



DOCUMENTATION D'ARCHITECTURE

PROJET INFRA & SI

MISTRAL / PHAM / MARTHELY | Ynov 2021/2022

Sommaire

1. Définition du réseau

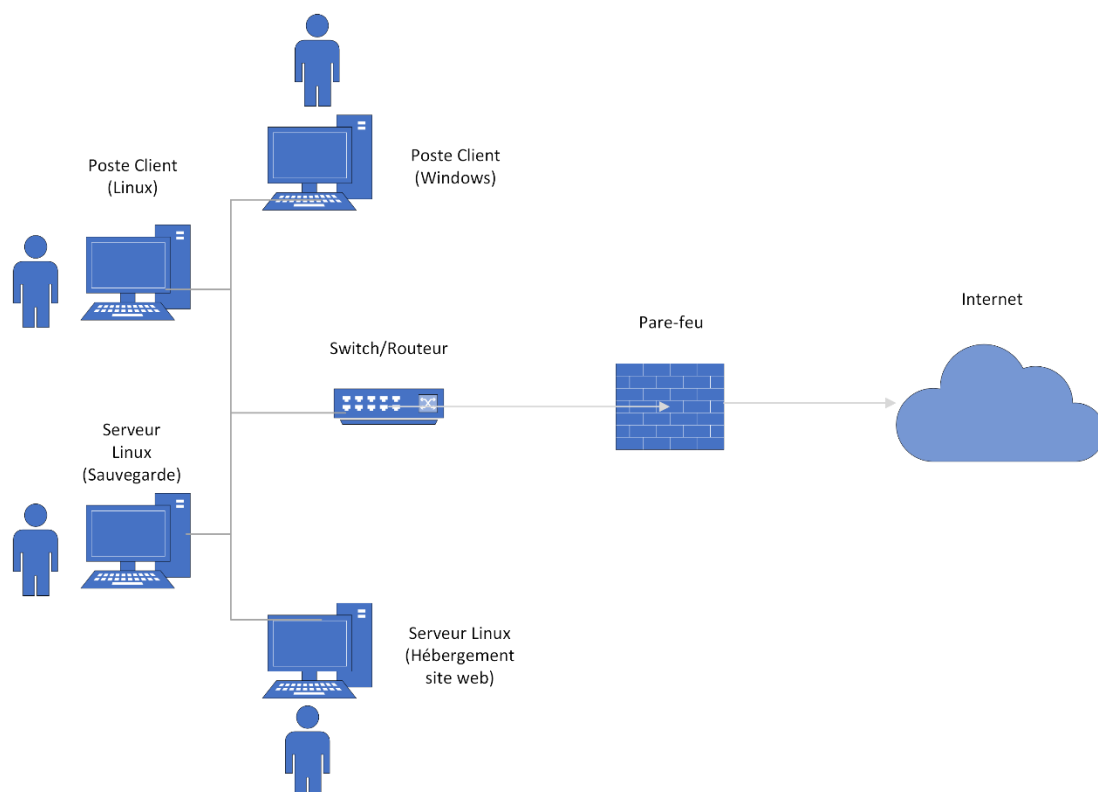
- Schéma Réseau
- Plan d'adressage

2. Mise en œuvre de la solution

- Configuration du Pare-Feu
- Configuration des Clients
- Configuration du Serveur
- Configuration du Service de Backup

1. Définition du réseau

SCHEMA RESEAU



Notre schéma réseau est composé de 2 clients (un sous Windows l'autre sous Linux), 2 serveurs (un d'hébergement et l'autre de sauvegarde), d'un switch et d'un pare-feu. L'ensemble de nos clients, et de nos serveurs sont en LAN sur le même réseau. Ils sont ainsi connectés sur le même switch. Ce-dernier sera également connecté à un pare-feu. La passerelle est alors effectuée par le pare-feu, permettant la connexion internet.

PLAN D'ADRESSAGE

Service	Adresse Réseau	Masque	Passerelle
Client 1	10.10.10.1	255.255.255.248	10.10.10.6
Client 2	10.10.10.2	255.255.255.248	10.10.10.6
Serveur Web	10.10.10.3	255.255.255.248	10.10.10.6
Serveur Backup	10.10.10.4	255.255.255.248	10.10.10.6
Libre	Libre	Libre	Libre
Pare-feu	10.10.10.6	255.255.255.248	10.10.10.6

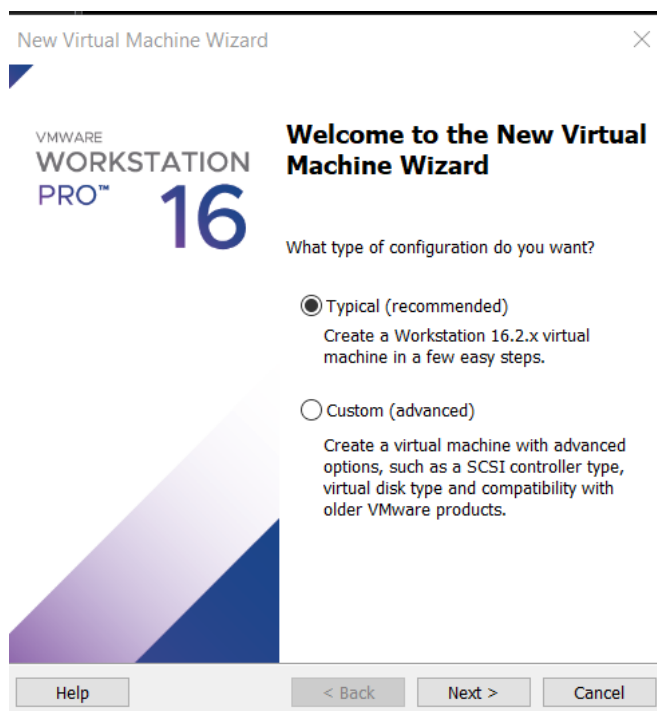
Nous avons choisi un masque de sous-réseau de 255.255.255.248, car cela permet de connecter un maximum de 6 appareils. Limiter ainsi le nombre permet de ne pas gaspiller des adresses IP ainsi que la bande passante et en même temps d'avoir une place libre si besoin de rajout d'un autre appareil.

Etant limité à 6, nos adresses réseau ne dépasseront pas 10.10.10.6, attribuée ici à notre pare-feu qui fera office de passerelle. Ce qui explique que chaque élément a pour passerelle 10.10.10.6.

2. Mise en œuvre de la solution

– Configuration du 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 (car limitation du projet à du virtuel).



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

New Virtual Machine Wizard ×

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

☐ Installer disc:

No drives available

☒ Installer disc image file (iso):

C:\Users\davym\Downloads\Utilitaire\pfsense\pfSens Browse...

FreeBSD version 10 and earlier 64-bit detected.

☐ I will install the operating system later.

The virtual machine will be created with a blank hard disk.

Help < Back Next > Cancel

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:

FreeBSD version 10 and earlier 64-bit (2)

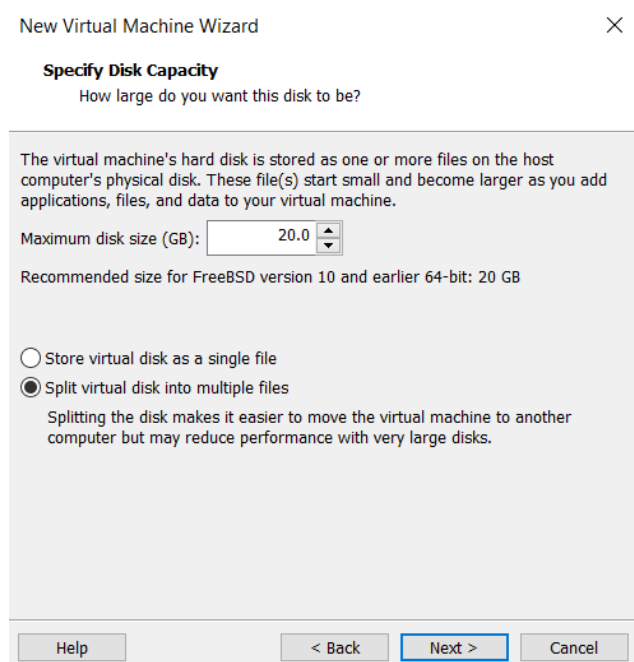
Location:

C:\Users\davym\OneDrive\ドキュメント\Virtual Machines\FreeB Browse...

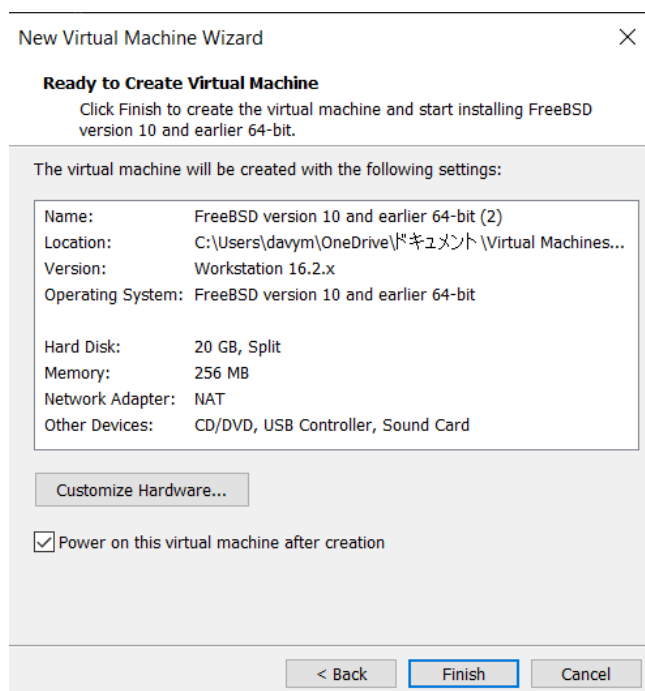
The default location can be changed at Edit > Preferences.

< Back Next > Cancel

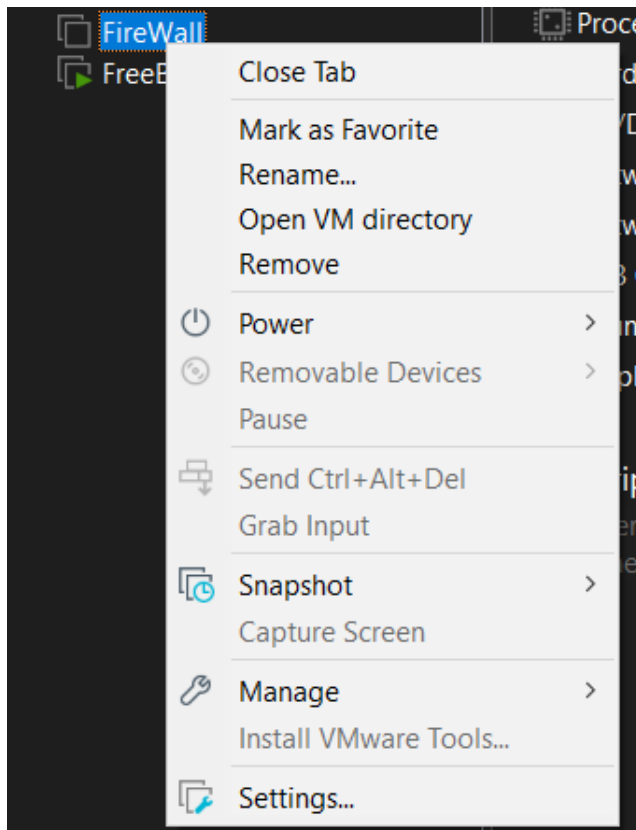
Ici il est possible de renommer directement le nom de la VM ainsi que son emplacement. L'emplacement n'est pas nécessaire à la modification cependant.



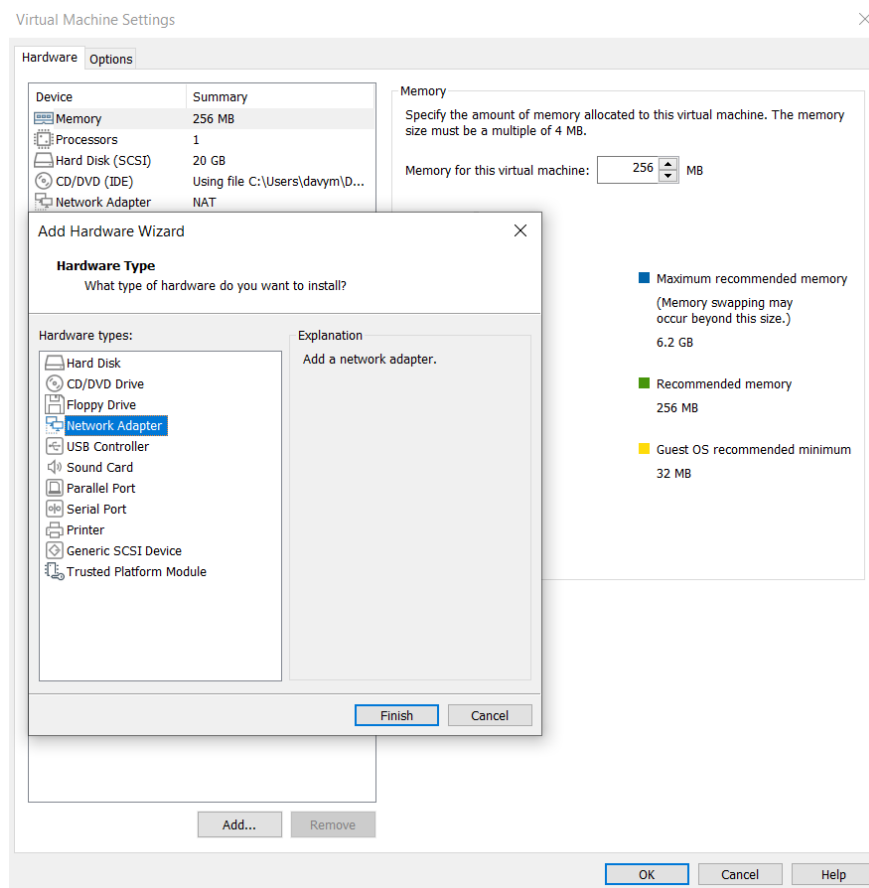
Vient ensuite la possibilité d'allocation de l'espace disque, ici nous mettons 20GB de façon à être large mais le pare-feu ne demande pas autant d'espace. Sélectionner l'option de séparation du disque virtuel en plusieurs fichiers.



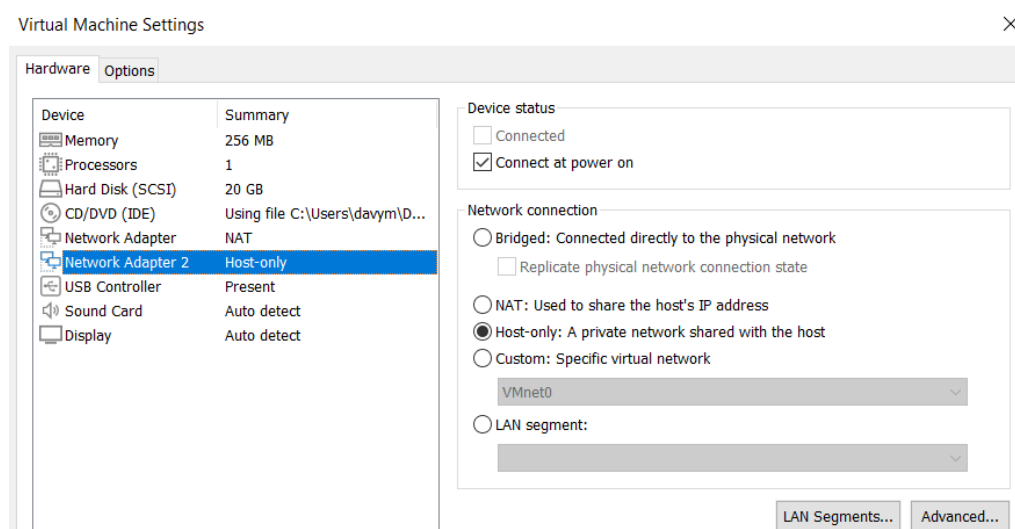
Ici vient le récap de la création de notre VM. Pour finir le processus appuyer tout simplement sur « Finish » si tous les éléments vous conviennent



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 ».

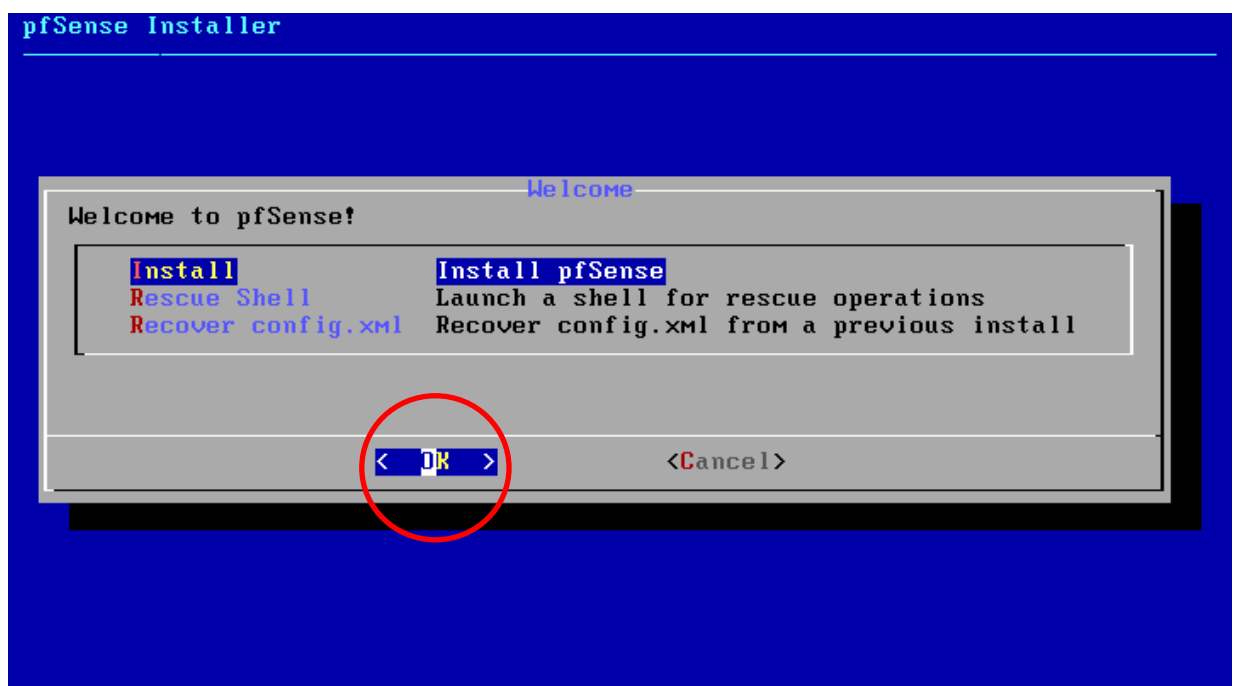
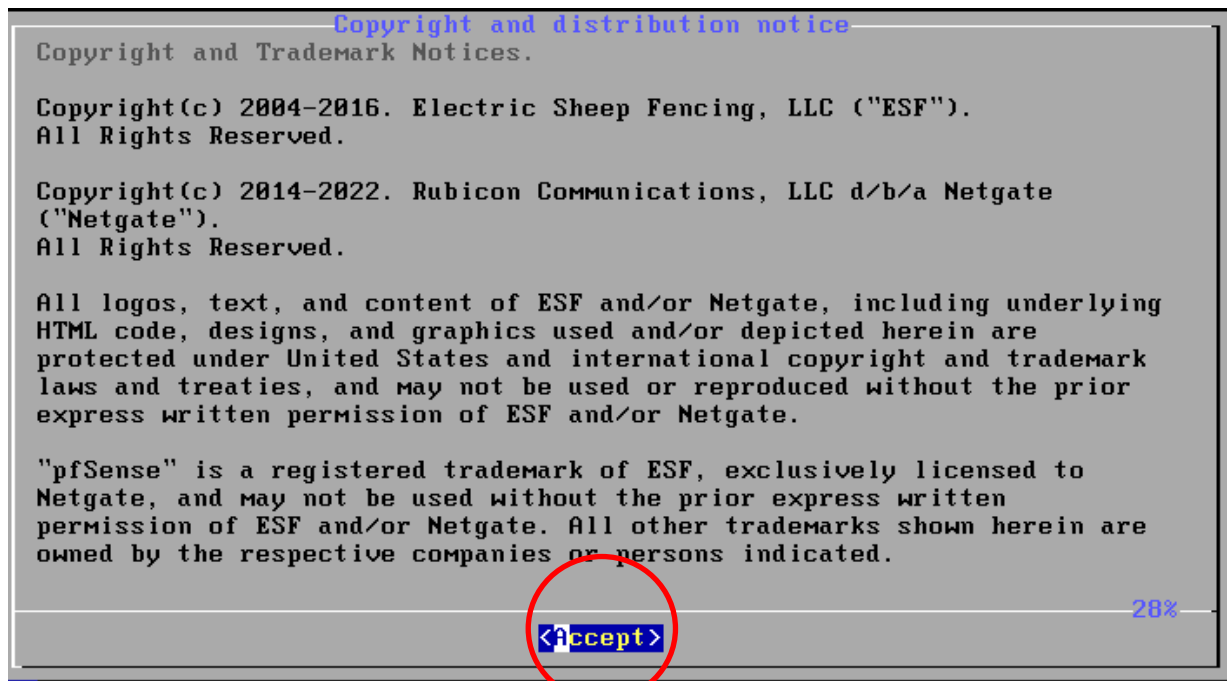


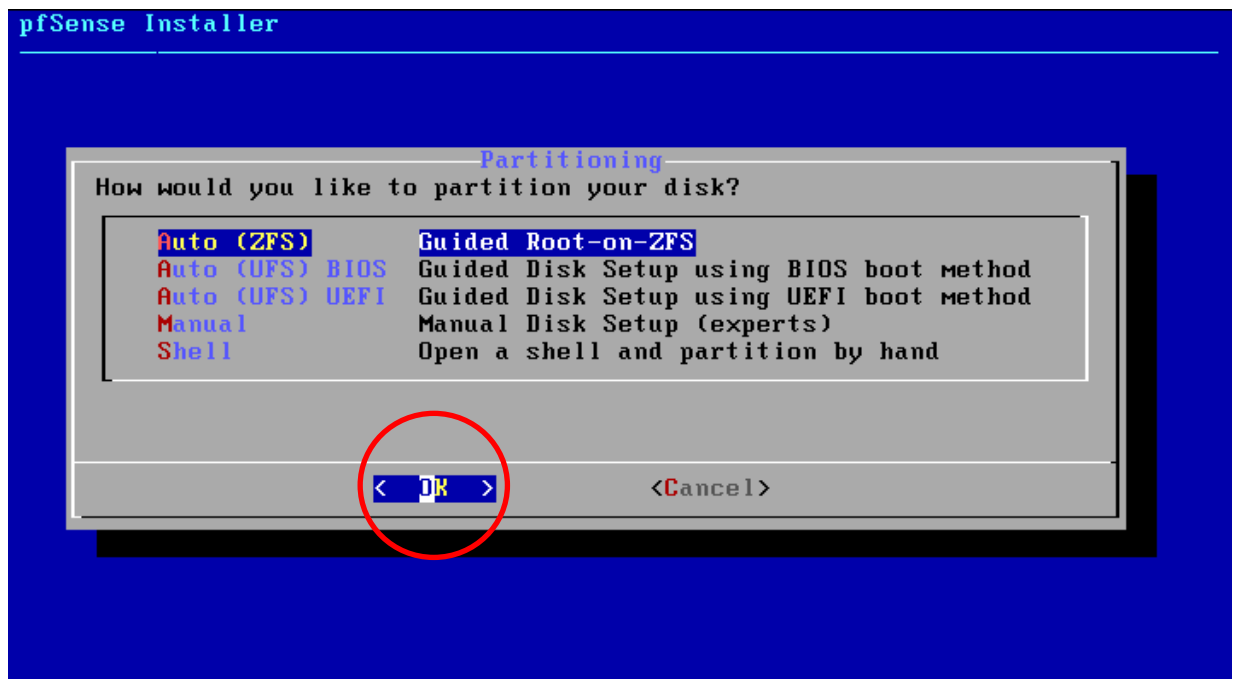
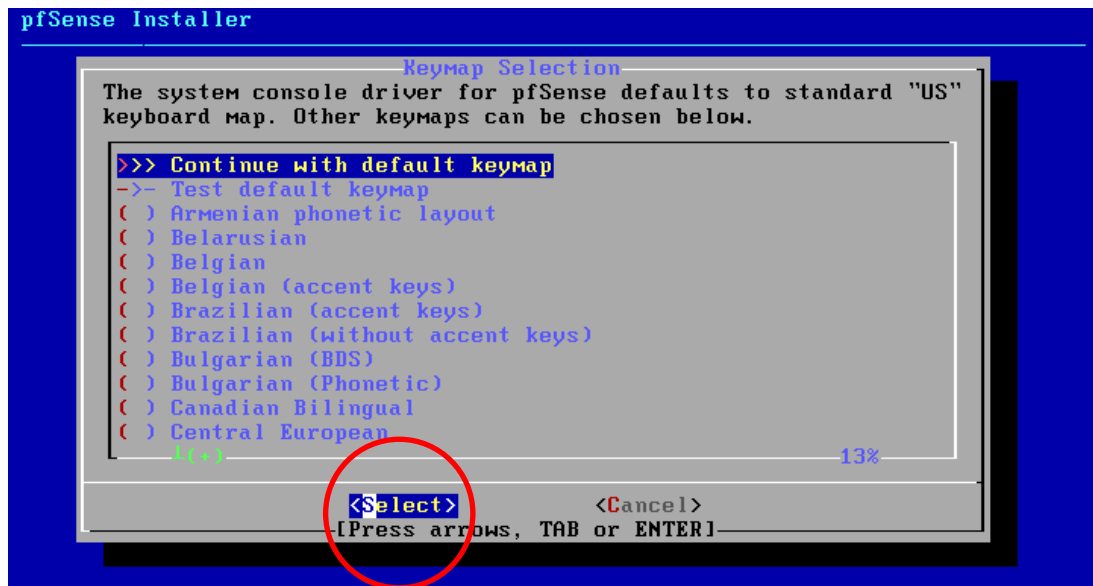
Appuyer sur « Add », ensuite sélectionner « Network Adpatater ».

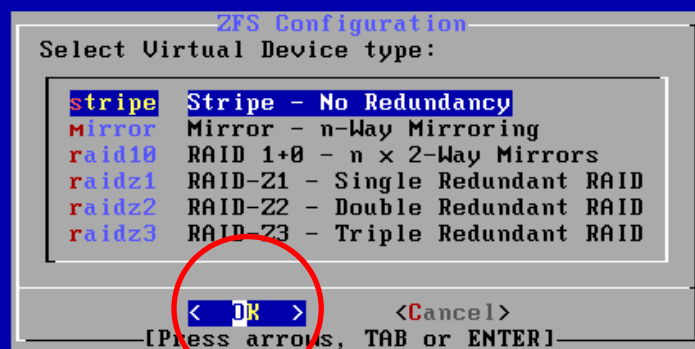
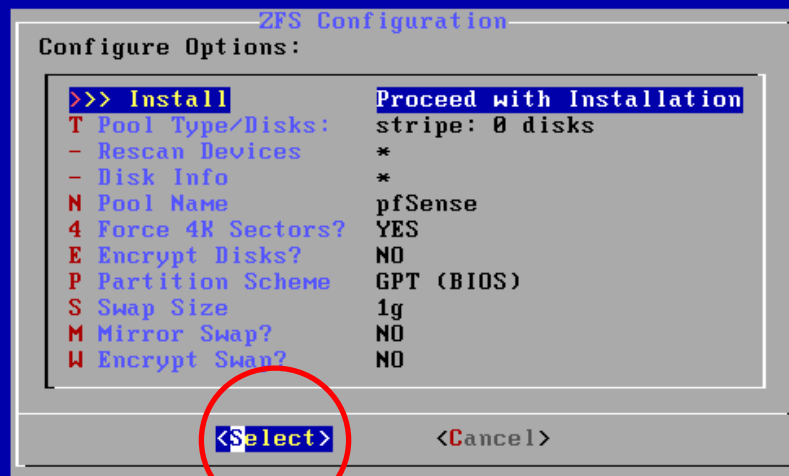


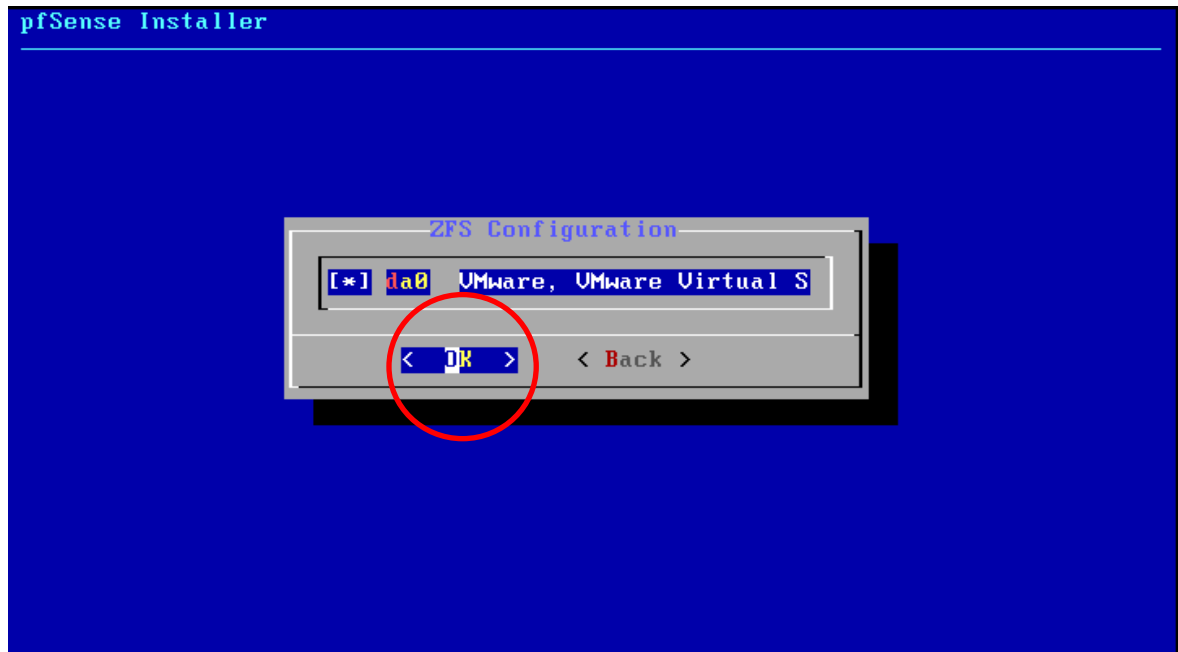
Une fois ce nouvel adaptateur ajouté, mettre celui-ci en « host-only ». Il ne reste plus qu'à lancer maintenant le pare-feu.

Ci-joint une série de captures des étapes à suivre

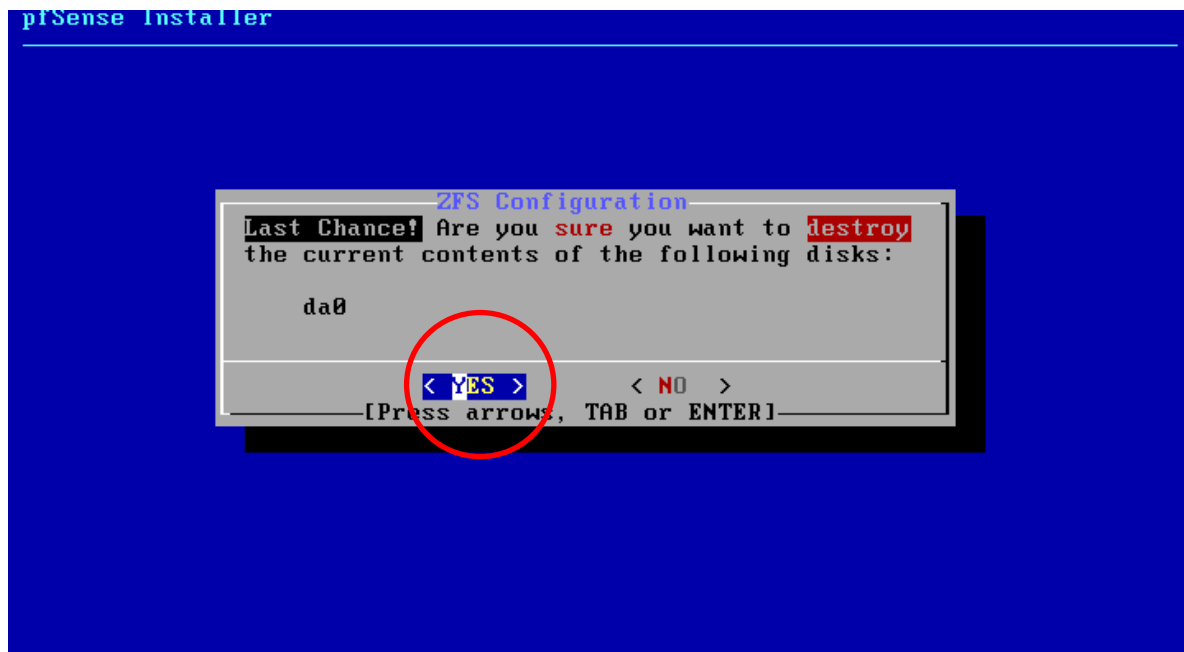


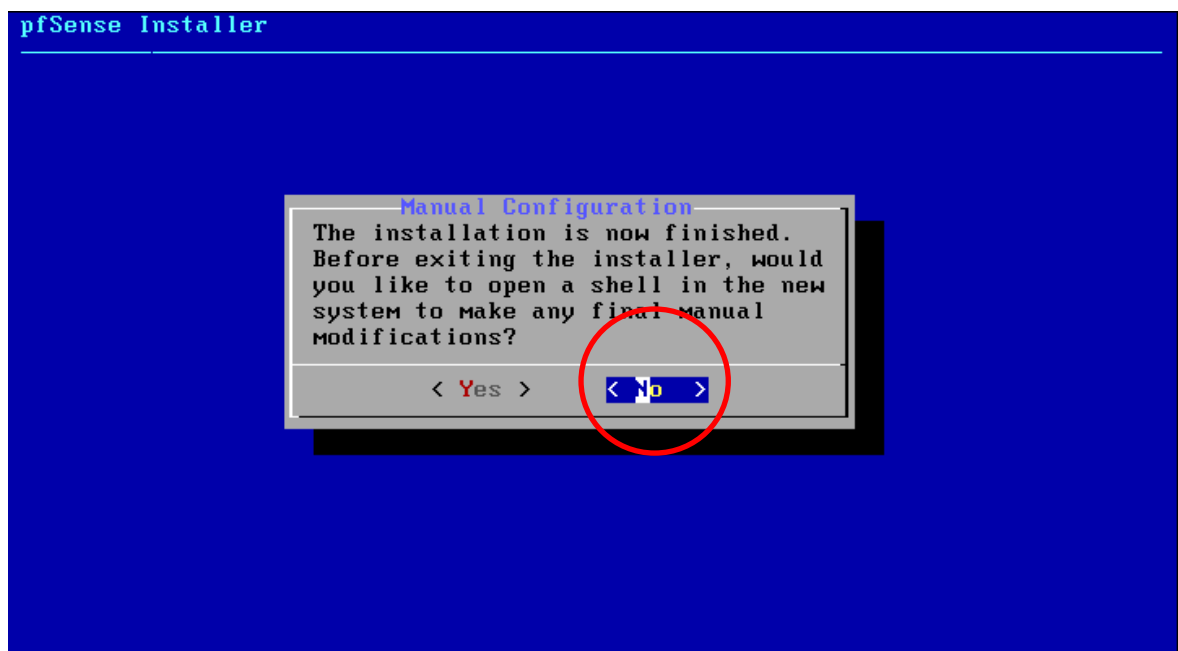
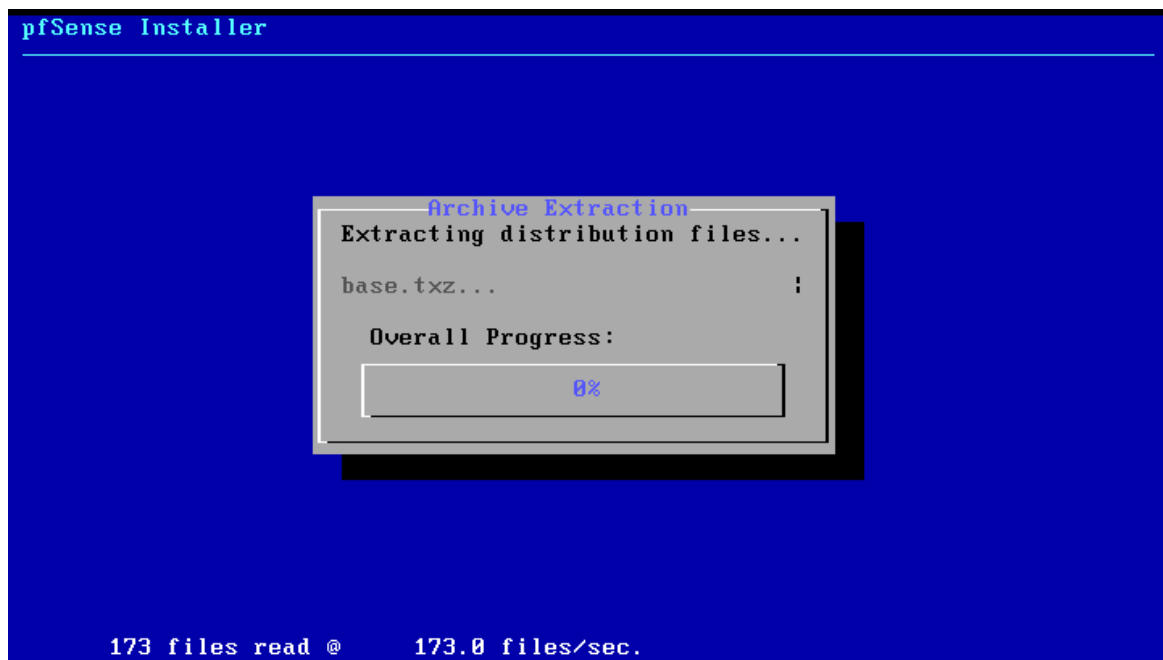


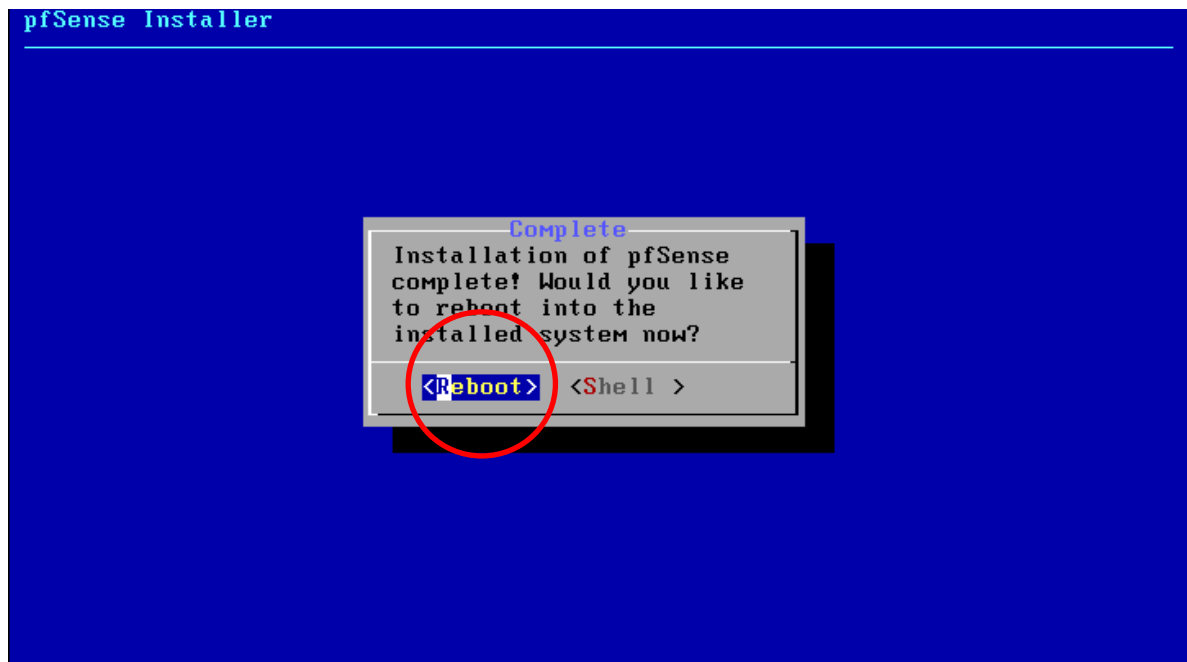




Ici appuyer sur la touche espace pour que l'étoile apparaisse signifiant ainsi « all »







```
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VMware Virtual Machine - Netgate Device ID: da27cc013a53124acad1

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

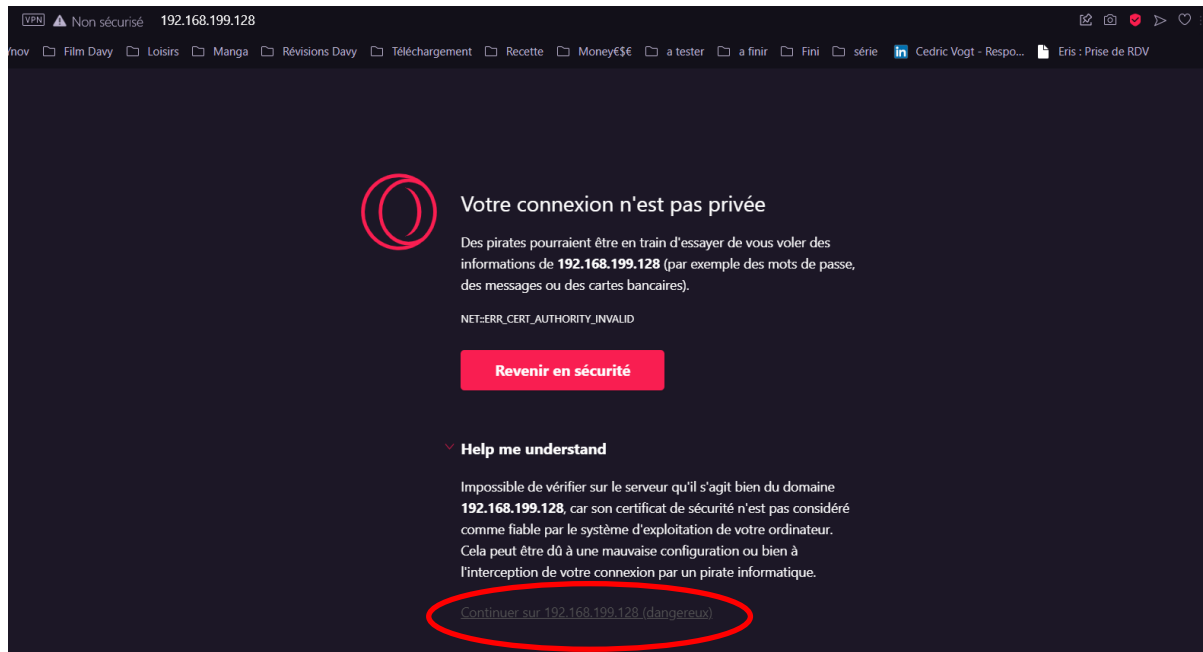
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.199.128/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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

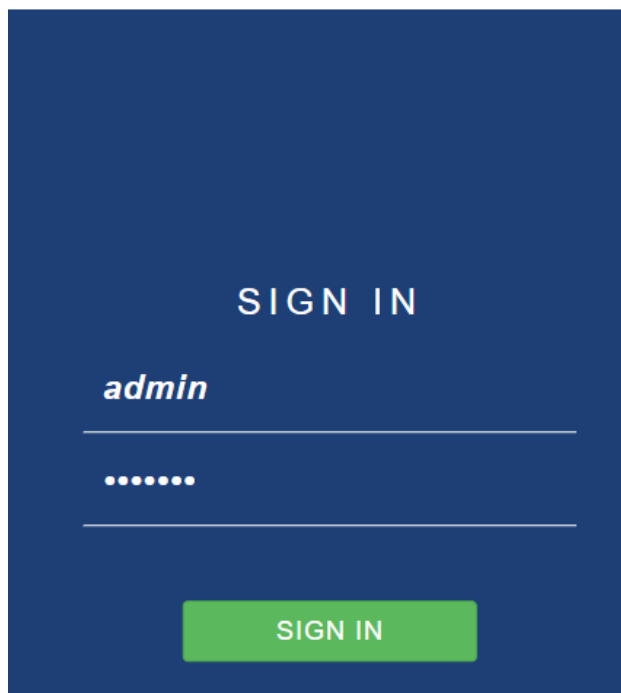
Enter an option: 8

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

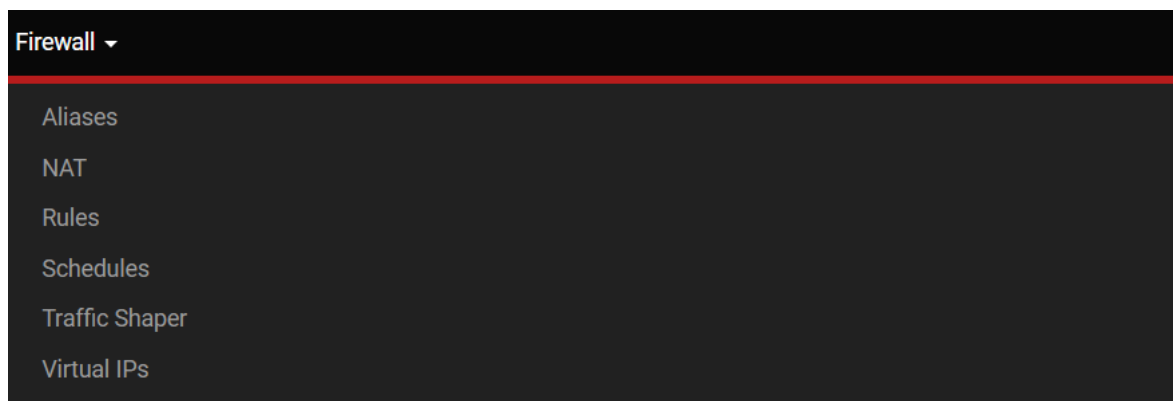
Nous remarquons ici la présence d'un WAN et d'un LAN avec chacun une adresse IP attitrée. Appuyer sur 8 pour accéder à l'interface de commande qui nous sera utile par la sui



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



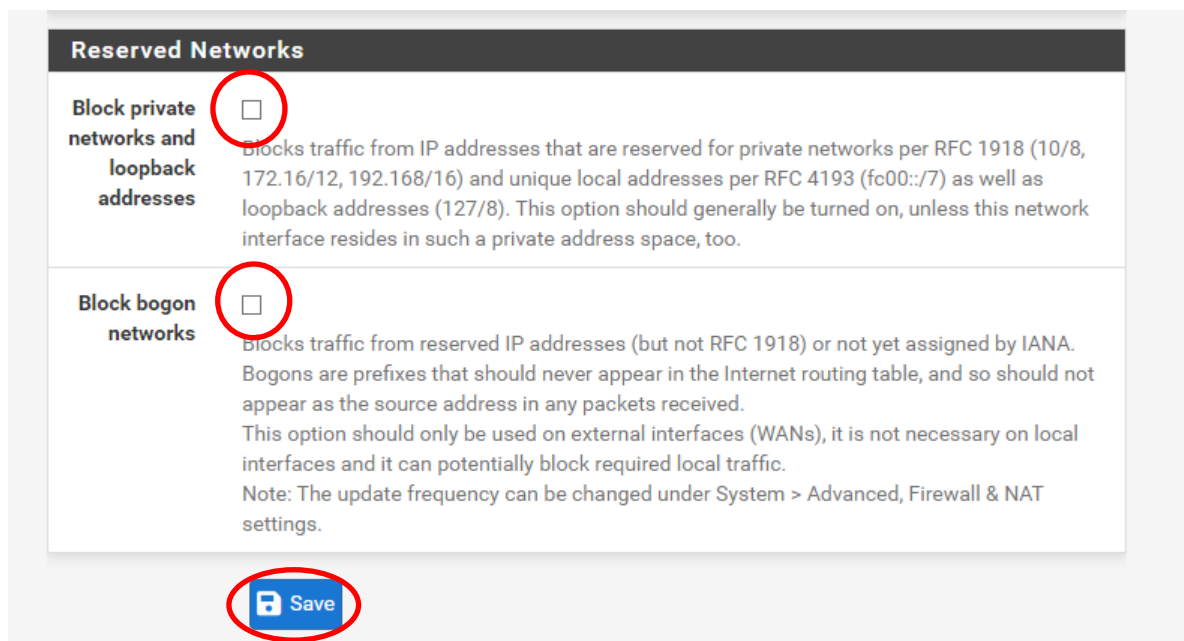
Une fois sur cette page ID : admin, Mot de passe : pfsense. Afin d'accéder à l'interface PfSense



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



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				
<u>Destination</u>	<input type="checkbox"/> Invert match	WAN address		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 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 (

Custom

From

Custom

HTTPS (

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 « Https » 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.

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	*	*	10.10.10.3	*	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	WAN address	80 (HTTP)	*	none			
<input type="checkbox"/>	✓ 2/1.40 MB	IPv4 TCP	*	*	WAN address	443 (HTTPS)	*	none			

Afin de permettre un accès externe, on établit une règle autorisant les protocoles TCP vers l'adresse IP du serveur (pour nous 10.10.10.3).

Status / Dashboard

System Information

Name	pfSense.home.arpa
User	admin@192.168.199.1 (Local Database)
System	VMware Virtual Machine Netgate Device ID: da27cc013a53124cad1
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

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:
>
```

Après avoir rentré la nouvelle adresse IP, et le sous-réseau. Taper « Entrer » pour passer la configuration IPv4 du WAN

```
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
```

Pas besoin non plus de configuration de l'IPv6, taper « Entrer » pour passer. Nul besoin de « webConfigurator protocol » également.

```
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.
```

Patienter le temps de finition de la configuration, taper « Entrer » ensuite

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: █

Ca y est, votre LAN est configurée !

Tableau de filtrage :

Règles LAN :

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	6/274.03 MiB	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	

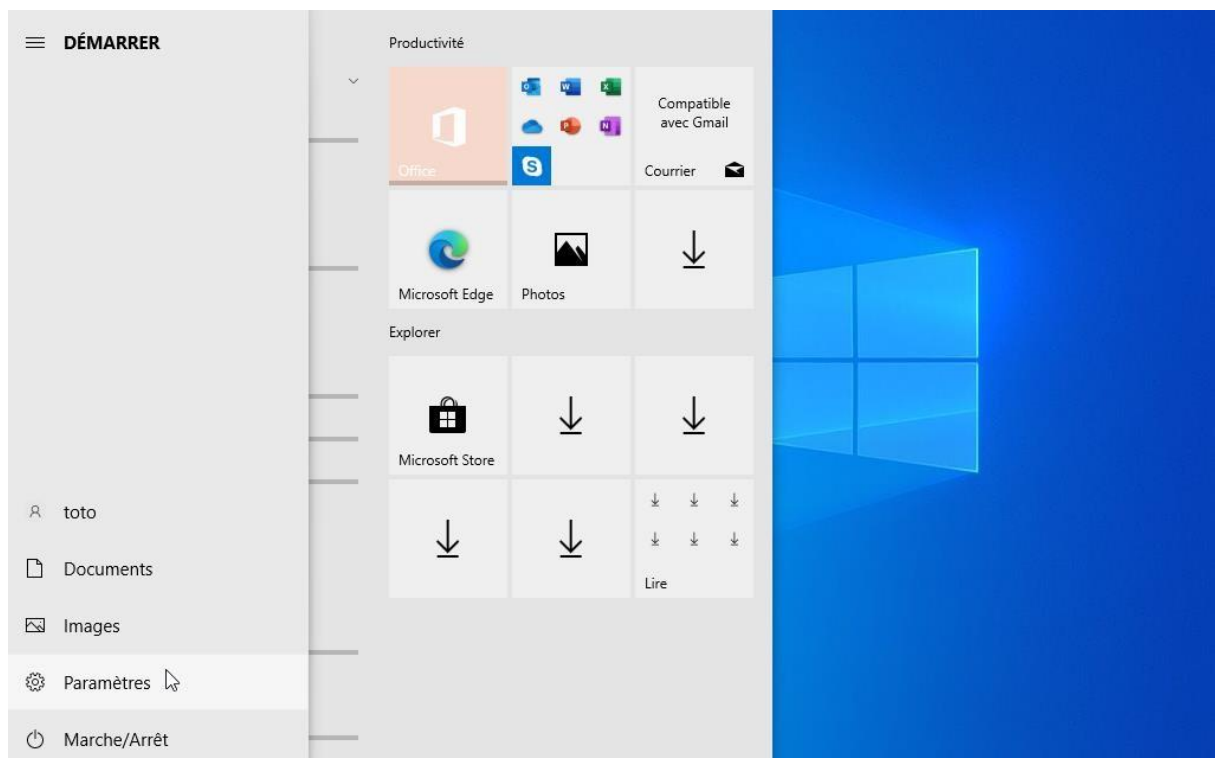
Règles WAN :

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	*	*	10.10.10.3	*	*	none			
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	WAN address	80 (HTTP)	*	none			
<input type="checkbox"/>	2/1.40 MiB	IPv4 TCP	*	*	WAN address	443 (HTTPS)	*	none			

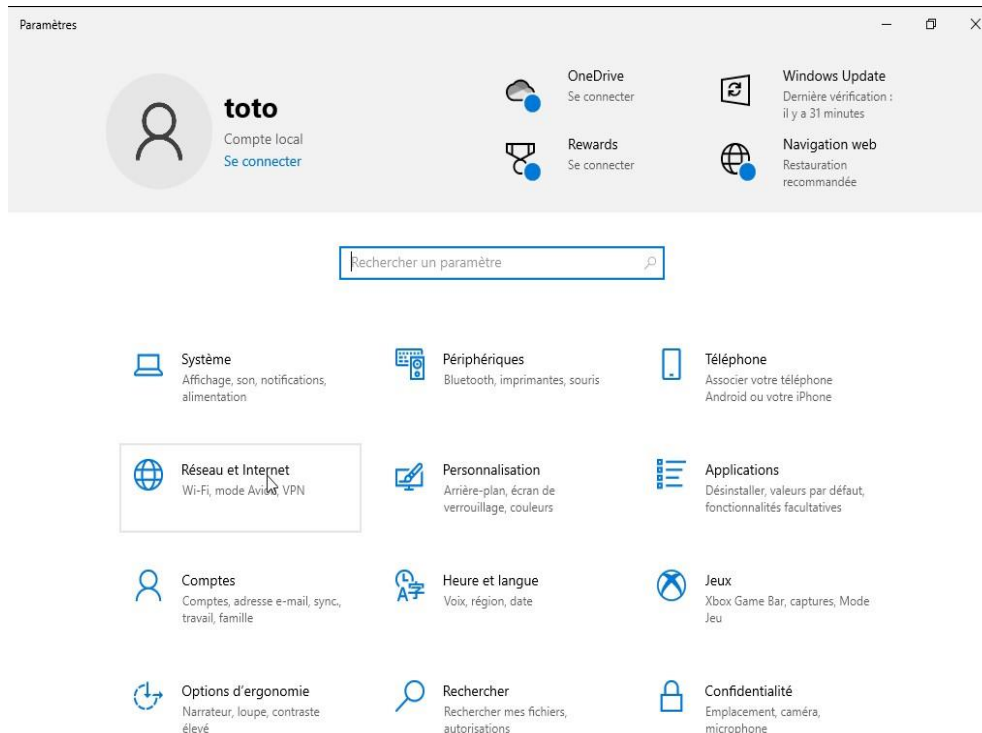
- Configuration des Clients

Dans cette partie, nous allons traiter de la configuration nécessaire aux machines clientes de notre sous-réseau.

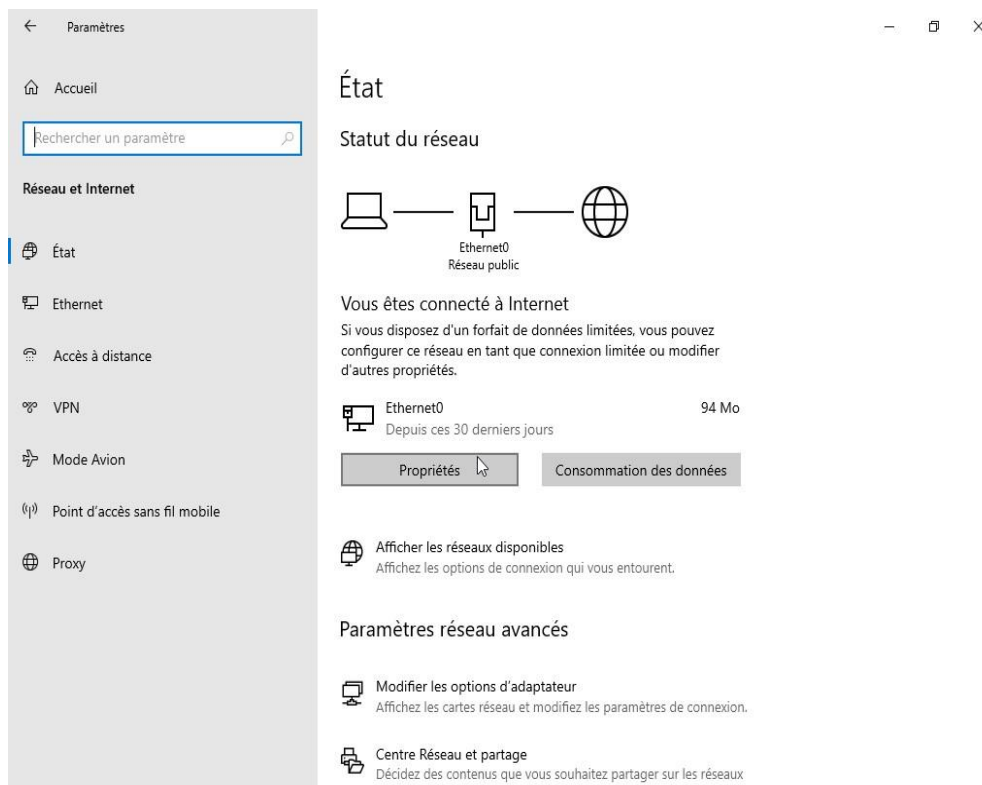
SOUS WINDOWS



Aller dans les paramètres



Sélectionner « réseau et Internet »



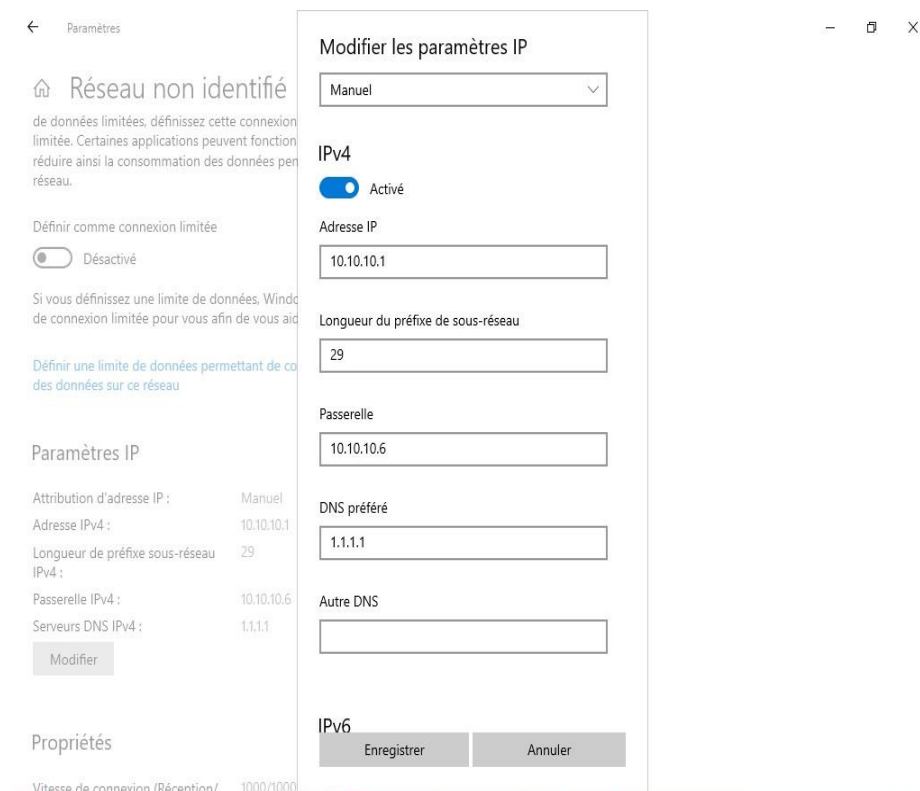
Puis aller dans « Propriétés »

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 »

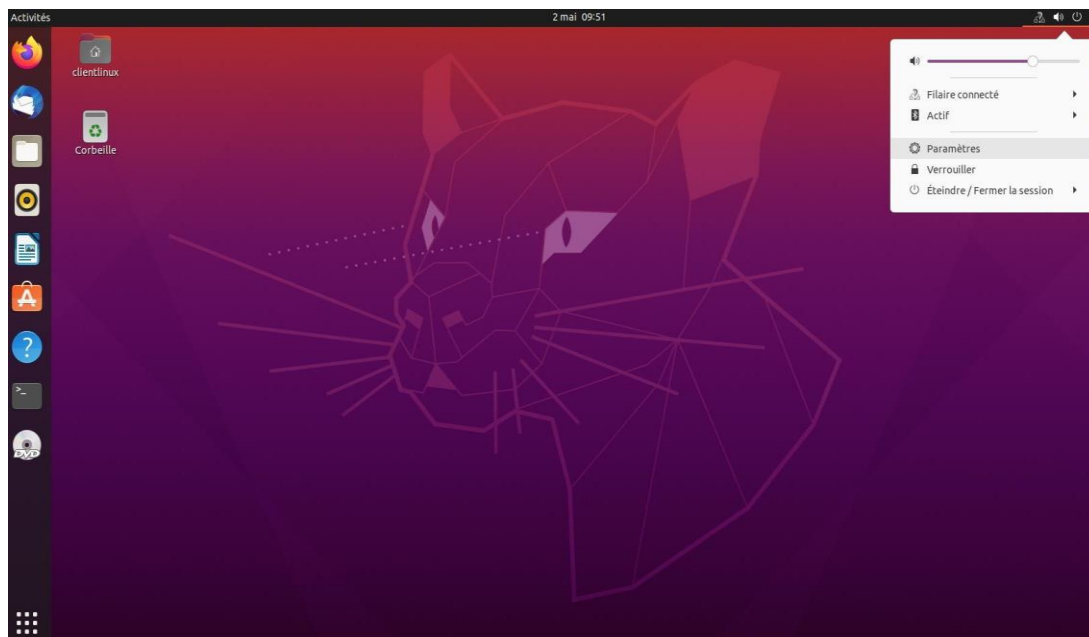


Basculer en mode « Manuel » si nécessaire et configurer l'adresse IP de votre Pc. La longueur du sous-réseau, de même que la passerelle correspondent à celles de votre pare-feu préalablement

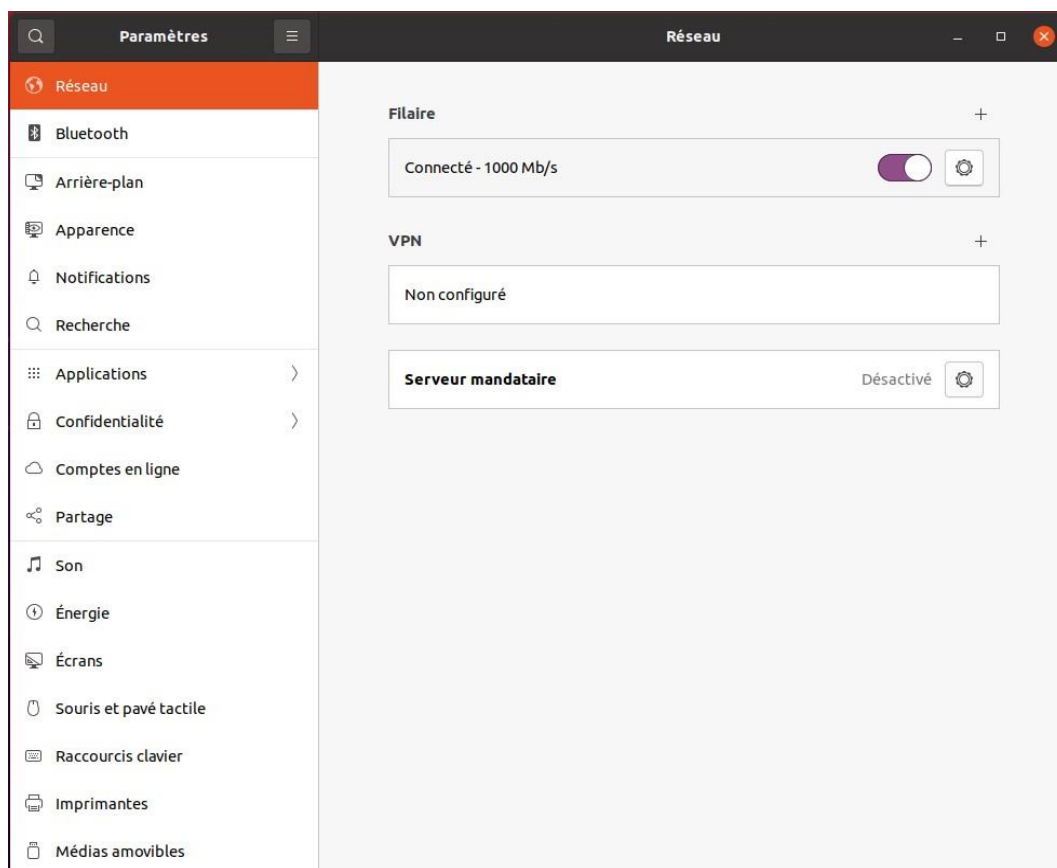
configuré. Le DNS quant à lui peu rester du « 1.1.1.1 » le choix ici n'est pas très important.

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

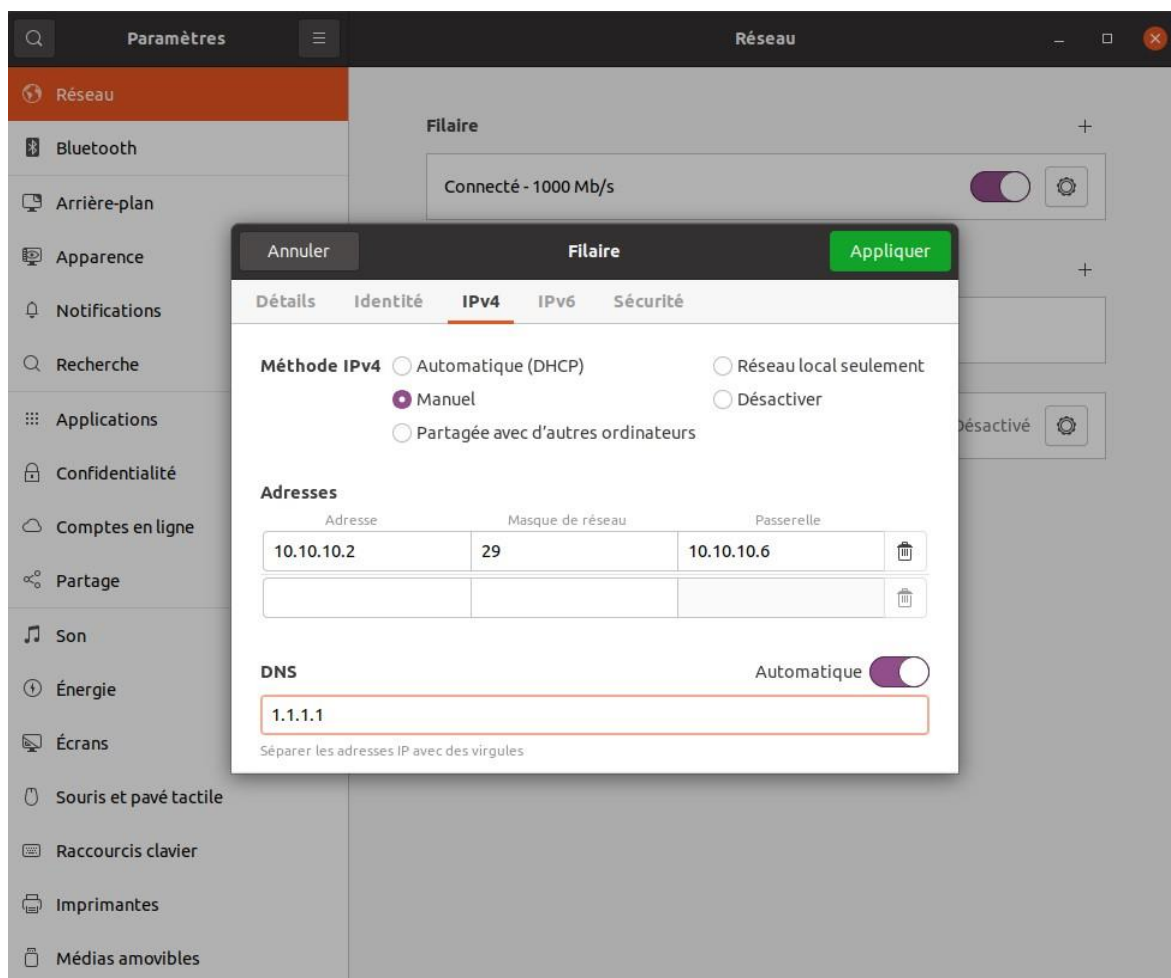
SOUS LINUX



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

– Configuration du Serveur

Dans cette partie, nous allons traiter de l'installation de notre serveur web.

Tout d'abord, il faudra configurer l'IP de votre machine en lui attribuant l'IP de votre choix comme montré précédemment.

Ensuite, dans le terminal de commande de votre machine, tapez la commande « `sudo apt install nginx` ». Ceci va installer l'outil Nginx, qui nous permettra de configurer et d'héberger notre serveur.

Après cela nous allons faire « `sudo nano /etc/nginx/sites-enabled/` », ce qui va ouvrir un éditeur de texte sur le fichier de configuration de notre page Nginx.

```
server {
    listen 80 default_server;
    listen [::]:80 default_server;

    # SSL configuration
    #
    # listen 443 ssl default_server;
    # listen [::]:443 ssl default_server;
    #
    # Note: You should disable gzip for SSL traffic.
    # See: https://bugs.debian.org/773332
    #
    # Read up on ssl_ciphers to ensure a secure configuration.
    # See: https://bugs.debian.org/765782
    #
    # Self signed certs generated by the ssl-cert package
    # Don't use them in a production server!
    #
    # include snippets/snakeoil.conf;

    root /home/hebergementlinux/Documents/ServerFiles/Web;

    # Add index.php to the list if you are using PHP
    index index.html index.htm index.nginx-debian.html;

    server_name _;

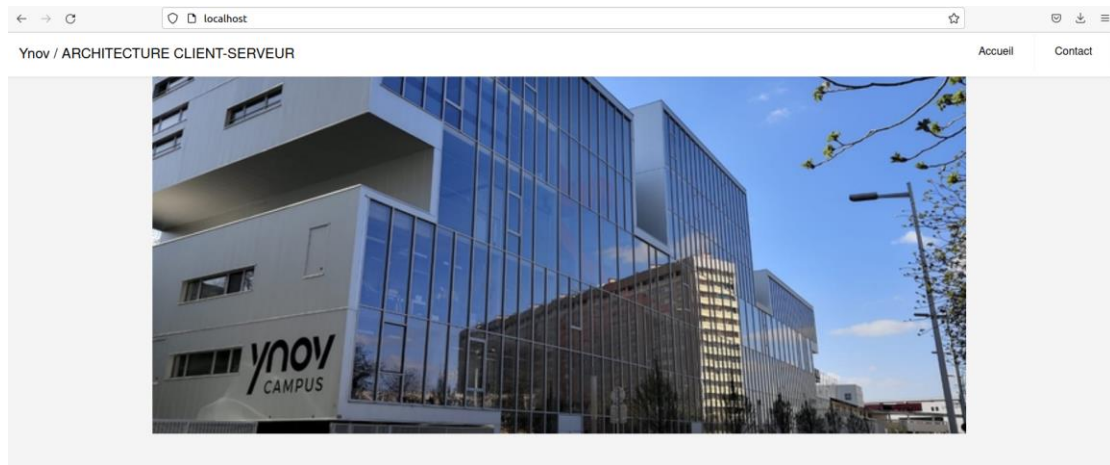
    location / {
        # First attempt to serve request as file, then
        # as directory, then fall back to displaying a 404.
        #try_files $uri $uri/ =404;
        root /home/hebergementlinux/Documents/ServerFiles/Web;
    }

    # pass PHP scripts to FastCGI server
    #
    #location ~ \.php$ {
```

Dans les deux rectangles en rouge ci-dessous, il faudra alors indiquer le chemin pointant vers les fichiers composant votre site web (html, css, etc.).

Quittez alors l'éditeur en sauvegardant, puis tapez « `service nginx restart` » afin de redémarrer votre serveur et appliquer les changements.

Maintenant aller sur votre navigateur internet et tapez « localhost » et ainsi vous verrez votre site web :



La configuration de votre serveur est alors terminé.

– Configuration du Service de Backup

Dans cette partie, nous allons voir comment instaurer une sauvegarde des fichiers du site web.

Pour ce faire, nous devons mettre en place un script sur notre machine de backup.

Tout d'abord, en allant dans le terminal de commande, entrer la commande « `sudo su root` ». Ceci va nous permettre de rentrer dans le mode root du terminal, ainsi nous pourrons paramétrer nos configurations de la même manière que le mode cron (que nous verrons plus tard).

Une fois en mode root, nous allons entrer la commande « `ssh-keygen` » :

```
root@backuonline-virtual-machine:/home/backuonline/Documents/backup# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:8dER+fvtHizdv0R/bxjhaX46xiPtTL2crJ4dF4WJXTk root@backuonline-virtual-machine
The key's randomart image is:
+---[RSA 3072]-----+
|          oo  o|
|         .+. E |
|        . . o.+ o|
|       o . o . |
|      S . . *  |
|             X.+|
|            *.XB|
|           .o/ #|
|          .B=/*|
+-----[SHA256]-----+
```

Ceci vient de créer une clé publique et privé d'identification.

Suite à ça, il faut entrer la commande suivante « `ssh-copy-id USER@ADDRESS` » (où USER = le nom de compte d'utilisateur de la machine serveur et ADDRESS = adresse IP de la machine serveur) :

```

root@backuplinux-virtual-machine:/home/backuplinux/Documents/backup# ssh-copy-id hebergementlinux@10.10.10.3
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
hebergementlinux@10.10.10.3's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'hebergementlinux@10.10.10.3'"
and check to make sure that only the key(s) you wanted were added.

```

Cette commande va ainsi copier la clé publique de notre machine de backup dans les fichiers de notre machine serveur. Ainsi, lors de notre transfert de données, les clés d'identifications ne seront pas demandées car elles seront déjà renseigné.

Nous allons maintenant passer à l'élaboration de notre script de récupération.

Il faut d'abord créer un fichier .sh, dans lequel nous mettrons ces lignes suivantes :

```

1 #! /bin/bash
2
3 newFile="backup_$(date +%Y-%m-%d_%T)"
4
5 mkdir /home/backuplinux/Documents/backup/WebArchive/$newFile
6
7 scp hebergementlinux@10.10.10.3:/home/hebergementlinux/Documents/ServerFiles/Web/index.html /home/backuplinux/Documents/backup/WebArchive/
  $newFile
8
9 scp hebergementlinux@10.10.10.3:/home/hebergementlinux/Documents/ServerFiles/Web/index.css /home/backuplinux/Documents/backup/WebArchive/
  $newFile

```

Explication des lignes :

3 – Création d'une variable qui servira de nom de fichier de sauvegarde (« backup_{date/heure} »)

5 – Création du nouveau dossier qui accueillera la sauvegarde

7 – Commande SCP qui va récupérer le fichier index.html en indiquant d'abord le nom de l'utilisateur sur la machine visé, son adresse IP, puis le chemin où se trouve le fichier voulu, et ensuite on indique le chemin dans lequel le fichier récupéré doit être mit

8 – Même commande mais pour le fichier index.css

Etc... répéter cette ligne de commande autant de fois que nécessaire selon les fichiers à sauvegarder (pages web, ressources, images...)

Maintenant, passons à la dernière étape, l'automatisation de ce script.

Pour ce faire, nous devons ouvrir l'outil « crontab ». Il s'agit d'un outil d'automatisation de tâches, dans lequel on peut indiquer une fréquence de réalisation. Toujours dans le terminal de commande, nous allons faire la commande « crontab -e » :

```
backuplinux@backuplinux-virtual-machine:~$ crontab -e
```

Ce qui va ouvrir un éditeur de texte du fichier crontab :

```
GNU nano 4.8 /tmp/crontab.8kv1Xr/crontab
00 12 * * * bash /home/backuplinux/Documents/backup/GetBackup.sh
```

Dans ce fichier la ligne présente ci-dessus va faire en sorte de lancer le script « GetBackup.sh » (notre script de récupération) tous les jours à 12h00.

Et voilà, notre système de récupération des données est établie et fonctionnel !