement configuré. Le DNS quant à lui peut rester du « 1.1.1.1 » le choix ici n'est pas très important.

Une fois ces modifications effectuées, appuyer sur « Enregistrer ». Ça y est votre Client Windows est lié à votre pare-feu et à un accès internet fonctionnel grâce à ce dernier.

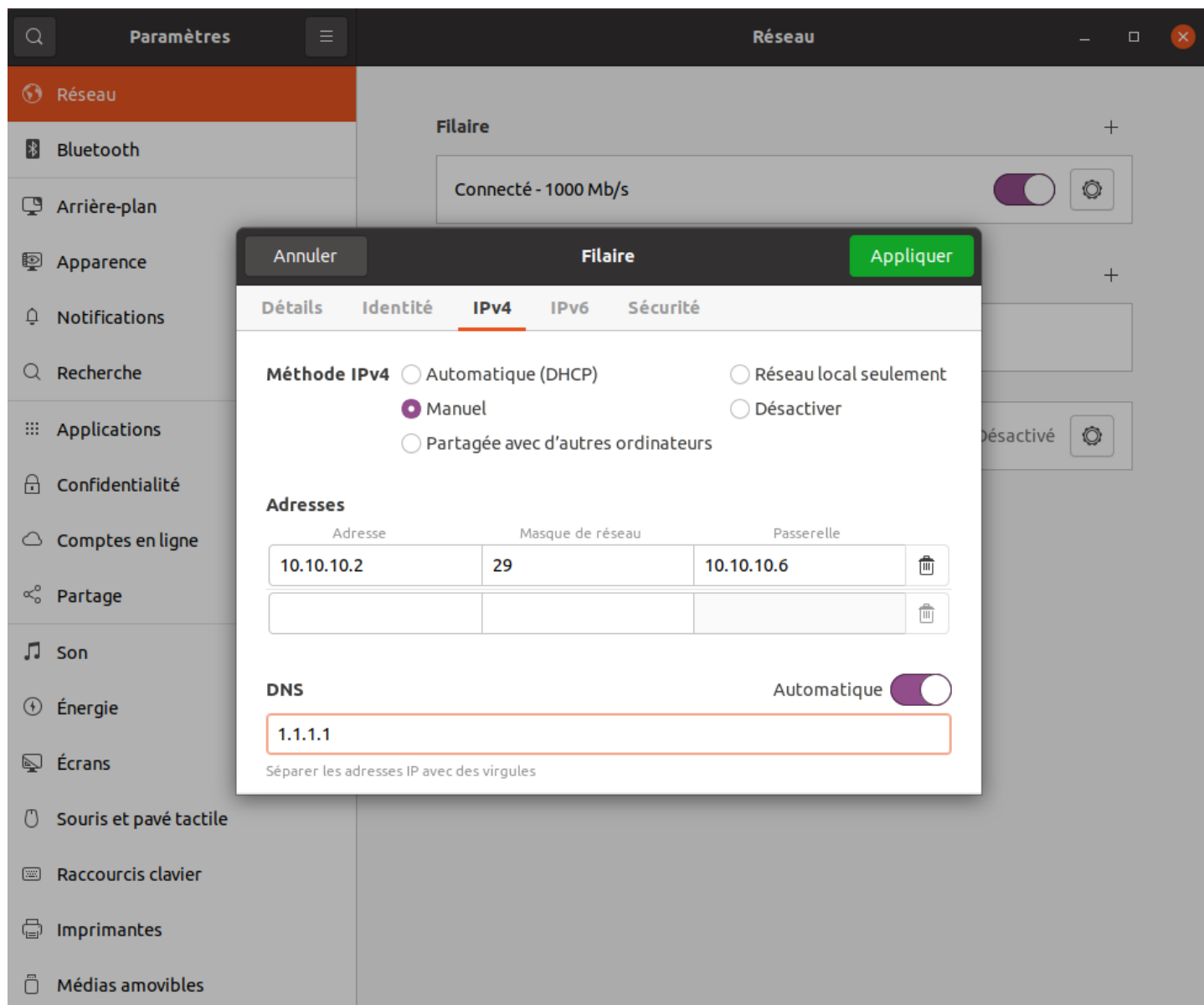
SOUS LINUX



En haut à droite sélectionner le menu démarrer, puis cliquer sur « Paramètres »



Appuyer sur l'engrenage de « Filaire » pour entrer dans le menu de configuration



Sélectionner ensuite « IPv4 », puis passer en mode « Manuel ». Il ne vous reste plus qu'à définir tout comme votre client Windows, votre adresse IP, ainsi que le masque de sous-réseau et la passerelle (correspondant ici aussi au pare-feu). Le DNS lui aussi peut rester 1.1.1.1