DOCUMENTATION D'ARCHITECTURE

PROJET INFRA & SI

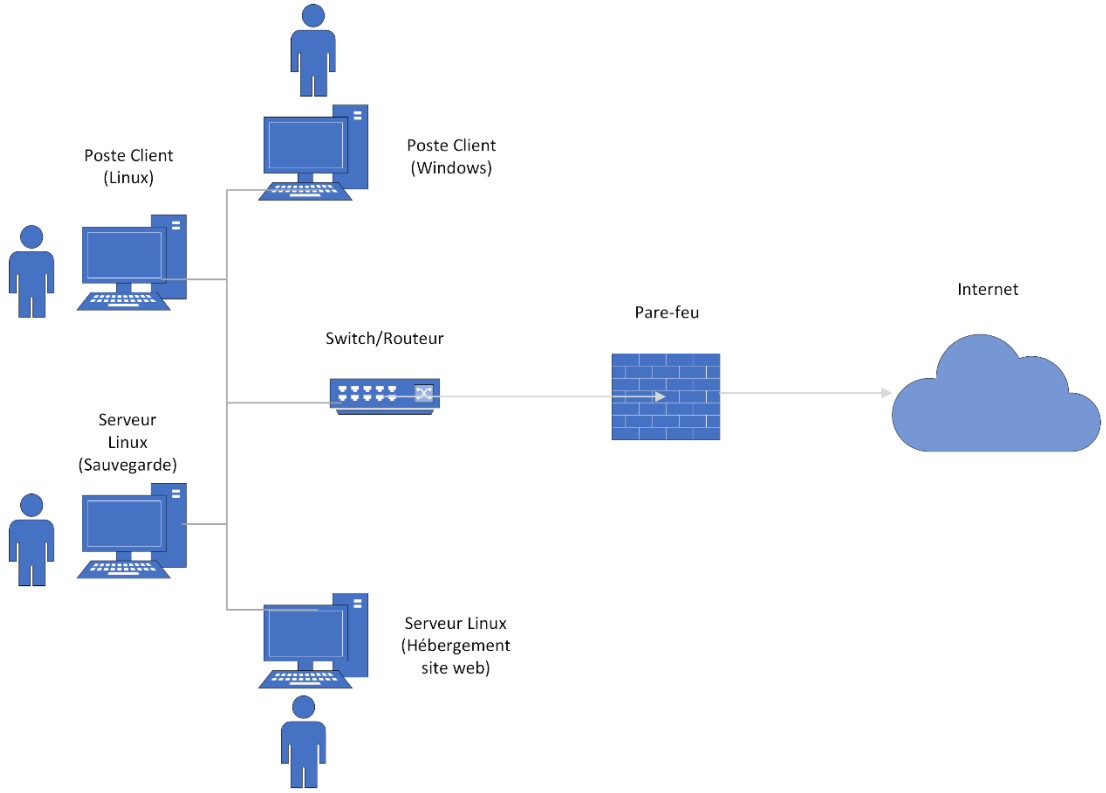
MISTRAL / PHAM / MARTHELY | Ynov 2021/2022

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.

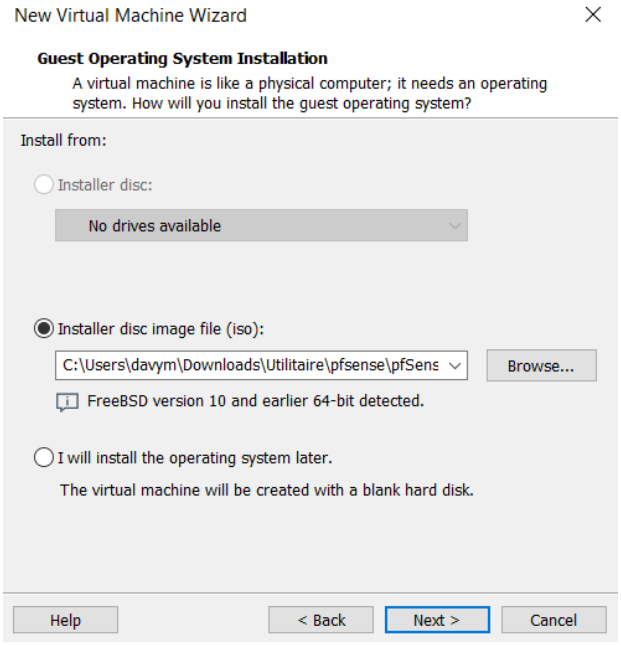
Etant limité à 6, nos adresses réseau ne dépasseront pas 10.10.10.6, attribuée ici à notre pare-feu qui fera office de passerelle. Ce qui explique que chaque élément à pour passerelle 10.10.10.6.

2.Mise en œuvre de la solution

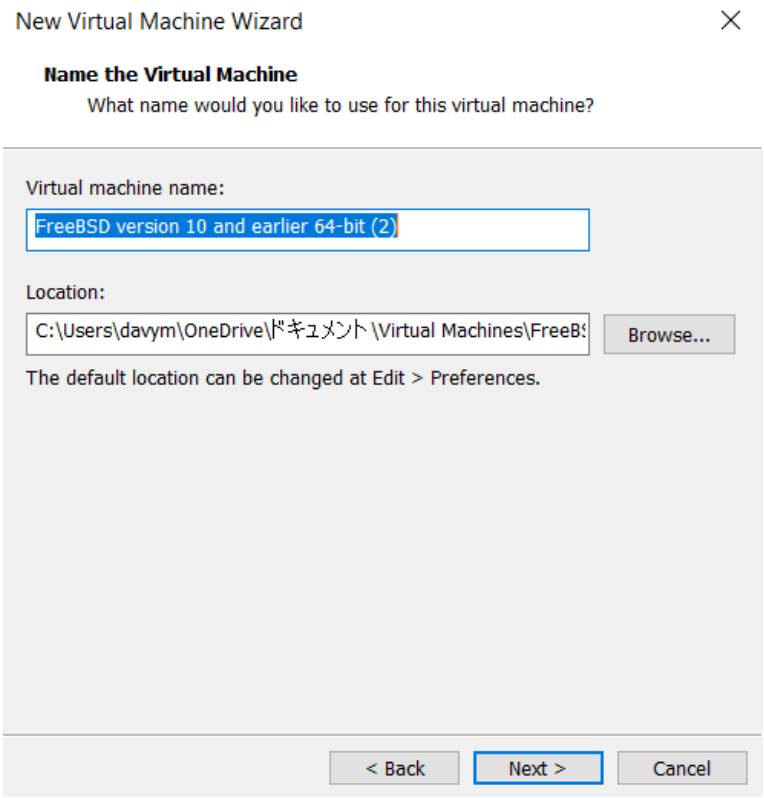
- Configuration du Pare-Feu

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).

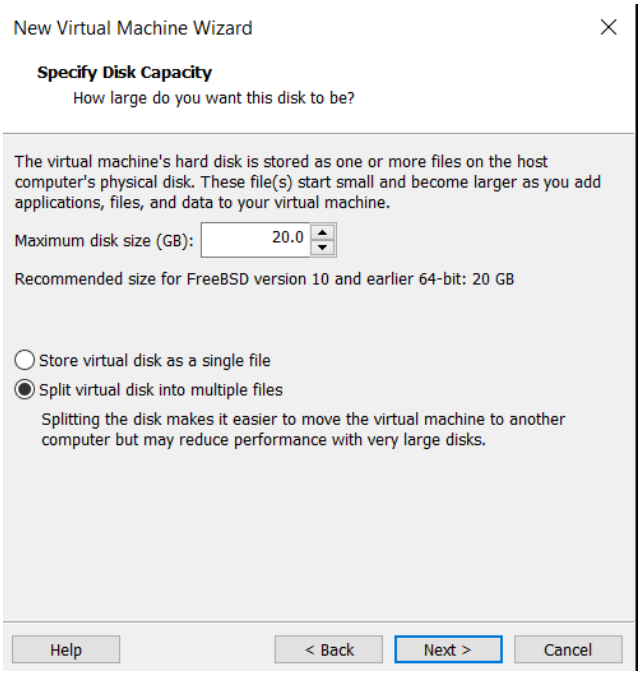
Utiliser le type de configuration « Typical » qui est celle recommandée, pas besoin d'option avancée pour le moment



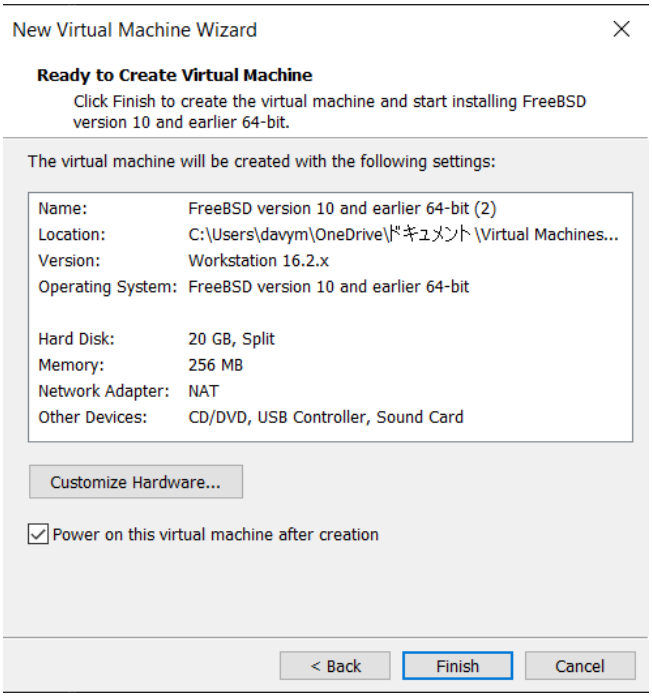
Après avoir préalablement télécharger l'iso PfSense, indiquer le chemin de ce dernier à la VM



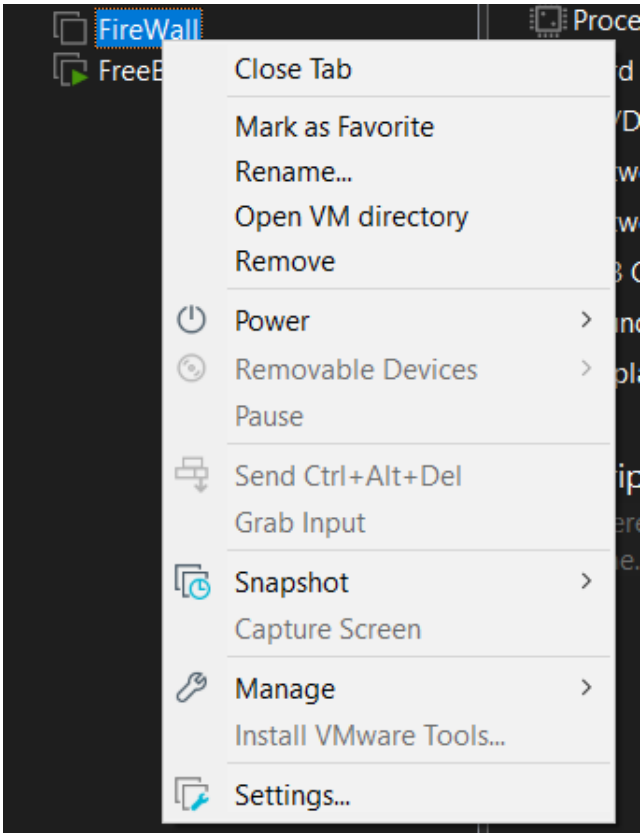
Ici il est possible de renommer directement le nom de la VM ainsi que son emplacement. L'emplacement n'est pas nécessaire à la modification cependant.



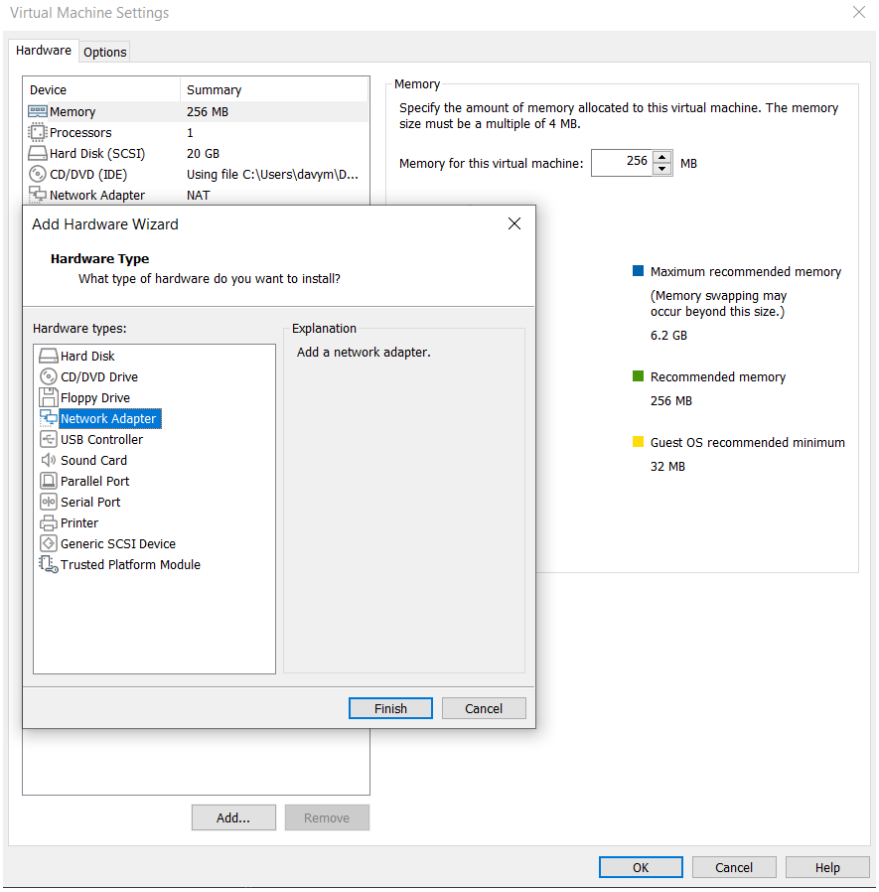
Vient ensuite la possibilité d'allocation de l'espace disque, ici nous mettons 20GB de façon à être large mais le pare-feu ne demande pas autant d'espace. Sélectionner l'option de séparation du disque virtuel en plusieurs fichiers.



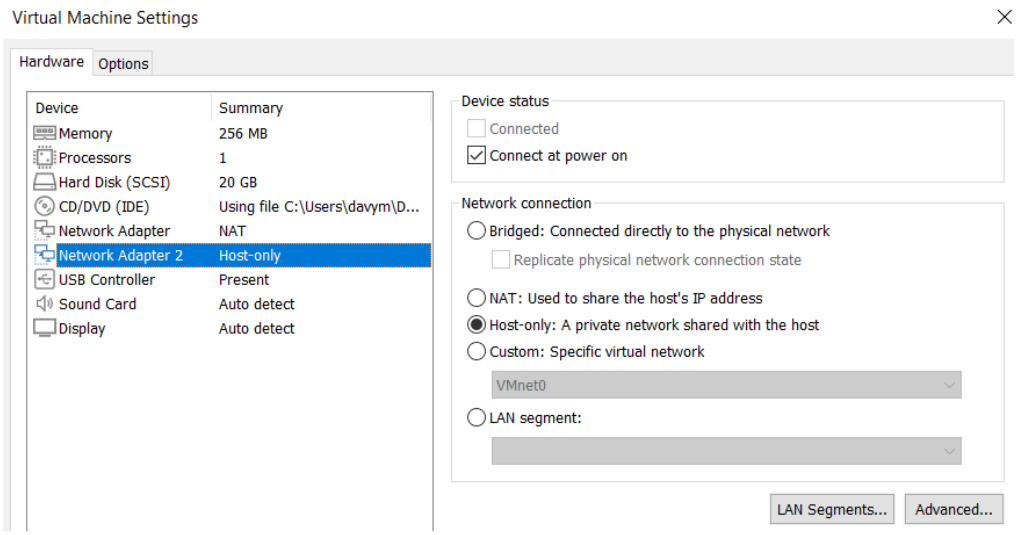
Ici vient le récap de la création de notre VM. Pour finir le processus appuyer tout simplement sur « Finish » si tous les éléments vous conviennent



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 ».

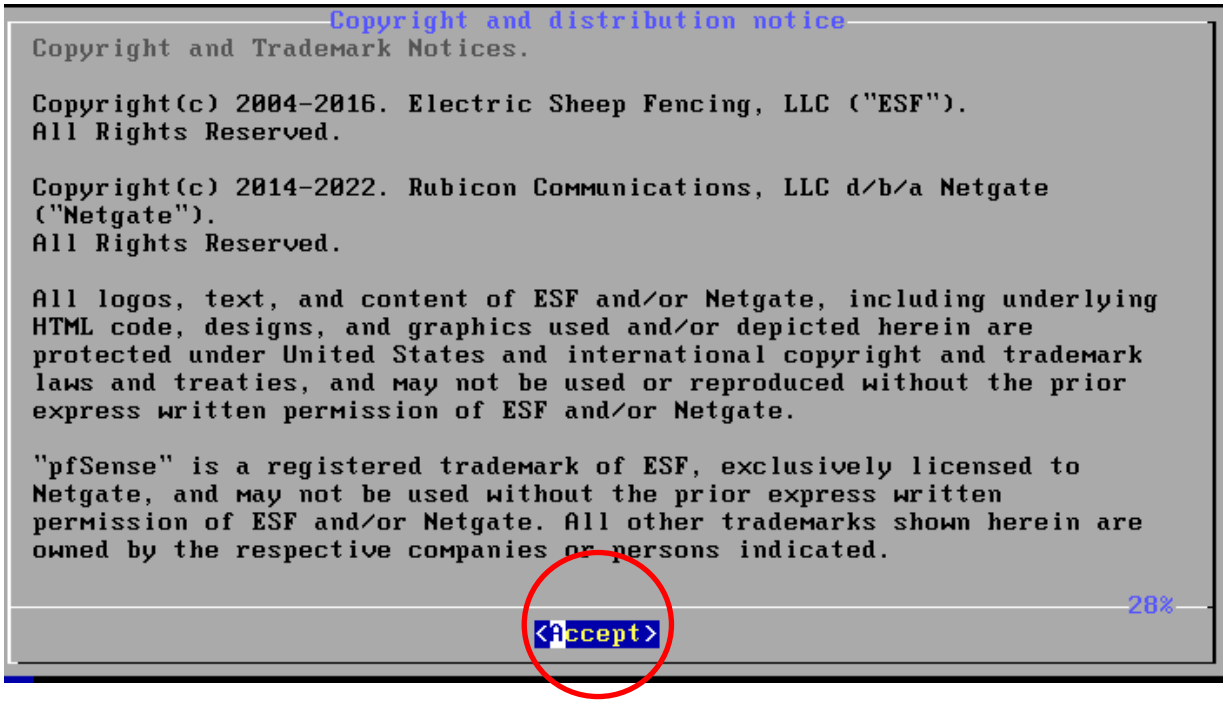


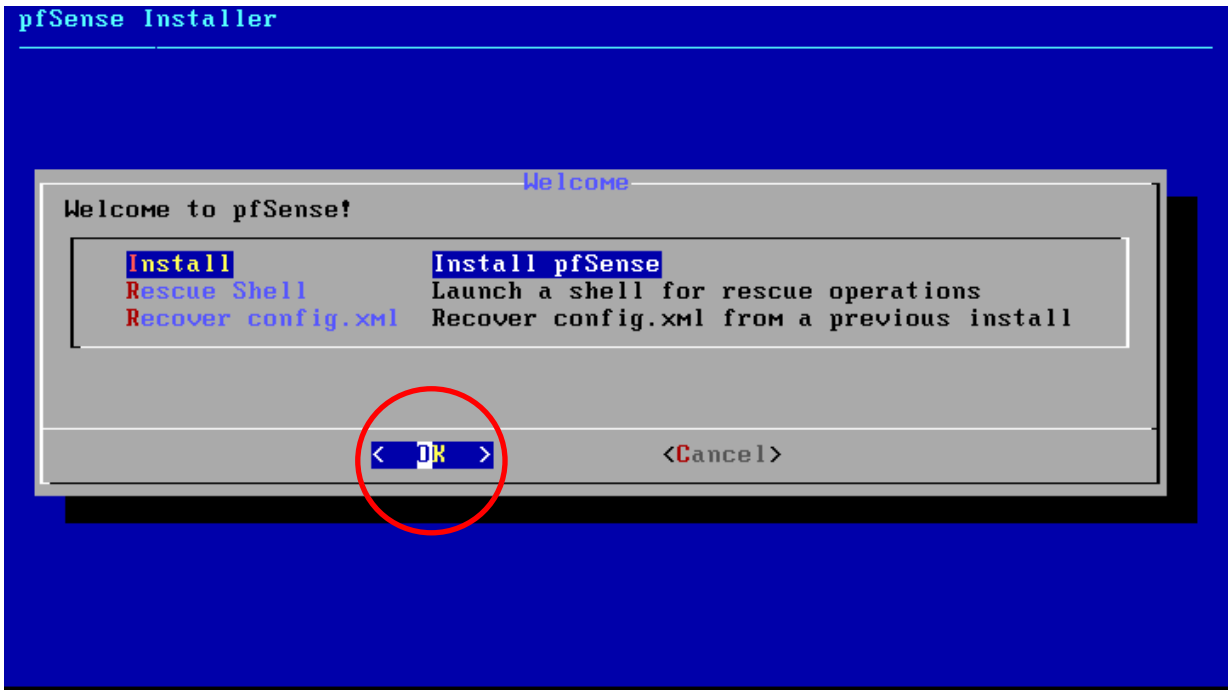
Appuyer sur « Add », ensuite sélectionner « Network Adpatater ».

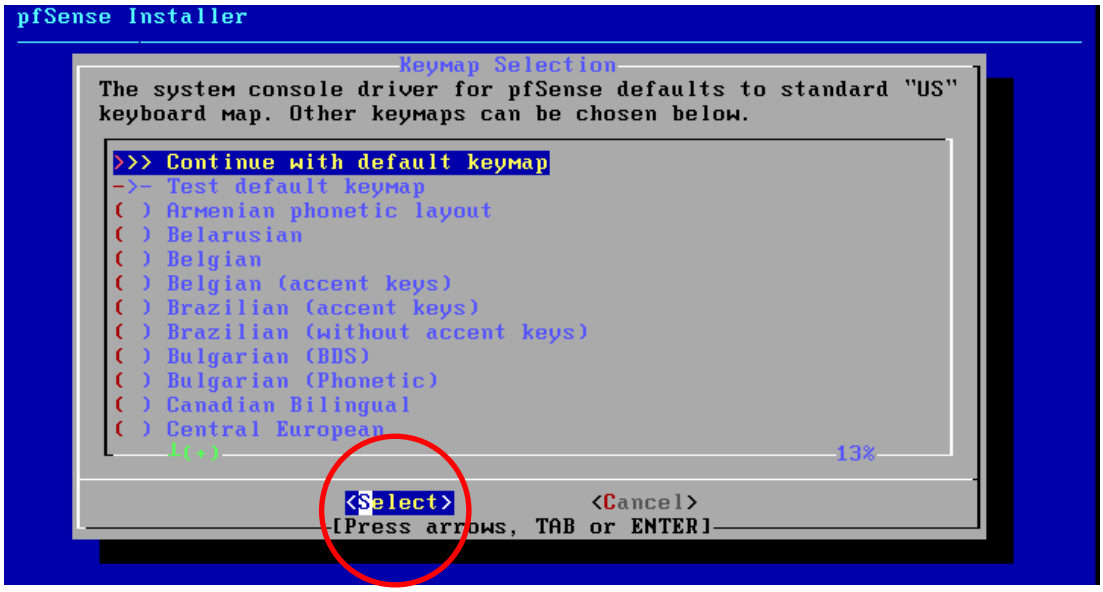


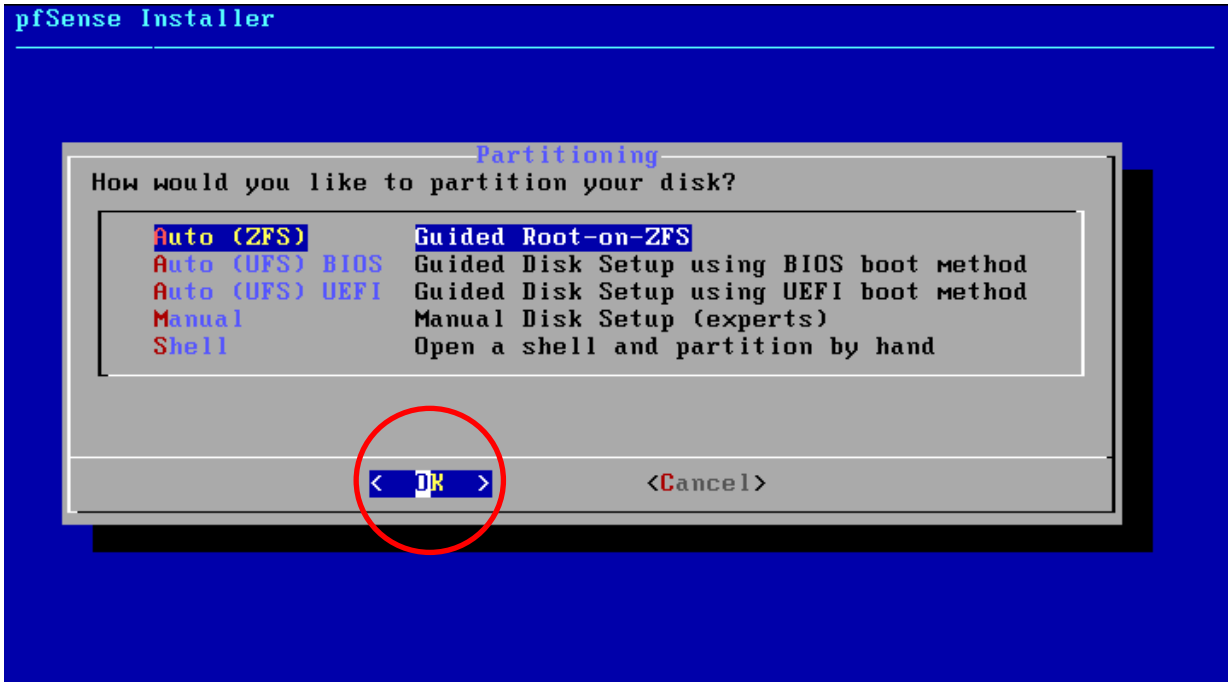
Une fois ce nouvel adaptateur ajouté, mettre celui-ci en « host-only ». Il ne reste plus qu'à lancer maintenant le pare-feu.

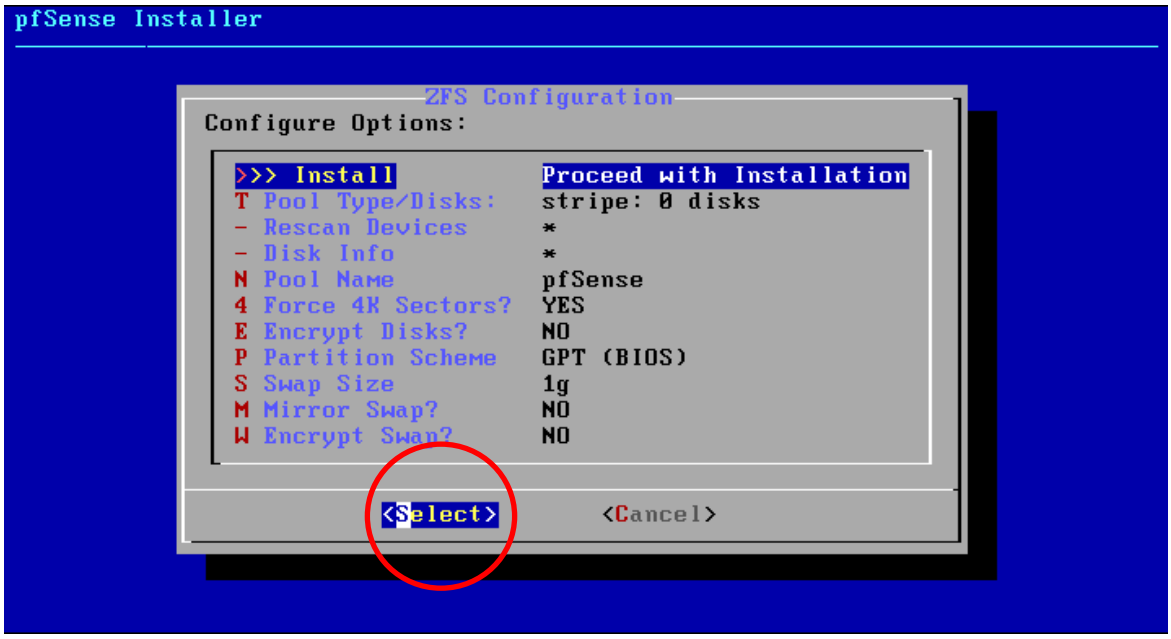
Ci-joint une série de captures des étapes à suivre

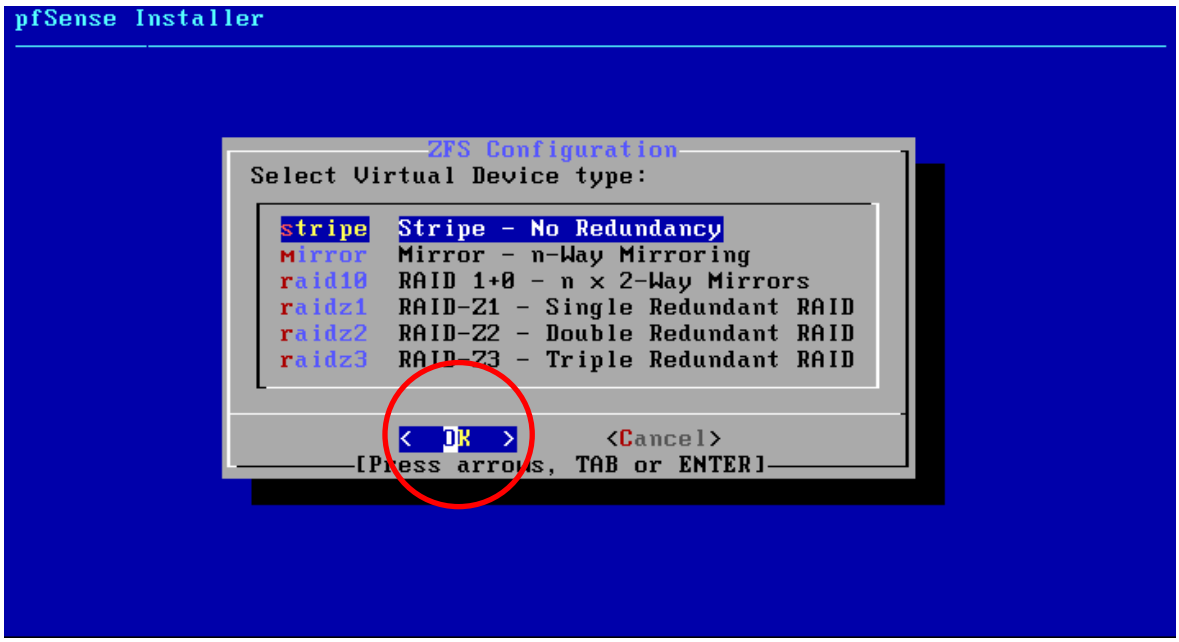


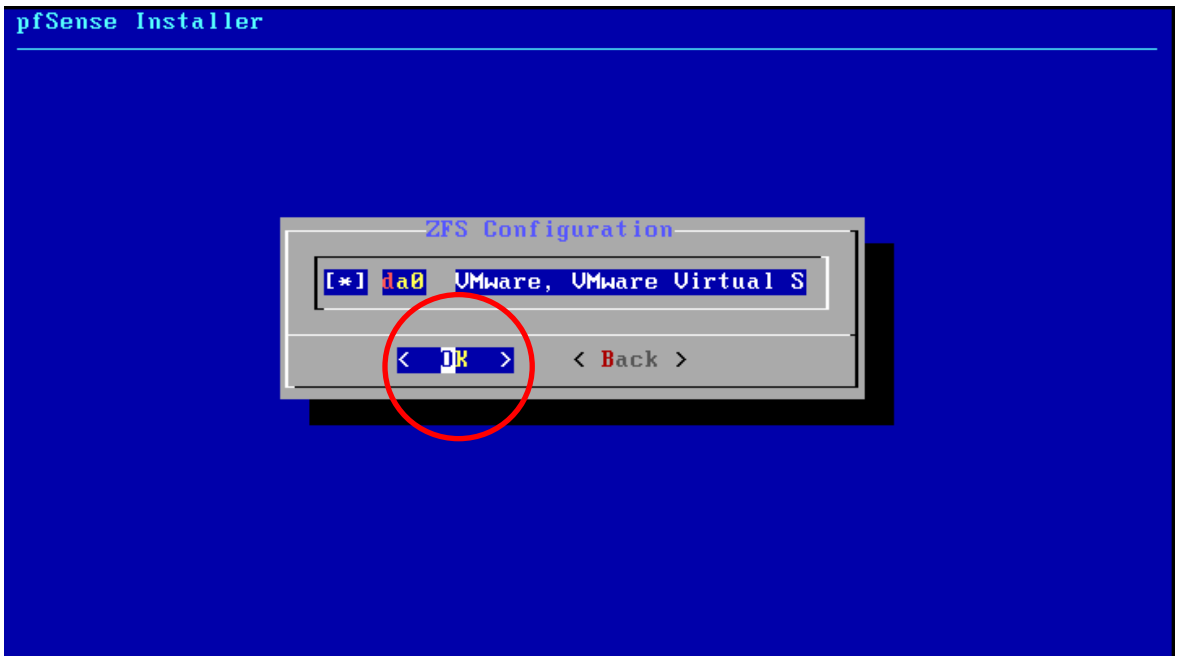



pfSense Installer
Keymap Selection
The system console driver for pfSense defaults to standard "US"
keyboard map. Other keymaps can be chosen below.
>>> Continue with default keymap
->- Test default keymap
( ) Armenian phonetic layout
( ) Belarusian
( ) Belgian
( ) Belgian (accent keys)
( ) Brazilian (accent keys)
( ) Brazilian (without accent keys)
( ) Bulgarian (BDS)
( ) Bulgarian (Phonetic)
( ) Canadian Bilingual
( ) Central European
13%
<Select>
<Cancel>
[Press arrows, TAB or ENTER]

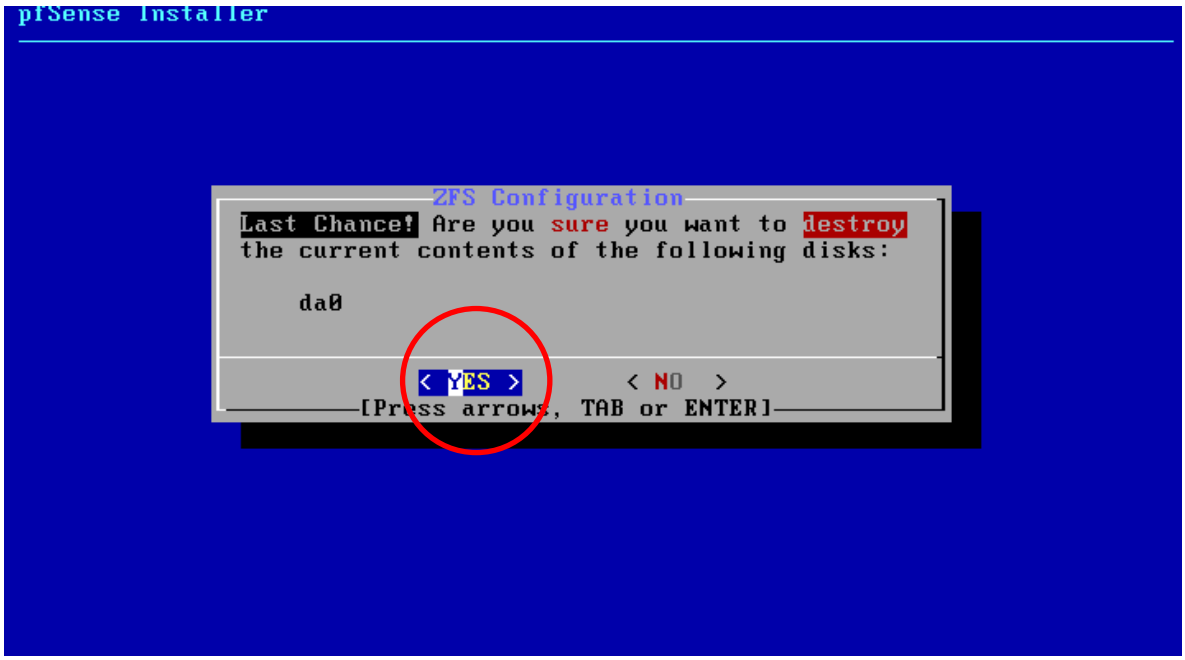

pfSense Installer
Partitioning
How would you like to partition your disk?
Auto (ZFS) Guided Root-on-ZFS
Auto (UFS) BIOS Guided Disk Setup using BIOS boot method
Auto (UFS) UEFI Guided Disk Setup using UEFI boot method
Manual Manual Disk Setup (experts)
Shell Open a shell and partition by hand
< OK >
<Cancel>

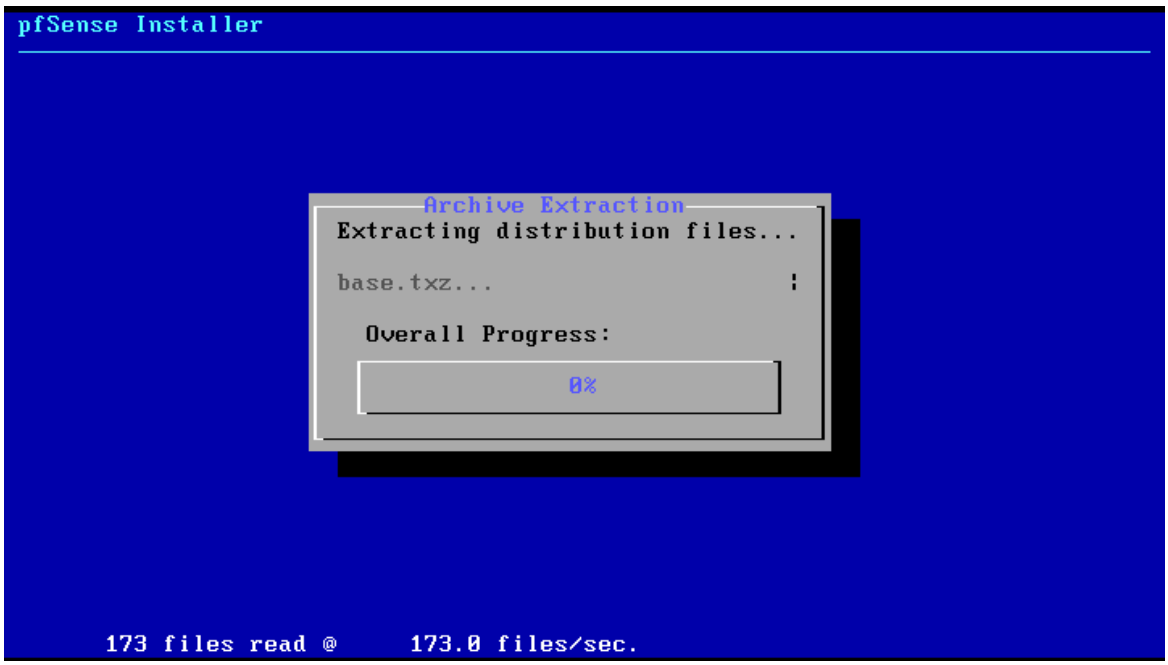

pfSense Installer
ZFS Configuration
Configure Options:
>>> Install Proceed with Installation
T Pool Type/Disks: stripe: 0 disks
- Rescan Devices *
- Disk Info *
N Pool Name pfSense
4 Force 4K Sectors? YES
E Encrypt Disks? NO
P Partition Scheme GPT (BIOS)
S Swap Size 1g
M Mirror Swap? NO
W Encrypt Swap?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

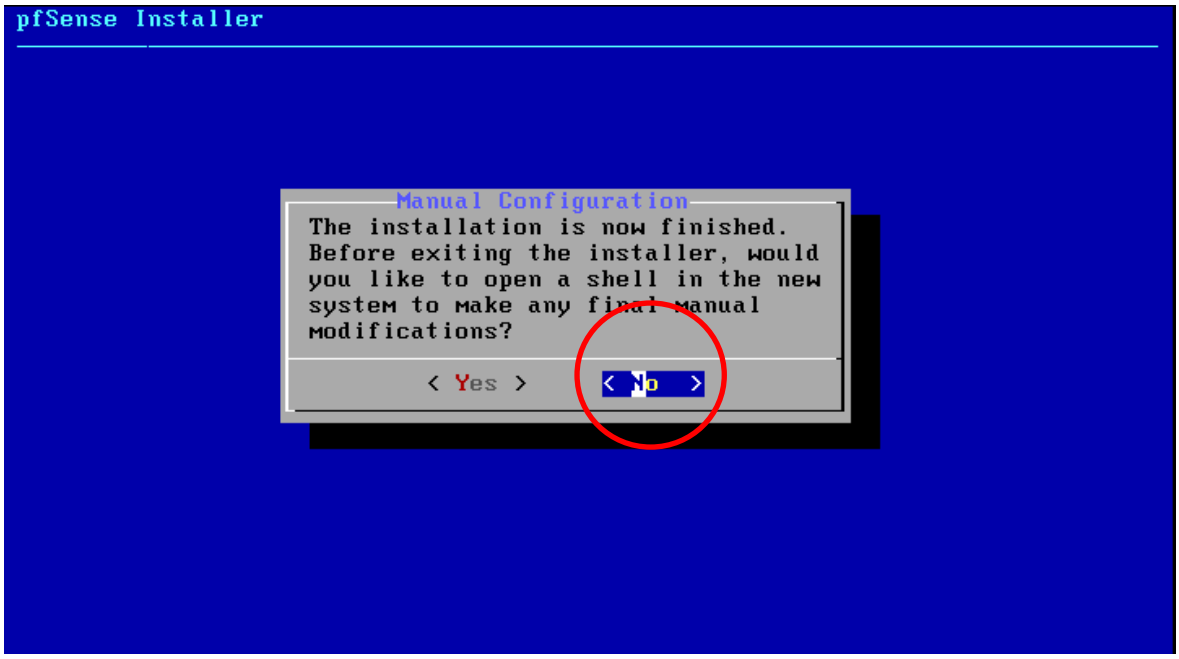

pfSense Installer
ZFS Configuration
Select Virtual Device type:
stripe Stripe - No Redundancy
mirror Mirror - n-Way Mirroring
raid10 RAID 1+0 - n x 2-Way Mirrors
raidz1 RAID-Z1 - Single Redundant RAID
raidz2 RAID-Z2 - Double Redundant RAID
raidz3 RAID-Z3 - Triple Redundant RAID
< OK >
<Cancel>
[Press arrows, TAB or ENTER]

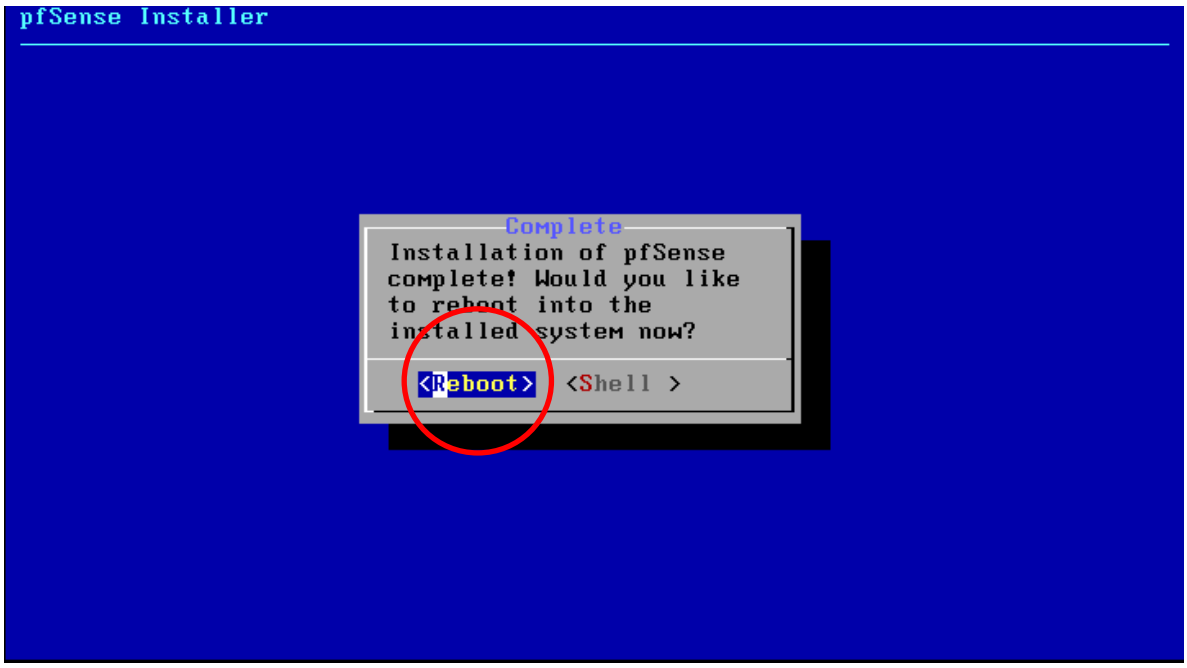


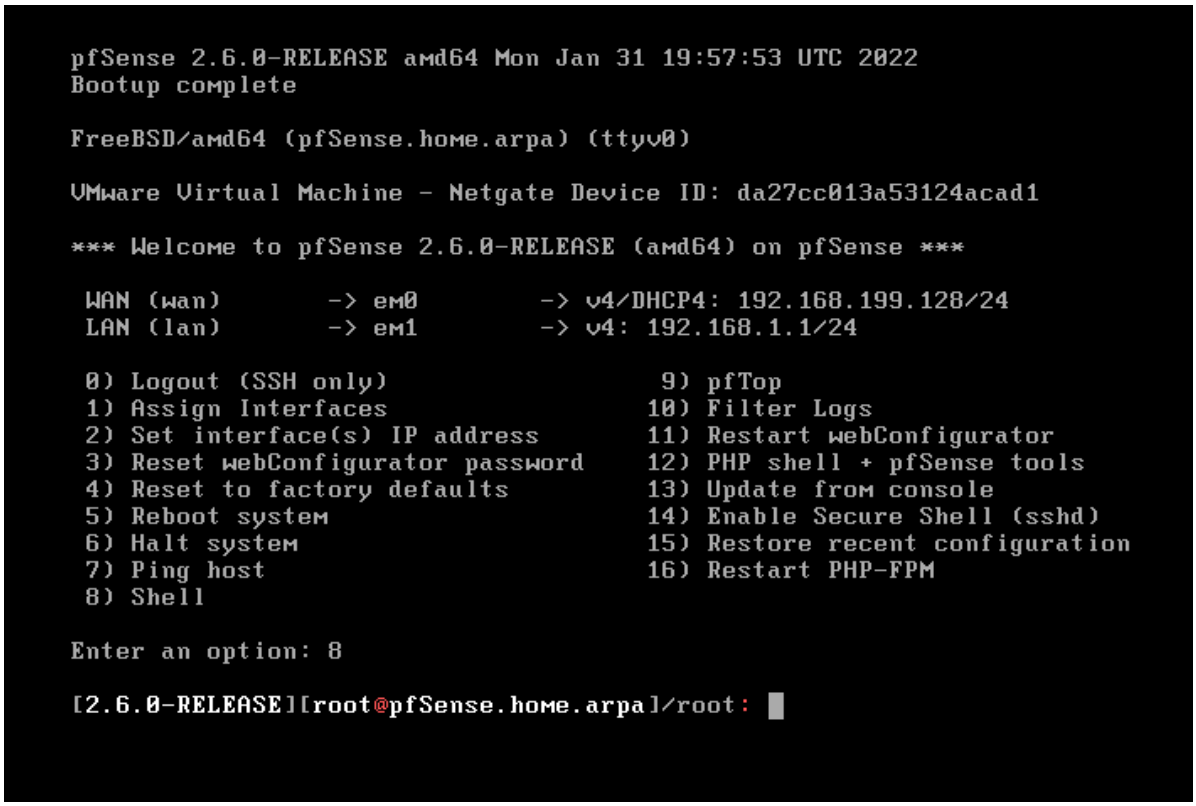
Ici appuyer sur la touche espace pour que l'étoile apparaisse signifiant ainsi « all »



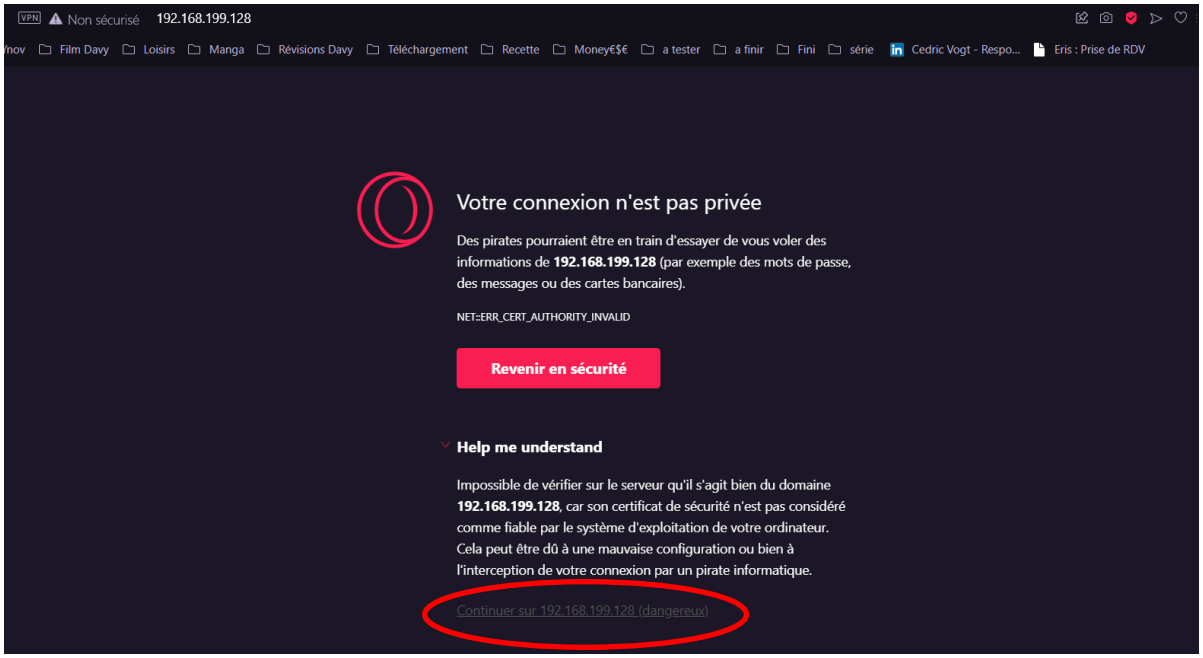

pfSense Installer
Archive Extraction
Extracting distribution files...
base.txz...
Overall Progress:
0%
173 files read @ 173.0 files/sec.


pfSense Installer
Manual Configuration
The installation is now finished.
Before exiting the installer, would
you like to open a shell in the new
system to make any final manual
modifications?
< Yes >
< No >

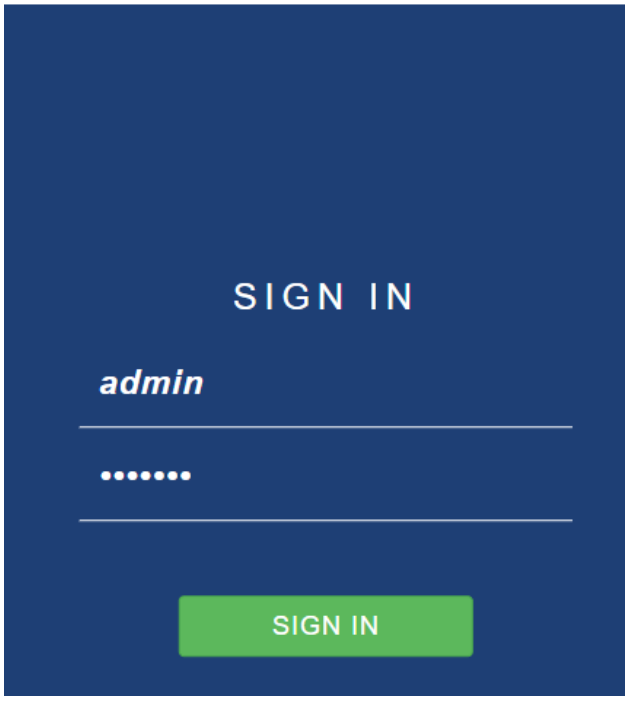




Nous remarquons ici la présence d'un WAN et d'un LAN avec chacun une adresse IP attitrée. Appuyer sur 8 pour accéder à l'interface de commande qui nous sera utile par la sui

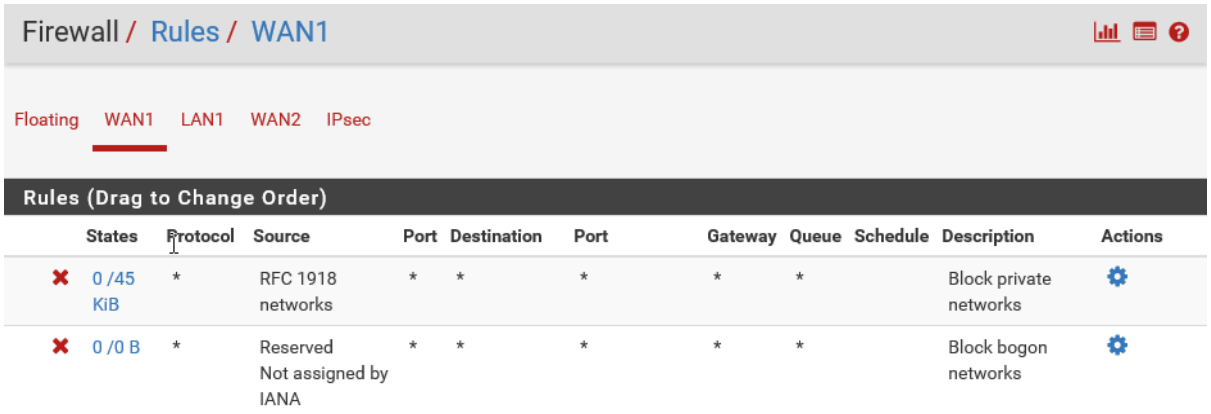


Entrer l'adresse IP Emo (WAN) dans le navigateur internet de votre choix. Il est normal de tomber sur cette page, sélectionner simplement « continuer sur *adresse_ip-emo* »

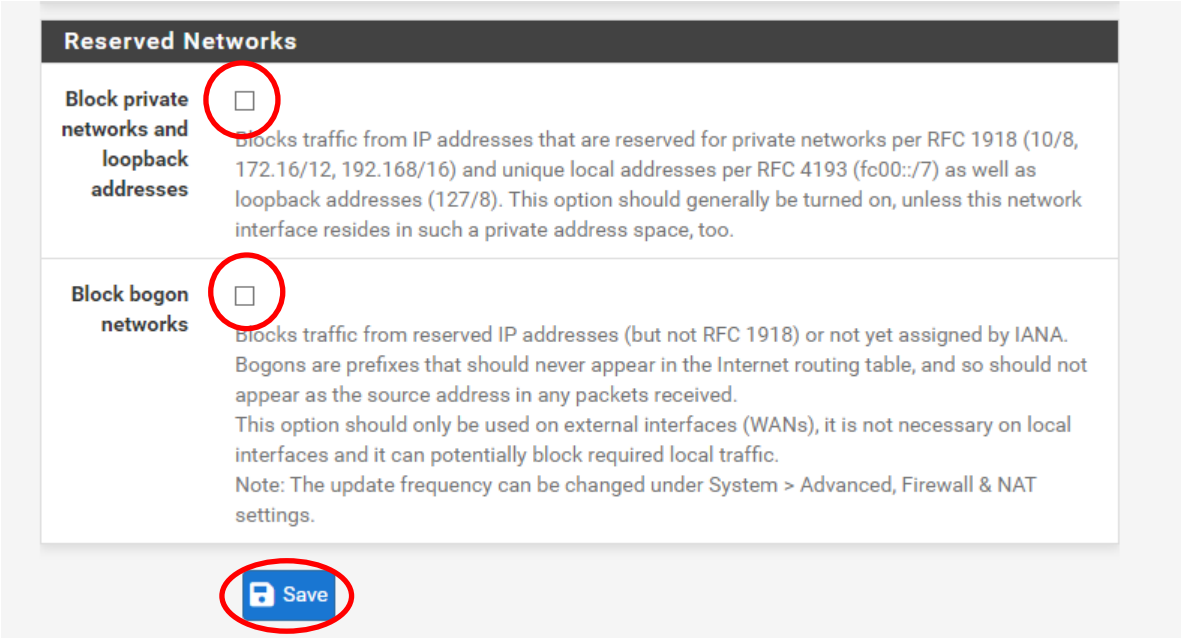


Une fois sur cette page ID : admin, Mot de passe : pfsense. Afin d'accéder à l'interface PfSense

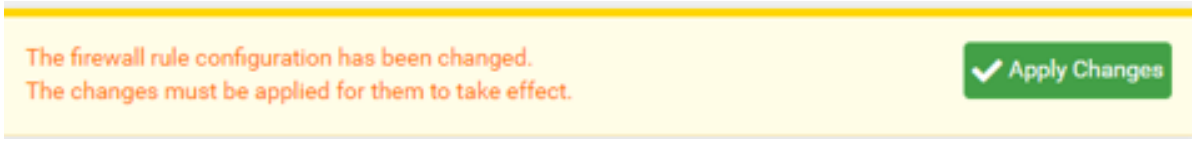
Dans le menu dépliant sélectionner « Firewall » puis « Rules »



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



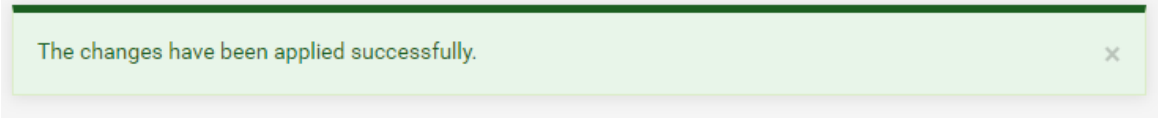
Aller en bas de page et désélectionner ces 2 options. Puis appuyer sur « Save ».



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

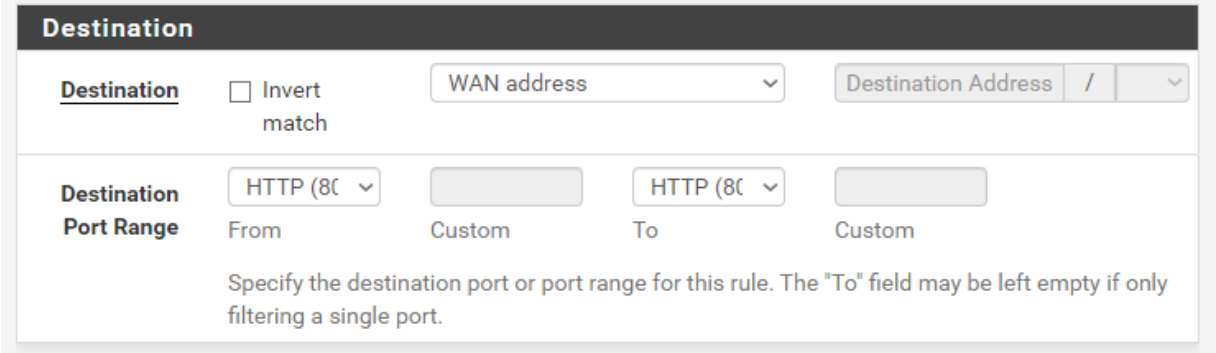
```
[2.6.0-RELEASE][root@pfSense.home.arpa]/root: pfctl -d
pf disabled
```

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.

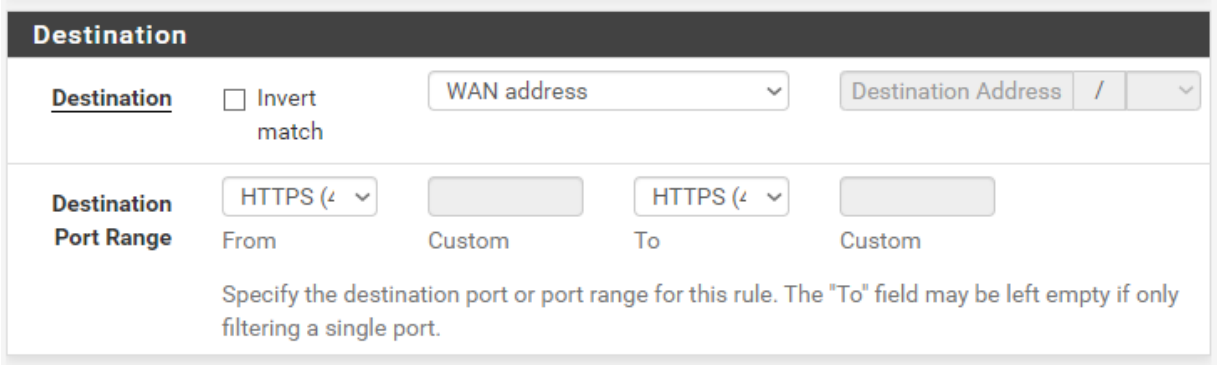


En retournant sur notre navigateur nous avons ce message qui s'affiche nous confirmant notre opération

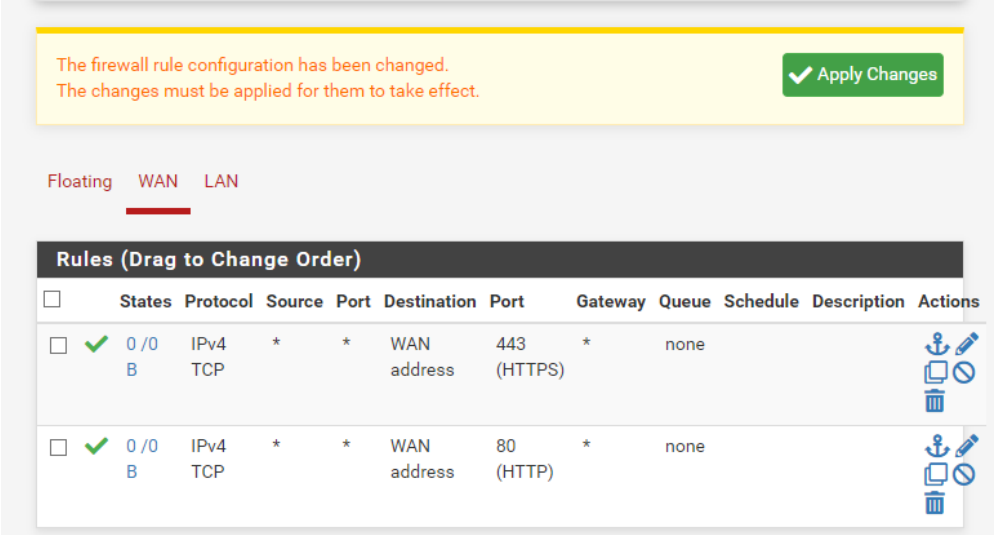
Juste en dessous de la liste des règles sélectionner l'un des boutons « Add »

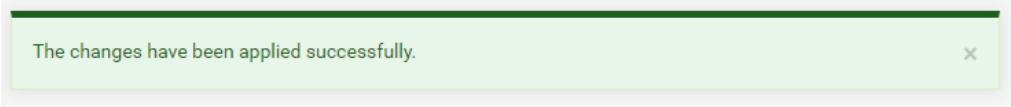


Dans le champ « Destination », changer le type en « Wan adress » et le Port Range en « http ». Puis sur « Save »



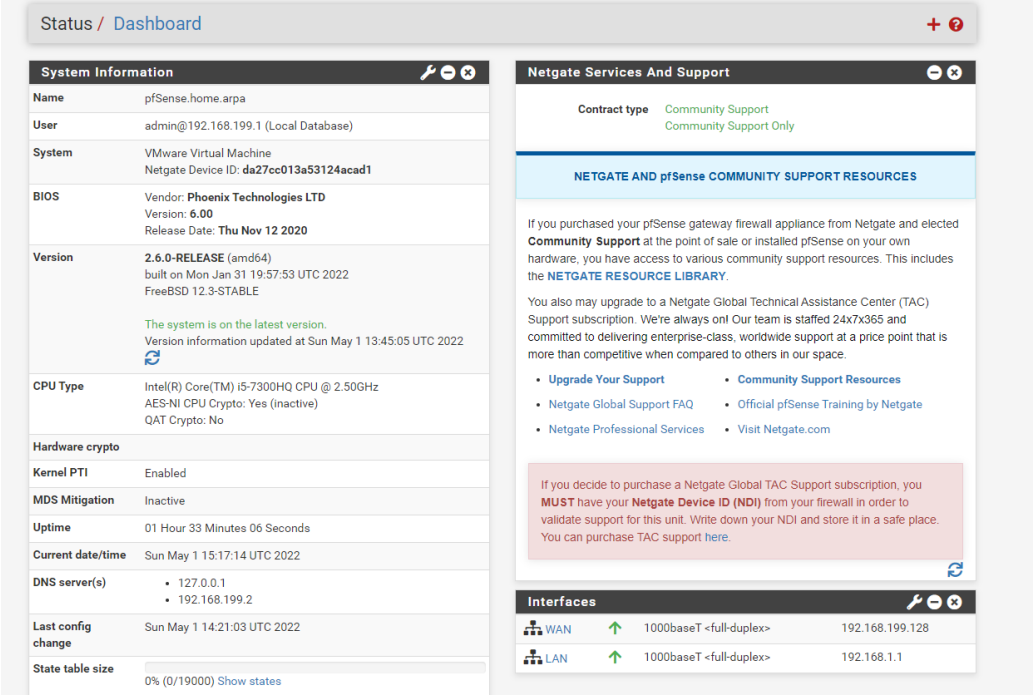
Réitérer l'opération pour le port « Https » cette fois-ci afin de pouvoir complètement utiliser notre pare-feu sans avoir à le désactiver à chaque fois.



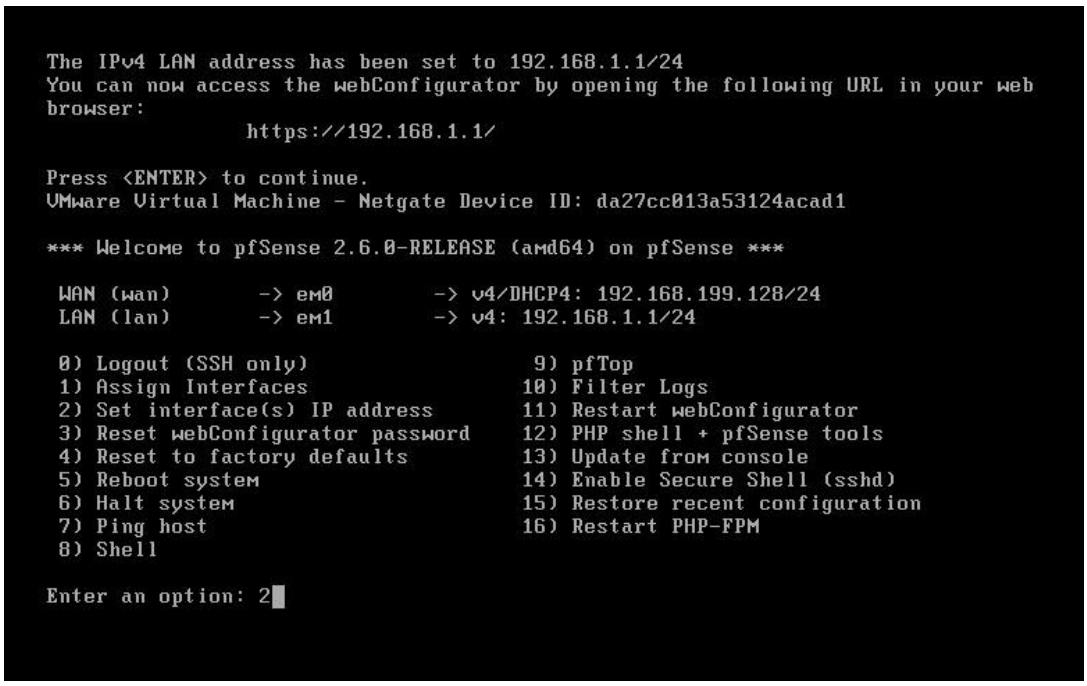


Tout comme pour la suppression des règles principales après avoir fait la « Save », appuyer sur « Apply Changes » et taper dans l'interface de commande du pare-feu sur la VM la commande *pfctl -d* pour appliquer les changements. Une l'opération terminée le message de confirmation s'affichera.

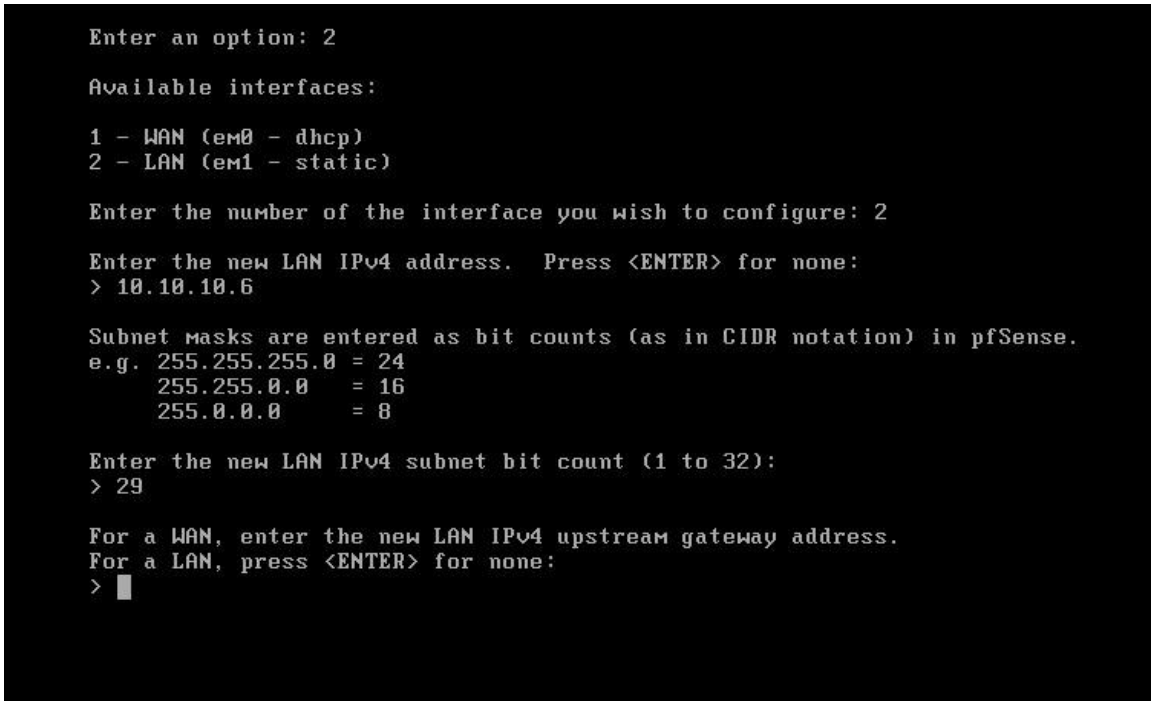
Afin de permettre un accès externe, on établit une règle autorisant les protocoles TCP vers l'adresse IP du serveur (pour nous 10.10.10.3).



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.

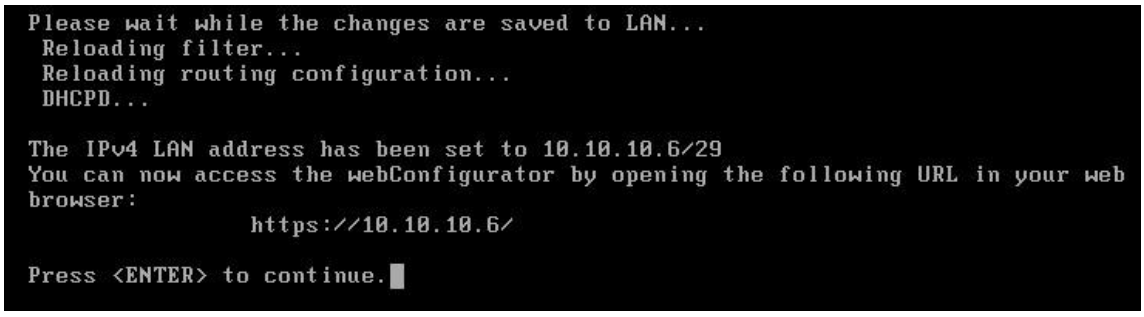


Une fois ces étapes passées, nous allons configurer notre adresse IP de notre LAN. Pour ce faire taper « 2 » dans l'interface de commande du pare-feu

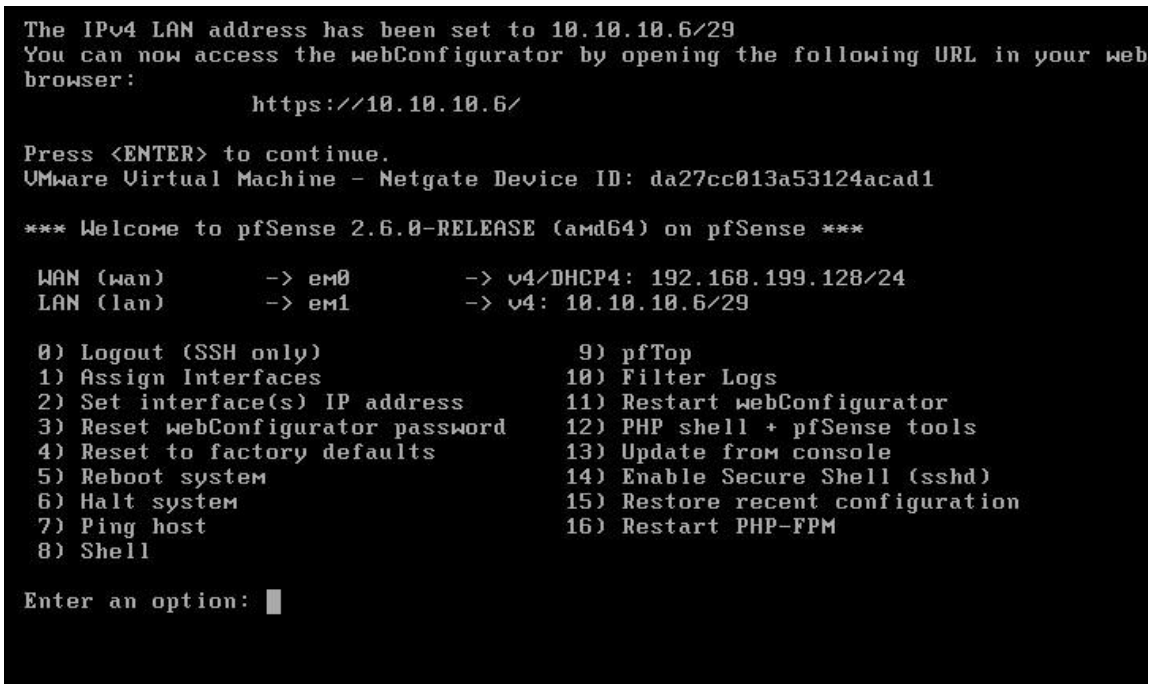


Après avoir rentré la nouvelle adresse IP, et le sous-réseau. Taper « Entrer » pour passer la configuration IPv4 du WAN

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



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



Ca y est, votre LAN est configurée !

Tableau de filtrage :

Règles LAN :

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0 /0 B	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
✓	6 /274.03 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Règles WAN :

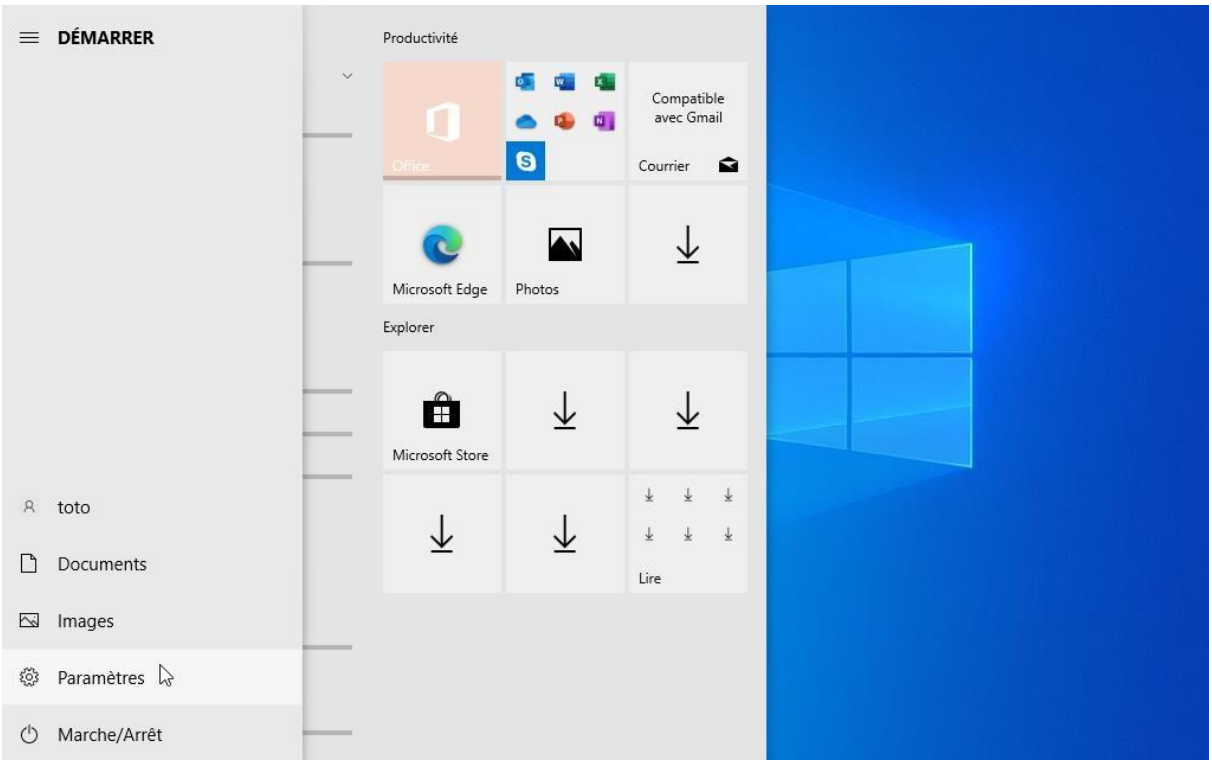
Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0 /0 B	IPv4 TCP	*	*	10.10.10.3	*	*	none			
✓	0 /0 B	IPv4 TCP	*	*	WAN address	80 (HTTP)	*	none			
✓	2 /1.40 MiB	IPv4 TCP	*	*	WAN address	443 (HTTPS)	*	none			

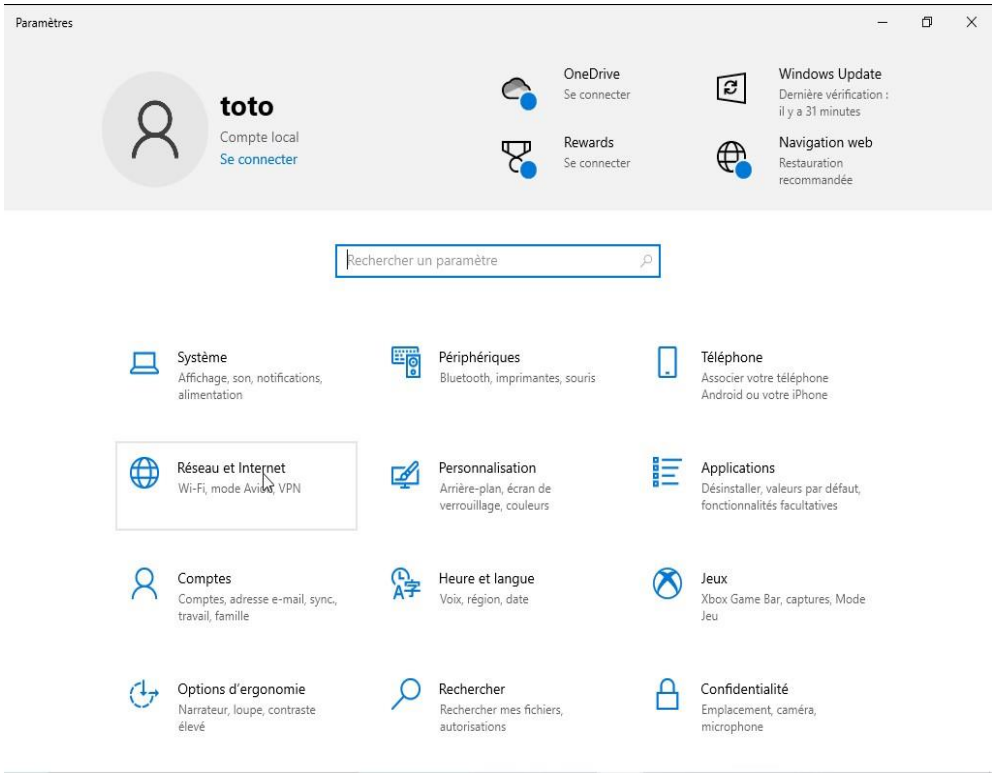
- Configuration des Clients

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

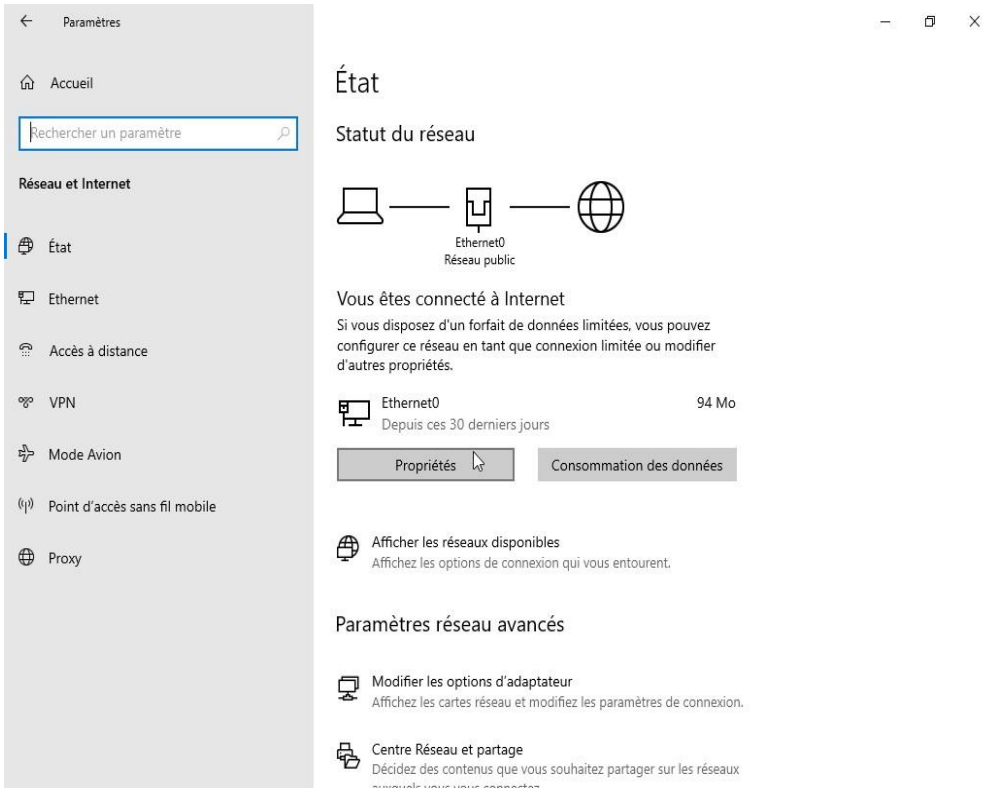
SOUS WINDOWS



Aller dans les paramètres

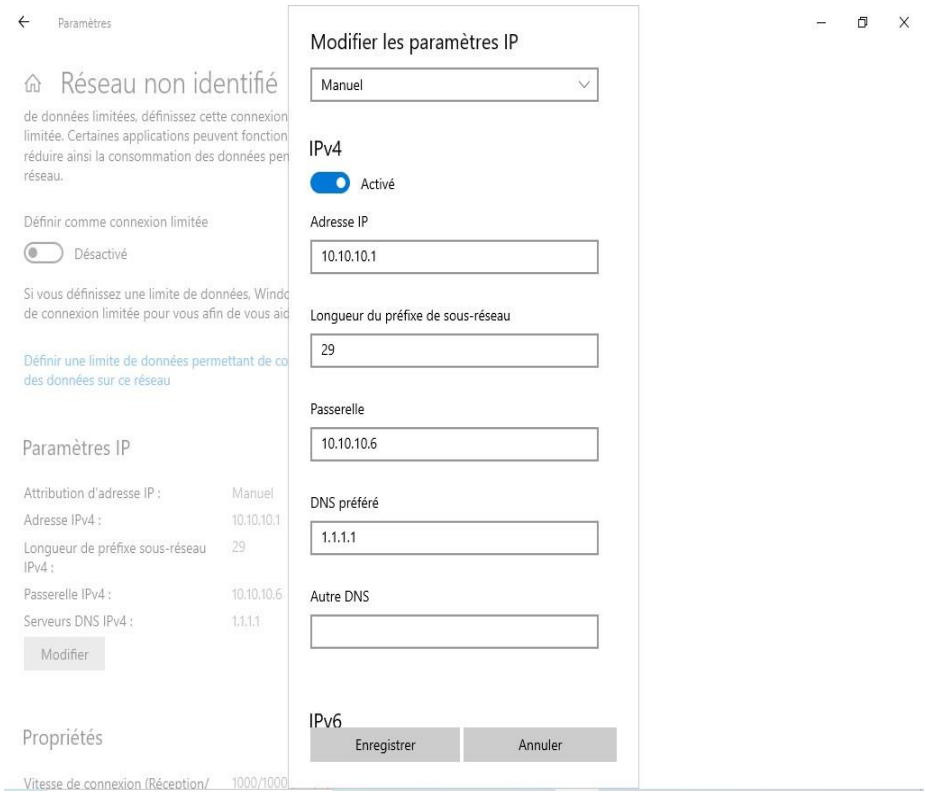


Sélectionner « réseau et Internet »



Puis aller dans « Propriétés »

Ensuite sur « Modifier »

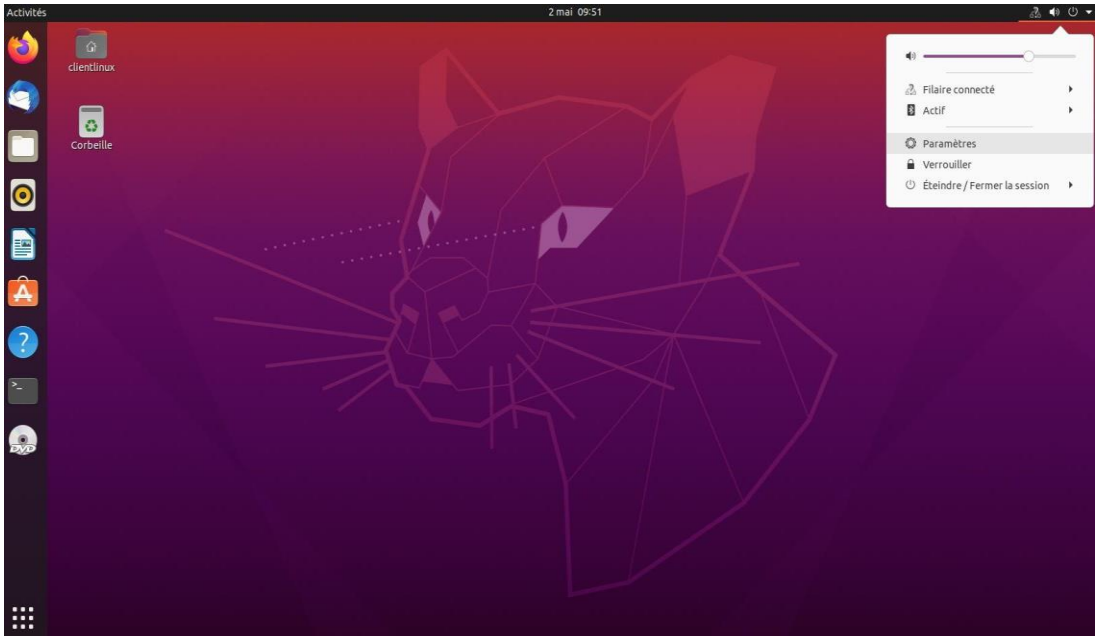


Basculer en mode « Manuel » si nécessaire et configurer l'adresse IP de votre Pc. La longueur du sous-réseau, de même que la passerelle correspondent à celles de votre pare-feu préalablement

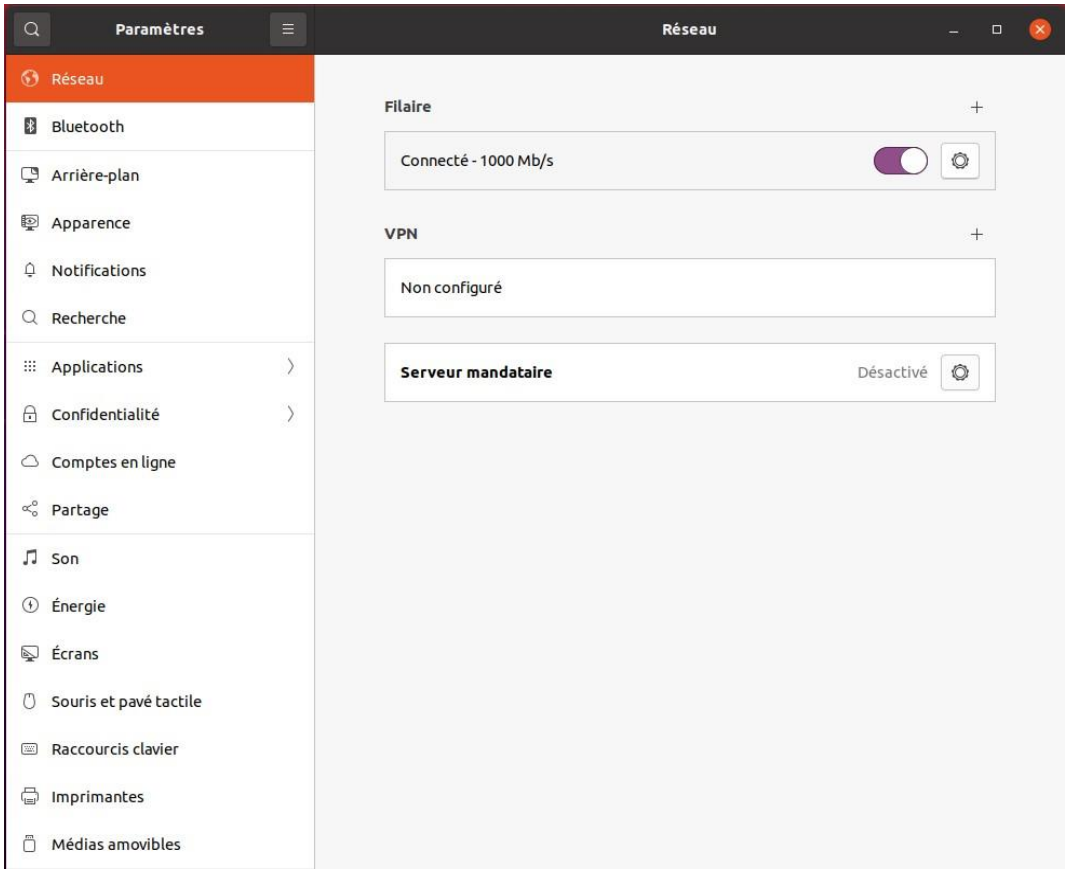
configuré. Le DNS quant à lui peu rester du « 1.1.1.1 » le choix ici n'est pas très important.

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.

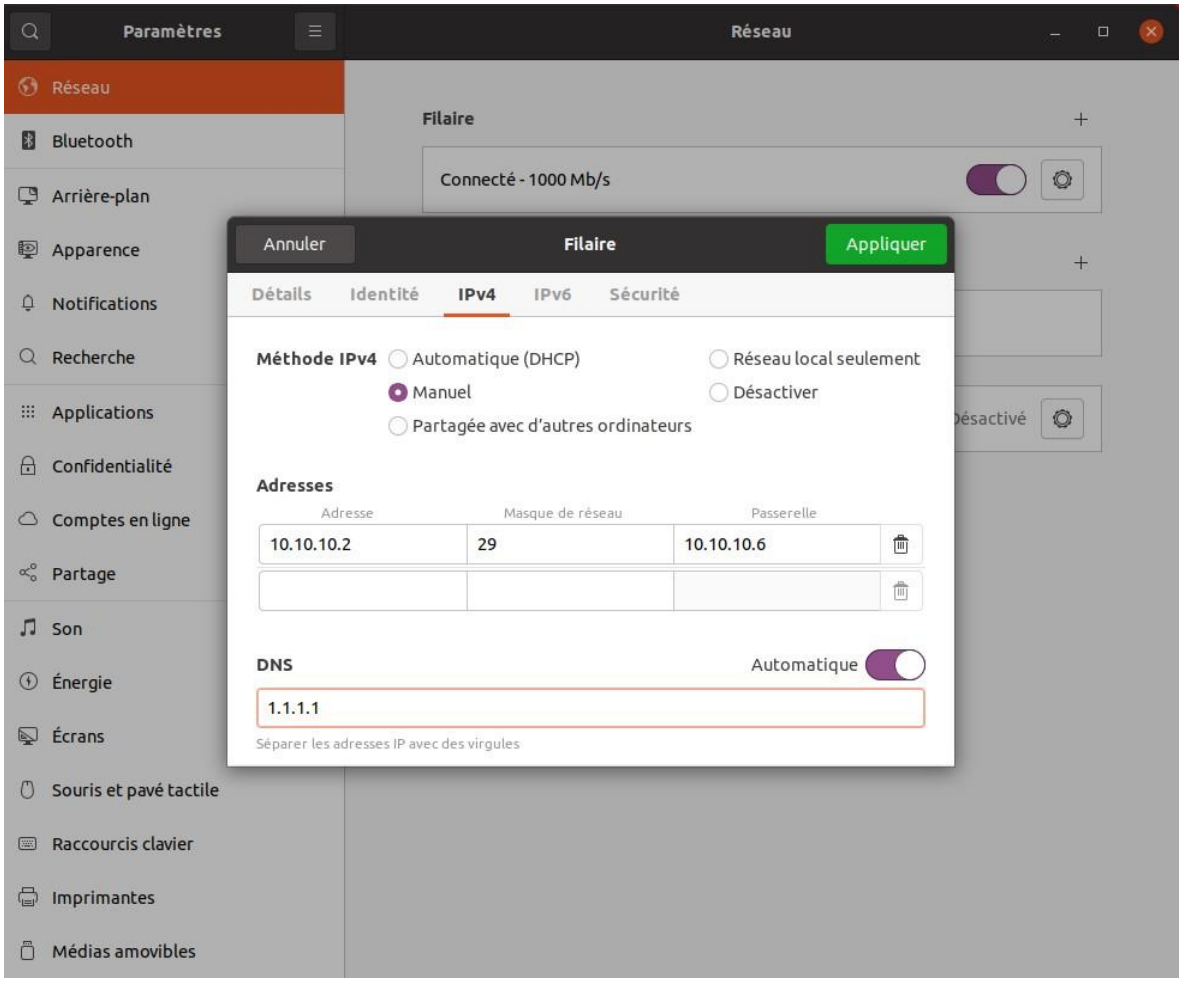
SOUS LINUX



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.

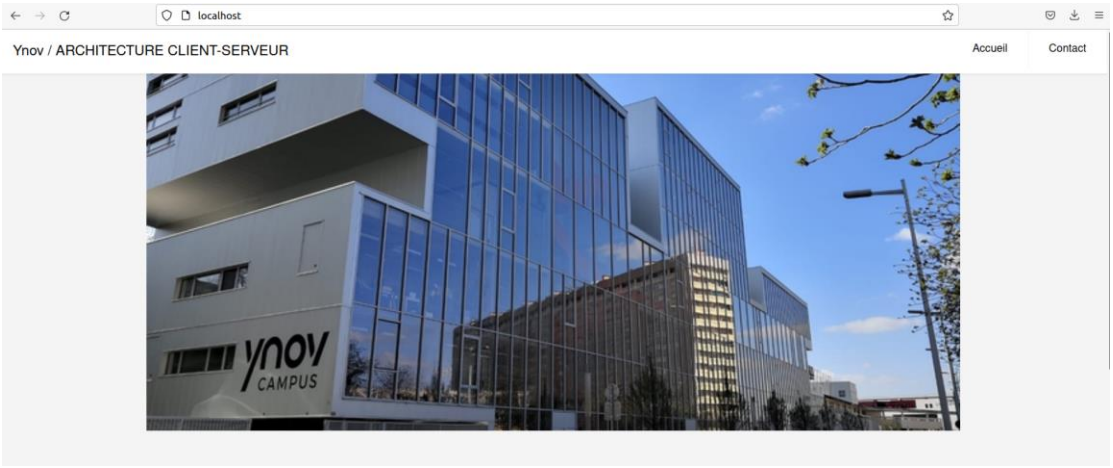
Après cela nous allons faire « sudo nano /etc/nginx/sites-enabled/ », ce qui va ouvrir un éditeur de texte sur le fichier de configuration de notre page Nginx.

```
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@backuplinux-virtual-machine:/home/backuplinux/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@backuplinux-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 !