





**SOMMAIRE**

Table des matières

1. **Introduction**………………………………………………………………………………………………………………………………3
2. Pfsense c’est quoi ?.....................................................................................................................3
3. Contexte ………………………………………………………………………………………………………………………….……3
4. Besoin…………………………………………………………………………………………………………………………………… 3
5. Schéma…………………………………………………………………………………………………………………………………..3
6. Cahier des charges …………………………………………………………………………………………………………………4
7. **Mise en Place**…………………………………………………………………………………………………………………………….**4**
8. Installation des machines……………………………………………………………………………………………………….5

a-PFsense……………………………………………………………………………………………………………………………….5

b-serveur web………………………………………………………………………………………………………………………11

c-machine Debian dans le LAN…………………………………………………………………………………………..…16

1. Configuration de la DMZ……………………………………………………………………………………………………. 17
2. Machine du wan …………………………………………………………………………………………………………………20
3. **Phase 1 …………………………………………………………………………………………………………………………….…22**
4. Autoriser les accès au serveur Web depuis Internet et depuis le LAN……………………….22
5. Autoriser les accès FTP sur le serveur de la DMZ depuis le LAN…………………………………24
6. Autoriser les accès Internet depuis le LAN et la DMZ en passant par le Firewall……..…28
7. Interdire tout accès au LAN depuis l'Internet ou la DMZ……………………………………………32
8. **Phase 2 …………………………………………………………………………………………………………………………….…13**
9. Installer un serveur de base de données MariaDB dans le LAN et, autoriser les requêtes SQL du serveur WEB vers le serveur MariaDB …………………………………………………………..14

# **INTRODUCTION**

## **PFsense c’est quoi ?**

PFsense est un système d'exploitation open source ayant pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD. À l'origine un fork de m0n0wall, il utilise le pare-feu à états Packet Filter ainsi que des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. pfSense convient pour la sécurisation d'un réseau domestique ou d'entreprise.

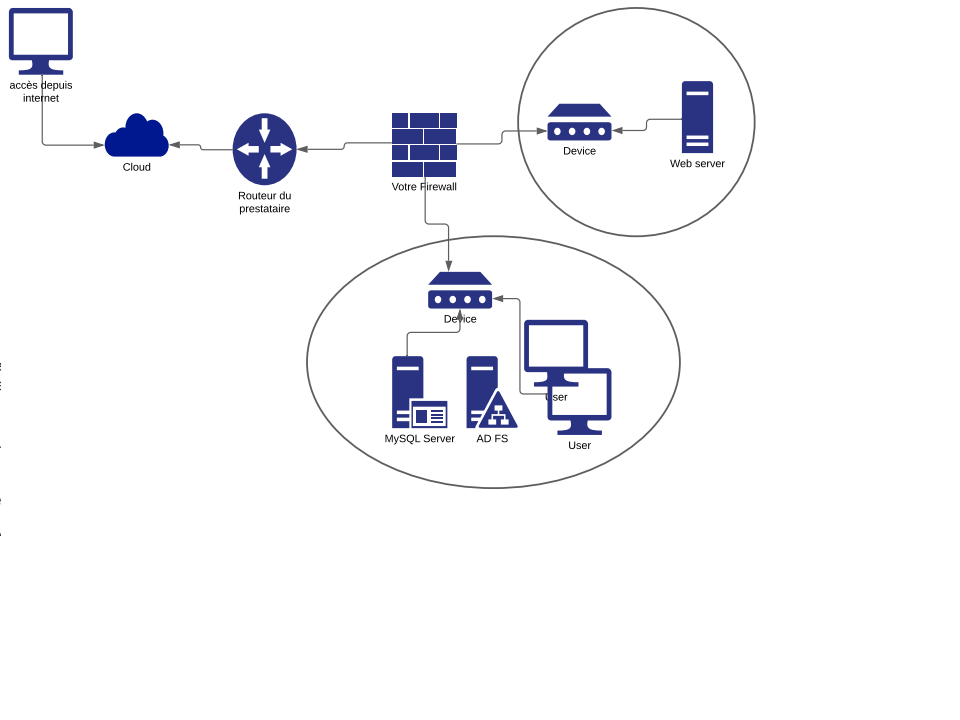
## **Contexte :**

# Dans le cadre de la sécurisation des accès aux serveurs de l’entreprise, il a été décidé de créer un réseau dit DMZ pour contenir tous les services accessibles depuis l’extérieur. La 1ère partie de ce déploiement ne portera que sur le serveur WEB qui sera déplacé du LAN vers cette DMZ

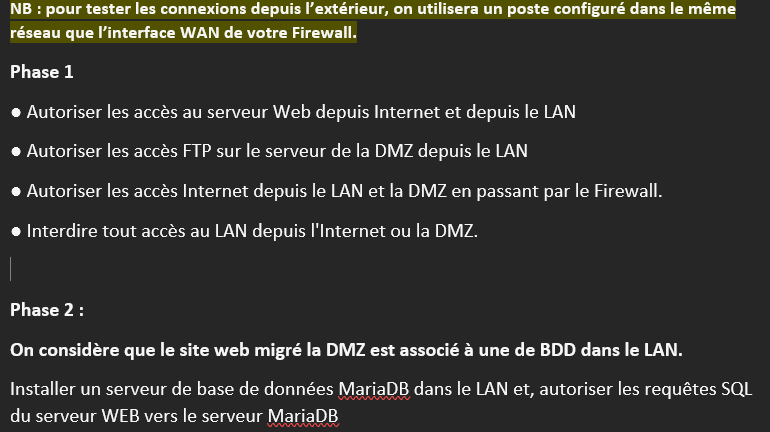
## **Besoin :**

Le besoin fondamental est la **sécurisation des accès externes** aux ressources critiques, avec une solution spécifique (mise en place d’une DMZ et déplacement du serveur WEB) pour répondre à cet objectif.

## **d - Schéma :**

****

## **e-Cahier des charges :**



# **Mise en Place :**

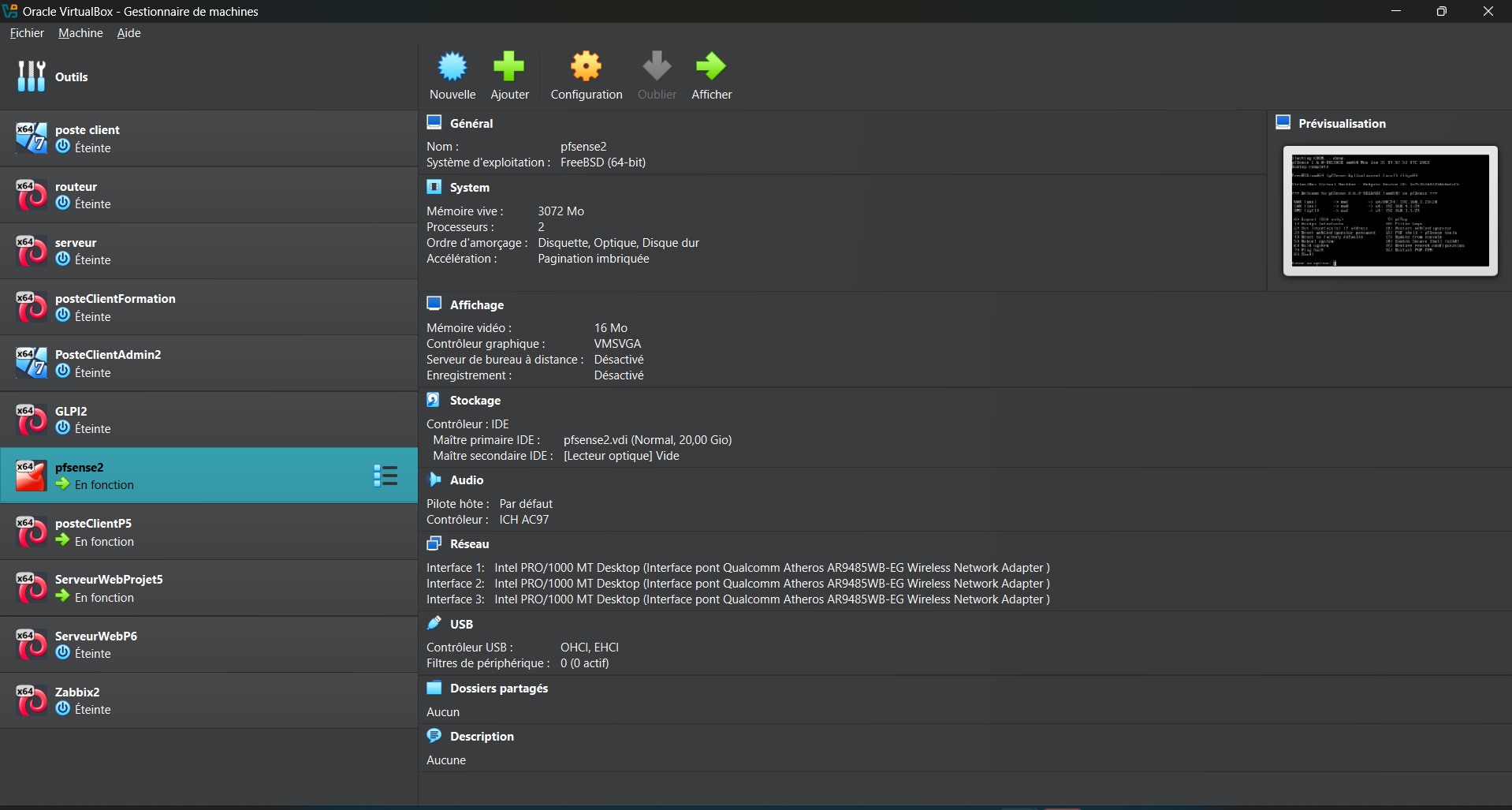
## **Installation des machines**

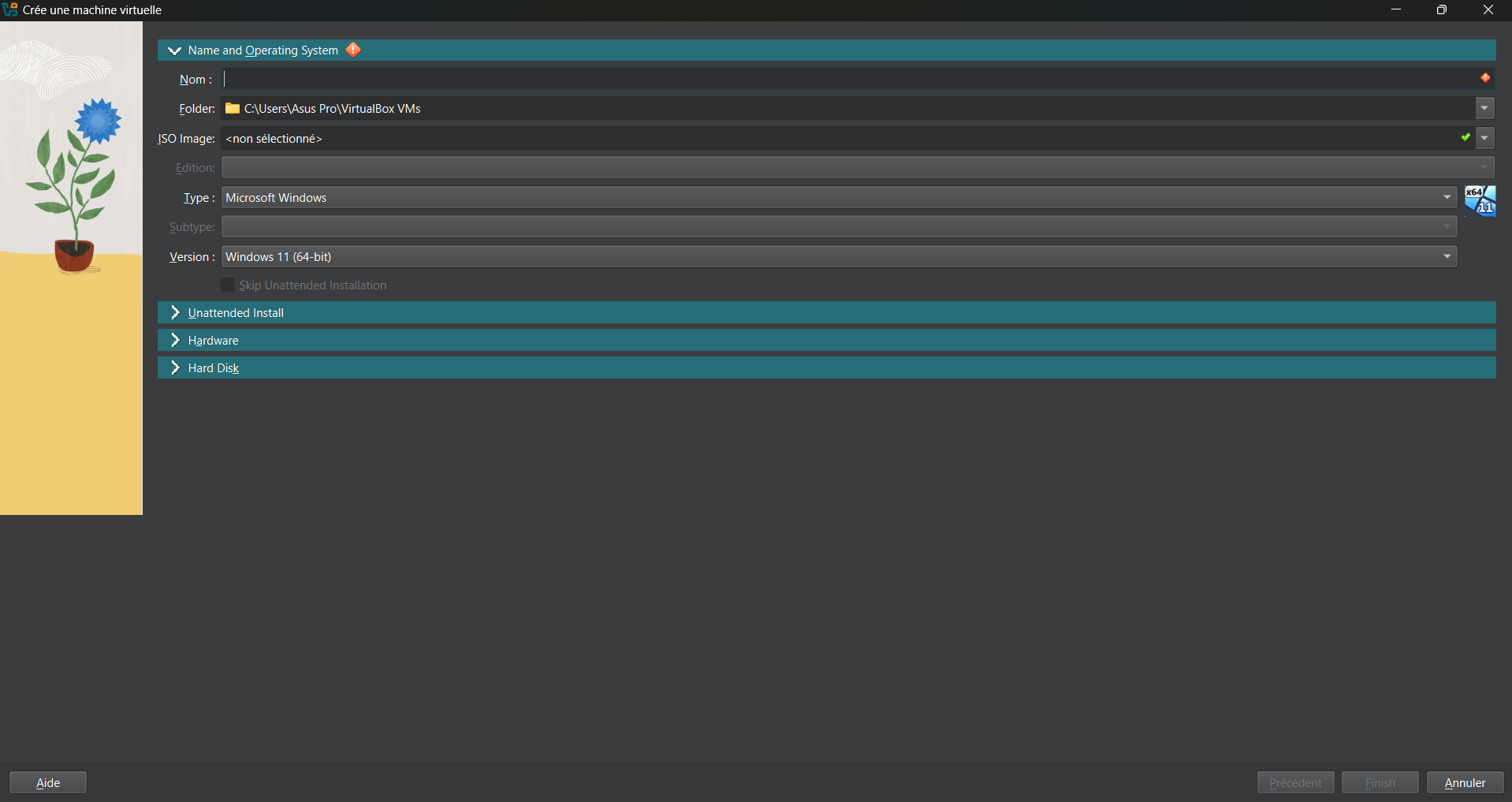
## **PFsense :**

1. Trouver l’iso PFsense et l’installer => Pfsense : <https://www.pfsense.org/download/>

Puis, il faut cliquer sur download puis sur le premier lien de la liste. Ensuite il faut dézipper le fichier tar.gz pour obtenir notre iso en utilisant un logiciel comme Winrar par exemple.

Ensuite ouvrir votre virtualiseur (moi j’utilise VirtualBox)



Ensuite allez dans l’onglet « nouvelle » 

**Dans : Name and Operating System**

Nom : le nom qui s’affichera pour cette machine sur votre virtualiseur ex : pfsense

Iso image : l’iso que vous venez de télécharger

Type : BSD

Subtype : freeBSD

Version : freeBSD (64-bit)

**Dans : Unattended install**

Username : votre nom ex : kylian (sans majuscule sinon il va vous demandez de le changer)

Password : votre mot de passe

Repeat Password : votre mot de passe

**Dans : HardWare**

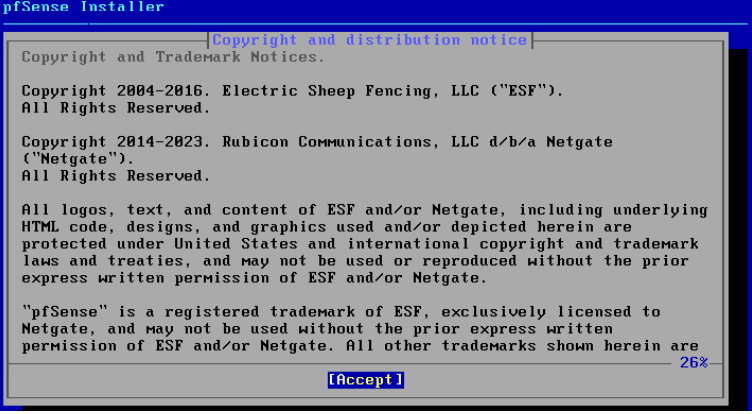
Mémoire vive : minimun 1024MB (de mon côté j’ai mis 2048MB)

Processeurs : minimum 2 (de mon coté j’ai mis 2 processeurs)

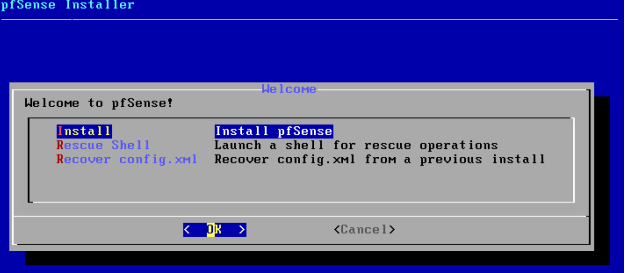
**Dans Hard Disk :**

Hard disk file : minimun 16go (de mon coté j’ai mis 20go)

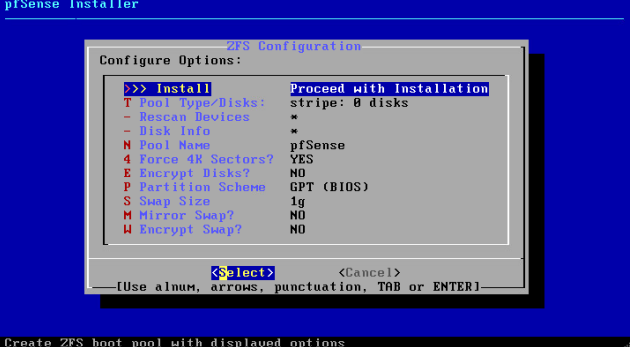
Puis finish

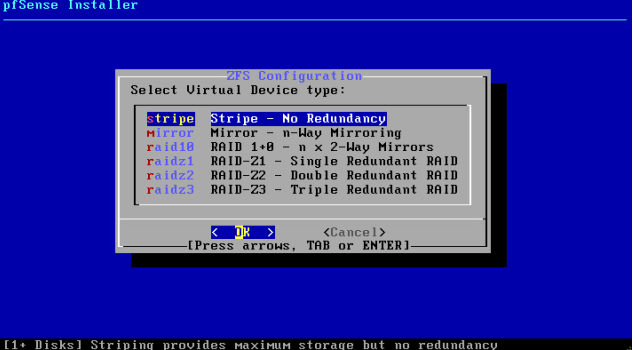
****

**Sur l’interface d’installation, on appuie sur entrée pour passer à la suite**

****

****

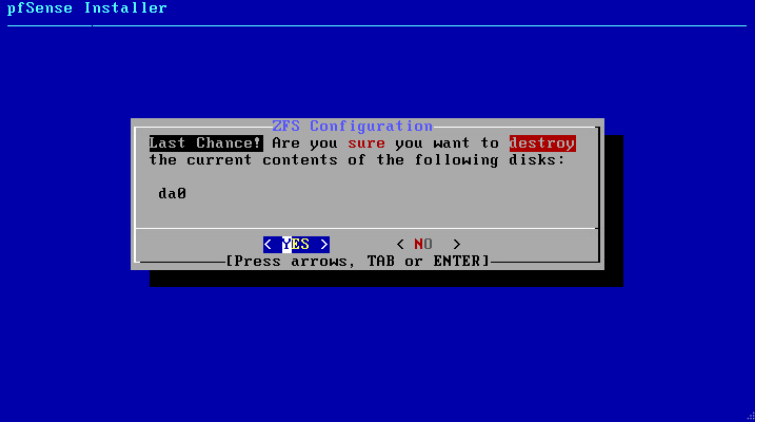
****

****

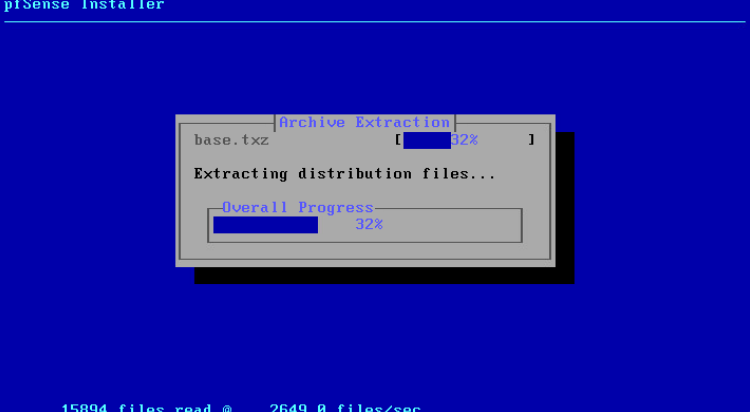
**Sur les quatre images précédentes on appuie sur entrer pour continuer**

****

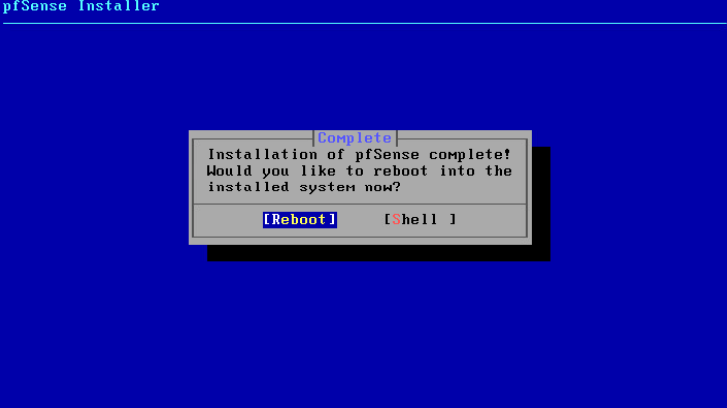
**Sur celle-ci, avant de faire entrer, il faut valider à l’aide de la barre espace de notre clavier pour sélectionner notre disque et poursuivre l’installation.**

****

**À ce niveau-là de l’installation, il faut déplacer notre entrée sur yes avec les flèches pour continuer l’installation du Pfsense.**

****

**L’installation sur le disque s’effectue, notre Pfsense sera bientôt installé sur la machine virtuelle.**

****

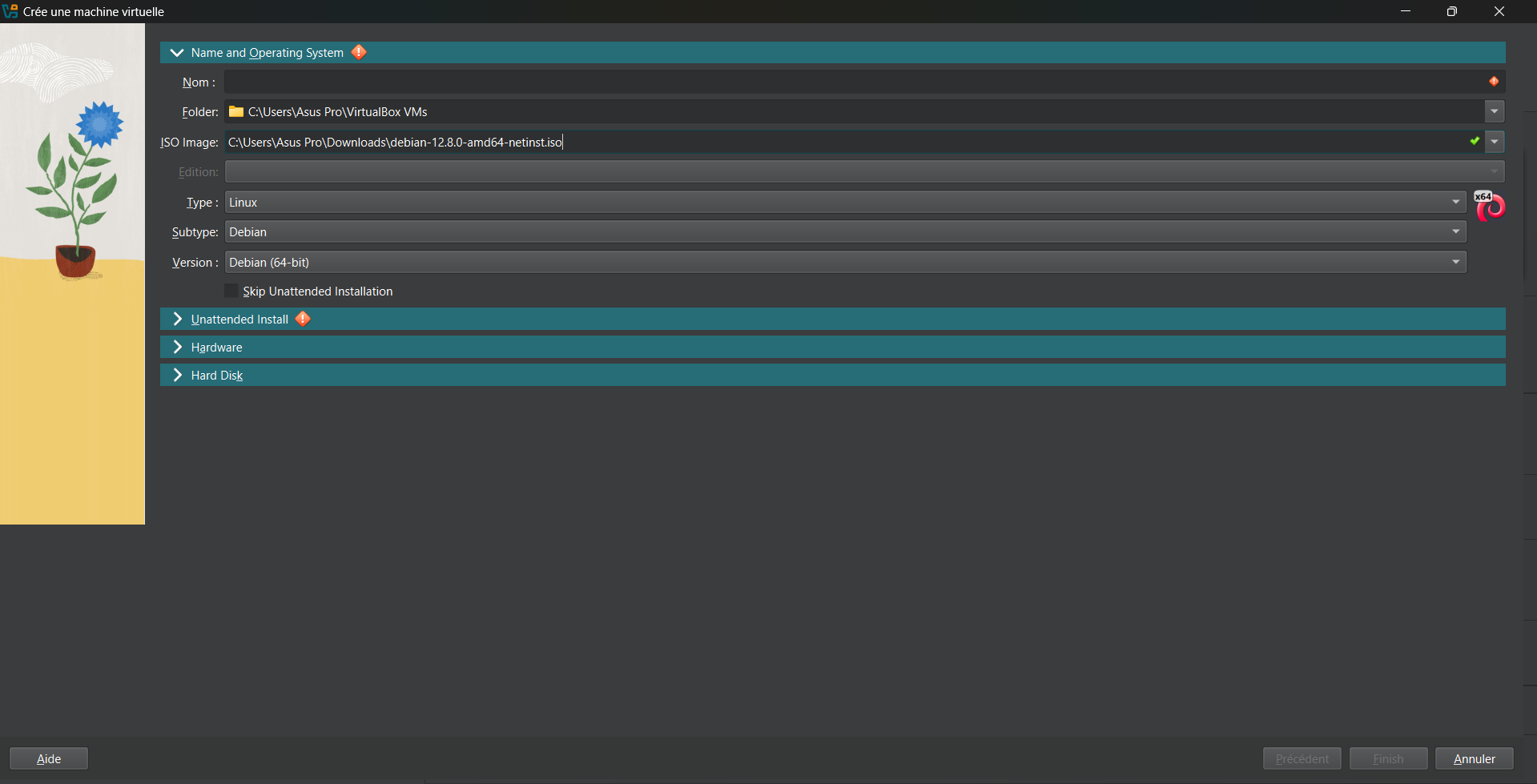
**Il ne manque plus qu’à reboot la machine en appuyant sur entrée et la machine redémarre sur notre Pfsense.**

### **Serveur web (DMZ) :**

1. **On installe un iso Debian 12 =>** [**https://www.debian.org/download.fr.html**](https://www.debian.org/download.fr.html)

**Puis on ouvre notre virtualiseur préféré**

**Ensuite « Nouvelle »**

****

**Dans : Name and Operating System**

Nom : le nom qui s’affichera pour cette machine sur votre virtualiseur ex : ServerWeb

Iso image : l’iso que vous venez de télécharger

Type : Linux

Subtype : Debian

Version : Debian (64-bit)

**Dans : Unattended install**

Username : votre nom ex : kylian (sans majuscule sinon il va vous demandez de le changer)

Password : votre mot de passe

Repeat Password : votre mot de passe

**Dans : HardWare**

Mémoire vive : minimun 2048MB (de mon coté j’ai mis 3072MB)

Processeurs : minimum 2 (de mon coté j’ai mis 2 processeurs)

**Dans Hard Disk :**

Hard disk file : minimun 20go (de mon coté j’ai mis 20go)

Puis finish

1. Ensuite lorsque la vm est installé, on va préparer notre serveur web. On va donc installer Apache2 et proftpd
2. On commence par mettre à jour le cache des paquets
3. Ensuite, on installe le paquet "apache2" afin d'obtenir la dernière version d'Apache

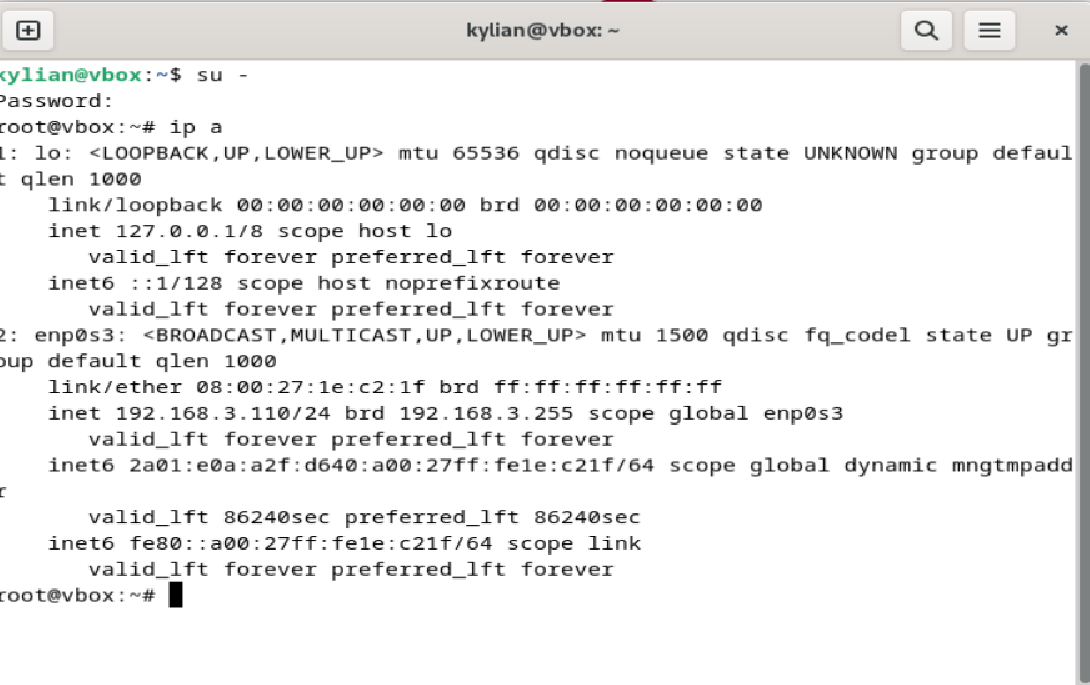


1. Pour qu'Apache démarre automatiquement en même temps que Debian, saisissez la commande ci-dessous (même si normalement c'est déjà le cas) :



1. Suite à l'installation du paquet, le serveur Apache démarre directement. On devrait pouvoir accéder à sa page par défaut. Pour cela, il suffit de récupérer l'adresse IP du serveur :





1. Puis, à l'aide d'une machine équipée d'un navigateur, on peut accéder à notre serveur Apache :



#### Pour proftpd

1. Installe le paquet ProFTPD (-y pour accepter directement l'installation)

Le paquet ProFTPd étant installé sur notre système, nous allons le configurer.

1. On va ensuite créer notre fichier config "ftp-perso.conf" :



1. Dans ce fichier, indiquez la configuration suivante après l'avoir lue et adaptée si besoin :

**# Nom du serveur (identique à celui définit dans /etc/hosts)**

ServerName "IT-CONNECT"

**# Message de connexion**

DisplayLogin "Bienvenue sur le FTP IT-Connect"

**# Désactiver IPv6**

UseIPv6 off

**# Chaque utilisateur accède seulement à son home (pour les membres du groupe ftp2100)**

DefaultRoot ~ ftp2100

**# Port (défaut = 21)**

Port 2100

**# Refuser la connexion super-utilisateur "root"**

RootLogin off

**# Nombre de clients FTP max.**

MaxClients 2

**# Autoriser la connexion seulement aux membres du groupe "ftp2100" grâce à la directive DenyGroup.**

**# En précisant "!" on refuse tout sauf le groupe "ftp2100"**

<Limit LOGIN>

DenyGroup !ftp2100

</Limit>

1. La configuration étant finalisée, nous allons recharger ProFTPd :



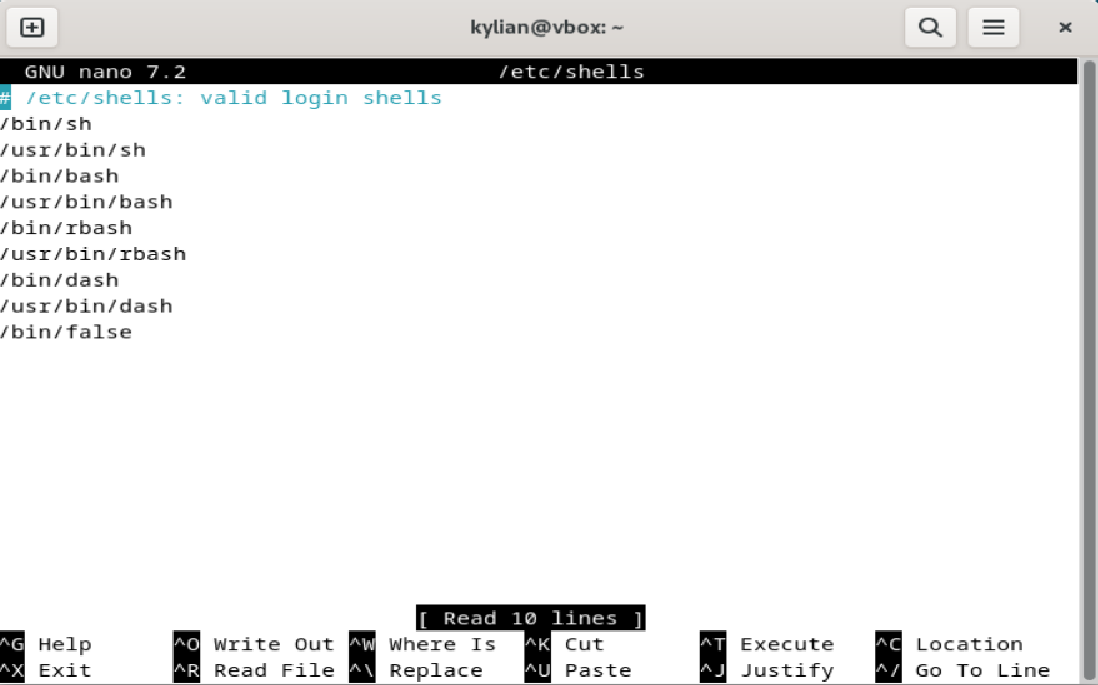
1. Dernière étape avant les tests : la création du groupe ftp2100 et d'un utilisateur pour tester que tout fonctionne.

Le fichier "**/etc/shells**" référence les Shell du système, on va créer un faux Shell (car il pointe vers un binaire qui n'existe pas) en indiquant "**/bin/false**" pour l'attribuer ensuite à notre utilisateur FTP. L'intérêt de cette manipulation c'est que l'utilisateur ne pourra pas se connecter en shell sur le serveur, il peut donc utiliser seulement l'accès FTP.

Pour ajouter cette valeur, exécutez cette commande en tant que *sudo* :



Si on ouvre le fichier on trouve ceci,



1. Maintenant, on va créer le groupe sur notre système Debian :
2. Ensuite, créez l'utilisateur "*votrechoix*" et ajoutez-le au groupe *ftp2100* :



Le Serveur Web est prêt !

### **Machines Debian du LAN**

Refaire une installation de Debian 12 pour la machine qui se trouvera dans le LAN.

Quand l’installations est terminé, on va installer MariaDB

1. Pour cela il faut mettre à jour le système pour s’assurer d’obtenir les dernières mises à jour et correctifs de sécurité.



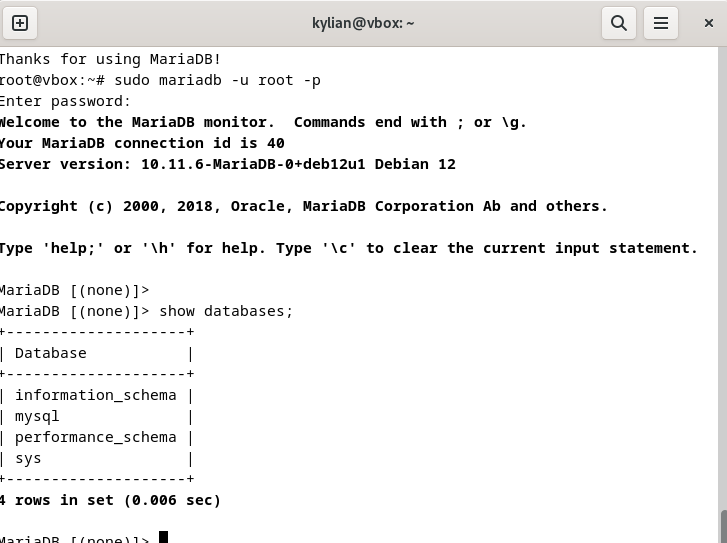
1. Utilisez la commande suivante pour installer le serveur MariaDB



1. Puis vous allez pouvoir définir un mot de passe pour le compte "root" de MariaDB, empêcher les connexions distantes sur votre instance à l'aide du compte "root", empêcher les connexions anonymes et supprimer la base de test.
2. Avant de passer à la suite, vérifiez que vous parvenez à vous connecter à votre instance MariaDB :



1. Saisissez le mot de passe "root". Ensuite, vous avez accès à la console MariaDB / MySQL. Vous pouvez saisir vos requêtes SQL ici. Par exemple, pour lister les bases de données de votre instance :



1. Pour sortir de la console, saisissez la commande suivante puis redémarrer MariaDB

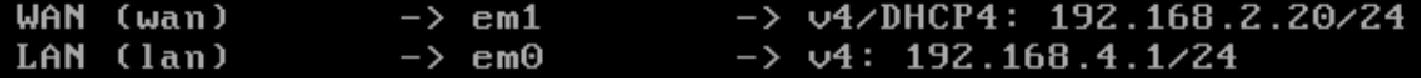


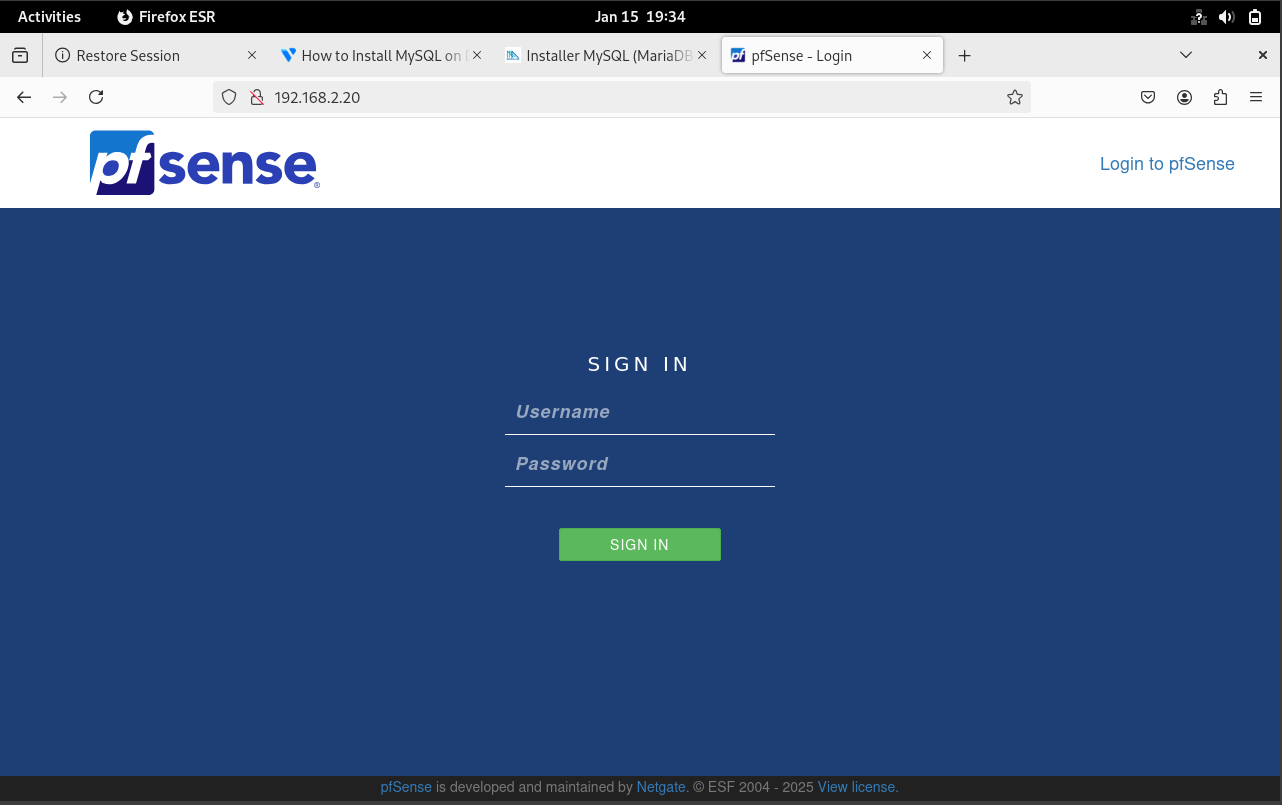
## Configuration de l’interface DMZ

Maintenant il faut configurer la 3ème interface, celle qui servira à relier notre firewall PFsense et notre DMZ

1. Ajouter une nouvelle carte réseau à votre PFsense et mettais la en bridge

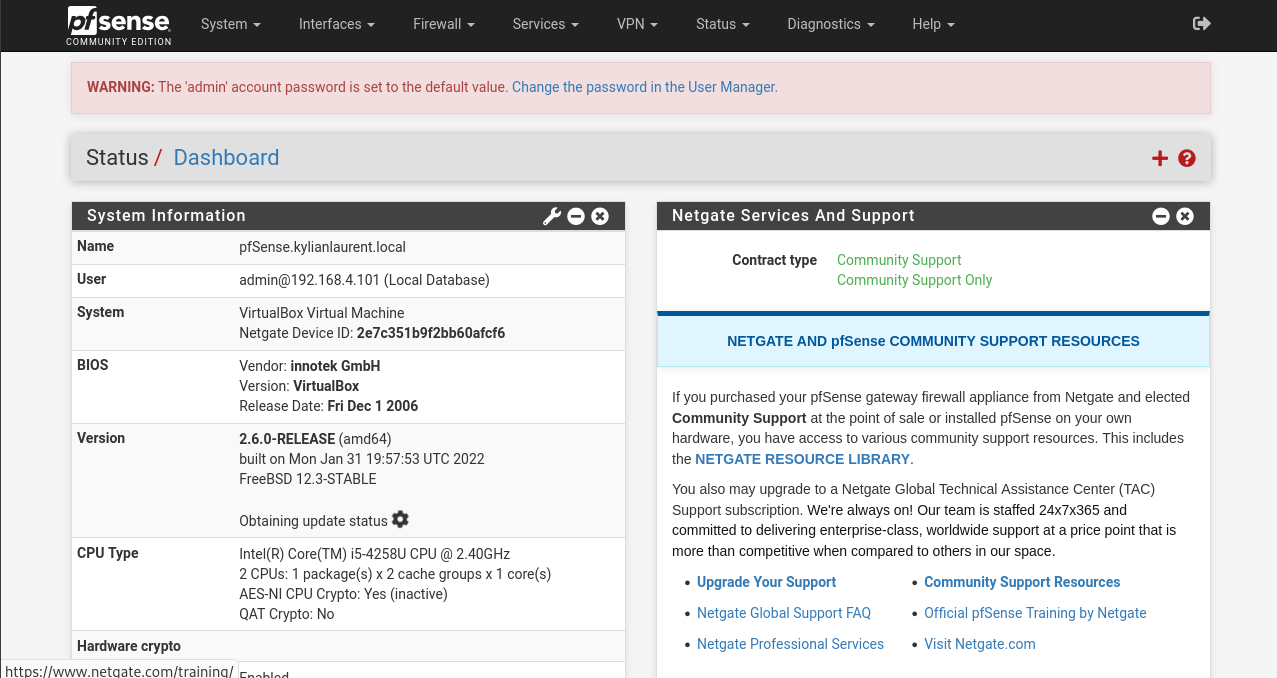
1. Vous allez sur votre machine Debian qui se trouve dans le Lan, puis sur un navigateur. Ensuite vous rentrez l’ip de votre interface WAN





**Username : admin**

**Password : pfsense**

****

1. Ensuite, vérifiez que la nouvelle carte réseau est reconnue :

Allez dans Interfaces > Assignments.

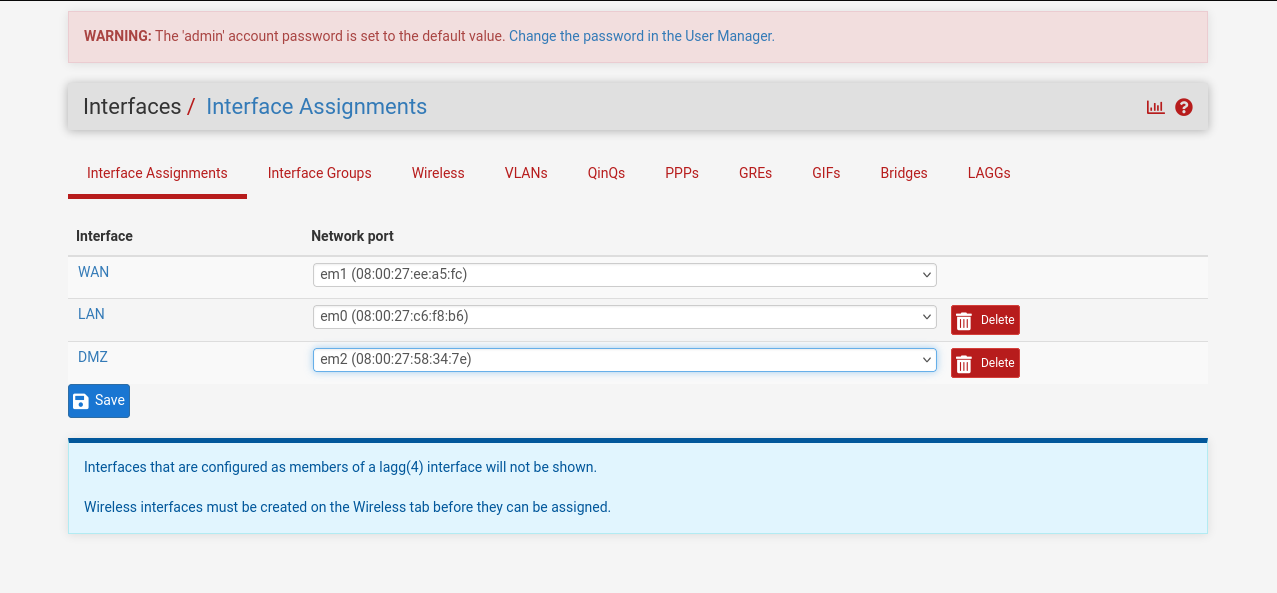
Vous verrez une liste des interfaces disponibles dans la section Available Network Ports.

La nouvelle carte réseau apparaîtra sous un nom comme em2, ew2, etc.

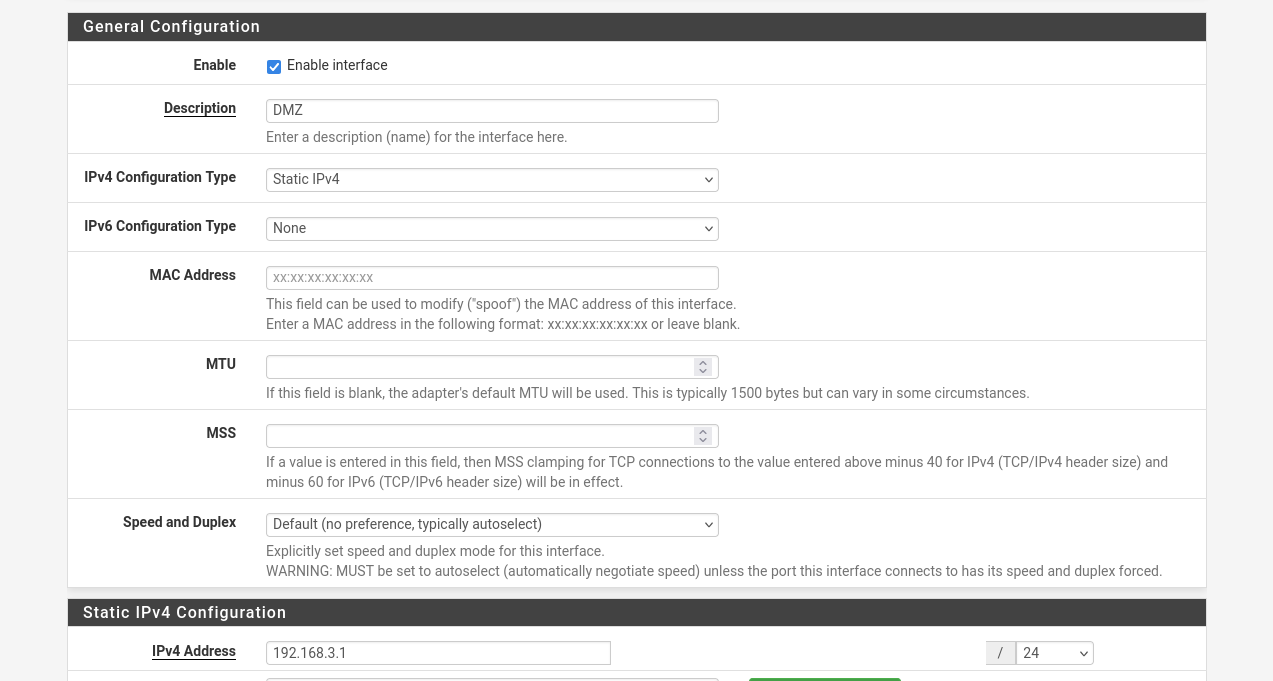
1. Ajoutez une nouvelle interface

Dans Interfaces > Assignments, sélectionnez la nouvelle interface dans le menu déroulant sous Available Network Ports.

Cliquez sur Add pour l'ajouter.



1. Enfin vous allez sur interfaces/lenomdelanouvelleinterface (chez moi DMZ)



**Enable** : pour activer la carte

**Description** : pour décrire l’interface

**Ipv4 configuration type** : static ipv4

**Ipv4 configuration type** : none

**Ipv4 address** : votre choix /24 **ATTENTION !!!! : votre interface doit être dans un réseau différent des autres cartes**

**Ipv4 upstream gateway** : none

1. Enfin save puis apply changes



Notre nouvelle interface est configurée

## **Machine Debian du WAN**

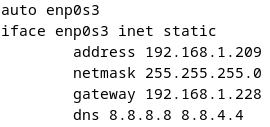
On va maintenant créer la machine du Wan donc on va refaire une installation de Debian 12 et mettre la VM en Bridge. Puis on configure son adresse IP avec la commande ci-dessous



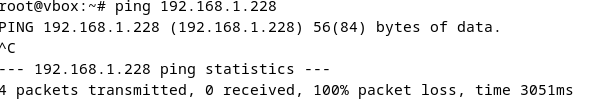
Il faut mettre notre machine dans le même reseau que notre WAN, on va donc récupérer notre ip WAN

(l’ip WAN a changé puisque je suis maintenant à l’école)

Puis on configure



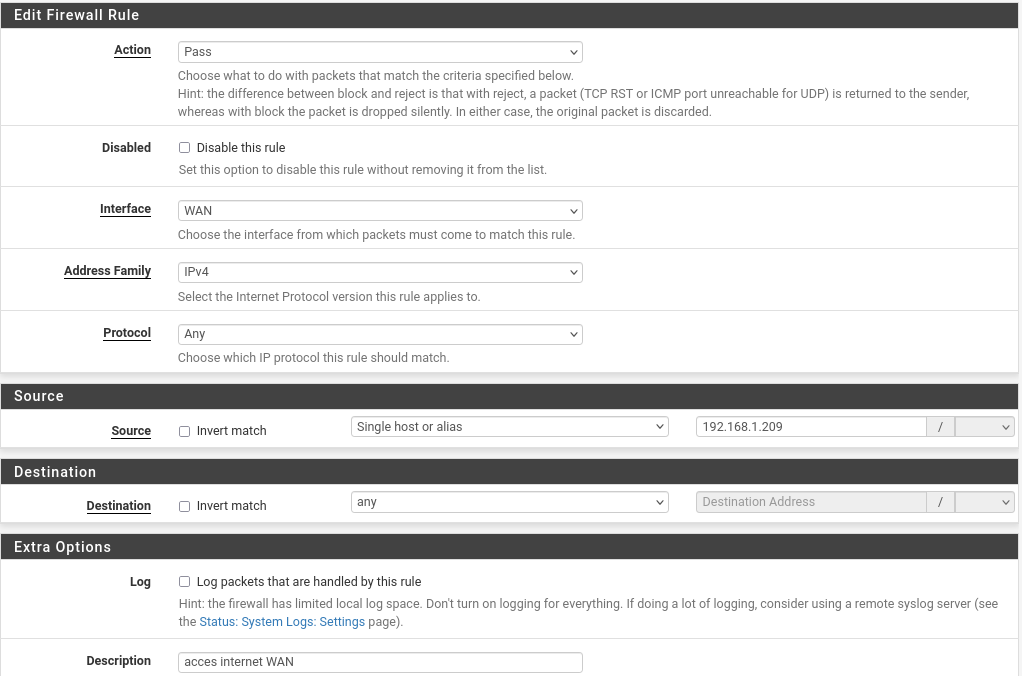
On teste...



Ça ne marche pas donc on va créer des règles

### Règle pour ping Internet

On va donc créer une nouvelle règle



**Action**: Pass

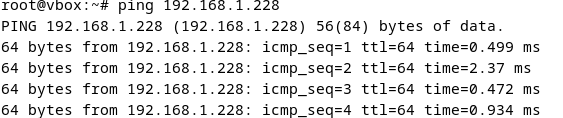
**Interface** : WAN

**Address Family** : IPv4

**Protocol** : Any

**Source** : Single host or alias 192.168.1.209 (ip de la machine)

**Destination** : Any







Donc notre machine à bien accès à Internet en passant par notre interface WAN

## 

# **Phase 1 :**

## **Autoriser les accès au serveur Web depuis Internet et depuis le LAN**

On veut maintenantautoriser les accès au serveur Web depuis Internet et depuis le LAN

On va donc créer des règles :

1ère règle : Redirection Serveur Web (Configuration du port forwarding)

Connectez-vous à l'interface d'administration de pfSense.

Allez dans Firewall/NAT/Port Forward.

Cliquez sur "Add" pour créer une nouvelle règle :

* + Interface : WAN
  + Protocol : TCP
  + Destination port range : HTTP (80) to HTTPS (443)
  + Redirect target IP : 192.168.3.110 (ip du serveur web)
  + Redirect target port : HTTP (80) to HTTPS (443)
  + Description : Accès serveur Web

Cliquez sur "Save" puis "Apply Changes"

2ème règle : Autoriser accès serveur web depuis Internet

Allez dans Firewall > Rules > WAN.

Ajoutez une nouvelle règle :

* + Action : Pass
  + Interface : WAN
  + Protocol : TCP
  + Source : any
  + Destination : WAN address
  + Destination port range : HTTP (80) to HTTPS (443)
  + Description : Autoriser accès Web depuis WAN

3ème règle : Autoriser accès serveur web depuis LAN

Allez dans Firewall/Rules/LAN.

Assurez-vous qu'une règle existe pour autoriser le trafic du LAN vers le serveur Web :

Action : Pass

Interface : LAN

Protocol : TCP

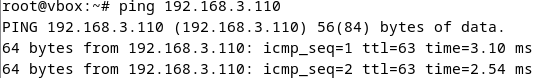
Source : LAN net (192.168.4.0/24)

Destination : 192.168.3.110

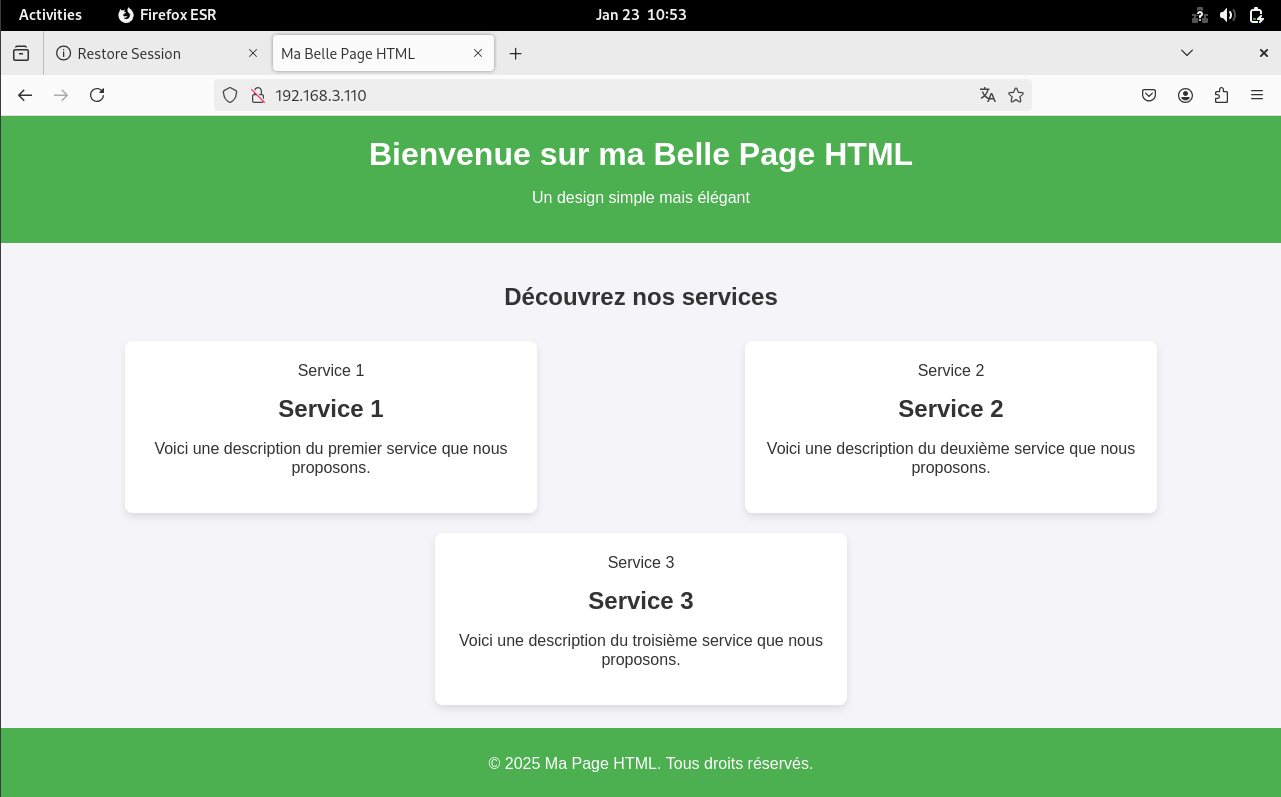
Destination port range : HTTP (80) to HTTPS (443)

Description : Autoriser accès Web depuis LAN

Depuis mon Lan je fais un ping pour voir si j’arrive à atteindre mon serveur web



Je le ping donc je tape l’ip de mon serveur depuis un navigateur sur un poste du LAN



On voit donc que mon LAN a bien accès à mon Serveur Web

Depuis Internet on fait également la même chose.



On ping bien le serveur donc on essaie depuis un navigateur

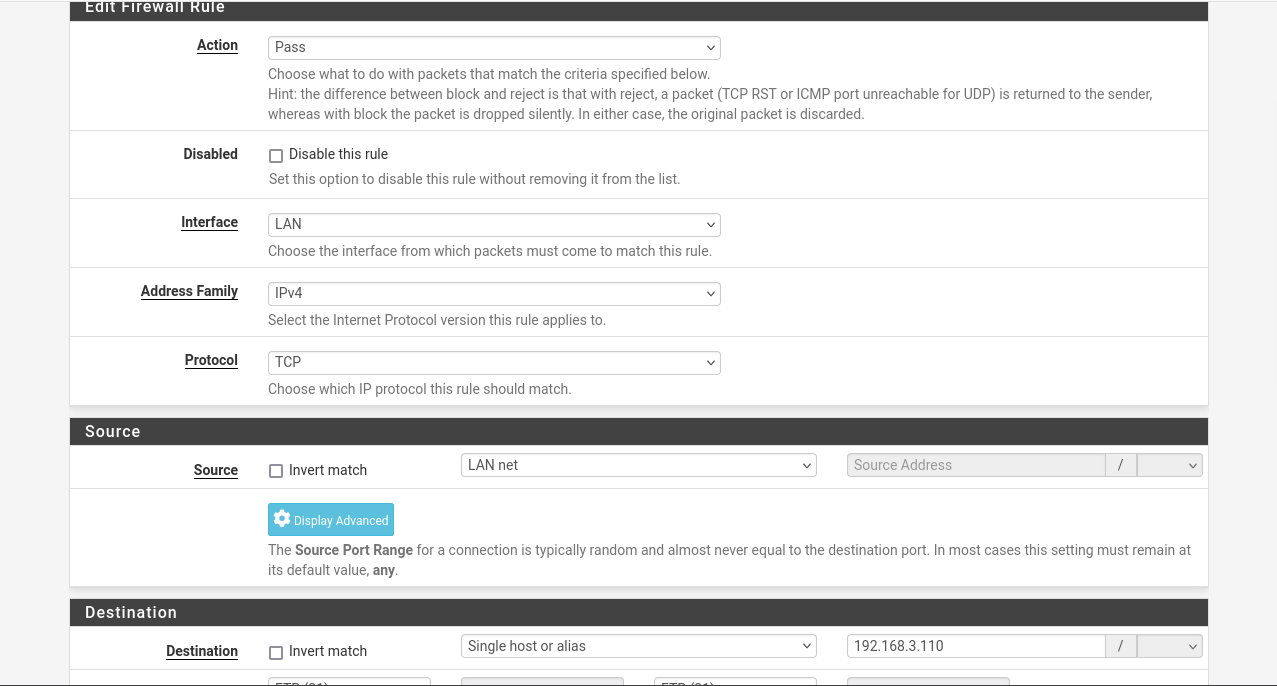


Un poste à bien accès à mon serveur en passant par l’ip WAN

## **Autoriser les accès FTP sur le serveur de la DMZ depuis le LAN**

Maintenant on va autoriser notre LAN à accéder à notre Server FTP donc à notre serveur ProFTPD.

1. On va donc créer de nouvelles règles.



**Action** : pass

**Interface** : LAN

**Address Family** : IPv4

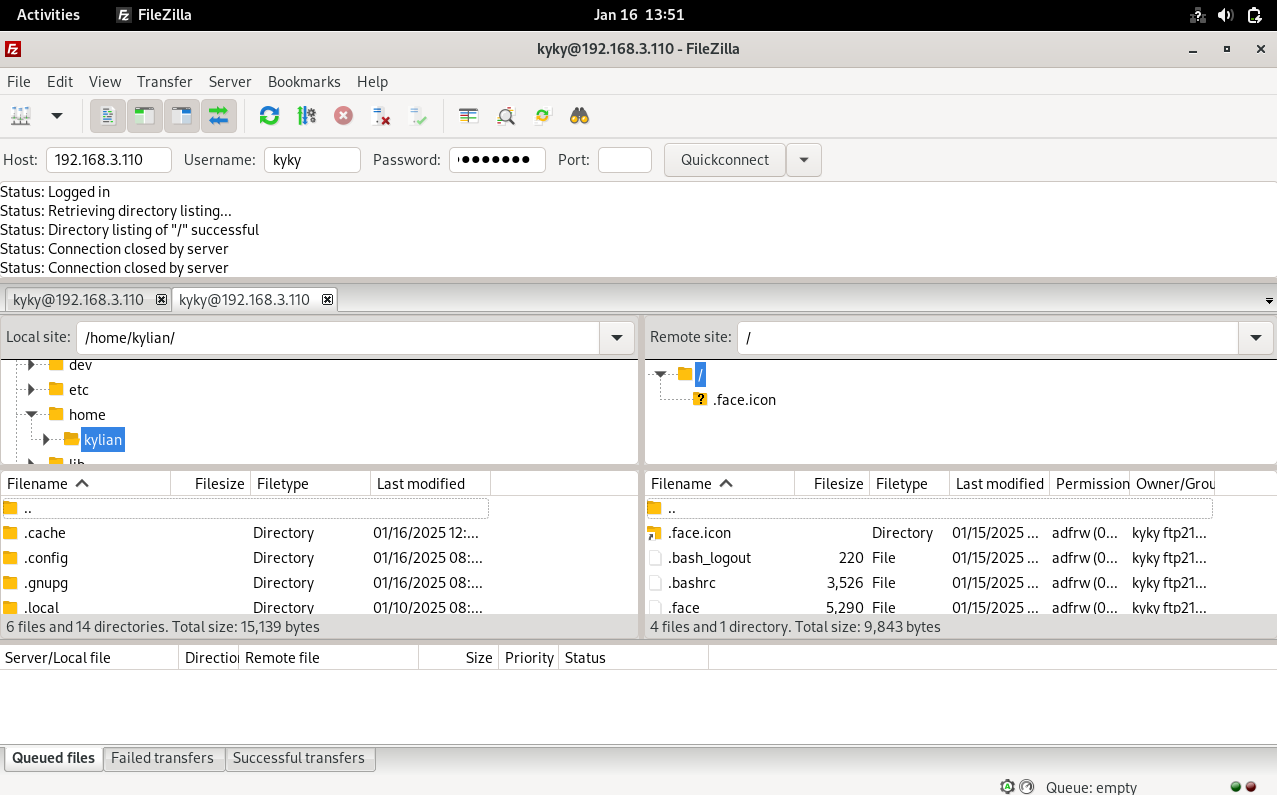
**Protocol** : TCP

**Source** : LAN net

**Destination** : Single host or alias 192.168.3.110

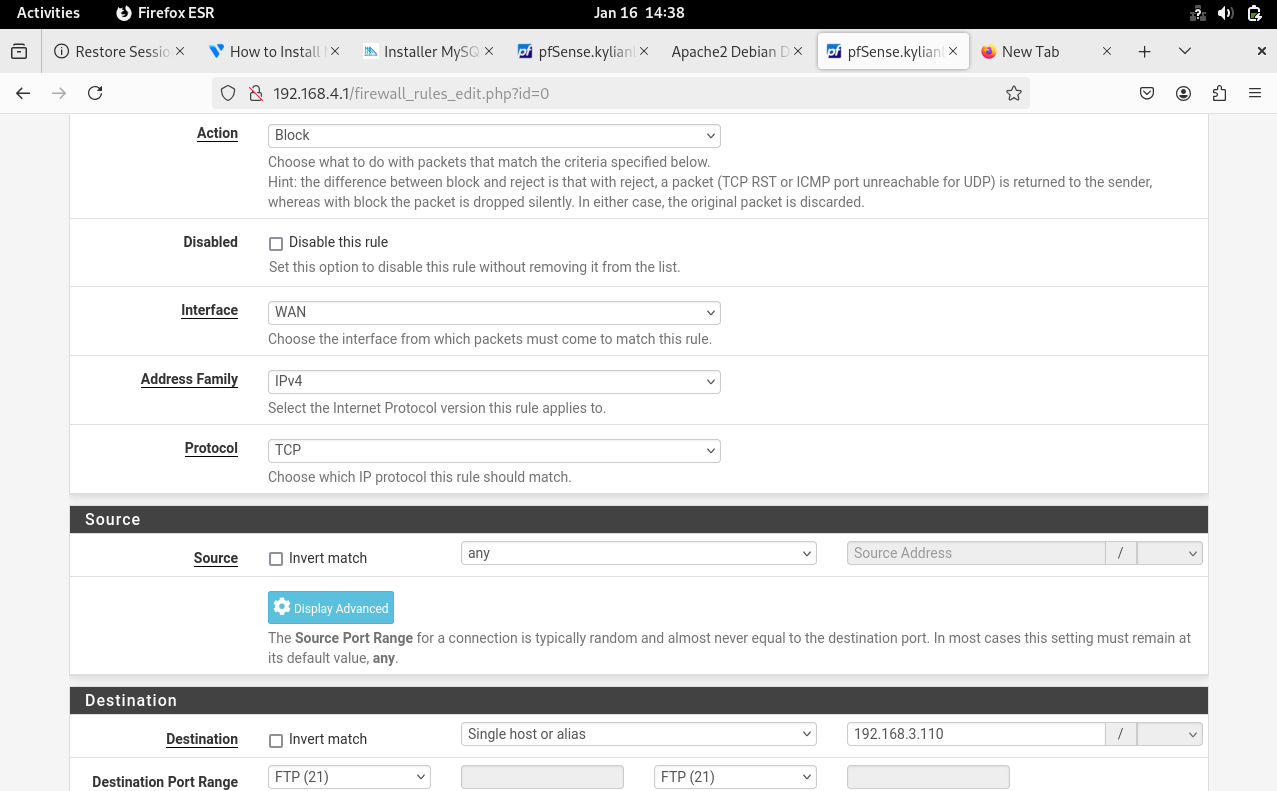
**Destination Port range** : FTP FTP

Cette règle autorise le LAN à accéder au FTP.



Mais comme on veut que seul les membre du Lan ai accès au Serveur FTP, il faut bloquer les autres

1. On va donc créer une règle qui bloque tout le reste.



**Action** : Block

**Interface** : WAN

**Address Family** : IPv4

**Protocol** : TCP

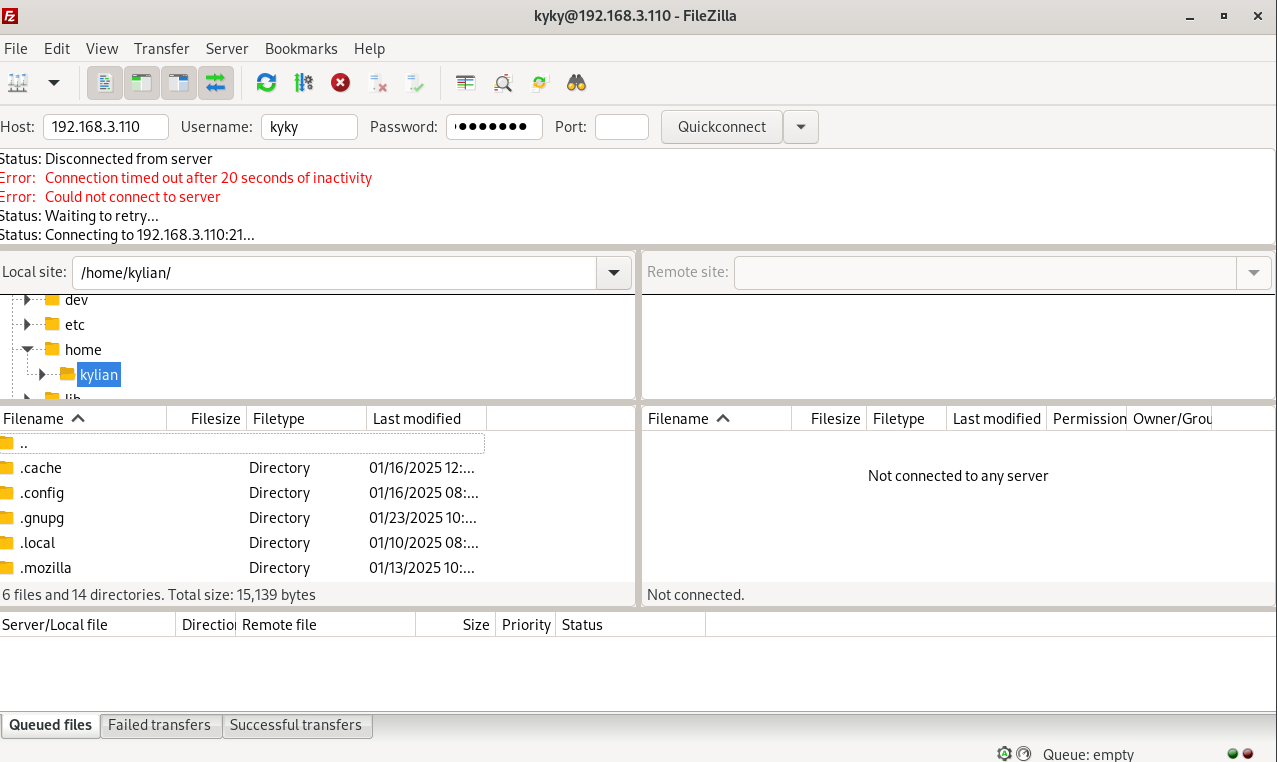
**Source** : ANY

**Destination** : 192.168.3.110

**Destination port range** : ftp ftp

Cette règle va bloquer le WAN et donc le serveur FTP ne sera pas disponible depuis l’extérieur

J’essaie depuis un poste du WAN



Mais l’accès lui a bien été refusé

Donc l’accès au serveur FTP à bien été autorisé pour et seulement pour les membres du LAN

## **Autoriser les accès Internet depuis le LAN et la DMZ en passant par le Firewall**

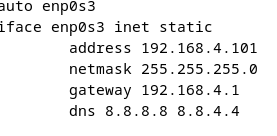
Le plus simple est de commencer par le Lan donc :

1. On va sur la machine du Lan et on va taper la commande ci-dessous pour configurer une ip static dans le même réseau que l’interface LAN

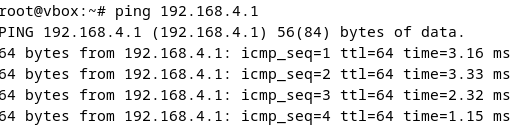


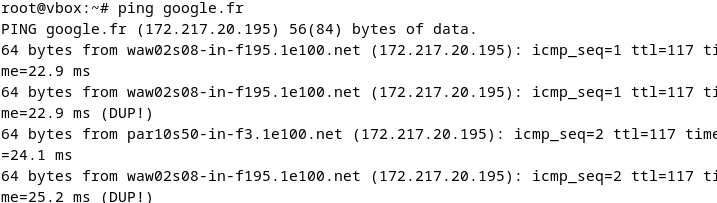
1. On regarde donc l’ip de l’interface LAN et on rentre une ip dans le même réseau avec comme gateway cette interface





1. On essaie de ping notre interface, puis google.fr







Notre Lan a donc bien accès à Internet en passant par notre firewall pfsense

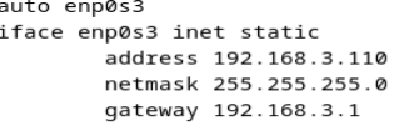
# **DMZ**

1. On va sur le serveur web et on va taper la commande ci-dessous pour configurer une ip static dans le même réseau que l’interface DMZ

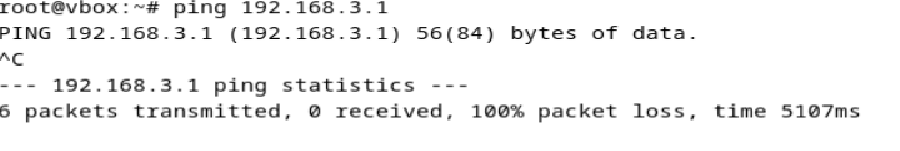


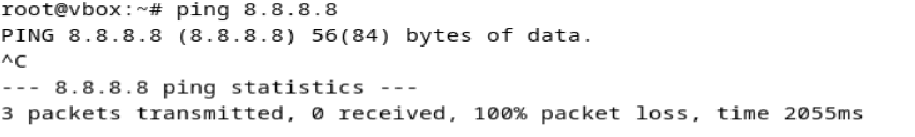
1. On regarde donc l’ip de l’interface DMZ et on rentre une ip dans le même réseau avec comme gateway cette interface





Mais si on essaie de ping notre interface ou internet ça ne marche pas





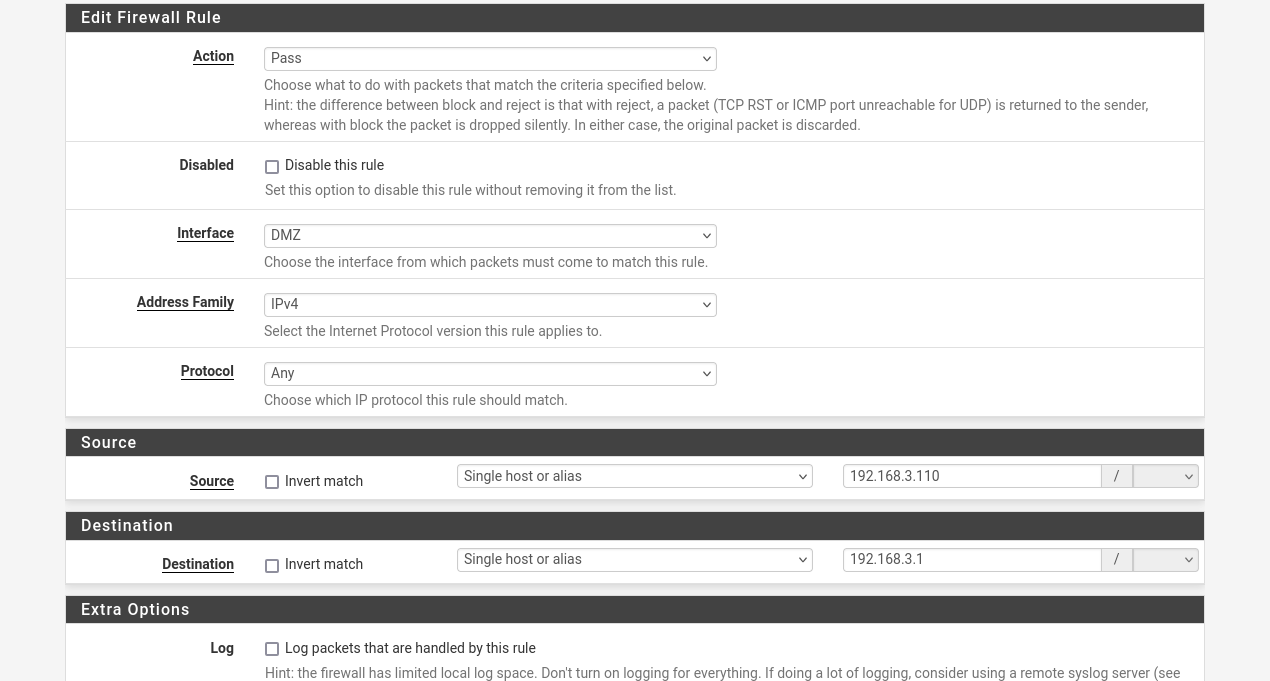
1. On va donc rajouter des règles pour autoriser la connexion à l’interface et à internet

### Pour réussir à ping l’interface

1. Se reconnecter à l’interface web de pfsense sur un navigateur

Puis on va sur fiwewall/rules/dmz

Appuyez sur ADD



**Action** : pass

**Interface** : DMZ

**Address Family** : IPv4

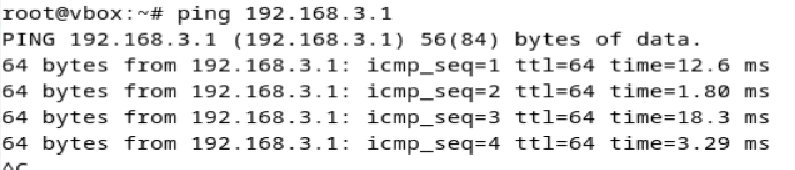
**Protocol** : Any

**Source** : Single host or alias ip de votre serveur web

**Destination** : single host or alias ip de votre interface

**Description** : pour décrire à quoi sert là règle

1. Puis save et apply changes

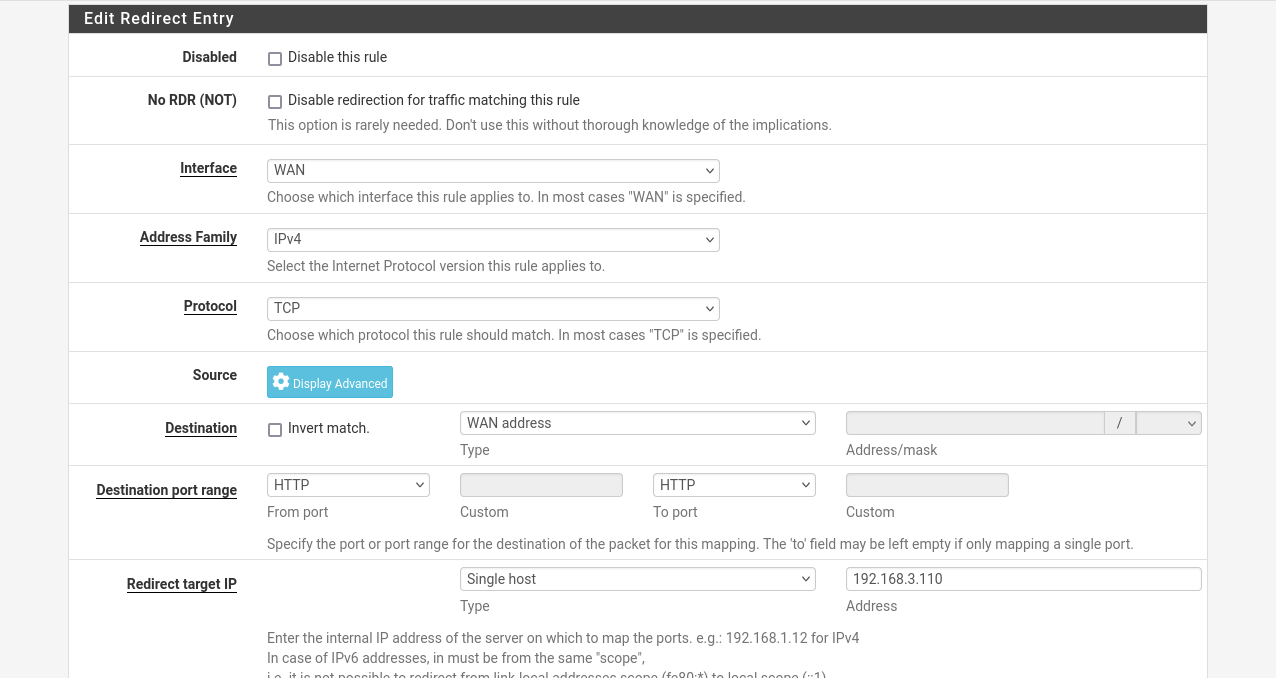


Nous arrivons à ping notre interface

### Pour réussir à ping Internet

1. On va sur fiwewall/Nat/Port Forward

Appuyez sur add



**Interface** : WAN

**Address Family** : IPv4

**Protocol** : TCP

**Destination** : WAN address

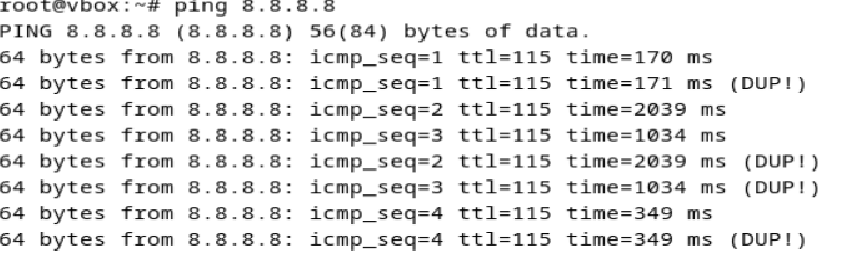
**Destination port range** : from port : http to port : http

**Redirect target ip**: **type** : single host **address** : adresse du serveur web

**Redirect target port** : http

**Description** : pour décrire à quoi sert là règle

Enfin save puis apply changes





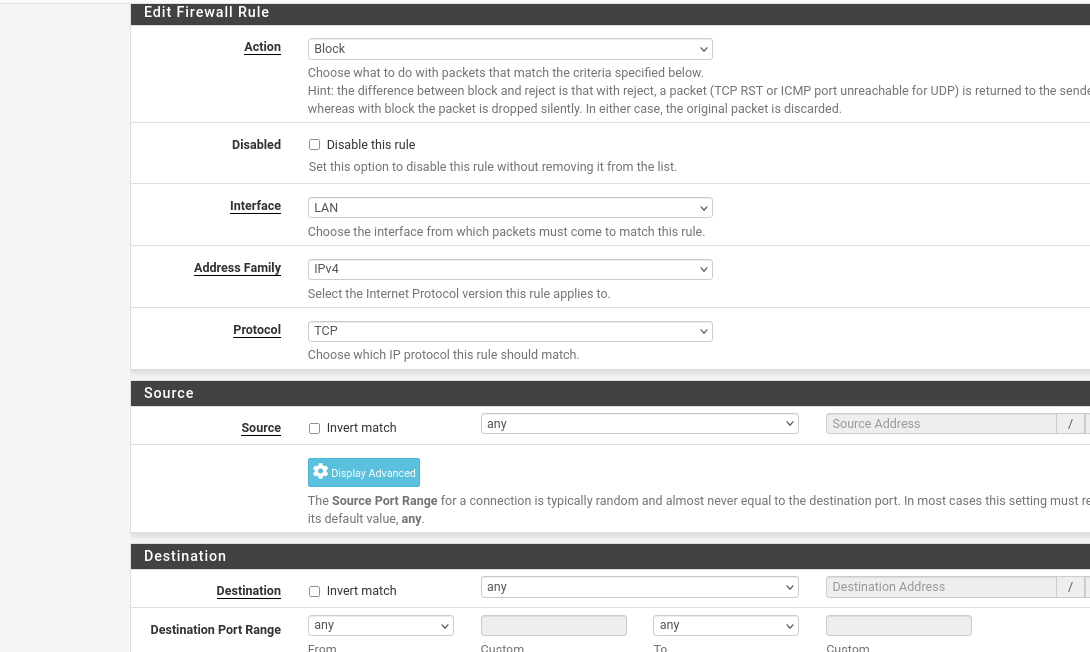
Le serveur web a donc lui aussi bien accès à Internet en passant par mon firewall PFsense !

## **Interdire tout accès au LAN depuis Internet ou la DMZ**

Maintenant on veut interdire l’accès au LAN depuis Internet et depuis la DMZ

**DMZ**

1. On va sur l’interface DMZ et on va bloquer tout le reste



Action : Block

Interface : LAN

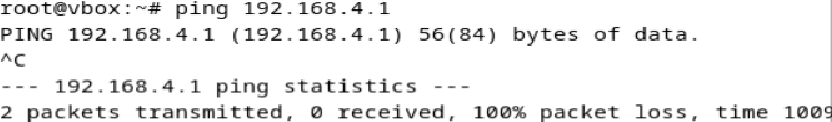
Protocol : Any

Source : Any

Destination : Any

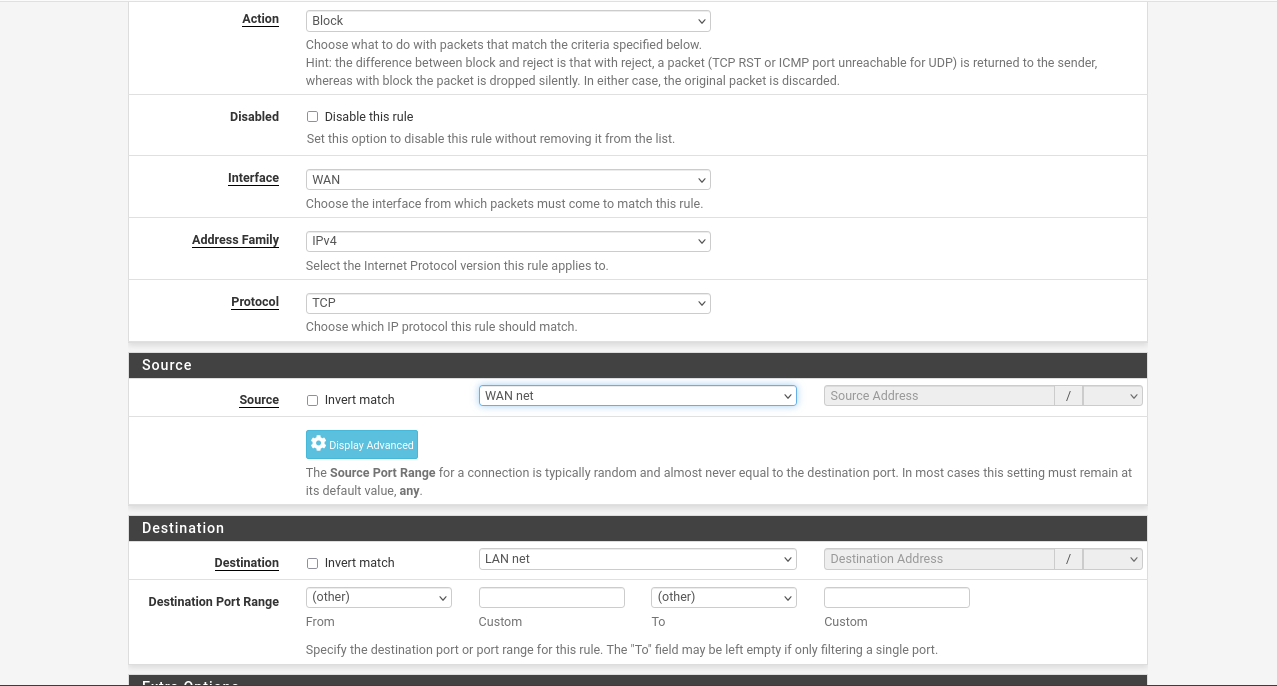
Description : Pour bloquer tout le reste

1. On regarde si la DMZ à accès au LAN



Donc non notre règle bloque bien l’accès au LAN

**WAN**



Action : Block

Interface : WAN

Protocol : Any

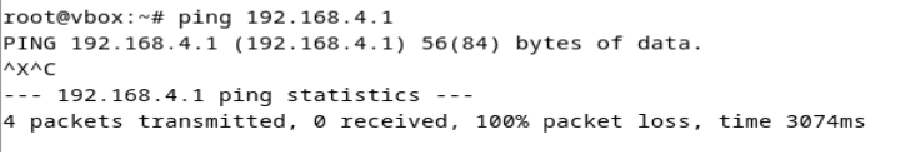
Source : any

Destination : LAN net

Description : Bloquer l'accès au LAN depuis le WAN

Attention : Quand une règle a pour but de bloquer, on la met à la fin !

* Maintenant on teste



Notre règle bloque bien l’accès au LAN depuis le WAN

# **4-Phase 2**

Maintenant on veut installer un serveur de base de données MariaDB dans le LAN et, autoriser les requêtes SQL du serveur WEB vers le serveur MariaDB.

1. On commence par installer mariadb



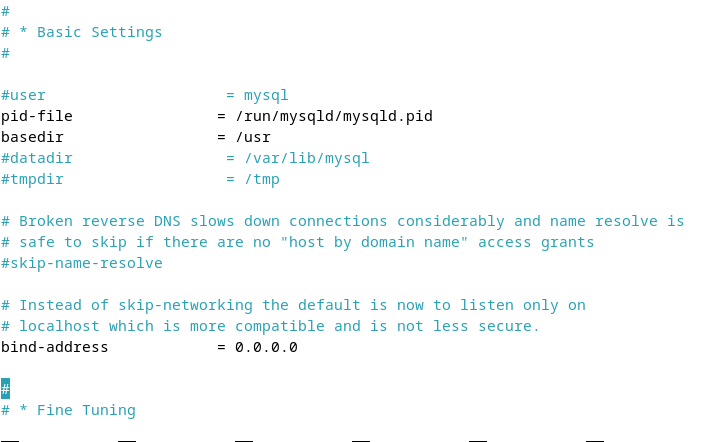
1. Puis on va sécuriser l’installation



1. Configurer MariaDB pour accepter les connexions distantes



1. On rajoute la ligne bind-address et on remplace l’ip par 0.0.0.0 (elle autorise toute les ip)



1. Ensuite depuis notre LAN on va autoriser l’utilisateur de la base de données de la DMZ à accéder à la base de données de notre LAN

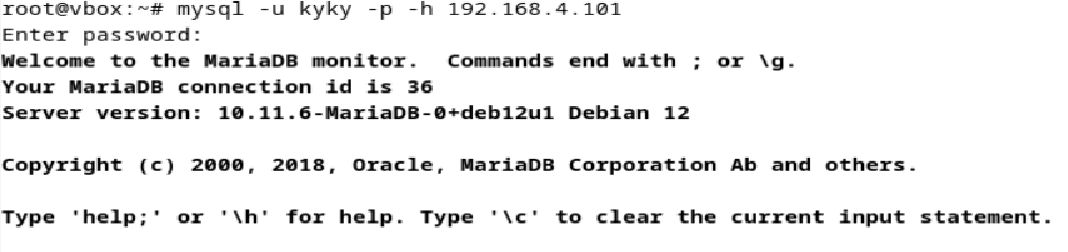
Donc on se connecte à notre base de données en root



1. Et on donne tous les privilèges à l’utilisateur et on spécifie bien l’ip de notre DMZ



1. Pour finir on teste



J’ai pu me connecter donc mon utilisateur peut taper des commandes sur la bdd du LAN.